

Cisco Secure Firewall Management Center Device Configuration Guide, 7.4

First Published: 2023-09-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I **Getting Started with Device Configuration** 73

CHAPTER 1 **Device Registration** 1

About device registration 1

Firewall management center overview 1

Firewall Management Center and device management 2

Devices managed by a Secure Firewall Management Center 2

Management connection 3

Beyond policies and events 4

Device management interfaces 4

Management and event interfaces on the Firewall Threat Defense 4

Using the Firewall Threat Defense data interface for management 5

Management interface support per device model 6

Network routes on device management interfaces 7

NAT environments 8

Management and event traffic channel examples 10

Prerequisites for device registration 12

Log into the Command-Line Interface on the device 13

Complete the Firewall Threat Defense initial configuration for manual registration 15

Complete the Firewall Threat Defense Initial Configuration Using the Firewall Device Manager 15

Complete the Firewall Threat Defense Initial Configuration Using the CLI 21

Configure an event interface 28

Device registration management 30

About the device management page 30

Add a Device Group 31

Registration with the management center 32

Add a Device Using a Registration Key 32
Add a Device Using the Serial Number (Zero-Touch Provisioning) 36
Add a chassis 43
Register with a new management center 46
Resolve serial number (zero-touch provisioning) registration issues 47
Register with a new management center 53
Delete (Unregister) a Device from the Firewall Management Center 54
Shut down or restart the device 55
Download the managed device list 56
Migrate Firewall Threat Defense devices 56
Supported Devices for Migration 57
License for Firewall Threat Defense migration 57
Prerequisites for migration 57
Configurations that the wizard migrates 57
Guidelines and limitations for migration 59
Best practices for Threat Defense device migration 60
Switch managers 61
Switch from the Firewall Device Manager to the Firewall Management Center 61
Switch from Firewall Management Center to Firewall Device Manager 65
History for device registration 67

CHAPTER 2 **Transparent or Routed Firewall Mode** 71
Firewall mode 71
Routed firewall mode 71
Transparent firewall mode 72
Transparent firewall network usage 72
Passing traffic for routed-mode features 73
Bridge groups 73
Bridge virtual interfaces 73
Bridge groups in transparent firewall mode 74
Bridge groups in routed firewall mode 75
Allow layer 3 traffic 76
Allowed MAC addresses 76
BPDUs handling 76

MAC address and route lookups 77
Unsupported features for bridge groups in transparent mode 79
Unsupported features for bridge groups in routed mode 80
Default settings 81
Guidelines for firewall mode 81
Set the firewall mode 82

CHAPTER 3 CLI Users 85
CLI users 85
Internal and external users 85
CLI access 86
CLI user roles 86
Guidelines for CLI users 87
Add an internal user at the CLI 87
External authentication for the Firewall Threat Defense 90
External authentication for the Firewall Threat Defense 90
LDAP 91
RADIUS 91
Add an LDAP external authentication object for Firewall Threat Defense 92
Add a RADIUS external authentication object for Firewall Threat Defense 98
External authentication for users on Firewall Threat Defense devices 103
Troubleshoot LDAP authentication connections 103
History for CLI users 105

CHAPTER 4 Change Management 107
Change management 107
Make configuration changes in the change management workflow 107
Create separate approver and configuration roles 108
Policies and objects that support change management 109
Requirements and prerequisites for change management 111
Guidelines and limitations for change management 111
Enabling or disabling change management 112
Manage tickets 113
Create change management tickets 114

Opening a ticket for configuration changes 115
Preview a ticket 116
Submit a ticket 116
Discard a ticket 117
Approving or rejecting a ticket 117
History for change management 118

CHAPTER 5 **Configuration Deployment** 121
Configuration deployment 121
Configuration changes that require deployment 121
Deployment preview 122
Guidelines for selective policy deployment 123
System username 126
Auto-enabling of application detectors 126
Asset rediscovery with network discovery policy changes 127
Snort restart scenarios 127
Inspection interruption warnings during deployment 127
Inspect traffic during policy apply 128
Snort restart traffic behavior 129
Configurations that restart the snort process when deployed or activated 131
Actions that immediately restart the snort process 132
Requirements and prerequisites for deployment management 133
Best practices for deploying configuration changes 133
Configuration deployment 134
Deploy configuration changes 135
Redeploy existing configurations to a device 140
Deployment management 141
Deployment status 141
View deployment history 141
Set the number of configuration versions to retain 146
Deployment rollback 147
Perform a rollback 149
View the deployment rollback transcript 150
Download policy changes report for multiple devices 151

Compare policies 152
Generate current policy reports 153
History for configuration deployment 154

PART II **High Availability and Scalability** 157

CHAPTER 6 **Multi-Instance Mode** 159
Multi-instance mode 159
Multi-instance modes and appliance modes 159
Chassis management interface 160
Instance interfaces 161
Interface types 161
Chassis interfaces vs. instance interfaces 161
Shared interface scalability 163
Shared interface best practices 164
How the chassis classifies packets 166
Classification examples 167
Cascading container instances 167
Typical multi-instance deployments 168
Automatic MAC addresses for instance interfaces 169
Performance scaling factors for multi-instance modes 170
Instances and high availability 170
Licenses for instances 171
Requirements and prerequisites for instances 171
Guidelines and limitations for instances 172
Instance configuration 175
Enable multi-instance mode 175
Add a multi-instance chassis to the Firewall Management Center 177
Chassis interface configuration 180
Configure a physical interface 180
Configure an EtherChannel 183
Configure a subinterface 187
Add an instance 189
System configuration customization 195

Configure SNMP 196
Import or export the chassis configuration 196
Chassis platform settings 199
Create a chassis platform settings policy 199
Configure DNS 200
Configure SSH and SSH access list 201
Configure syslog 206
Configure time synchronization 211
Configure time zones 213
Multi-instance mode management 214
Change interfaces assigned to an instance 214
Change chassis management settings at the FXOS CLI 216
Multi-instance mode 219
Multi-instance setups 219
Instance interfaces 220
Multi-instance mode feature and version history 222

CHAPTER 7 **Logical Devices on the Firepower 4100/9300** 223
Supported interfaces 223
Chassis management interface 223
Interface types 224
FXOS interfaces and application interfaces 226
Shared interface scalability 228
Shared interface best practices 229
Shared Interface Usage Examples 231
View shared interface resources 237
Inline set link state propagation for the Firewall Threat Defense 238
Logical devices 238
Standalone and clustered logical devices 239
Logical device application instances 239
Container instance interfaces 239
How the chassis classifies packets 240
Classification examples 240
Cascading container instances 244

Typical multi-instance deployment 245
Automatic MAC Addresses for Container Instance Interfaces 246
Container instance resource management 247
Performance scaling factor for multi-instance capability 247
Container instances and high availability 247
Container instances and clustering 247
Licenses for container instances 247
Requirements and prerequisites for logical devices 248
Requirements and prerequisites for hardware and software combinations 248
Requirements and prerequisites for container instances 250
Requirements and prerequisites for high availability configuration 251
Requirements and prerequisites for clustering 251
Guidelines and limitations for logical devices 255
Guidelines and limitations for interface configuration 255
General guidelines for firewall mode, HA, and multi-instance configurations 258
Configure interfaces 259
Enable or disable an interface 259
Configure a physical interface 259
Add an EtherChannel (port channel) 261
Add a VLAN subinterface for container instances 263
Configure logical devices 264
Add a resource profile for container instances 264
Add a Standalone Firewall Threat Defense 265
Add a high availability pair 271
Change an Interface on a Firewall Threat Defense Logical Device 272
Connect to the Console of the Application 274
History for logical devices 276

CHAPTER 8 **High Availability for Devices** 283
Secure Firewall Threat Defense high availability 283
High availability system requirements 284
Hardware requirements 284
Software requirements 285
License requirements for Firewall Threat Defense devices in a high availability pair 285

Failover and stateful failover links 285
Failover link 286
Stateful failover links 288
Failover and data link interruption avoidance 288
MAC addresses and IP addresses in High availability 290
Stateful failover 292
Supported features 292
Unsupported features 294
Bridge group requirements for high availability 294
Failover health monitoring 295
Unit health monitoring 295
Heartbeat module redundancy 296
Interface monitoring 296
Failover triggers and detection timing 298
Active/standby failover 300
Primary/secondary roles and active/standby status 300
Active unit determination at startup 300
Failover events 301
Config-sync optimization 302
Requirements and prerequisites for high availability 303
Guidelines for High availability 303
Add a high availability pair 306
Configure optional high availability parameters 309
Configure standby IP addresses and interface monitoring 309
Edit high availability failover criteria 310
Configure virtual MAC addresses 310
Manage High availability 311
Switch the Active Peer in the Firewall Threat Defense High Availability Pair 312
Refresh node status for a single Firewall Threat Defense high availability pair 312
Suspend and resume high availability 313
Replace a unit in Firewall Threat Defense high availability pair 314
Replace a Primary Firewall Threat Defense HA Unit with no Backup 314
Replace a Secondary Firewall Threat Defense HA Unit with no Backup 315
Break a high availability pair 316

Delete (Unregister) a High Availability Pair and Register to a New Firewall Management Center 318
Monitoring High availability 319
View failover history 319
View stateful failover statistics 319
Troubleshoot configuration sync failure 320
History for high availability 320

CHAPTER 9 **Clustering: Secure Firewall 3100/4200 323**
Clustering for the Secure Firewall 3100/4200 323
How a cluster fits into your network 323
Control and data node roles 324
Cluster interfaces 324
Cluster control links 324
Configuration replication 324
Management network 325
Licenses for clustering 325
Prerequisites for clustering 325
Guidelines for clustering 326
Clustering configuration 331
Cluster interfaces 331
Cluster control link 331
Spanned EtherChannels 333
Cable and add devices to the Firewall Management Center 336
Create a Cluster 338
Configure interfaces 345
Configure cluster health monitor settings 346
Cluster node management 351
Add a new cluster node 351
Break a node 353
Break the cluster 354
Disable clustering 355
Rejoin the cluster 356
Change the control node 356
Edit the cluster configuration 357

Reconcile cluster nodes 358
Delete (Unregister) the Cluster or Nodes and Register to a New Firewall Management Center 360
Monitor the cluster 361
Cluster health monitor dashboard 363
View cluster health 363
Cluster metrics 365
Troubleshoot the cluster 365
Perform a ping on the cluster control link 367
Clustering examples 368
Firewall on a stick 368
Traffic segregation 369
Reference for Clustering 370
Firewall Threat Defense features and clustering 370
Unsupported features with clustering 370
Centralized features for clustering 371
Connection settings and clustering 372
FTP and Clustering 372
NAT and clustering 372
Dynamic routing 374
SIP inspection and clustering 374
SNMP and clustering 374
Syslog and clustering 375
Cisco TrustSec and clustering 375
VPN and clustering 375
Performance scaling factor 375
Control node election 376
High availability within clusters 376
Node health monitoring 377
Interface monitoring 377
Status after failure 377
Rejoin the cluster 378
Data path connection state replication 378
How the cluster manages connections 379
Connection roles 379

New connection ownership 380
Sample data flow for TCP 380
Sample data flows for ICMP and UDP 381
History for Clustering 382

CHAPTER 10 **Clustering: Private Cloud 385**
About clustering: private cloud 385
How the cluster fits into your network 385
Control and data node roles 386
Individual interfaces 386
Policy-based routing 387
Equal-cost multi-path routing 387
Cluster Control Link 388
Cluster control link traffic overview 388
Configuration replication 389
Management network 389
Licenses for clustering: Private cloud 389
Prerequisites for clustering: Private cloud 390
Guidelines for clustering: Private cloud 391
Configure clustering: private cloud 392
Add nodes to the Management Center 392
Create a cluster 392
Configure interfaces 400
Configure Cluster Health Monitor Settings 401
Manage cluster nodes 404
Add a new cluster node 404
Break a node 406
Break the cluster 407
Disable clustering 408
Rejoin the cluster 409
Change the control node 409
Edit the cluster configuration 410
Reconcile cluster nodes 411
Delete (Unregister) the cluster or nodes and register to a New Firewall Management Center 413

Monitor cluster status 414
Cluster health monitor 416
View the cluster health monitor 417
Troubleshoot the cluster 419
Perform a ping on the cluster control link 420
Reference for clustering 422
Threat Defense features and clustering 422
Unsupported features and clustering 422
Centralized features for clustering 422
Connection settings and clustering 423
Dynamic routing and clustering 423
FTP and clustering 424
NAT and clustering 424
SIP inspection and clustering 426
SNMP and clustering 426
Syslog and clustering 426
Cisco trustsec and clustering 426
VPN and clustering 426
Performance scaling factor 427
Control node election 427
High availability within the cluster 428
Node health monitoring 428
Interface monitoring 428
Status after failure 428
Rejoining the cluster 429
Data path connection state replication 429
How the cluster manages connections 430
Connection roles 430
New connection ownership 431
Sample data flow for TCP 431
Sample data flow for ICMP and UDP 432
History for clustering: private cloud 434

CHAPTER 11 **Clustering: Public Cloud** 437

About Threat Defense Virtual clustering in the public cloud 437
How the cluster fits into your network 438
Individual interfaces 438
Control and data node roles 439
Cluster Control Link 439
Cluster control link traffic overview 440
Configuration replication 440
Management network 440
Licenses for Threat Defense Virtual clustering 440
Requirements and prerequisites for Threat Defense Virtual clustering 441
Guidelines for Threat Defense Virtual clustering 443
Deploy the cluster in AWS 444
AWS gateway load balancer and Geneve single-arm proxy 444
Sample topology 445
End-to-end process for deploying Threat Defense Virtual cluster on AWS 446
Templates 448
Deploy the Stack in AWS Using a CloudFormation template 448
Manual cluster deployment in AWS 461
Create the Day0 configuration for AWS 461
Deploy cluster nodes 463
Target failover for Secure Firewall Threat Defense Virtual clustering with GWLB in AWS 464
Enable target failover for Secure Firewall Threat Defense Virtual clustering in AWS 465
Deploy the cluster in Azure 466
Sample topology for GWLB-based cluster deployment 466
Azure gateway load balancer and paired proxy 467
End-to-end process for deploying Threat Defense Virtual cluster in Azure with GWLB 468
Templates 470
Prerequisites for Azure GWLB cluster deployment 470
Deploy cluster on Azure with GWLB using an Azure resource manager template 471
Sample topology for NLB-based cluster deployment 473
End-to-end process for deploying Threat Defense Virtual cluster in Azure with NLB 474
Templates 476
Prerequisites for Azure NLB cluster deployment 476
Deploy cluster on Azure with NLB using an Azure resource manager template 478

Manual cluster deployment in Azure 479
Create the Day0 configuration for Azure 479
Deploy cluster nodes manually - GWLB-based deployment 481
Deploy cluster nodes manually - NLB-based deployment 483
Troubleshoot cluster deployment in Azure 484
Deploy the cluster in GCP 485
Sample topology for GCP clustering autoscale solution 485
End-to-end process for deploying Threat Defense Virtual cluster in GCP 486
Templates 488
Deploy the instance group in GCP using an instance template 488
Manual cluster deployment in GCP 490
Create the Day0 configuration with a fixed configuration for GCP 490
Deploy cluster nodes manually 491
Allow health checks for GCP network load balancers 491
Add the cluster to the Management Center (manual deployment) 493
Edit cluster health monitor settings 500
Manage cluster nodes 503
Disable clustering 503
Rejoin the cluster 504
Reconcile Cluster Nodes 504
Delete (Unregister) the cluster or nodes and register with a new Firewall Management Center 505
Monitor cluster status 506
Cluster health monitor 508
View the cluster health monitor 509
Troubleshoot the cluster 512
Perform a ping on the cluster control link 513
Upgrade the cluster 514
Reference for clustering 515
Threat Defense features and clustering 515
Unsupported features and clustering 515
Centralized features for clustering 515
Cisco Trustsec and clustering 516
Connection settings and clustering 516
Dynamic routing and clustering 516

FTP and clustering 517
NAT and clustering 517
SIP inspection and clustering 519
SNMP and clustering 519
Syslog and clustering 519
VPN and Clustering 519
Performance scaling factor 520
Control node election 520
High availability within the cluster 521
Node health monitoring 521
Interface monitoring 521
Status after failure 522
Rejoining the cluster 522
Data path connection state replication 522
How the cluster manages connections 523
Connection roles 523
New connection ownership 524
Sample data flow for TCP 524
Sample data flow for ICMP and UDP 525
History for Threat Defense Virtual clustering in the public cloud 527

CHAPTER 12 **Clustering: Firepower 4100/9300** 529
About clustering on the Firepower 4100/9300 chassis 529
Bootstrap configuration 530
Cluster members 530
Cluster control link 530
Size the cluster control link 531
Cluster control link redundancy 531
Cluster control link reliability for inter-chassis clustering 532
Cluster control link network 532
Management network 532
Management interface 532
Cluster interfaces 532
Spanned EtherChannels 533

Connecting to a redundant switch system 533
Configuration replication 533
Licenses for clustering 534
Requirements and prerequisites for clustering 534
Clustering guidelines and limitations 538
Configure clustering 541
FXOS: Add a Firewall Threat Defense cluster 541
Create a Firewall Threat Defense cluster 541
Add more cluster nodes 552
Firewall Management Center: Add a cluster 556
Firewall Management Center: Configure cluster, data interfaces 562
Firewall Management Center: Configure Cluster Health Monitor Settings 564
FXOS: Remove a cluster node 567
Firewall Management Center: Manage cluster members 569
Add a new cluster member 569
Replace a cluster member 570
Deactivate a member 571
Rejoin the cluster 572
Delete (Unregister) a data node 572
Change the control unit 573
Reconcile cluster members 574
Firewall Management Center: Monitor the cluster 574
Cluster Health Monitor Dashboard 577
Viewing cluster health 578
Cluster metrics 580
Troubleshoot the cluster 581
Perform a ping on the cluster control link 582
Examples for Clustering 583
Firewall on a stick 583
Traffic segregation 584
Reference for clustering 585
Firewall Threat Defense features and clustering 585
Unsupported features with clustering 585
Centralized features for clustering 586

Connection settings 586
Dynamic routing and clustering 587
FTP and clustering 587
Multicast routing and clustering 587
NAT and clustering 587
SIP inspection and clustering 589
SNMP and clustering 589
Syslog and clustering 589
TLS/SSL connections and clustering 589
Cisco TrustSec and clustering 589
VPN and clustering 589
Performance scaling factor 590
Control unit election 590
High availability within the cluster 591
Chassis-application monitoring 591
Unit health monitoring 591
Interface monitoring 591
Decorator application monitoring 592
Status after failure 592
Rejoining the cluster 592
Data path connection state replication 593
How the cluster manages connections 593
Connection roles 593
New connection ownership 595
Sample data flow for TCP 595
Sample data flow for ICMP and UDP 596
History for clustering 597

PART III **Interfaces and Device Settings** 603

CHAPTER 13 **Interface Overview** 605
Management interface 605
Management interface 605
Diagnostic interface 606

Interface Mode and Types 607
Security zones and interface groups 607
Auto-MDI/MDIX feature 609
Redundant interfaces (deprecated) 609
Default settings for interfaces 609
Create security zone and interface group objects 610
Enable the physical interface and configure Ethernet settings 611
Configure EtherChannel interfaces 614
About EtherChannels 614
EtherChannels 614
Guidelines for EtherChannels and redundant interfaces 617
Configure an EtherChannel 619
Sync Interface Changes with the Firewall Management Center 622
Network module management for Secure Firewall 3100/4200 625
Configure breakout ports 626
Add a network module 630
Hot swap the network module 632
Replace the network module with a different type 634
Remove the network module 638
Merge the management and diagnostic interfaces 640
Unmerge the management interface 644
History for interfaces 645

CHAPTER 14 **Regular Firewall Interfaces** 649
Requirements and prerequisites for regular firewall interfaces 649
Configure switch ports 650
About switch ports 650
Switch ports and interfaces 650
Auto-MDI/MDIX feature 651
Prerequisites for switch ports 651
Guidelines for switch ports 651
Configure switch ports and power over ethernet 653
Enable or disable switch port mode 653
Configure a VLAN interface 653

Configure switch ports as access ports 655
Configure switch ports as trunk ports 657
Configure Power over Ethernet 660
Loopback interfaces 661
Guidelines for Loopback Interfaces 662
Configure a loopback interface 662
Rate-Limit traffic to the loopback interface 663
VLAN subinterfaces and 802.1Q trunking 667
Guidelines for VLAN subinterfaces 667
Maximum number of VLAN subinterfaces by device model 668
Add a subinterface 669
Configure VXLAN Interfaces 671
VXLAN interfaces 671
encapsulation 671
VXLAN tunnel endpoints 671
VTEP source interface 672
VNI interfaces 672
How VXLAN and Geneve packets are processed 673
Peer VTEPs 674
VXLAN use cases 675
Requirements and prerequisites for VXLAN interfaces 679
Guidelines for VXLAN interfaces 679
Configure VXLAN or Geneve interfaces 680
Configure VXLAN interfaces 680
Configure geneve interfaces 683
Allow gateway load balancer health checks 685
Configure routed and transparent mode interfaces 686
Routed and transparent mode interfaces 686
Dual IP stack (IPv4 and IPv6) 686
31-bit subnet masks 686
Guidelines and limitations for routed and transparent mode interfaces 687
Configure routed mode interfaces 690
Bridge group interfaces 695
Configure general bridge group member interface parameters 695

Configure the bridge virtual interface (BVI) 698
Configure IPv6 addressing 699
About IPv6 699
IPv6 prefix delegation client configuration 700
Configure a global IPv6 address 704
Configure IPv6 neighbor discovery 709
Advanced interface settings 711
About advanced interface configuration 711
MAC addresses 711
MTU 712
TCP MSS 714
ARP inspection for bridge group traffic 715
MAC address tables 716
Default settings 716
Guidelines for ARP inspection and the MAC address table 716
Configure the MTU 717
Configure the MAC address 718
Add a static ARP entry 718
Add a static MAC address and disable MAC learning for a bridge group 720
Set security configuration parameters 720
History for Regular Firewall Interfaces 723

CHAPTER 15 **Inline Sets and Passive Interfaces** 727
IPS interfaces 727
Inline sets 727
Multiple inline pairs and asynchronous routing 728
Passive interfaces 729
Hardware Bypass for inline sets 730
Hardware Bypass triggers 730
Hardware bypass switchover 730
Snort Fail Open vs. Hardware Bypass 731
Hardware Bypass status 731
Requirements and prerequisites for inline sets 731
Guidelines for configuring inline sets and passive interfaces 733

Configure a passive interface 735
Configure Inline Sets 736
History for inline sets and passive interfaces 740

CHAPTER 16 Device Settings 743
Edit general settings 743
Generate troubleshooting files 745
View CLI output 747
Copy a configuration to another device 749
Export and import the device configuration 751
Edit license settings 755
View system information 756
View device inventory 756
View the inspection engine 757
Edit health settings 757
Edit management settings 757
Configure a redundant manager access data interface 758
Change manager access interface settings 763
Change the device IP address 763
Change the Firewall Management Center IP Address 774
Change both Firewall Management Center and Threat Defense IP addresses 776
Change the manager access interface 779
Troubleshoot the management connection 790
Manually Roll Back the configuration if the Firewall Management Center loses Connectivity 791
Troubleshoot Management Connectivity on a Data Interface 792
View inventory details 793
Edit applied policies 794
Edit advanced settings 796
Configure automatic application bypass 797
Configure object group search 798
Configure interface object optimization 799
Edit deployment settings 800
Edit cluster health monitor settings 802
Hot swap an SSD 805

Configure SNMP for FXOS 808
Enable SNMP for FXOS 808
Create an SNMP Trap for FXOS 809
Create an SNMP user for FXOS 811
Configure alarms for the ISA 3000 811
About alarms 812
Alarm input interfaces 812
Alarm output interface 813
Syslog alarms 813
SNMP Alarms 813
Defaults for alarms 813
Prerequisites for alarms 814
Configure alarms for the ISA 3000 814
Configure alarm input contacts 814
Configure power supply alarms 817
Configure temperature alarms 819
Turn off the external alarm 822
Monitoring alarms 822
Monitoring alarm status 822
Monitoring syslog messages for alarms 822
History for Device Settings 823

CHAPTER 17 DHCP and DDNS 827
About DHCP and DDNS services 827
DHCPv4 servers 827
DHCP options 828
DHCPv6 stateless server 828
DHCP relay agents 829
Requirements and prerequisites for DHCP and DDNS 829
Guidelines for DHCP and DDNS services 829
Configure the DHCPv4 server 831
DHCPv6 stateless server configuration 833
Create a DHCP IPv6 pool 833
Enable the DHCPv6 stateless server 836

Configure the DHCP relay agent 837
Configure Dynamic DNS 838
History for DHCP and DDNS 844

CHAPTER 18 Platform Settings 847
Platform settings policies 848
List requirements and prerequisites for platform settings policies 848
Manage platform settings policies 849
Chassis platform settings 850
Configure ARP inspection 850
Configure a banner 852
Configure DNS server settings 852
Configure external authentication 855
Configure an LDAP External Authentication Object 857
Configure a RADIUS Authentication Object 860
Configure fragment settings 861
Configure HTTP access 862
Configure ICMP access 864
Configure NetFlow 865
Add a collector in NetFlow 866
Add a traffic class to NetFlow 867
Configure Secure Shell (SSH) access 867
Configure an SMTP server 869
Configure SNMP for a security device 870
SNMP protocol 871
List SNMP terminology 871
Describe MIBs and traps 872
List of supported tables and objects in MIBs 873
Add SNMPv3 users 877
Add SNMP hosts 880
Configure SNMP traps 882
Configure SSL Settings 884
Configure SSL settings 885
Syslog 888

Syslog messages 889
Syslog message severity levels 889
Syslog message filters 890
Syslog message classes and associated message ID numbers 891
Guidelines for logging 894
Configure syslog logging for Firewall Threat Defense devices 895
Firewall Threat Defense platform settings that apply to security event syslog messages 896
Configure logging and basic settings 897
Enable logging destinations 898
Configure syslog messages to be sent to an e-mail address 900
Create a custom event list 900
Configure syslog rate limits 902
Configure syslog settings 903
Configure a syslog server 904
Configure timeouts 906
Synchronize time on FTD devices 908
Configure a time zone for a device 911
Configure UCAPL/CC compliance 911
Configure a performance profile 912
History for platform settings 913

CHAPTER 19 **FlexConfig policies 921**
FlexConfig policy overview 921
Recommended usage for FlexConfig policies 922
CLI commands in FlexConfig objects 922
Determine the ASA software version and current CLI configuration 923
Prohibited CLI commands 924
Template scripts 926
FlexConfig variables 926
Variable processing 927
Evaluate device variable results 930
FlexConfig policy object variables 932
FlexConfig system variables 933
Predefined FlexConfig objects 934

Predefined text objects 939
Requirements and prerequisites for FlexConfig policies 942
Guidelines and limitations for FlexConfig 943
Customize device configuration with FlexConfig policies 943
Configure FlexConfig objects 945
Add a policy object variable to a FlexConfig object 948
Configure secret keys 949
Configure FlexConfig text objects 950
Configure the FlexConfig policy 951
Set target devices for a FlexConfig policy 952
Preview the FlexConfig policy 953
Verify the deployed configuration 954
Remove features configured using FlexConfig 956
Convert from FlexConfig to managed feature 958
Examples for FlexConfig 958
Configure precision time protocol (ISA 3000) 958
Configure automatic hardware bypass for power failure (ISA 3000) 962
Migrate FlexConfig policies 964
History for FlexConfig 966

PART IV **Routing** 971

CHAPTER 20 **Static and Default Routes** 973
Static and default routes overview 973
Default routes 973
Static routes 974
Route to null0 interface to drop unwanted traffic 974
Route priorities 974
Transparent firewall mode and bridge group routes 975
Static route tracking 975
Requirements and prerequisites for static routes 976
Guidelines for static and default routes 976
Add a static route 977
Reference for routing 978

Path determination 978
Supported route types 979
Static versus dynamic routing algorithms 979
Single-path versus multipath 979
Flat versus hierarchical routing 979
Link-state versus distance vector 980
Supported internet protocols for routing 980
Routing tables 981
How the routing table is populated 981
How forwarding decisions are made 983
Dynamic routing and High availability 984
Dynamic routing in Clustering 984
Dynamic routing in individual interface mode 985
Routing table for management traffic 986
Equal-cost multi-path routing 987
Routing GRE traffic 988
About route maps 988
Permit and deny clauses 988
Match and set clause values 989

CHAPTER 21 **Virtual Routers** 991
Virtual routers and virtual routing and forwarding (VRF) 991
Virtual router applications 992
Global and user-defined virtual routers 992
Virtual-router-aware policies 993
Virtual router interconnection 994
Best practice for overlapping IP addresses 996
Configuring SNMP on user-defined virtual routers 997
Maximum number of virtual routers by device model 997
Requirements and prerequisites for virtual routers 999
Guidelines and limitations for virtual routers 999
Manage virtual routers 1001
Create a virtual router 1002
Configure a virtual router 1002

Modify a virtual router 1004
Remove Virtual Routers 1005
Monitor virtual routers 1006
Configuration examples for virtual routers 1006
Route to a distant server through virtual routers 1006
How to Provide Internet Access with Overlapping Address Spaces 1011
Allow RA VPN access to internal networks in virtual routing 1018
Secure traffic from networks in multiple virtual routers over a site-to-site VPN 1021
Secure traffic from networks with multiple virtual routers over a site-to-site VPN with dynamic VTI 1025
Route traffic between two overlapping network hosts in virtual routing 1027
Manage overlapping segments in routed firewall mode with BVI interfaces 1030
Configure user authentication with overlapping networks 1034
Interconnect virtual routers using BGP 1040
History for virtual routers 1045

CHAPTER 22 **ECMP** 1047
ECMP routing methods 1047
Guidelines and limitations for ECMP 1048
Manage ECMP zones for virtual routers 1049
Create an ECMP zone 1049
Configure an equal cost static route 1050
Modify an ECMP zone 1051
Remove an ECMP zone 1052
Configure ECMP zones on your device 1053
History for ECMP in Secure Firewall Threat Defense 1056

CHAPTER 23 **Bidirectional Forwarding Detection Routing** 1057
BFD routing protocol 1057
Guidelines for BFD routing 1057
Configure BFD 1059
Configure BFD policies 1059
Configure a single-hop BFD policy 1060
Configure a multi-hop BFD policy 1061

History for BFD routing 1062

CHAPTER 24 OSPF 1063

OSPF 1063

OSPF routing 1063

OSPF support for fast hello packets 1065

OSPF fast hello packets configuration prerequisites 1065

OSPF hello interval and dead interval 1065

OSPF fast hello packets 1065

Benefits of OSPF fast hello packets 1066

OSPFv2 and OSPFv3 implementation differences 1066

Requirements and prerequisites for OSPF 1067

Guidelines for OSPF 1067

OSPFv2 configuration 1070

Configure OSPF areas, ranges, and virtual links 1070

Configure OSPF redistribution 1073

Configure OSPF Inter-Area filtering 1075

Configure OSPF filter rules 1076

Configure OSPF summary addresses 1077

Configure OSPF interfaces and neighbors 1078

Configure OSPF Advanced Properties 1080

OSPFv3 configuration 1083

Configure OSPFv3 Areas, Route Summaries, and Virtual Links 1083

Configure OSPFv3 redistribution 1085

Configure OSPFv3 summary prefixes 1087

Configure OSPFv3 interfaces, authentication, and neighbors 1088

Configure OSPFv3 Advanced Properties 1090

History for OSPF 1093

CHAPTER 25 EIGRP 1095

EIGRP routing 1095

Requirements and prerequisites for EIGRP 1096

Guidelines and limitations for EIGRP routing 1097

Configure EIGRP routing on firewall devices 1098

Configure EIGRP settings 1099
Configure EIGRP neighbors settings 1099
Configure EIGRP filter rules 1100
Configure EIGRP redistribution settings 1101
Configure EIGRP summary address settings 1102
Configure EIGRP interfaces settings 1103
Configure EIGRP advanced settings 1104
History for EIGRP 1106

CHAPTER 26 BGP 1107
BGP 1107
Routing tables 1107
BGP usage scenarios 1108
BGP path selection 1109
BGP multipath 1109
Requirements and prerequisites for BGP 1111
Guidelines for BGP 1111
Configure BGP 1112
Configure basic BGP settings 1113
Configure BGP general settings 1115
Configure BGP Neighbor Settings 1117
Configure BGP aggregate address settings 1121
Configure BGPv4 filtering settings 1122
Configure BGP network settings 1123
Configure BGP redistribution settings 1123
Configure BGP route injection settings 1124
Configure BGP route import and export 1125
History for BGP 1127

CHAPTER 27 RIP 1129
RIP 1129
How RIP routing updates work 1130
RIP routing metric 1130
RIP stability features 1130

RIP timers 1131
Requirements and prerequisites for RIP 1132
Guidelines for RIP 1132
Configure RIP 1133

CHAPTER 28 **Multicast** 1137
Multicast routing 1137
IGMP Protocol 1138
Stub multicast routing 1138
PIM multicast routing 1139
PIM sparse mode 1139
PIM source specific multicast support 1139
Multicast Bidirectional PIM 1140
PIM bootstrap router (BSR) 1140
PIM bootstrap router (BSR) terminology 1141
Multicast group concept 1141
Multicast Addresses 1142
Clustering 1142
Prerequisites for Multicast Routing 1142
Guidelines for multicast routing 1142
Configure IGMP features 1143
Enable multicast routing 1144
Configure IGMP protocol 1145
Configure IGMP access groups 1146
Configure IGMP static groups 1147
Configure IGMP join groups 1148
Configure PIM features 1149
Configure PIM protocol 1149
Configure PIM neighbor filters 1150
Configure PIM bidirectional neighbor filters 1151
Configure PIM rendezvous points 1152
Configure PIM route trees 1153
Configure PIM request filters 1154
Configure the Firewall Threat Defense device as a candidate bootstrap router 1154

Configure multicast routes 1155
Configure multicast boundary filters 1156

CHAPTER 29 Policy-Based Routing 1159
About policy-based routing 1159
Licenses for policy-based routing 1161
Best practices for policy-based routing 1161
Path monitoring metrics for best path route determination 1163
Configure path monitoring settings 1165
Add path monitoring dashboard 1166
Configure policy-based routing policy 1166
Configure policy-based routing 1169
Configure PBR with path monitoring 1175
Useful CLIs for monitoring PBR 1177
Troubleshoot PBR 1179
History for policy-based routing 1182

PART V Network Policies 1185

CHAPTER 30 Network Address Translation 1187
NAT functions 1187
NAT basics 1188
NAT terminology 1188
NAT types 1188
NAT in routed and transparent mode 1189
NAT in routed mode 1189
NAT in transparent mode or within a bridge group 1190
Auto NAT and Manual NAT 1191
Auto NAT 1191
Manual NAT 1191
Comparing Auto NAT and Manual NAT 1192
NAT rule order 1192
NAT interfaces 1194
NAT exemption 1195

Configuring routing for NAT 1195
Addresses on the same network as the mapped interface 1196
Addresses on a unique network 1196
The same address as the real address (identity NAT) 1196
Requirements and prerequisites for NAT policies 1197
Guidelines for NAT 1197
Firewall mode guidelines for NAT 1197
IPv6 NAT guidelines 1198
IPv6 NAT best practices 1198
NAT support for inspected protocols 1198
FQDN destination guidelines 1200
Additional guidelines for NAT 1201
Manage NAT policies 1203
Create NAT policies 1204
Configure NAT policy targets 1204
Configure NAT for threat defense 1205
Customize NAT rules for multiple devices 1207
Search and filter the NAT rule table 1209
Enable, disable, or delete multiple rules 1210
Dynamic NAT 1210
About dynamic NAT 1211
Dynamic NAT disadvantages and advantages 1212
Configure dynamic auto NAT 1212
Configure dynamic manual NAT 1214
Dynamic PAT 1216
About dynamic PAT 1216
Dynamic PAT disadvantages and advantages 1217
PAT pool object guidelines 1217
Configure dynamic auto PAT 1218
Configure dynamic manual PAT 1220
Configure PAT with port block allocation 1223
Static NAT 1226
About static NAT 1226
Configure static auto NAT 1230

Configure static manual NAT 1232
Identity NAT 1235
Configure identity auto NAT 1236
Configure identity manual NAT 1237
NAT rule properties for Firewall Threat Defense 1239
Interface objects NAT properties 1240
Translation properties for auto NAT 1241
Translation properties for manual NAT 1242
PAT pool NAT properties 1243
Advanced NAT properties 1244
Translating IPv6 networks 1245
NAT64/46: translating IPv6 addresses to IPv4 1246
NAT64/46 example: inside IPv6 network with outside IPv4 internet 1246
NAT64/46 example: inside IPv6 network with outside IPv4 internet and DNS translation 1248
NAT66: translating IPv6 addresses to different IPv6 addresses 1252
NAT66 example, static translation between networks 1252
NAT66 example, simple IPv6 interface PAT 1255
Monitoring NAT 1258
Examples for NAT 1259
Providing access to an inside web server (static auto NAT) 1259
Dynamic auto NAT for inside hosts and static NAT for an outside web server 1261
Configure inside load balancer with multiple mapped addresses 1268
Single address for FTP, HTTP, and SMTP (static auto NAT with port translation) 1270
Different translation depending on the destination (dynamic manual PAT) 1278
Configure dynamic manual PAT with different destination ports 1285
NAT and site-to-site VPN 1291
DNS query and response rewriting using NAT 1296
DNS64 reply modification 1297
Create DNS reply modification with DNS server on outside 1304
Configure DNS reply modification with DNS server on host network 1307
History for Firewall Threat Defense NAT 1310

CHAPTER 31 **Quality of Service** 1313
QoS 1313

QoS policies 1314
Requirements and prerequisites for QoS 1314
Guidelines and limitations for QoS policies 1315
Rate limiting with QoS policies 1315
Create a QoS policy 1316
Set target devices for a QoS policy 1317
Filter QoS rules by device 1317
Configuring QoS rules 1318
QoS rule components 1319
QoS rule conditions 1320
Interface rule conditions 1320
Network rule conditions 1321
User rule conditions 1321
Application rule conditions 1322
Best practice: use application-based rules over port-based rules 1323
Recommendation: use URL conditions for website access control 1324
Custom SGT rule conditions 1325
ISE SGT versus custom SGT rule conditions 1325
Autotransition from custom Security Group Tags to ISE Security Group Tags 1325
History for QoS 1326

PART VI **Secure Connections** 1327

CHAPTER 32 **Secure Connections Overview** 1329
VPN types 1329
VPN basics 1330
Internet Key Exchange (IKE) 1331
IPsec 1332
VPN packet flow 1333
IPsec flow offload 1333
VPN licensing 1334
VPN encryption and performance 1334
Comply with security certification requirements 1334
Decide encryption algorithms for VPN policies 1334

Decide which hash algorithms to use 1335
Decide which Diffie-Hellman modulus group to use 1336
Decide VPN authentication methods 1336
Pre-shared keys 1337
PKI infrastructure and digital certificates 1337
Deprecated hash algorithms, encryption algorithms, and Diffie-Hellman modulus groups 1339
VPN topologies 1340
Point-to-point VPN topologies 1340
Hub and spoke VPN topology 1341
Full mesh VPN topology 1342
Implicit topologies 1343

CHAPTER 33 Site-to-Site VPN 1345
Site-to-site VPN 1345
Guidelines for configuring site-to-site VPN in Secure Firewall Threat Defense devices 1347
Limitations for configuring site-to-site VPN in Threat Defense devices 1347
Types of site-to-site VPN topologies 1348
License requirements for site-to-site VPN 1348
Prerequisites for site-to-site VPN 1349
Manage site-to-site VPNs 1349
Configure a policy-based site-to-site VPN 1351
Firewall Threat Defense VPN endpoint options 1352
Firewall Threat Defense VPN IKE options 1356
Firewall Threat Defense VPN IPsec options 1358
Firewall Threat Defense advanced site-to-site VPN deployment options 1360
Firewall Threat Defense VPN advanced IKE options 1361
Firewall Threat Defense VPN advanced IPsec options 1362
Firewall Threat Defense advanced site-to-site VPN tunnel options 1362
Configure virtual tunnel interfaces 1364
Virtual tunnel interfaces 1364
Static VTI 1365
Dynamic VTI 1366
Guidelines for virtual tunnel interfaces 1368
Limitations for Virtual Tunnel Interfaces 1370

Add a VTI interface 1371
Create a route-based site-to-site VPN 1373
Configure endpoints for a point-to-point VPN topology 1374
Configure endpoints for a hub and spoke topology 1376
Configure multiple hubs in a route-based VPN 1380
Route traffic through a backup VTI tunnel 1383
Configure dynamic VTI for a route-based site-to-site VPN 1384
Configure a virtual router with dynamic VTI 1384
Configure routing and AC policies for VTI 1385
View virtual tunnel interface details 1388
Deploy a SASE tunnel on Umbrella 1388
Guidelines for configuring SASE tunnels on Umbrella 1388
Limitations for configuring SASE tunnels on Umbrella 1389
Deploy a SASE tunnel on Umbrella 1389
Prerequisites for configuring Umbrella SASE tunnels 1390
Map Management Center Umbrella parameters and Cisco Umbrella API keys 1390
Configure a SASE tunnel for Umbrella 1392
Monitor site-to-site topologies 1395
Monitor site-to-site VPNs using Site-to-Site VPN summary page 1395
Monitor site-to-site VPNs using Site-to-Site VPN dashboard 1395
Tunnel status widget 1396
Site-to-site VPN connection event monitoring 1399
View site-to-site VPN connection events 1400
History for site-to-site VPN 1400

CHAPTER 34 **SD-WAN** 1405
SD-WAN capabilities 1405
SD-WAN features 1406
Use cases for SD-WAN capabilities 1407
Monitor SD-WAN topologies 1408
SD-WAN summary dashboard 1408
Prerequisites for using SD-WAN summary dashboard 1408
Monitor WAN devices and interfaces using the SD-WAN summary dashboard 1411

Monitor application performance metrics of WAN interfaces using SD-WAN summary dashboard 1413

CHAPTER 35 **Remote Access VPN** 1415

Remote Access VPN Overview 1415
Remote Access VPN Features 1416
Secure Client Components 1418
Remote Access VPN Authentication 1418
Understanding Policy Enforcement of Permissions and Attributes 1420
Understanding AAA Server Connectivity 1420
License Requirements for Remote Access VPN 1421
Requirements and Prerequisites for Remote Access VPN 1421
Remote Access VPN Guidelines and Limitations 1422
Configuring a New Remote Access VPN Connection 1425
Prerequisites for Configuring Remote Access VPN 1426
Create a New Remote Access VPN Policy 1426
Update the Access Control Policy on the Secure Firewall Threat Defense Device 1429
(Optional) Configure NAT Exemption 1430
Configure DNS 1431
Add Secure Client Profile XML File 1431
(Optional) Configure Split Tunneling 1432
(Optional) Configure Dynamic Split Tunneling 1433
Verify Dynamic Split Tunneling Configuration 1434
Verify the Configuration 1434
Create a Copy of an Existing Remote Access VPN Policy 1435
Set Target Devices for a Remote Access VPN Policy 1435
Associate Local Realm with Remote Access VPN Policy 1436
Additional Remote Access VPN Configurations 1436
Configure Connection Profile Settings 1436
Configure IP Addresses for VPN Clients 1437
Configure AAA Settings for Remote Access VPN 1439
Create or Update Aliases for a Connection Profile 1454
Configure Access Interfaces for Remote Access VPN 1455
Configure Advanced Options for Remote Access VPN 1457

Cisco Secure Client Image 1457
Remote Access VPN Address Assignment Policy 1459
Configure Certificate to Connection Profile Mapping 1460
Configure Group Policies 1461
Configuring LDAP Attribute Mapping 1462
Configuring VPN Load Balancing 1463
Configure IPsec Settings 1467
Customize Cisco Secure Client 1472
Configure Secure Client Management VPN Tunnel 1485
Requirements and Prerequisites for Secure Client Management VPN Tunnel 1485
Limitations of Secure Client Management VPN Tunnel 1486
Configuring Secure Client Management VPN Tunnel on Firewall Threat Defense 1486
Multiple Certificate Authentication 1488
Guidelines and Limitations of Multiple Certificate Authentication 1488
Configuring Multiple Certificate Authentication 1489
Customizing Remote Access VPN AAA Settings 1490
Authenticate VPN Users via Client Certificates 1490
Configure VPN User Authentication via Client Certificate and AAA Server 1492
Manage Password Changes over VPN Sessions 1493
Send Accounting Records to the RADIUS Server 1494
Delegating Group Policy Selection to Authorization Server 1495
Override the Selection of Group Policy or Other Attributes by the Authorization Server 1496
Deny VPN Access to a User Group 1497
Restrict Connection Profile Selection for a User Group 1498
Update the Secure Client Profile for Remote Access VPN Clients 1498
RADIUS Dynamic Authorization 1499
Configuring RADIUS Dynamic Authorization 1500
Two-Factor Authentication 1501
Configuring RSA Two-Factor Authentication 1501
Configuring Duo Two-Factor Authentication 1502
Secondary Authentication 1504
Configure Remote Access VPN Secondary Authentication 1504
Single Sign-On Authentication with SAML 2.0 1506
Guidelines and Limitations for SAML 2.0 1507

Configuring a SAML Single Sign-On Authentication 1508
Configuring SAML Authorization 1509
Advanced Secure Client Configurations 1511
Configure Secure Client Modules on a Firewall Threat Defense 1511
Types of Secure Client Modules 1511
Prerequisites for Configuring Secure Client Modules 1512
Guidelines for Configuring Secure Client Modules 1513
Install Secure Client Modules using a Firewall Threat Defense 1514
Configure a Remote Access VPN Group Policy with Secure Client Modules 1515
Verify Secure Client Modules Configuration 1515
Configure Application-Based (Per App VPN) Remote Access VPN on Mobile Devices 1516
Prerequisites and Licensing for Configuring Per App VPN Tunnels 1516
Determine the Application IDs for Mobile Applications 1517
Configure Application-Based VPN Tunnels 1518
Verify Per App Configuration 1519
Remote Access VPN Examples 1519
How to Limit Secure Client Bandwidth Per User 1519
How to Use VPN Identity for User-Id Based Access Control Rules 1520
Configure Firewall Threat Defense Multiple Certificate Authentication 1520
Monitor Remote Access VPNs 1524
Remote Access VPN Dashboard 1524
VPN Session and User Information 1526
Viewing Remote Access VPN Active Sessions 1526
Viewing Remote Access VPN User Activity 1526
History for Remote Access VPNs 1526

CHAPTER 36 **Dynamic Access Policies** 1531
Firewall Threat Defense dynamic access policies 1531
Hierarchy of policy enforcement of permissions and attributes in a Firewall Threat Defense device 1532
Prerequisites for dynamic access policy 1533
Guidelines and limitations for dynamic access policies 1533
Configure a Dynamic Access Policy (DAP) 1534
Create a dynamic access policy 1534
Create a dynamic access policy record 1534

Configure AAA criteria settings for a DAP record 1535
Configure endpoint attribute selection criteria in DAP 1536
Add an anti-malware endpoint attribute to a DAP record 1536
Add a device endpoint attribute to a DAP record 1537
Add Secure Client endpoint attributes to a DAP record 1538
Add NAC endpoint attributes to a DAP record 1539
Add an application attribute to a DAP record 1539
Add a personal firewall endpoint attribute to a DAP record 1540
Add an operating system endpoint attribute to a DAP record 1541
Add a process endpoint attribute to a DAP 1541
Add a registry endpoint attribute to a DAP record 1542
Add a file endpoint attribute to a DAP record 1542
Add certificate authentication attributes to a DAP record 1543
Configure advanced settings for DAP 1543
Associate dynamic access policy with remote access VPN 1544
History for dynamic access policy 1544

PART VII **Zero Trust Network Access** 1547

CHAPTER 37 **Zero Trust Network Access Overview** 1549
Zero Trust Access 1549
How Threat Defense Works with Zero Trust Access 1550
Zero trust network access 1551
Components of a Clientless Zero Trust Network Access Configuration 1551
Clientless Zero Trust Network Access Workflow 1552
Limitations for Clientless Zero Trust Network Access 1553
Prerequisites for Zero Trust Application Policy 1554
Manage Zero Trust Application Policies 1555
Create a Zero Trust Application Policy 1555
Create an Application Group 1557
Create an Application 1558
Set Targeted Devices for Zero Trust Access Policy 1560
Edit a Zero Trust Application Policy 1560
Monitor Zero Trust Sessions 1562

History for zero trust network access 1564

PART VIII **Access Control Policy Basics** 1567

CHAPTER 38 **Access Control Policies** 1569

Access control policies 1569

Access control policy components 1570

Access control policy default actions 1570

Access control policy inheritance 1572

Rule and other policy warnings 1573

Requirements and prerequisites for access control policies 1574

Manage access control policies 1575

Creating a basic access control policy 1575

Editing an access control policy 1576

Lock an access control policy 1578

Configure the access control default action 1579

Manage access control policy inheritance 1580

Choose a base access control policy 1581

Lock settings in descendant access control policies 1581

Inherit access control policy settings from the base policy 1582

Enforce an access control policy in a domain 1583

Assign access control policy to devices 1583

Logging settings for access control policies 1584

Associate prefilter, decryption, and identity policies with an access control 1585

View rule hit counts 1586

Analyzing rule conflicts and warnings 1588

Search for rules 1589

History for access control policies 1591

CHAPTER 39 **Security Intelligence** 1595

Security intelligence 1595

License requirements for security intelligence 1596

Requirements and prerequisites for security intelligence 1596

Best practices for security intelligence 1596

Guidelines and limitations for security intelligence 1597
Security intelligence sources 1598
Configure security intelligence 1599
Security intelligence options 1601
Security intelligence categories 1602
Block list icons 1604
Configuration example: Security intelligence blocking 1605
Security intelligence monitoring 1606
Override security intelligence blocking 1606
Troubleshooting security intelligence 1607
Security intelligence categories missing from the Available Options List 1607
History for security intelligence block listing 1608

CHAPTER 40 Access Control Rules 1609
Access control rules 1609
Access control rule management 1611
Access control rule components 1611
Access control rule order 1613
Access control rule actions 1614
Access control rule monitor action 1614
Access control rule trust action 1614
Access control rule blocking actions 1615
Access control rule interactive blocking actions 1615
Access control rule allow action 1616
Deep inspection using file and intrusion policies 1617
File and intrusion inspection order 1618
How access control traffic handling works with intrusion and file policies 1619
Requirements and prerequisites for access control rules 1620
Guidelines and limitations for access control rules 1621
Best practices for application control 1622
Recommendations for application control 1622
Best practice for choosing between application matching and port matching 1624
Application-specific requirements for filtering 1625
Best practices for access control rules 1625

General best practice for access control 1626
Best practices for ordering rules 1627
Application rule order 1627
Rule preemption 1628
Best practice for rule actions and rule order 1628
Best practices for simplifying and focusing rules 1629
Maximum number of access control rules and intrusion policies 1630
Access control rule management 1630
Add an access control rule category 1630
Create and edit access control rules 1631
Access control rule conditions 1633
Enable and disable access control rules 1641
Copy access control rules from one access control policy to another 1641
Move access control rules to a prefilter policy 1642
Position an access control rule 1643
Add comments to an access control rule 1644
Examples for access control rules 1645
How to control access using security zones 1645
Control application usage 1645
Block threats 1646
History for access control rules 1649

CHAPTER 41 **URL Filtering Rules** 1651
URL filtering 1651
URL filtering with category and reputation 1652
URL category and reputation descriptions 1653
URL filtering data from the Cisco cloud 1653
Best practices for URL filtering 1654
HTTPS traffic filtering 1657
Use categories in URL filtering 1658
QUIC Fingerprinting 1659
License requirements for URL filtering 1659
Requirements and prerequisites for URL filtering 1660
Configure URL filtering with category and reputation 1660

Enable URL filtering using category and reputation 1662
URL filtering options 1662
Configure URL conditions 1663
Rules with URL conditions 1665
URL rule order 1665
DNS filtering 1665
Enable DNS filtering to identify URLs during domain lookup 1666
DNS filtering behavior for block actions 1667
DNS filtering and events 1667
Manual URL filtering 1667
Manual URL filtering options 1668
Supplement or selectively override category and reputation-based URL filtering 1668
HTTP response pages 1669
Limitations to HTTP response pages 1669
Requirements and prerequisites for HTTP response pages 1670
Choose HTTP response pages 1671
Interactive blocking with HTTP response pages 1671
Configure interactive blocking 1672
Set the user bypass timeout for a blocked website 1673
Configure URL filtering health monitors 1673
Dispute URL category and reputation 1673
Take action if the URL category set changes 1674
URL category and reputation changes 1675
Troubleshoot URL filtering 1676
History for URL filtering 1678

CHAPTER 42 **Content Restriction** 1681
About content restriction 1681
Requirements and prerequisites for content restriction 1682
Guidelines and limitations for content restriction 1683
Using access control rules to enforce content restriction 1683
Safe search options for access control rules 1684
Use a DNS sinkhole to enforce content restriction 1684

CHAPTER 43 **Intrusion Prevention Overview** 1687

Network Analysis and Intrusion Policy Basics 1687

How Policies Examine Traffic For Intrusions 1689

Decoding, Normalizing, and Preprocessing: Network Analysis Policies 1690

Access Control Rules: Intrusion Policy Selection 1691

Intrusion Inspection: Intrusion Policies, Rules, and Variable Sets 1692

Intrusion Event Generation 1693

System-Provided and Custom Network Analysis and Intrusion Policies 1694

System-Provided Network Analysis and Intrusion Policies 1694

Benefits of Custom Network Analysis and Intrusion Policies 1696

Benefits of Custom Network Analysis Policies 1696

Benefits of Custom Intrusion Policies 1697

Limitations of custom policies 1698

License Requirements for Network Analysis and Intrusion Policies 1700

Requirements and Prerequisites for Network Analysis and Intrusion Policies 1700

Guidelines and Limitations for Network Analysis and Intrusion Policies 1700

The Navigation Panel: Network Analysis and Intrusion Policies 1701

Conflicts and Changes: Network Analysis and Intrusion Policies 1702

Exiting a Network Analysis or Intrusion Policy 1704

PART IX **Decryption Policies and Encrypted Visibility for Access Control** 1705

CHAPTER 44 **Traffic Decryption Overview** 1707

Traffic decryption 1707

How TLS/SSL handshakes work 1708

ClientHello message handling 1709

How ServerHello and server certificate messages work 1712

Decryption rule and policy basics 1713

Guidelines for traffic decryption 1714

Best practice for deciding when to decrypt traffic 1714

Decrypt and re-sign (outgoing traffic) 1715

Known key decryption for incoming traffic 1716

Other decryption rule actions 1716

Decryption rule components 1716
Decryption Rule order evaluation 1717
Multi-rule example 1718
TLS crypto acceleration 1720
TLS crypto acceleration guidelines and limitations 1721
View the status of TLS crypto acceleration 1722
History for decryption policy 1723

CHAPTER 45 **Decryption Policies** 1727
About Decryption Policies 1727
Requirements and Prerequisites for Decryption Policies 1728
Create a decryption policy 1728
Create a decryption policy with outbound connection protection 1728
Create a decryption policy with inbound connection protection 1730
Configure Decryption policy exclusions 1731
Generate an internal CA for outbound protection 1735
Upload an internal CA for outbound protection 1736
Upload an internal certificate for inbound protection 1737
Create a decryption policy with other rule actions 1737
Decryption policy default actions 1739
Default handling options for undecryptable traffic 1739
Set default handling for undecryptable traffic 1741
Decryption policy advanced options 1742
TLS 1.3 decryption best practices 1743

CHAPTER 46 **Decryption Rules** 1745
Decryption Rule overview 1745
Requirements and prerequisites for Decryption Rules 1745
Decryption Rules guidelines and limitations 1746
Guidelines for using TLS/SSL decryption 1746
Decryption Rules unsupported features 1747
Guidelines for TLS/SSL Do Not Decrypt configuration 1748
TLS/SSL Decrypt - Resign guidelines 1749
TLS/SSL Decrypt - Known Key Guidelines 1751

TLS/SSL block guidelines 1752
TLS/SSL certificate pinning guidelines 1752
TLS/SSL heartbeat guidelines 1752
TLS/SSL anonymous cipher suite limitation 1753
TLS/SSL normalizer guidelines 1753
Other Decryption Rule guidelines 1753
Decryption Rule traffic handling 1754
Encrypted traffic inspection configuration 1756
Decryption Rule order evaluation 1757
Decryption Rule conditions 1758
Security zone rule conditions 1759
Security zone conditions in multidomain environments 1760
Network rule conditions 1760
VLAN tag rule conditions 1760
User rule conditions 1761
Application rule conditions 1761
Best practice: use application-based rules over port-based rules 1763
Category rule conditions 1763
Server certificate-based rule conditions 1764
Certificate rule conditions 1765
Conditions for distinguished name rules in decryption policies 1765
Trust external certificate authorities 1770
Certificate Status Decryption rule conditions 1771
Cipher suite rule conditions 1774
Encryption protocol version rule conditions 1777
Decryption Rule actions 1777
Decryption rule monitor action 1777
Decryption rule Do Not Decrypt action 1778
Decryption rule blocking actions 1779
Decryption rule decrypt actions 1779
Monitor TLS/SSL hardware acceleration 1780
Informational counters 1780
Alert counters 1781
Error counters 1781

Fatal counters 1781
Troubleshoot Decryption Rules 1782
TLS/SSL oversubscription 1782
Troubleshoot TLS/SSL oversubscription 1782
TLS heartbeat 1783
Troubleshoot TLS heartbeat 1784
TLS/SSL pinning 1784
Troubleshoot TLS/SSL pinning 1785
Troubleshoot unknown or bad certificates or certificate authorities 1787
Verify TLS/SSL cipher suites 1789
Troubleshoot using crypto archives 1790

CHAPTER 47 **Decryption rules and Policy Example** 1793
Decryption rule Examples 1793
1793
: Decrypt Specific Test Traffic 1794
Decryption rules: Block or Monitor Certificates and Protocol Versions 1794
Example: Decryption rule to Monitor or Block Certificate Status 1794
Example: Decryption rule to Monitor or Block Protocol Versions 1795
Optional Example: Manual Decryption rule to Monitor or Block Certificate Distinguished Name 1797
Associate the Decryption policy with an Access Control Policy and Advanced Settings 1798
Traffic to Prefilter 1800
Decryption rule Settings 1801

CHAPTER 48 **Encrypted Visibility Engine** 1803
Encrypted Visibility Engine 1803
How EVE works 1804
Indications of compromise events 1805
QUIC fingerprinting in EVE 1806
Configure EVE 1806
View Encrypted Visibility Engine events 1807
View EVE dashboard 1808
Configure EVE Exception Rules 1809
Add exception rule from unified events 1810

Use case - Block Traffic Based on the EVE Threat Confidence Score 1810
About Encrypted Visibility Engine 1810
Benefits 1811
Sample Business Scenario 1811
Prerequisites 1811
High-Level Workflow 1811
Configure Block Thresholds in EVE 1811
View EVE Events 1815
Additional References 1816

PART X **Identity Policies for Access Control** 1817

CHAPTER 49 **Identity Overview** 1819
User identity 1819
Identity terminology 1819
About user identity sources 1820
Best practices for user identity 1822
Identity deployments 1824
Set up an identity policy 1825
User activity database 1828
Users database 1828
Host and user limits 1830
Host limits 1830
User limits for microsoft active directory 1831
Recommendation: identity realm limit 1833
User limits for microsoft azure active directory realms 1833

CHAPTER 50 **Realms** 1835
Realms and realm sequences 1835
Realms and trusted domains 1837
Supported servers for realms 1841
Supported server object class and attribute names 1842
License requirements for realms 1843
Requirements and prerequisites for realms 1843

Prerequisites for kerberos authentication 1843
Realm fields 1844
Realm directory and synchronize fields 1848
Create a Microsoft Azure AD Realm 1850
How Entra ID and Cisco ISE authentication with resource owned password credentials works 1851
How Entra ID and Cisco ISE authentication works with TEAP/EAP-TLS 1852
Create a Microsoft Azure AD realm 1853
Configure Microsoft Entra ID 1854
Configure Cisco ISE for Microsoft Azure AD 1855
Get required information For Your Microsoft Azure AD realm 1855
Create an Azure AD realm 1858
Azure AD user session timeout 1860
Create an LDAP realm or an Active Directory realm and realm directory 1860
Configure the Realm 1862
Connect securely to Active Directory or LDAP 1862
Find the active directory server's name 1863
Export the active directory server's root certificate 1863
Synchronize users and groups 1865
Create a realm sequence 1867
Cross-domain trust setups with Firewall Management Center 1868
Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories 1869
Configure the Secure Firewall Management Center for cross-domain trust Step 2: Synchronize users and groups 1874
Configure the Secure Firewall Management Center for cross-domain trust step 3: Resolve issues 1875
Manage a realm 1876
Compare realms 1877
Troubleshoot realms and user downloads 1877
Detect realm or user mismatches 1881
Troubleshoot cross-domain trust 1882
History for realms 1885

CHAPTER 51 **Identity Source: Captive Portal** 1887
Captive portal identity source 1887

Hostname redirect 1888
License requirements for captive portal 1888
Requirements and prerequisites for captive portal 1888
Best practices for captive portal guidelines and limitations 1889
Configure the captive portal for user control 1891
Create a network object 1892
Create an identity policy and active authentication rule 1894
Update a custom authentication form 1896
Create a TCP port access control rule 1896
Create a user access control rule 1898
Create a decryption policy with an outbound rule 1899
Create A decryption policy with a Decrypt-Resign rule 1901
Associate Identity and decryption policies with the access control policy 1903
Captive portal fields 1903
Exclude applications from captive portal 1905
Troubleshoot the captive portal identity source 1906
History for captive portal 1907

CHAPTER 52 **Identity Source: ISE/ISE-PIC** 1911
The ISE/ISE-PIC identity source 1911
Source and destination security group tag (SGT) matching 1912
License requirements for ISE/ISE-PIC 1913
Requirements and prerequisites for ISE/ISE-PIC 1913
Best practices for ISE/ISE-PIC integration 1914
ISE/ISE-PIC configurations for user control 1916
Configure ISE/ISE-PIC without a realm 1916
Configure ISE/ISE-PIC for user control using a realm 1917
ISE/ISE-PIC configuration 1919
Configure security groups and SXP publishing in ISE 1919
Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center 1921
Export a system certificate 1922
Generate a self-signed certificate 1923
Import ISE/ISE-PIC certificates 1924
Configure ISE for user control 1924

ISE/ISE-PIC configuration fields 1926
Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues 1927
History for ISE/ISE-PIC 1929

CHAPTER 53 **Identity Source: Remote Access VPN** 1931
Remote access VPN identity sources 1931
Configure Remote Access VPN for AD-authenticated users 1932
Hybrid Entra ID and on-premises AD deployments 1933
Troubleshooting guidelines for remote access VPN identity source 1934
Not Observing Correct Settings for VPN Statistics 1934
History for RA VPN 1935

CHAPTER 54 **Identity source: TS agent** 1937
Terminal services agent identity source 1937
Best practices for TS agent configuration 1938
Identity source: TS agent 1938
Troubleshoot the TS agent identity source 1938
History for TS agent 1939

CHAPTER 55 **Identity Policies** 1941
Identity policies 1941
License requirements for identity policies 1942
Requirements and prerequisites for identity policies 1942
Create an identity policy 1943
Create an identity mapping filter 1944
Identity rule conditions 1945
Security zone rule conditions 1945
Security zone conditions in multidomain environments 1946
Network rule conditions 1946
Redirect to host name network rule conditions 1946
VLAN tag rule conditions 1947
Best practice: use application-based rules over port-based rules 1948
Port, protocol, and ICMP code rule conditions (concept) 1948
Realm & settings rule conditions 1949

Create an identity rule 1952
Identity rule fields 1953
Sample identity policies and rules 1954
Create an identity policy with a passive authentication rule 1955
Create a sample identity policy with an active authentication rule 1956
Active authentication using a realm 1958
Active authentication using a realm sequence 1959
Manage an identity policy 1961
Manage an identity rule 1961
Troubleshoot user control 1962

PART XI **Advanced Policies and Settings for Access Control** 1965

CHAPTER 56 **Prefilter Policies** 1967
Prefilter policies 1967
Default prefilter policy 1968
Prefilter policy rule order 1968
Tunnel vs prefilter rules 1969
How the system processes plain-text tunnels 1969
Using tunnel zones to apply access control at the tunnel level 1970
Large flow offloads 1971
Restrictions for flow offload implementation 1973
Prefilter vs access control policy 1974
Requirements and prerequisites for prefilter policies 1976
Guidelines and limitations for the prefilter policy 1976
Guidelines and limitations for encapsulated traffic handling 1977
Best practices for fastpath prefiltering 1978
Configure prefilter policies 1979
Configuring the default action 1981
Configure prefilter rules 1981
VLAN tags rule conditions 1983
Port rule conditions for prefilter rules 1983
Configure tunnel rules 1984
Creating tunnel zones 1986

Move prefilter rules to an access control policy 1987
Examples of prefilter policy 1988
Rezone tunnels for customized inspection 1988
Offload large flows 1991
History for the prefilter policy 1992

CHAPTER 57 **DNS Policies for Security Intelligence** 1993
DNS policies 1993
Cisco umbrella DNS policies 1994
DNS policy components 1995
License requirements for DNS policies 1996
Requirements and prerequisites for DNS policies 1996
Managing DNS and Umbrella DNS Policies 1996
Create basic DNS policies 1997
Edit DNS policies 1998
DNS rules 1998
Create and edit DNS rules 1999
DNS rule management 2000
Enable and disable DNS rules 2000
DNS rule order evaluation 2001
DNS rule actions 2001
DNS rule conditions 2002
Security zone rule conditions 2003
Network rule conditions 2003
VLAN tag rule conditions 2004
DNS policy rule conditions 2004
DNS rules 2005
Control traffic based on DNS and security zone 2005
Control traffic based on DNS and network 2006
Control traffic based on DNS and VLAN 2006
Control traffic based on DNS list or feed 2007
Requirement: deploy DNS policy configuration changes 2008
Cisco umbrella DNS policies 2008
Redirect DNS requests to Cisco umbrella 2009

Prerequisites for configure the umbrella DNS connector 2010
Configure Cisco umbrella connection settings 2011
Create an umbrella DNS policy 2012
Edit Umbrella DNS policies and rules 2012
Associate the umbrella DNS policy with an access control policy 2013

CHAPTER 58 **File Policies for Network Malware Protection** 2015
Network malware protection and file policies 2015
File policies 2015
Prerequisites for file policies 2016
License requirements for file and malware policies 2017
Best practices for file policies and malware detection 2017
File rule best practices 2017
File detection best practices 2018
File blocking best practices 2019
File policy best practices 2020
Configure malware protection 2021
Plan and prepare for malware protection 2022
Configure file policies 2023
Add file policies to your access control configuration 2023
Configure an access control rule to perform malware protection 2024
Verify and monitor malware protection 2025
Cloud connections for malware protection 2026
AMP cloud connection configurations 2027
Prerequisites and best practices for AMP cloud connections 2027
Choose an AMP cloud 2028
Cisco AMP private cloud 2028
Manage connections to the AMP cloud (public or private) 2030
Change AMP options 2031
Dynamic analysis connections 2031
Prerequisites for dynamic analysis 2031
View the default dynamic analysis connection 2032
Dynamic analysis on-premises appliance (Cisco Secure Malware Analytics) 2032
Enable access to dynamic analysis results in the public cloud 2034

Maintain your system: file types eligible for dynamic analysis 2034
File policies and file rules 2035
Create or edit a file policy 2035
Advanced and archive file inspection options 2036
Manage file policies 2039
File rules 2040
File rule components 2041
File rule actions 2042
Create file rules 2050
Access control rule logging for malware protection 2051
Retrospective disposition changes 2051
File and malware inspection performance and storage options 2052
Tune file and malware inspection performance and storage 2053
(Optional) Malware protection with Secure Endpoint 2054
Comparison of malware protection: Firepower vs. Secure Endpoint 2054
Integrate Secure Firewall with Secure Endpoint 2055
Benefits of integrating Firepower and Secure Endpoint 2055
Secure Endpoint and AMP private cloud 2056
Integrate Firepower and Secure Endpoint 2056
History for network malware protection and file policies 2058

CHAPTER 59 **Dynamic Attributes Connector** 2061
About the dynamic attributes connector 2061
How Cisco secure dynamic attributes connector works 2061
System requirements for the dynamic attributes connector 2063
Enable the dynamic attributes connector 2063
Configure networks and subnets for Docker containers 2064
Dashboard 2065
Dashboard of an unconfigured system 2066
Dashboard of a configured system 2067
Add, edit, or delete connectors 2069
Add, edit, or delete dynamic attributes filters 2070
Connectors 2072
Amazon Web Services connector user permissions and imported data 2072

Create an AWS user with minimal permissions for the dynamic attributes connector 2073
Create an AWS connector 2074
Azure connector—About user permissions and imported data 2075
Create an Azure user with minimal permissions for the dynamic attributes connector 2076
Create an Azure connector 2078
Create an Azure service tags connector 2079
Create a generic text connector 2080
Create a GitHub connector 2082
Google cloud connector user permissions and imported data 2082
Create a Google Cloud user with minimal permissions for the dynamic attributes connector 2083
Create a google cloud connector 2084
Create an office 365 connector 2085
vCenter connector—About user permissions and imported data 2086
Create a vCenter user with minimal permissions for the dynamic attributes connector 2086
Create a vCenter connector 2088
Create a Webex connector 2090
Create a Zoom connector 2091
Create dynamic attributes filters 2092
Dynamic attribute filter examples 2093
Manually get a certificate authority (CA) chain 2094
Dynamic objects in access control rules 2097
Create dynamic attributes filters 2098
Dynamic attributes rule conditions 2099
Create access control rules using dynamic attributes filters 2100
Dynamic Firewall 2101
Dynamic Firewall 2102
How to configure the dynamic firewall 2102
Enable the dynamic attributes connector 2104
Get required information for Identity Intelligence 2105
Create an identity source and realm for the dynamic firewall 2106
Create a dynamic firewall instance 2107
Associate an identity source with Identity Intelligence 2108
Configure Identity Intelligence 2109
View system-defined filters 2110

View system-defined access control rules 2111
Edit the user exclusion list 2113
View and edit the system-created access control policy 2114
Create dynamic attributes filters 2115
Disable the dynamic attributes connector 2116
Troubleshoot the Dynamic Attributes Connector 2117
Troubleshoot using the Secure Firewall Management Center 2117
Recommendation: security requirements for network deployment 2117
Internet access requirements 2117
History for the dynamic attributes connector 2119

CHAPTER 60 **Threat Intelligence Director** 2121
Secure Firewall Threat Intelligence Director 2121
Threat Intelligence Director and Security Intelligence 2123
Performance impact of Threat Intelligence Director 2123
Requirements and prerequisites for threat intelligence director 2124
Platform, element, and license requirements 2124
Source requirements 2125
Source content limitations 2126
Set up Threat Intelligence Director 2126
Configure policies to support Threat Intelligence Director 2127
Options for ingesting data sources 2128
Fetch TAXII feeds to use as sources 2129
Fetch sources from a URL 2130
Upload a local file to use as a source 2132
Handling of duplicate indicators 2133
Configure TLS/SSL settings for a Threat Intelligence Director source 2133
User roles with Threat Intelligence Director access 2135
About backing up and restoring Threat Intelligence Director data 2135
Analyze Threat Intelligence Director incident and observation data 2136
Observation and incident generation 2136
View and manage incidents 2138
Incident summary information 2139
Incident details 2139

View events for a Threat Intelligence Director observation 2143
Threat Intelligence Director observations in Secure Firewall Management Center events 2144
Factors that affect the action taken 2144
Threat Intelligence Director - Firewall Management Center action prioritization 2145
View and change Threat Intelligence Director configurations 2148
View Threat Intelligence Director status of elements (managed devices) 2149
View and manage sources 2149
Source summary information 2150
Source status details 2151
View and manage indicators 2152
Indicator summary information 2153
Indicator details 2154
View and manage observables 2155
Observable summary information 2156
Filter Threat Intelligence Director data in table views 2156
Inheritance in Threat Intelligence Director configurations 2157
Inheritance of TID settings from multiple parents 2158
Overriding inherited TID settings 2158
Edit Threat Intelligence Director actions at the source, indicator, or observable Level 2159
Pausing publishing 2160
Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements 2161
Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level 2161
Modify the observable publication frequency 2162
Adding Threat Intelligence Director observables to the Do Not Block list 2163
Add Threat Intelligence Director observables to a Do Not Block list 2164
View a STIX source file 2164
Troubleshoot Threat Intelligence Director 2164
History for Threat Intelligence Director 2166

CHAPTER 61 **Advanced Settings for Access Control** 2169
Requirements and prerequisites for advanced settings 2169
Configure advanced settings for the access control policy 2170
General settings 2172
TLS server identity discovery 2173

Intelligent application bypass 2175
Configure intelligent application bypass 2176
IAB logging and analysis 2178
Transport/network layer preprocessor settings 2181
Detection enhancement settings 2182
Adaptive profile updates 2183
Adaptive profile updates and recommended rules 2184
Performance settings 2184
Latency-based performance settings 2186
History for advanced settings for the access control policy 2187

CHAPTER 62 **Service Policies** 2191
Threat defense service policies 2191
Service policy relationships with FlexConfig and other features 2192
Connection settings 2192
Requirements and prerequisites for service policies 2193
Guidelines and limitations for service policies 2193
Configure threat defense service policies 2194
Configure a service policy rule 2195
Bypass TCP state checks for asymmetrical routing (TCP state bypass) 2198
The asymmetrical routing problem 2198
Guidelines and limitations for TCP state bypass 2199
Configure TCP state bypass 2200
Disable TCP sequence randomization 2202
Monitor service policies 2203
Examples for service policy rules 2204
Protect servers from a SYN flood DoS attack (TCP intercept) 2204
Configure the Firewall Threat Defense device to appear on traceroutes 2207
History for threat defense service policy 2208

CHAPTER 63 **Threat Detection** 2211
Portscan detection and prevention 2211
Pre-defined sensitivity levels for portscan detection 2211
Detection in the low sensitivity level 2213

Requirements and prerequisites for threat detection 2213
Limitations for threat detection configuration 2214
Best practices for portscan prevention 2214
Configure portscan detection and prevention 2215
Monitoring threat detection 2217
View portscan alerts 2217
Monitor portscan on the firewall 2218
Unblocking a host 2219
History for threat detection 2219

CHAPTER 64 **Elephant Flow Detection** 2221
Elephant flow detection and remediation 2221
Elephant flow upgrade from Intelligent Application Bypass 2222
Configure elephant flow detection 2222
Use case - Configure Elephant Flow Detection Outcomes 2225
Elephant flows 2225
Benefits of elephant flow detection and remediation 2225
How elephant flows work 2225
Sample business scenarios 2226
Prerequisites 2227
Configure elephant flow parameters 2227
View events for elephant flows 2229
Configure elephant flow remediation exemption 2231
View events for elephant flow remediation exemption 2234
Additional references 2234

PART XII **Network Discovery** 2235

CHAPTER 65 **Network discovery overview** 2237
Detection of host, application, and user data 2237
Host and application detection fundamentals 2238
Passive detection of operating system and host data 2238
Active detection of operating system and host data 2239
Current identities for applications and operating systems 2239

Current user identities 2241
Application and operating system identity conflicts 2241
NetFlow data 2242
Requirements for using NetFlow data (principle) 2243
Differences between NetFlow and managed device data 2244

CHAPTER 66 **Host identity sources** 2247
Host data collection overview 2247
Requirements and prerequisites for host identity sources 2248
Determine which host operating systems the system can detect 2248
Identifying host operating systems 2249
Custom fingerprinting 2249
Manage fingerprints 2250
Activate and deactivate fingerprints 2250
Edit an active fingerprint 2251
Edit an inactive fingerprint 2252
Create a custom fingerprint for clients 2252
Create a custom fingerprint for servers 2254
Host input data 2257
Requirements for using third-party data 2257
Third-party product mappings 2258
Map third-party products 2258
Map third-party product fixes 2259
Map third-party vulnerabilities 2260
Custom product mappings 2261
Create custom product mappings 2261
Edit custom product mapping lists 2263
Activate and deactivate custom product mappings 2263
Configure the host input client 2263
Nmap scanning 2264
Nmap remediation options 2265
Nmap scanning guidelines 2269
Example: Use Nmap to resolve unknown operating systems 2270
Example: Using Nmap to respond to new hosts 2271

Manage Nmap scanning 2272
Add an Nmap scan instance 2273
Edit an Nmap scan instance 2274
Add an Nmap scan target 2275
Edit an Nmap scan target 2276
Create an Nmap remediation 2276
Edit an Nmap remediation 2278
Run an on-demand Nmap scan 2279
Nmap scan results 2280
View Nmap scan results 2280
Nmap scan results fields 2281
Import Nmap scan results 2282
History for host identity sources 2282

CHAPTER 67 **Application detection** 2283
Application detection 2283
Application detectors 2284
Identification of application protocols in the web interface 2285
Implied application protocol detection from client detection 2286
Host limits and discovery event logging 2287
Special considerations for application detection 2287
Disable application detection in Snort 3 2288
Requirements and prerequisites for application detection 2289
Custom application detectors 2289
Custom application detector and user-defined application fields 2290
Configure custom application detectors 2293
Create a user-defined application 2294
Specifying detection patterns in basic detectors 2295
Specify detection criteria in advanced detectors 2296
Specifying EVE process assignments 2297
Testing a custom application protocol detector 2298
View or download detector details 2298
Sort the detector list 2299
Filter the detector list 2299

Filter groups for the detector list 2300
Navigate to other detector pages 2301
Activate and deactivate detectors 2301
Edit custom application detectors 2302
Deleting detectors 2303

CHAPTER 68 **Network Discovery Policies** 2305
Network discovery policies overview 2305
Requirements and prerequisites for network discovery policies 2306
Network discovery customization 2306
Configure the network discovery policy 2307
Network discovery rules 2307
Configure network discovery rules 2308
Actions and discovered assets 2309
Monitored networks 2309
Port exclusions 2311
Zones in network discovery rules 2313
Traffic-based detection identity sources 2314
Configure advanced network discovery options 2316
Network discovery general settings 2317
Configuring network discovery general settings 2318
Network discovery identity conflict settings 2318
Configure network discovery identity conflict resolution 2319
Network discovery vulnerability impact assessment options 2319
Enable network discovery vulnerability impact assessment 2320
Indications of compromise 2320
Enable indications of compromise rules 2321
Add NetFlow exporters to a network discovery policy 2321
Network discovery data storage settings 2322
Configure network discovery data storage 2323
Configure network discovery event logging 2324
Add network discovery OS and server identity sources 2324
Troubleshoot your network discovery strategy 2325

PART XIII **Objects and Certificates** 2329

CHAPTER 69 **Object Management** 2331

Objects 2332

Use the object manager 2334

Import objects 2334

Edit objects 2337

View objects and their usage 2338

Filter objects or object groups 2339

Object groups 2340

Group reusable objects 2340

Object overrides 2342

Manage object overrides 2343

Allow object overrides 2344

Add object overrides 2344

Edit an object override 2345

AAA servers 2345

Add a RADIUS server group 2346

RADIUS server group configuration options 2346

Configure RADIUS server options 2347

Add a single sign-on server 2349

Access lists 2351

Configure an extended ACL object 2351

Configure a standard ACL object 2355

Configure address pools 2356

Create an application filter 2357

Configure an AS PATH object 2357

Configure a BFD template 2358

Cipher suite lists 2359

Create a cipher suite list 2360

Configure a community list 2360

Configure an extended community list 2361

DHCP IPv6 pools 2363

Distinguished names 2364
Create a distinguished name object 2366
DNS server groups 2366
Create a DNS server group object 2366
External attributes 2367
Dynamic objects 2367
Create dynamic objects for the first time 2368
Create dynamic objects with embedded Dynamic Attributes Connector 2370
Dynamic objects with Security Cloud Control 2371
Create dynamic objects with on-premises Dynamic Attributes Connector 2372
Dynamic objects page features 2374
Dynamic object mappings 2374
API-created dynamic objects 2375
Add or edit an API-created dynamic object 2375
Security group tags 2376
Create a security group tag object 2376
File lists 2377
Source files for file lists 2377
Add individual SHA-256 values to file lists 2378
Upload an individual file to a file list 2379
Upload source files to file lists 2380
Edit SHA-256 values in file lists 2381
Download source files from a file list 2381
FlexConfig objects 2382
Geolocation objects 2382
Create a geolocation object 2383
Interfaces 2383
Key chains 2384
Create a key chain object 2385
Networks 2386
Network wildcard masks 2387
Create a network object 2388
Import network objects 2389
PKI objects 2389

Internal certificate authority objects 2390
CA certificates and private key import 2391
Import a CA certificate and private key 2391
Generate a new CA certificate and private key 2392
Signed certificates 2392
Create an unsigned CA certificate and CSR 2393
Upload a signed certificate issued in response to a CSR 2394
CA certificates and private key downloads 2394
Download a CA certificate and private key 2395
Trusted certificate authority objects 2395
Trusted CA objects 2396
Add a trusted CA object 2396
Certificate revocation lists in trusted CA objects 2397
Add a certificate revocation list to a trusted CA object 2397
External certificate objects 2398
Add external certificate objects 2399
Internal certificate objects 2399
Add internal certificate objects 2400
Certificate enrollment objects 2400
Add certificate enrollment objects 2402
Add a certificate enrollment 2403
EST enrollment configuration options in Certificate Enrollment Object 2404
Certificate Enrollment Object SCEP options 2405
Certificate Enrollment Object certificate parameters in certificate requests 2406
Certificate Enrollment Object key options 2407
Enroll PKI certificates with weak-crypto 2408
Certificate Enrollment Object revocation options 2408
Configure a policy list 2409
Ports 2411
Create port objects 2412
Import port objects 2413
Prefix lists 2413
Configure an IPv6 prefix list 2413
Configure an IPv4 prefix list 2414

Configure a route map 2415
Security intelligence 2418
Modify security intelligence objects 2420
Global and domain security intelligence lists 2420
Security intelligence lists and multitenancy 2421
Add entries to global security intelligence lists 2422
Delete entries from global security intelligence lists 2423
List and feed updates for security intelligence feeds 2424
Change the update frequency for security intelligence feeds 2424
Custom security intelligence lists and feeds 2425
List custom lists and feeds requirements 2425
List URL syntax and matching criteria for URL lists and feeds 2426
Custom security intelligence feeds 2428
Create custom security intelligence feeds 2428
Update custom security intelligence feeds manually 2429
Custom Security Intelligence lists 2430
Upload new custom security intelligence lists to the Secure Firewall Management Center 2431
Update custom security intelligence lists 2431
Sinkhole objects 2432
Create a sinkhole object 2432
Configure an SLA monitor 2433
Time ranges 2435
Create a time range object 2435
Time zones 2436
Tunnel zones 2437
URLs 2437
Create a URL object 2438
Variable sets 2439
Variable sets in intrusion policies 2440
Variables 2440
List predefined default variables 2441
Network variables 2443
Port variables 2444
Advanced variables 2445

Variable resets 2446
Variable sets 2447
Examples: Adding user-defined variables to default sets 2447
Examples: User-defined variables in custom sets 2448
Nesting variables 2450
Manage variable sets 2451
Create a variable set 2452
Manage variables 2452
Add variables 2454
Edit variables values in a variable set 2455
VLAN tags 2456
Create a VLAN tag object 2456
VPN 2456
Certificate map objects 2457
Secure Client custom attributes objects 2458
Configure custom attributes for Secure Client 2458
Add custom attributes to your group policy 2460
Firewall Threat Defense group policy objects 2460
Configure a group policy object 2461
Group policy general options 2462
Group policy options for Secure Client 2464
Advanced group policy option fields and values 2467
Firewall Threat Defense IPsec proposals 2468
Configure an IKEv1 IPsec proposal object 2469
Configure an IKEv2 IPsec proposal object 2470
IKE policies 2470
Configure an IKEv1 policy object 2471
Configure an IKEv2 policy object 2472
Secure client customizations 2474
File objects 2474
History for object management 2477

CHAPTER 70 Certificates 2481
Requirements and prerequisites for certificates 2481

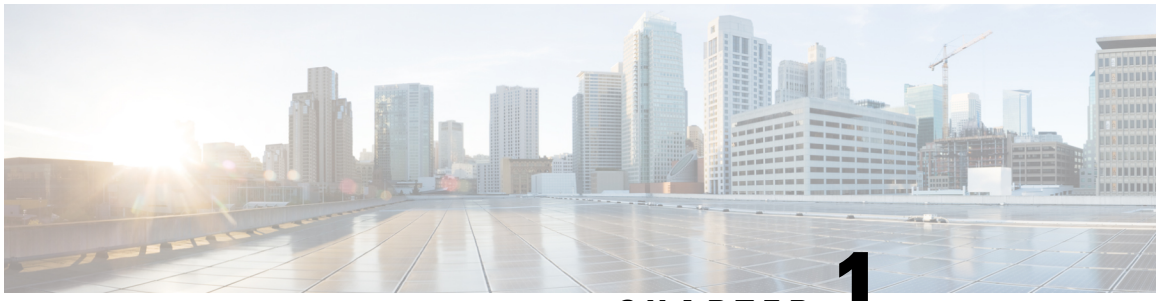
Secure Firewall Threat Defense VPN certificate guidelines and limitations 2481
Manage Firewall Threat Defense certificates 2483
Automatically update CA bundles 2484
Install a certificate using self-signed enrollment 2486
Install a certificate using EST enrollment 2487
Install a certificate using SCEP enrollment 2487
Install a certificate using manual enrollment 2488
Install a certificate using a PKCS12 file 2489
Troubleshoot Threat Defense certificates 2490
History for certificates 2491



PART I

Getting Started with Device Configuration

- Device Registration, on page 1
- Transparent or Routed Firewall Mode, on page 71
- CLI Users, on page 85
- Change Management, on page 107
- Configuration Deployment, on page 121



CHAPTER 1

Device Registration

You can add and manage devices in the Secure Firewall Management Center.

- About device registration, on page 1
- Prerequisites for device registration, on page 12
- Log into the Command-Line Interface on the device, on page 13
- Complete the Firewall Threat Defense initial configuration for manual registration, on page 15
- Device registration management, on page 30
- Switch managers, on page 61
- History for device registration, on page 67

About device registration

Register your devices to the Firewall Management Center.

Firewall management center overview

The Firewall Management Center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use the Firewall Management Center if you want a multi-device manager, and you require all features on the Firewall Threat Defense. The Firewall Management Center also provides powerful analysis and monitoring of traffic and events.

This guide applies to an *on-premises* Firewall Management Center, either as your primary manager or as an analytics-only manager. When using the Security Cloud Control Cloud-Delivered Firewall Management Center as your primary manager, you can use an on-prem Firewall Management Center for analytics. Do not use this guide for the Cloud-Delivered Firewall Management Center; see *Cisco Security Cloud Control: Secure Firewall Threat Defense Management*.

Note If you have a Security Cloud Control-managed device and are using the on-prem Firewall Management Center for analytics only, then the on-prem Firewall Management Center does not support policy configuration or upgrading. Some chapters and procedures in this guide related might not apply to devices whose primary manager is Security Cloud Control.

For the Firewall Management Center used as the primary manager: The Firewall Management Center is not compatible with other managers because the Firewall Management Center owns the Firewall Threat Defense

configuration, and you are not allowed to configure the Firewall Threat Defense directly, bypassing the Firewall Management Center.

Firewall Management Center and device management

When the Firewall Management Center manages a device, it sets up a two-way, SSL-encrypted communication channel between itself and the device. The Firewall Management Center uses this channel to send information to the device about how you want to analyze and manage your network traffic to the device. As the device evaluates the traffic, it generates events and sends them to the Firewall Management Center using the same channel.

By using the Firewall Management Center to manage devices, you can:

- configure policies for all your devices from a single location, making it easier to change configurations
- install various types of software updates on devices
- push health policies to your managed devices and monitor their health status from the Firewall Management Center

Note If you have a Security Cloud Control-managed device and are using the on-prem Firewall Management Center for analytics only, then the on-prem Firewall Management Center does not support policy configuration or upgrading. Chapters and procedures in this guide related to device configuration and other unsupported features do not apply to devices whose primary manager is Security Cloud Control.

The Firewall Management Center aggregates and correlates intrusion events, network discovery information, and device performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess the overall activity occurring on your network.

You can use the Firewall Management Center to manage nearly every aspect of a device's behavior.

Note Although the Firewall Management Center can manage devices running certain previous releases as specified in the compatibility matrix available at http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html, new features that require the latest version of Firewall Threat Defense software are not available to these previous-release devices. Some Firewall Management Center features may be available for earlier versions.

Devices managed by a Secure Firewall Management Center

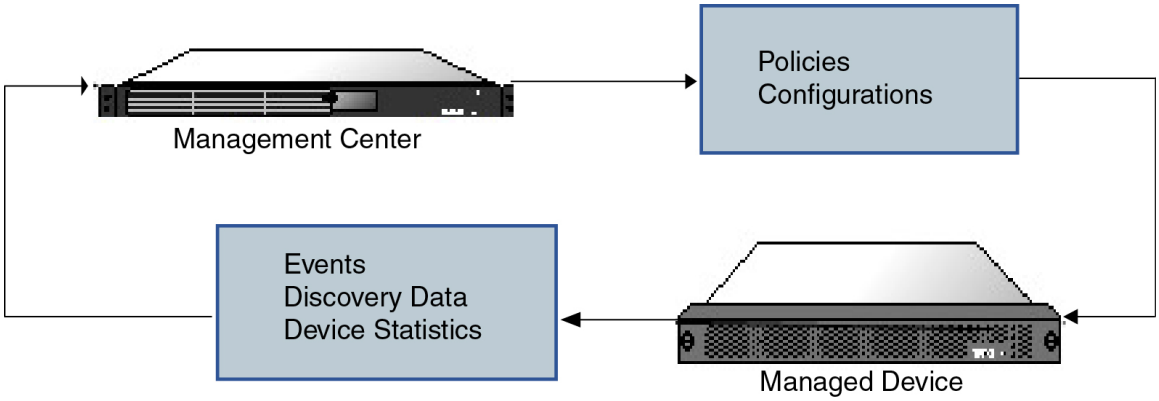
You can use the Secure Firewall Management Center as a central management point to manage Firewall Threat Defense devices.

Communication channel security

When you manage a device, information is transmitted between the Firewall Management Center and the device over a secure, TLS-1.3-encrypted communication channel. You do not need to run this traffic over an

additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

This illustration lists what is transmitted between the Firewall Management Center and its managed devices. Note that the types of events and policies that are sent between the appliances are based on the device type.



Management connection

After you configure the device with the Firewall Management Center information and after you add the device to the Firewall Management Center, either the device or the Firewall Management Center can establish the management connection. Depending on initial setup:

- Either the device or the Firewall Management Center can initiate.
- Only the device can initiate.
- Only the Firewall Management Center can initiate.

Connection initiation behavior

Initiation always originates with eth0 on the Firewall Management Center or with the lowest-numbered management interface on the device. Additional management interfaces are tried if the connection is not established. Multiple management interfaces on the Firewall Management Center let you connect to discrete networks or to segregate management and event traffic. However, the initiator does not choose the best interface based on the routing table.

Make sure the management connection is stable, without excessive packet loss, with at least 5 Mbps throughput. By default, the management connection uses TCP port 8305 (this port is configurable). If you place another Firewall Threat Defense between devices and the Firewall Management Center, to prevent potential management disruption, be sure to exempt management traffic from deep inspection by applying a prefilter policy for it.

Note The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

Beyond policies and events

In addition to deploying policies to devices and receiving events from them, you can also perform other device-related tasks on the Firewall Management Center.

Device management tasks

These tasks provide essential functions for maintaining and updating your managed devices:

- **Backing up a device**:

  You cannot back up a physical managed device from its CLI. To back up configuration data, and, optionally, unified files, use the Firewall Management Center that manages the device.

  To back up event data, perform a backup of the Firewall Management Center that is managing the device.

- **Updating devices**:

  Cisco periodically releases updates to the Firepower System, including:

  - intrusion rule updates, which may contain new and updated intrusion rules
  - vulnerability database (VDB) updates
  - geolocation updates
  - software patches and updates

  You can use the Firewall Management Center to install updates on the managed devices.

Device management interfaces

A device management interface is a network connection that

- enables communication with the Firewall Management Center,
- supports initial device setup through the management interface or console port, and
- facilitates communication with the Smart Licensing server, update downloads, and other management functions.

Interface configuration options

Each device includes a single dedicated Management interface for management communication. You can optionally configure the device to use a data interface for management instead of the dedicated Management interface.

Management and event interfaces on the Firewall Threat Defense

Management and event interfaces on the Firewall Threat Defense are network connections that

- handle initial device registration and ongoing management communications between the Firewall Management Center and managed device
- transmit event data from the managed device to the Firewall Management Center, and

- can be configured as separate interfaces to isolate management and event traffic for enhanced performance and security.

Connection establishment behavior

When you set up your device, you specify the Firewall Management Center IP address or hostname that you want to connect to, if known. In this case, the device initiates the connection, and both management and event traffic go to this address at initial registration. If the Firewall Management Center is not known, then the Firewall Management Center establishes the initial connection. In this case, it might initially connect from a different Firewall Management Center management interface than specified on the Firewall Threat Defense. Subsequent connections should use the Firewall Management Center management interface with the specified IP address.

Separate event-only interface configuration requirements:

- Always enable an event interface on the Firewall Management Center before configuring a separate event-only interface on the managed device. If the Firewall Management Center has a separate event-only interface, the managed device sends subsequent event traffic to the Firewall Management Center event-only interface if the network allows. In addition, some managed-device models include an additional management interface that you can configure for event-only traffic.
- If the event network goes down, then event traffic reverts to the regular management interfaces on the Firewall Management Center and/or on the managed device. If the device management interface is down, the eventing interface will be used to establish the management connection, even if you disable management traffic for it.
- Ensure that the Firewall Management Center and managed devices have consistent configurations regarding management and event interfaces to avoid communication issues.

Using the Firewall Threat Defense data interface for management

Using the Firewall Threat Defense data interface for management is a configuration option that

- allows communication with the Firewall Management Center through a regular data interface instead of the dedicated Management interface
- enables remote management from the outside interface when a separate management network is not available, and
- provides redundant secondary interface configuration to take over management functions if the primary interface goes down.

Manager access requirements

Manager access from a data interface has the requirements listed in this table.

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel, nor can you create a subinterface on the manager access interface. You can also use the Firewall Management Center to enable manager access on a single secondary interface for redundancy.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.

- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the Firewall Threat Defense and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the Firewall Management Center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command. For Firewall Threat Defense Virtual on Amazon Web Services, a console port is not available, so you should maintain your SSH access to the Management interface: add a static route for Management before you continue with your configuration. Alternatively, be sure to finish all CLI configuration (including the **configure manager add** command) before you configure the data interface for manager access and you are disconnected.
- You cannot use separate management and event-only interfaces.
- Clustering is not supported. You must use the Management interface in this case.

When using a data interface with device high availability, see the requirements that are listed in this table.

- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and zero-touch provisioning.

Note If you use zero-touch provisioning to register the device, when you use the outside interface for manager access, it uses DHCP by default. Before you can enable high availability, you need to change the IP address to a static address. See Change the device IP address, on page 763. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

- Have different static IP addresses in the same subnet.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

Management interface support per device model

This reference provides information about management interface support across different device models. See the hardware installation guide for your model for the management interface locations.

Note For the Firepower 4100/9300, the MGMT interface is for *chassis* management, not for Firewall Threat Defense logical device management. You must configure a separate interface to be of type MGMT (and/or firepower-eventing), and then assign it to the Firewall Threat Defense logical device.

For devices with Management and Eventing interfaces, if one interface is down, the other interface will be used as backup for management or eventing even if you disable that function for the interface.

Table 1: Management interface support on managed devices

Model	Management Interface	Optional Event Interface
Firepower 1000	management0 **Note** management0 is the internal name of the Management 1/1 interface.	No Support
Firepower 2100	management0 **Note** management0 is the internal name of the Management 1/1 interface.	No Support
Secure Firewall 3100	management0 **Note** management0 is the internal name of the Management 1/1 interface.	No Support
Secure Firewall 4200	management0 **Note** management0 is the internal name of the Management 1/1 interface.	management1 **Note** management1 is the internal name of the Management 1/2 interface.
Firepower 4100 and 9300	management0 **Note** management0 is the internal name of this interface, regardless of the physical interface ID.	management1 **Note** management1 is the internal name of this interface, regardless of the physical interface ID.
ISA 3000	br1 **Note** br1 is the internal name of the Management 1/1 interface.	No support
Secure Firewall Threat Defense Virtual	eth0	No support

Network routes on device management interfaces

Management interfaces (including event-only interfaces) support only static routes to reach remote networks. When you set up your managed device, the setup process creates a default route to the gateway IP address that you specify. You cannot delete this route; you can only modify the gateway address.

Note The routing for management interfaces is completely separate from routing that you configure for data interfaces. If you configure a data interface for management instead of using the dedicated Management interface, traffic is routed over the backplane to use the data routing table. The information in this section does not apply.

You can configure multiple management interfaces on some platforms (a management interface and an event-only interface). The default route does not include an egress interface, so the interface chosen depends on the gateway address you specify, and which interface's network the gateway belongs to. In the case of multiple interfaces on the default network, the device uses the lower-numbered interface as the egress interface.

At least one static route is recommended per management interface to access remote networks. We recommend placing each interface on a separate network to avoid potential routing problems, including routing problems from other devices to the Firewall Threat Defense.

Note The interface used for management connections is not determined by the routing table. Connections are always tried using the lowest-numbered interface first.

NAT environments

Network address translation (NAT) is a method of transmitting and receiving network traffic through a router that involves reassigning the source or destination IP address. The most common use for NAT is to allow private networks to communicate with the internet. Static NAT performs a 1:1 translation, which does not pose a problem for Firewall Management Center communication with devices, but port address translation (PAT) is more common. PAT lets you use a single public IP address and unique ports to access the public network; these ports are dynamically assigned as needed, so you cannot initiate a connection to a device behind a PAT router.

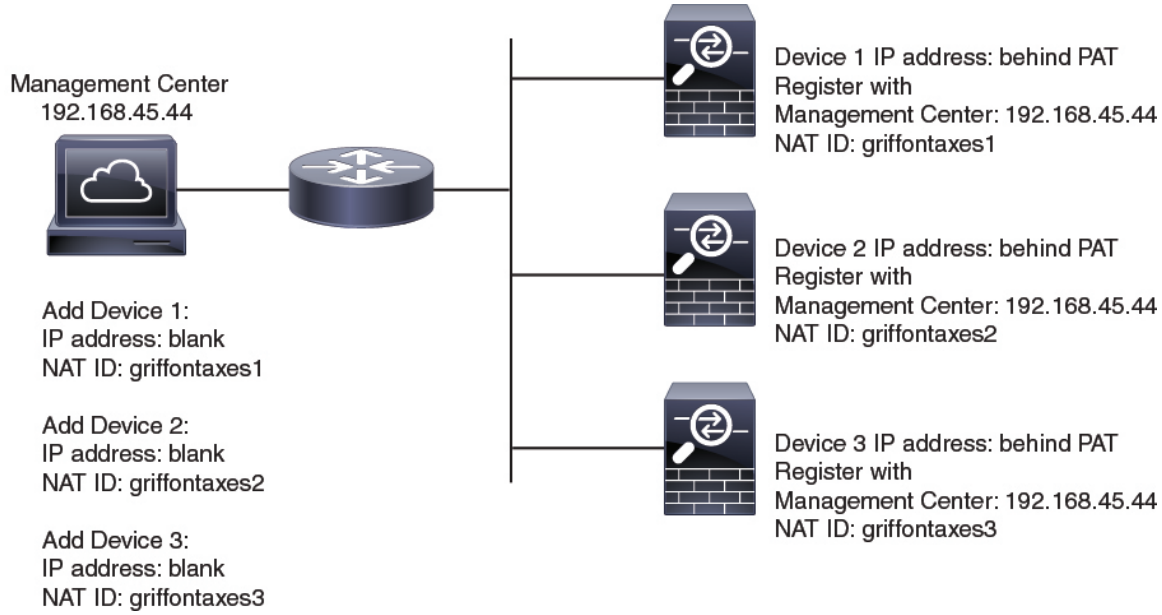
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the Firewall Management Center specifies the device IP address when you add a device, and the device specifies the Firewall Management Center IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The Firewall Management Center and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

For example, you add a device to the Firewall Management Center, and you do not know the device IP address (for example, the device is behind a PAT router), so you specify only the NAT ID and the registration key on the Firewall Management Center; leave the IP address blank. On the device, you specify the Firewall Management Center IP address, the same NAT ID, and the same registration key. The device registers to the Firewall Management Center's IP address. At this point, the Firewall Management Center uses the NAT ID instead of IP address to authenticate the device.

Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the Firewall Management Center. On the Firewall Management Center, specify a unique NAT ID for each device you want to add while leaving the IP address blank, and then on each device, specify both the Firewall Management Center IP address and the NAT ID. Note: The NAT ID must be unique per device.

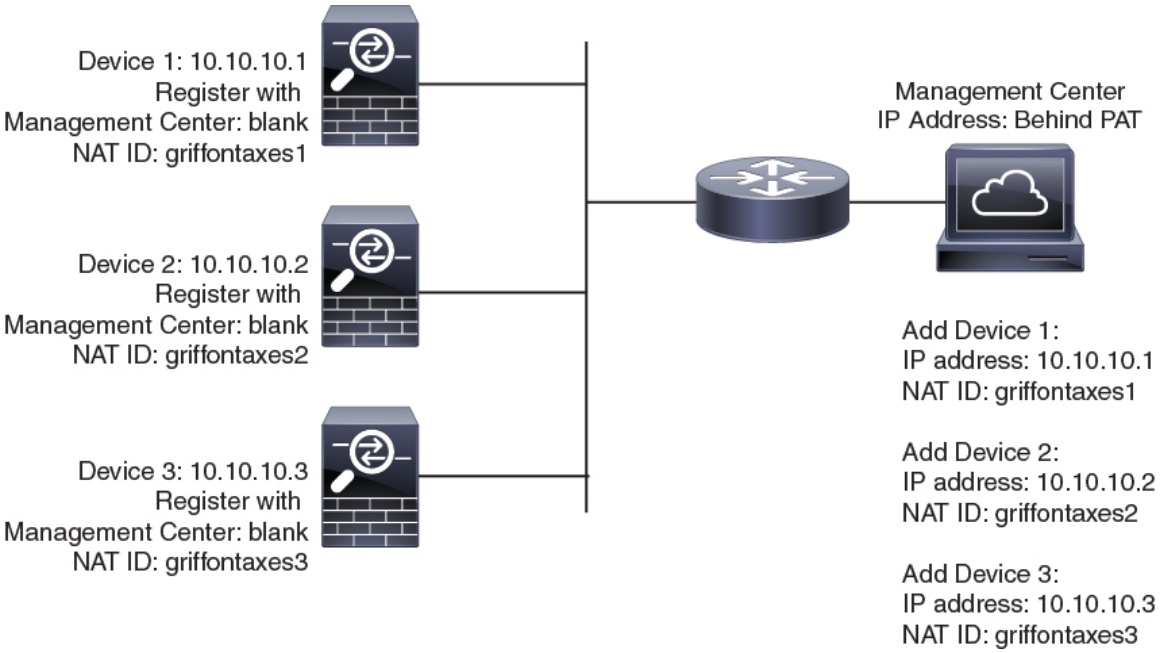
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the Firewall Management Center and the devices, and specify the Firewall Management Center IP address on the devices.

Figure 1: NAT ID for Managed Devices Behind PAT



The following example shows the Firewall Management Center behind a PAT IP address. In this case, specify a unique NAT ID per device on both the Firewall Management Center and the devices, and specify the device IP addresses on the Firewall Management Center.

Figure 2: NAT ID for Firewall Management Center Behind PAT



Management and event traffic channel examples

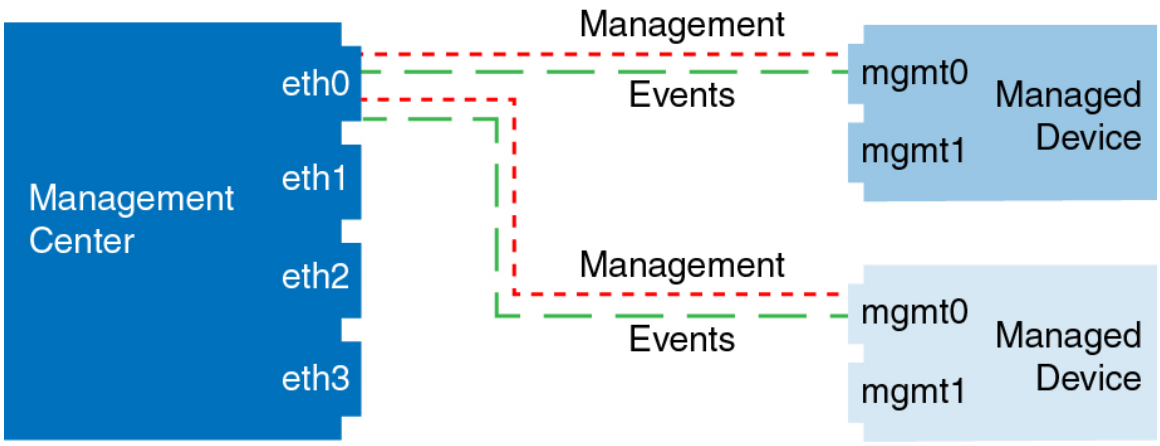
The management and event traffic channel examples illustrates the implementation and configuration of separate communication paths for network management and event reporting functions.

Note

- Configure a separate, dedicated event interface on both the Firewall Management Center and the managed device to segregate event traffic from management traffic. This separation improves performance and security by isolating event data flows.
- If Firewall Management Center uses a single interface for both management and event traffic, the managed device must send event traffic on that same interface. If the Firewall Management Center has a dedicated event interface, the managed device must also have a dedicated event interface configured.
- Mixing management and event channels on the same interface on the Firewall Management Center while the managed device uses a separate event interface can cause connectivity or event delivery issues. Ensure interface pairing is consistent between Firewall Management Center and managed devices.
- If you use a data interface for management on a Firewall Threat Defense, you cannot use separate management and event interfaces for that device.

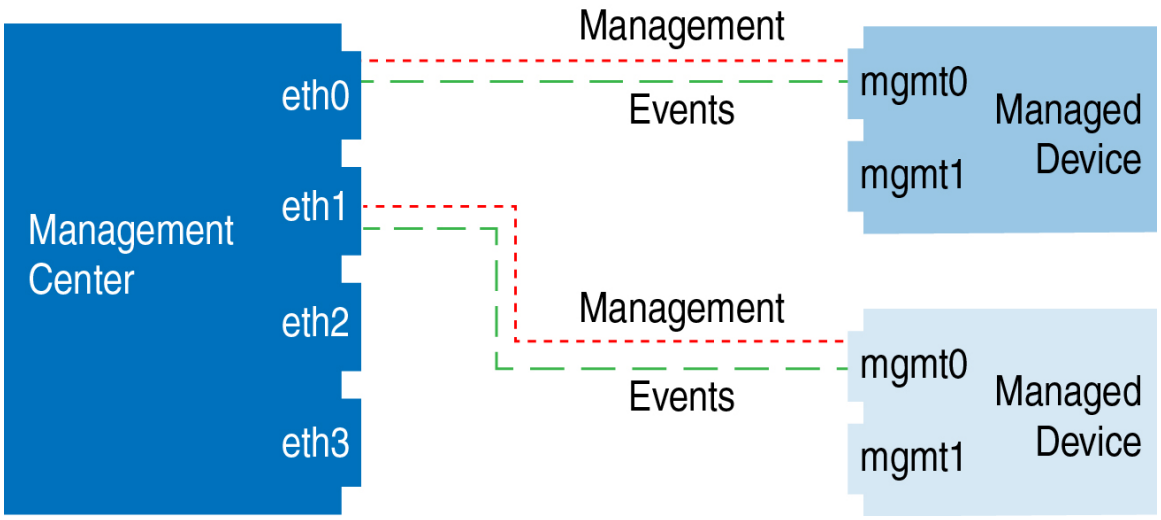
The following example shows the Firewall Management Center and managed devices using only the default management interfaces.

Figure 3: Single Management Interface on the Secure Firewall Management Center



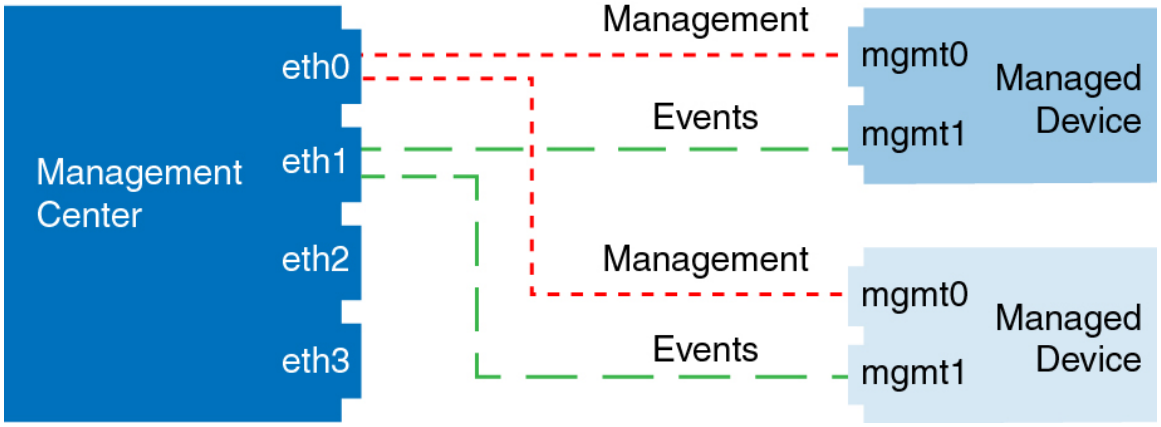
The following example shows the Firewall Management Center using separate management interfaces for devices; and each managed device using 1 management interface.

Figure 4: Multiple Management Interfaces on the Secure Firewall Management Center



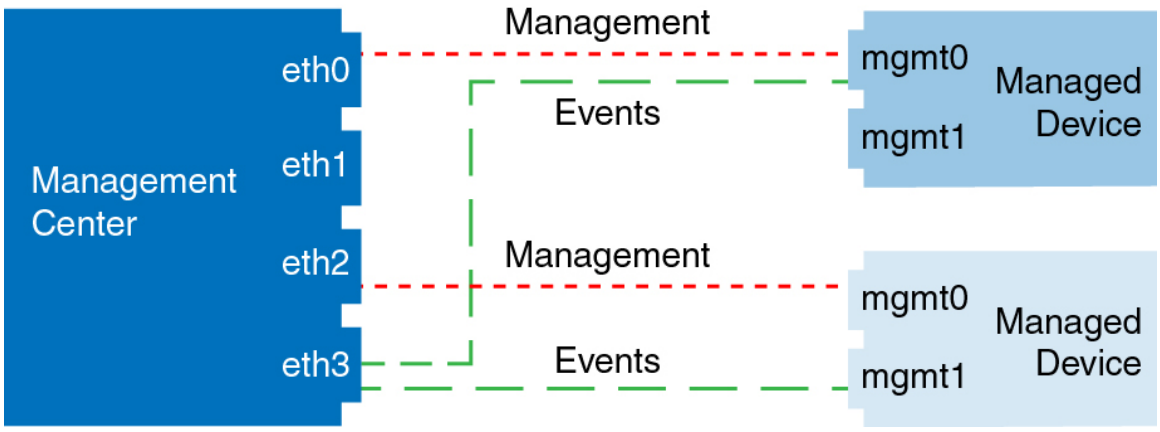
The following example shows the Firewall Management Center and managed devices using a separate event interface.

Figure 5: Separate Event Interface on the Secure Firewall Management Center and Managed Devices



The following example shows a mix of multiple management interfaces and a separate event interface on the Firewall Management Center and a mix of managed devices using a separate event interface, or using a single management interface.

Figure 6: Mixed Management and Event Interface Usage



Prerequisites for device registration

This reference provides the prerequisites and requirements that must be satisfied before registering a device with the management center, including domain requirements, user roles, connection specifications, and Zero-Touch Provisioning requirements.

Supported domains

The domain in which the device resides.

User roles

- Admin
- Network Admin

Management connection

Make sure the management connection is stable, without excessive packet loss, with at least 5Mbps throughput.

Zero-Touch Provisioning requirements

Zero-Touch Provisioning is not supported with clustering or multi-instance mode.

High availability is only supported when you use the Management interface because zero-touch provisioning uses DHCP, which is not supported for data interfaces and high availability.

Zero-Touch Provisioning is supported on these models using 7.4 or later:

- Firepower 1010
- Firepower 1100
- Secure Firewall 1200
- Firepower 2100 (on supported device versions)

- Secure Firewall 3100

Log into the Command-Line Interface on the device

You can log directly into the command-line interface on Firewall Threat Defense devices. If this is your first time logging in, complete the initial setup process using the default **admin** user; see Complete the Firewall Threat Defense Initial Configuration Using the CLI , on page 21 .

For zero-touch provisioning , if you must access the Firewall Threat Defense CLI and run through the setup script, answer **n** when prompted: `Do you want to configure IPv4? (y/n) [y]:` and `Do you want to configure IPv6? (y/n) [y]:` . You also must accept the default local manager: `Manage the device locally? (yes/no) [yes]:` . These settings will preserve zero-touch provisioning capability.

Note If a user makes three consecutive failed attempts to log in to the CLI via SSH, the system terminates the SSH connection.

Before you begin

- Create additional user accounts that can log in to the CLI using the **configure user add** command.
- If you get unreadable characters when connecting to the console port, verify the port settings. If they are correct, try the cable with another device using the same settings. If the cable is good, you might need to replace the hardware for the console port. Also consider trying a different workstation to make the connection.

Procedure

Step 1 Connect to the Firewall Threat Defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the Firewall Threat Defense device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. See Configure Secure Shell (SSH) access, on page 867 to allow SSH connections to specific data interfaces.

For physical devices, you can directly connect to the console port on the device. See the hardware guide for your device for more information about the console cable. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

The CLI on the console port is FXOS (with the exception of the ISA 3000, where it is the regular Firewall Threat Defense CLI) . Use the Firewall Threat Defense CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

For a chassis in multi-instance mode, you can connect to FXOS on the console port, or you can enable SSH for FXOS on the Management interface according to Configure SSH and SSH access list, on page 201 . SSH is disabled by default.

Step 2 Log in with the **admin** username and password.

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1
firepower#
```

Step 3 If you used the console port, access the Firewall Threat Defense CLI.

connect ftd

Multi-instance mode:

connect ftd *name*

To view the instance names, enter the command without a name.

Note This step does not apply to the ISA 3000.

Example:

```
firepower# connect ftd
>
```

Step 4 At the CLI prompt (>), use any of the commands allowed by your level of command line access.

To return to FXOS on the console port, enter **exit** .

Step 5 (Optional) If you used SSH, you can connect to FXOS.

connect fxos

To return to the Firewall Threat Defense CLI, enter **exit** .

Step 6 (Optional) Access the diagnostic CLI:

system support diagnostic-cli

Use this CLI for advanced troubleshooting. This CLI includes additional **show** and other commands.

This CLI has submodes: user EXEC mode, privileged EXEC mode . More commands are available in privileged EXEC mode than user EXEC mode. To enter privileged EXEC mode, enter the **enable** command; press enter without entering a password when prompted.

Example:

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

To return to the regular CLI, type **Ctrl-a** , **d** .

Complete the Firewall Threat Defense initial configuration for manual registration

You can complete the Firewall Threat Defense initial configuration using the CLI or the Firewall Device Manager for all models except for the Firepower 4100/9300.

Platform-specific configuration methods

For the Firepower 4100/9300, you complete initial configuration when you deploy the logical device. See Logical Devices on the Firepower 4100/9300, on page 223.

For zero-touch provisioning (serial number registration), you should not log in to the device or perform initial setup. See Add a Device Using the Serial Number (Zero-Touch Provisioning) , on page 36.



Note Devices registered to a Firewall Management Center (FMC) for analytics-only purposes count toward the FMC platform device capacity limit. As the number of devices increases, event processing requirements also increase. Properly size your virtual FMC (vFMC) tier when planning analytics-only deployments.

Complete the Firewall Threat Defense Initial Configuration Using the Firewall Device Manager

When you use the Firewall Device Manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration
- Ethernet 1/2 (or for the 1010), the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

If you perform additional interface-specific configuration within Firewall Device Manager before registering with the Firewall Management Center , then that configuration is preserved.

When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

- The Secure Firewall 4200 does not support the Firewall Device Manager . You need to use the CLI procedure: Complete the Firewall Threat Defense Initial Configuration Using the CLI , on page 21 .
- This procedure does not apply for Security Cloud Control -managed devices for which you want to use an on-prem Firewall Management Center *for analytics only*. The Firewall Device Manager configuration

is meant to configure the primary manager. See Complete the Firewall Threat Defense Initial Configuration Using the CLI , on page 21 for more information about configuring the device for analytics.

- This procedure applies to all other devices except for the Firepower 4100/9300 and the ISA 3000. You can use the Firewall Device Manager to onboard these devices to the Firewall Management Center , but because they have different default configurations than other platforms, the details in this procedure may not apply to these platforms.

Procedure

Step 1 Log into the Firewall Device Manager .

a) Enter the following URL in your browser.

- Inside— **https://192.168.95.1** .
- Management— **https://** *management_ip* . The Management interface is a DHCP client, so the IP address depends on your DHCP server. You will have to set the Management IP address to a static address as part of this procedure, so we recommend that you use the inside interface so you do not become disconnected.

b) Log in with the username **admin** , and the default password **Admin123** .

c) You are prompted to read and accept the End User License Agreement and change the admin password.

Step 2 Use the setup wizard when you first log into the Firewall Device Manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

After you complete the setup wizard, in addition to the default configuration for the inside interface, you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to the Firewall Management Center management.

a) Configure the following options for the outside and management interfaces, and click **Next** .

1. **Outside Interface Address** —This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

   If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

   Configure IPv4 —The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

   Configure IPv6 —The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

2. **Management Interface**

   You will not see Management Interface settings if you performed initial setup at the CLI.

   The Management interface settings are used even if you enable manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

DNS Servers —The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

Firewall Hostname —The hostname for the system's management address.

b) Configure the **Time Setting (NTP)** and click **Next** .

1. **Time Zone** —Select the time zone for the system.
2. **NTP Time Server** —Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

c) Select **Start 90 day evaluation period without registration** .

Do not register the Firewall Threat Defense with the Smart Software Manager; all licensing is performed on the Firewall Management Center .

d) Click **Finish** .

e) You are prompted to choose **Cloud Management** or **Standalone** . For Firewall Management Center management, choose **Standalone** , and then **Got It** .

Step 3 (Might be required) Configure the Management interface.

You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

a) To configure additional interfaces, including an interface other than outside or inside that you want to use for manager access, choose **Device**

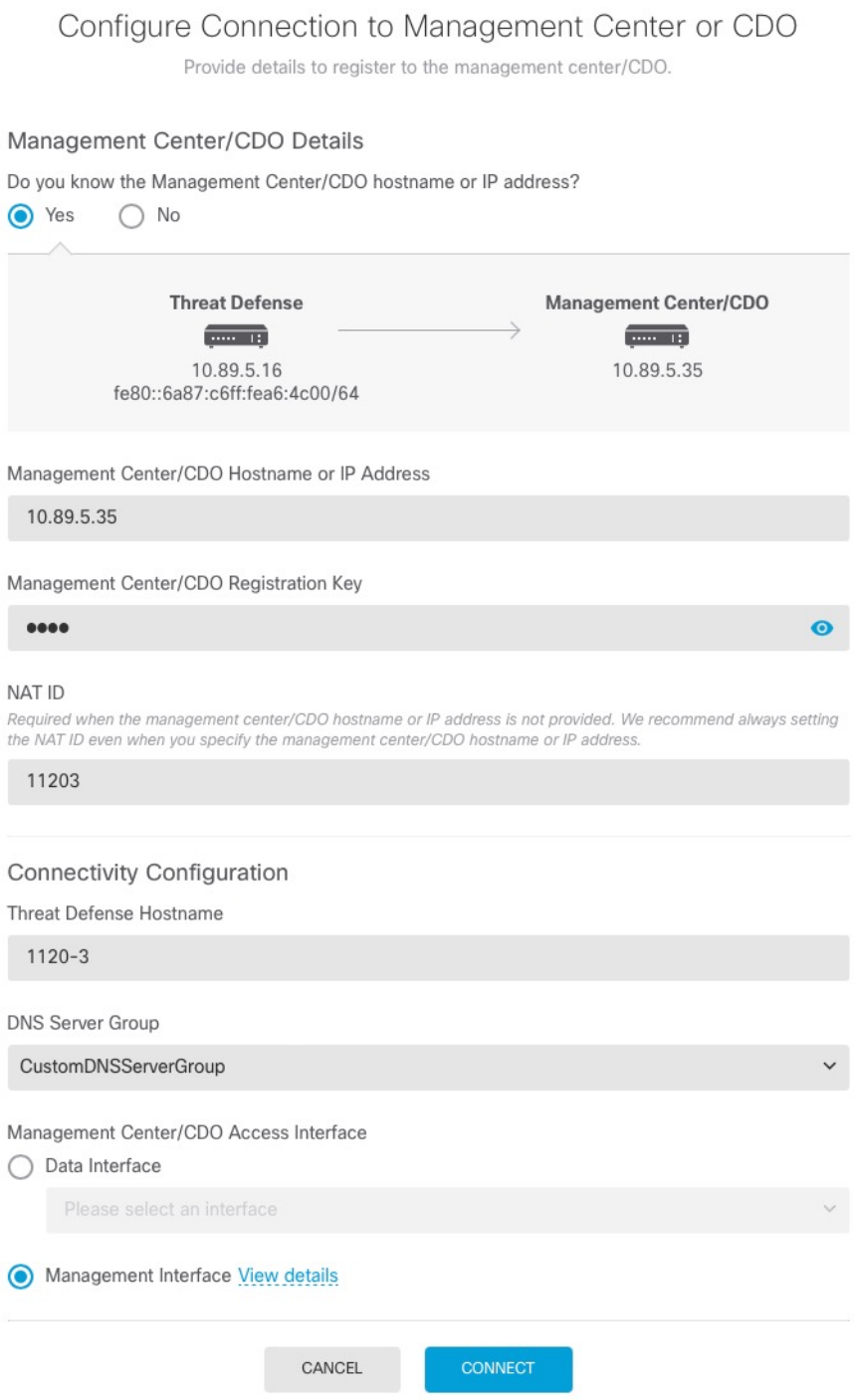
b) Click the link in the **Interfaces** summary.

Other Firewall Device Manager configuration will not be retained when you register the device to Firewall Management Center.

Step 4 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

Step 5 Configure the **Management Center/CDO Details**.

Figure 7: Management Center/Security Cloud Control Details



a) For **Do you know the Management Center/CDO hostname or IP address?**, click **Yes** if you can reach the Firewall Management Center using an IP address or hostname, or **No** if the Firewall Management CenterSecurity Cloud Control is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/CDO Hostname or IP Address**.

c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

Step 6 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/CDO Access Interface** access, then this FQDN will be used for this interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/CDO Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall Management Center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense device that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/CDO Access InterfaceFMC Access Interface**, then this setting configures the Management DNS server.

c) For the **Management Center/CDO Access Interface**, choose any configured interface.

You can change the manager interface after you register the Firewall Threat Defense device to the Firewall Management Center, to either the Management interface or another data interface.

Step 7 (Optional) If you chose a data interface, and it was not the outside interface, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the Firewall Management Center.

If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.

Step 8 (Optional) If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

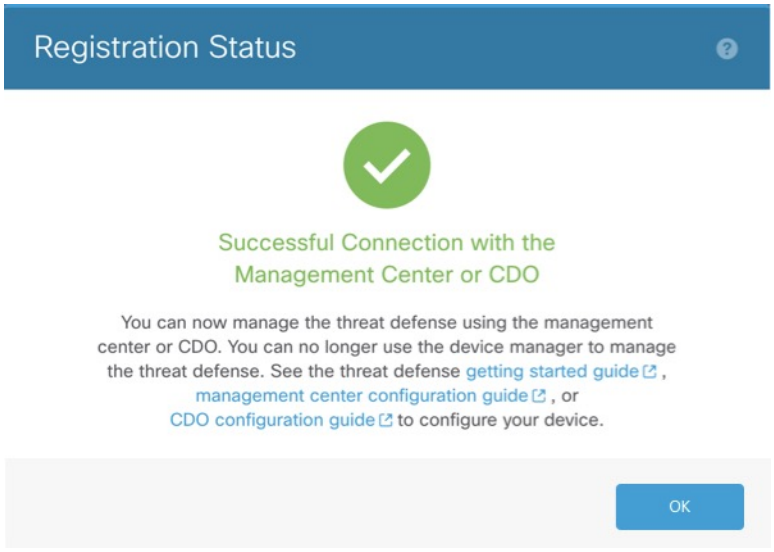
DDNS is not supported when using the Management interface for manager access.

Step 9 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/CDO Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall Device Manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center/CDO** dialog box, after which you will be disconnected from the Firewall Device Manager.

Figure 8: Successful Connection



Complete the Firewall Threat Defense Initial Configuration Using the CLI

Connect to the Firewall Threat Defense CLI to perform initial setup, including setting the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. If you do not want to use the Management interface for manager access, you can use the CLI to configure a data interface instead. You will also configure Firewall Management Center communication settings. When you perform initial setup using the Firewall Device Manager , *all* interface configuration completed in the Firewall Device Manager is retained when you switch to the Firewall Management Center for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

This procedure applies to all models except for the Firepower 4100/9300 . To deploy a logical device and complete initial configuration on the Firepower 4100/9300 , see Logical Devices on the Firepower 4100/9300, on page 223 .

Procedure

Step 1 Connect to the Firewall Threat Defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

The console port connects to the FXOS CLI. The SSH session connects directly to the Firewall Threat Defense CLI. The exception is for the ISA 3000, where the console connection connects to the Firewall Threat Defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123** .

At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the Firewall Threat Defense login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default.

For Firepower and Secure Firewall hardware, see the Reimage Procedures in the Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense .

For the ISA 3000, see the Cisco Secure Firewall ASA and Threat Defense Reimage Guide .

Example:

```
firepower login:
                          admin
Password:
                          Admin123
Successful login attempts for user 'admin' : 1
[...]
Hello admin. You must change your password.
Enter new password:
                          ********
Confirm new password:
                          ********
Your password was updated successfully.
[...]
firepower#
```

Step 3 If you connected to FXOS on the console port, connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the Firewall Threat Defense , you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference .

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter** .

Note The Management interface settings are used even when you enable manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?** —Enter **y** for at least one of these types of addresses.
- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface** —If you want to use a data interface for manager access instead of the Management interface, choose **manual** . Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface** and/or **Configure IPv6 via DHCP, router, or manually?** — If you want to use a data interface for manager access instead of the management interface, set the gateway to be **data-interfaces** . This setting forwards management traffic over the backplane so it can be routed through the manager access data interface. If you want to use the Management interface for manager access, you should set a gateway IP address on the Management 1/1 network.
- **If your networking information has changed, you will need to reconnect** —If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?** —Enter **no** to use the Firewall Management Center . A **yes** answer means you will use Secure Firewall Device Manager instead.
- **Configure firewall mode?** —We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface manager access is only supported in routed firewall mode.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]:
                        n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]:
                        10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]:
                        255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
                        10.89.5.1
Enter a fully qualified hostname for this system [firepower]:
```

```
                        1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []:
                        cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
Manage the device locally? (yes/no) [yes]:
                        no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy
You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.
When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 5 Identify the Firewall Management Center that will manage this Firewall Threat Defense .

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *reg_key* [*nat_id*] [*display_name*]

Note If you are using Security Cloud Control for management, use the Security Cloud Control -generated **configure manager add** command for this step.

- { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** }—Specifies either the FQDN or IP address of the Firewall Management Center . If the Firewall Management Center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id* . At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense , must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices. If you specify

DONTRESOLVE in this command, then the Firewall Threat Defense must have a reachable IP address or hostname.

- *reg_key* —Specifies a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense . The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id* —Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense . The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center . The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:
  - You set the Firewall Management Center IP address to **DONTRESOLVE** .
  - When adding the device on the Firewall Management Center , you do not specify a reachable device IP address or hostname.
  - You use the data interface for management, even if you specify IP addresses on both sides.
  - The Firewall Management Center uses multiple management interfaces.
- *display_name* —Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying Security Cloud Control as the primary manager and an on-prem Firewall Management Center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
  - *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword)
  - **manager-** *timestamp*

Example:

```
>
                        configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

If the Firewall Management Center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

```
>
                        configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

If the Firewall Threat Defense is behind a NAT device, enter a unique NAT ID along with the Firewall Management Center IP address or hostname, for example:

```
>
```

```
                        configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Step 6 If you are using Security Cloud Control as your primary manager and want to use an on-prem Firewall Management Center for analytics only, identify the on-prem Firewall Management Center .

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *reg_key* [*nat_id*] [*display_name*]

Example:

The following example uses the generated command for Security Cloud Control with a Security Cloud Control -generated display name and then specifies an on-prem Firewall Management Center for analytics only with the "analytics-FMC" display name.

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

Step 7 (Optional) Configure a data interface for manager access.

configure network management-data-interface

After pressing **Enter**, you are prompted to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command. See also Using the Firewall Threat Defense data interface for management, on page 5 .

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** { **ipv4** | **ipv6** } **manual** command. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues. If you did not already set the Management interface gateway to **data-interfaces** , this command will set it now.
- When you add the Firewall Threat Defense to the Firewall Management Center , the Firewall Management Center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In the Firewall Management Center , you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the Firewall Threat Defense or Firewall Management Center from re-establishing the management connection. If the management connection is disrupted, the Firewall Threat Defense includes the **configure policy rollback** command to restore the previous deployment.
- DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its Fully-Qualified Domain Name (FQDN) if the IP address changes. If you configure a DDNS server update URL, the Firewall Threat Defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense can validate the DDNS server certificate

for the HTTPS connection. The Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the Firewall Management Center , the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense . When you add the Firewall Threat Defense to the Firewall Management Center , the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the Firewall Management Center and the Firewall Threat Defense into sync.

  Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in the Firewall Management Center , including the DNS servers, to match the FTD configuration.

- You can change the management interface after you register the Firewall Threat Defense to the Firewall Management Center , to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data management, enter the **configure network management-data-interface disable** command.

Example:

```
>
                        configure network management-data-interface
Data interface to use for management:
                        ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:

https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
Setting IPv4 network configuration.
Network settings changed.
>
```

Example:

```
>
                        configure network management-data-interface
Data interface to use for management:
                        ethernet1/1
Specify a name for the interface [outside]:
```

```
                        internet
IP address (manual / dhcp) [dhcp]:
                        manual
IPv4/IPv6 address:
                        10.10.6.7
Netmask/IPv6 Prefix:
                        255.255.255.0
Default Gateway:
                        10.10.6.1
Comma-separated list of DNS servers [none]:
                        208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
Setting IPv4 network configuration.
Network settings changed.
>
```

Step 8 (Optional) Limit data interface access to a manager on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

Register your device to a Firewall Management Center .

Configure an event interface

You always need a management interface for management traffic. If your device has a second management interface, for example, the Firepower 4100/9300 and Secure Firewall 4200 , you can enable it for event-only traffic.

You can configure a separate event-only interface on both the Firewall Management Center and the managed device to isolate event traffic. This setup enhances performance and security by segregating event data from management operations.

If the event interface is unreachable, event traffic falls back to the management interface.

Before you begin

Ensure that you enable an event interface on the Firewall Management Center before configuring a separate event-only interface on the managed device. For more information, refer to *Cisco Secure Firewall Management Center Administration Guide* .

If you use a data interface for management on the managed device, you cannot configure separate management and event interfaces.

Procedure

Step 1 Enable the second management interface as an event-only interface.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

You can optionally disable events for the main management interface using the **configure network management-interface disable-events-channel** command. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management interface even if you disable the event channel.

You cannot disable both event and management channels on an interface.

Example:

```
> configure network management-interface enable management1
Configuration updated successfully
> configure network management-interface disable-management-channel management1
Configuration updated successfully
>
```

Step 2 Configure the IP address of the event interface.

The event interface can be on a separate network from the management interface, or on the same network.

a) Configure the IPv4 address:

configure network ipv4 manual *ip_address netmask gateway_ip* **management1**

Note that the *gateway_ip* in this command is used to create the default route for the device, so you should enter the value you already set for the management0 interface. It does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you create a static route separately for the event-only interface.

Example:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
>
```

b) Configure the IPv6 address:

- Stateless autoconfiguration:

  configure network ipv6 router management1

  Example:

  ```
  > configure network ipv6 router management1
  Setting IPv6 network configuration.
  Network settings changed.
  >
  ```

- Manual configuration:

  configure network ipv6 manual *ip6_address ip6_prefix_length* **management1**

  Example:

  ```
  > configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
  Setting IPv6 network configuration.
  ```

```
Network settings changed.
>
```

Step 3 Add a static route for the event-only interface if the Firewall Management Center is on a remote network; otherwise, all traffic will match the default route through the management interface.

configure network static-routes { **ipv4** | **ipv6** } **add management1** *destination_ip netmask_or_prefix gateway_ip*

For the *default* route, do not use this command; you can only change the default route gateway IP address when you use the **configure network ipv4** or **ipv6** commands (see, Step 2, on page 29).

Example:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully
> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
>
```

To display static routes, enter **show network-static-routes** (the default route is not shown):

```
> show network-static-routes

                        ---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

Device registration management

Register and unregister devices to the Firewall Management Center.

About the device management page

The **Devices** > **Device Management** page provides you with range of information and options.

- **View By**—View devices based on group, licenses, model, version, or access control policy.
- **Device State**—View devices based on state (**Error**, **Warning**, etc.). You can click on a state icon to view the devices belonging to it. The number of devices belonging to the states are provided within brackets.
- **Search Device**—Search for a device by device name, host name, or IP address.
- **Add**—Add devices and other manageable components.
- Columns—Click the column head to sort by that column.

- **Name**
- **Model**
- **Version**
- **Chassis**—For supported models, click **Manage** to bring up the integrated Chassis Manager. For the Firepower 4100/9300, the link cross-launches the Firewall Chassis Manager.
- **Licenses**
- **Access Control Policy**—Click on the link in the Access Control Policy column to view the policy that is deployed to the device.
- **Auto-Rollback**—Shows whether auto-rollback of the configuration is enabled ( ) or disabled) if the deployment causes the management connection to go down. See Edit deployment settings, on page 800.

- **Edit**—For each device, use the **Edit** ( ) icon to edit the device settings.

  You can also just click on the device name or IP address.

- **More**—For each device, click the **More** ( ) icon to execute other actions:
  - **Delete**—To unregister the device.
  - **Packet Tracer**—To navigate to the packet tracer page for examining policy configuration on the device by injecting a model packet into the system.
  - **Packet Capture**—To navigate to the packet capture page, where, you can view the verdicts and actions the system takes while processing a packet.
  - **Revert Upgrade**—To revert the upgrade and configuration changes that were made after the last upgrade. This action results in restoring the device to the version that was before the upgrade.
  - **Health Monitor**—To navigate to the device's health monitoring page.
  - **Troubleshoot Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.

Add a Device Group

The Firewall Management Center allows you to group devices so you can easily deploy policies and install updates on multiple devices. You can expand and collapse the list of devices in the group.

If you add the primary device in a high-availability pair to a group, both devices are added to the group. If you break the high-availability pair, both devices remain in that group.

Groups are not supported in a multidomain environment.

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 From the **Add** drop-down menu, choose **Add Group** .

To edit an existing group, click **Edit** ( ) for the group you want to edit.

Step 3 Enter a **Name** .

Step 4 Under **Available Devices** , choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.

Step 5 Click **Add** to include the devices you chose in the device group.

Step 6 Optionally, to remove a device from the device group, click **Delete** ( ) next to the device you want to remove.

Step 7 Click **OK** to add the device group.

Registration with the management center

Registration with the Firewall Management Center is a process that establishes communication and management between devices and the central management platform.

Available registration methods

The Firewall Management Center offers multiple methods to register your devices.

Add a Device Using a Registration Key

Use this procedure to add a single device to the Firewall Management Center using a registration key . If you plan to link devices for high availability, you must still use this procedure ; see Add a high availability pair, on page 306 . For clustering, see the clustering chapter for your model.

You can also use this procedure to add a device that is managed by a Cloud-Delivered Firewall Management Center , and you want to use the on-prem Firewall Management Center for event logging and analytics purposes only.

If you use Firewall Management Center high availability, add devices *only* to the active Firewall Management Center. Devices registered to the active Firewall Management Center are automatically registered to the standby.

Before you begin

- Set up the device to be managed by the Firewall Management Center. See:
  - Complete the Firewall Threat Defense initial configuration for manual registration, on page 15
  - The getting started guide for your model
- The Firewall Management Center must be registered to the Smart Software Manager. A valid evaluation license is sufficient, but if it expires, you will not be able to add new devices until you successfully register.
- If you registered a device using IPv4 and want to convert it to IPv6, you must delete and reregister the device.

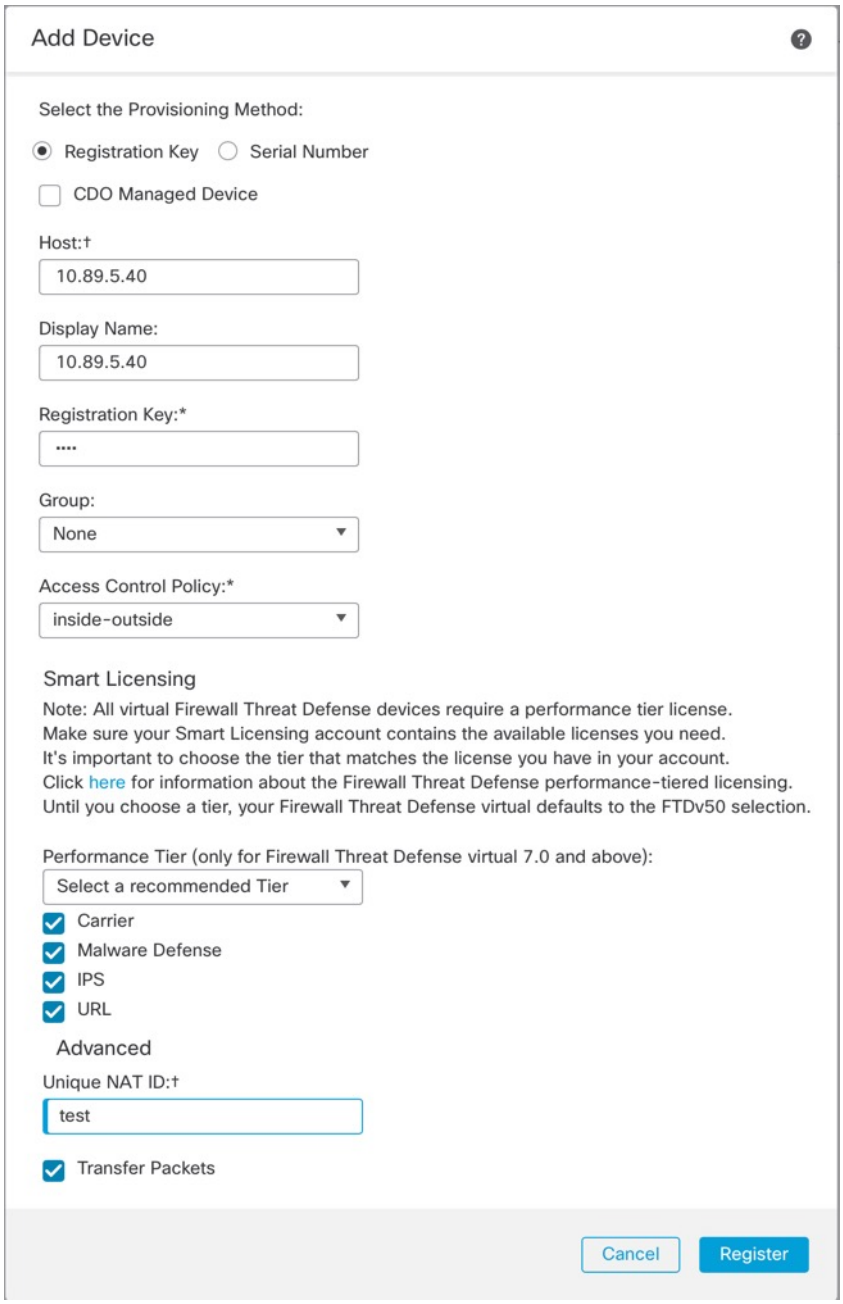
Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 From the **Add** drop-down menu, choose **Device** .

The **Registration Key** method is selected by default.

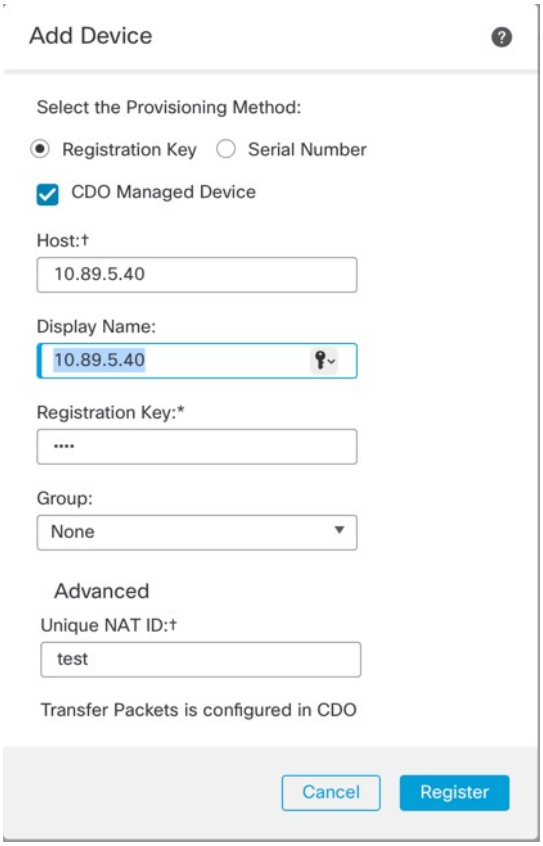
Figure 9: Add Device Using a Registration Key



Step 3 If you want to add a cloud-managed device to your on-prem Firewall Management Center for analytics only, check **CDO Managed Device** .

The system hides licensing and packet transfer settings because they are managed by Security Cloud Control (formerly CDO). You can skip those steps.

Figure 10: Add Device for Security Cloud Control



Step 4 For the **Host** , enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).

If you leave this field blank, the initial configuration on the device needs to include a reachable Firewall Management Center IP address or hostname plus the NAT ID. For more information, see NAT environments, on page 8 .

Step 5 For the **Display Name** , enter a name for the device as you want it to display in the Firewall Management Center . You cannot change this name later.

Step 6 For the **Registration Key** , enter the same registration key in your initial configuration. The registration key is a one-time-use shared secret. The key can be up to 37-characters in length and include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). The registration key does not need to be unique per device. Add the device to a device **Group**.

Step 7 Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If the device is incompatible with the policy you choose, deploying will fail. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other

misconfigurations. After you resolve the issue that caused the failure, manually deploy configurations to the device.

Step 8 Choose licenses to apply to the device.

You can also apply licenses after you add the device, from the **System** (⚙) > **Licenses** > **Smart Licenses** page.

For Firewall Threat Defense Virtual , you must also select the **Performance Tier** . It's important to choose the tier that matches the license you have in your account. Until you choose a tier, your device defaults to the FTDv50 selection. For more information about the performance-tiered license entitlements available for Firewall Threat Defense Virtual , see *FTDv Licenses* in the *Cisco Secure Firewall Management Center Administration Guide* .



Note If you are upgrading your Firewall Threat Defense Virtual to Version 7.0+, you can choose **FTDv - Variable** to maintain your current license compliance.

If you specified a NAT ID during initial configuration, in the **Advanced** section enter the same NAT ID for the **Unique NAT ID**.

The **Unique NAT ID** specifies a unique, one-time string of your choice that you will also specify on the device during initial configuration. It is required when one side does not specify a reachable IP address or hostname, for example if you left the **Host** field blank. Although technically optional, we recommend always specifying the NAT ID even when you know the IP addresses of both sides because it is required in certain situations. The ID can be up to 37-characters in length and include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center .

Step 9 Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent. Click **Register**.

It may take up to two minutes for the Firewall Management Center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the device fails to register, check the following items:

- Ping—Access the device CLI, and ping the Firewall Management Center IP address using the following command:

  ping system *ip_address*

  If the ping is not successful, check your network settings using the **show network** command. If you need to change the device IP address, use the **configure network** { **ipv4** | **ipv6** } **manual** command.

- Registration key, NAT ID, and Firewall Management Center IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the device using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error .

What to do next

Add a Device Using the Serial Number (Zero-Touch Provisioning)

Zero-Touch Provisioning lets you register devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with Security Cloud Control for this functionality.

When you use zero-touch provisioning , the following interfaces are preconfigured. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration
- Ethernet 1/2 (or for the Firepower 1010, the VLAN1 interface) — "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Zero-Touch Provisioning is not supported with clustering or multi-instance mode.

High availability is only supported when you use the Management interface because zero-touch provisioning uses DHCP, which is not supported for data interfaces and high availability.

Zero-Touch Provisioning is only supported on the following models using 7.2, 7.4 or later (prior to 7.2.4, the Firewall Management Center must be publicly reachable):

- Firepower 1010
- Firepower 1100
- Firepower 2100
- Secure Firewall 3100

Before you begin

- Make sure the device is unconfigured or a fresh install. Zero-Touch Provisioning is meant for new devices only. Pre-configuration can disable zero-touch provisioning , depending on your settings.
- Cable the outside interface or Management interface so it can reach the internet. If you use the outside interface for zero-touch provisioning , do not also cable the Management interface; if the Management interface gets an IP address from DHCP, the routing will be incorrect for the outside interface.
- Make sure you have at least one access control policy configured on the Firewall Management Center so you can assign it to new devices. You cannot add a policy using Security Cloud Control .
- If the device does not have a public IP address or FQDN, or you use the Management interface, set a public IP address/FQDN for the Firewall Management Center (if different from the Firewall Management Center management interface IP address; for example, it is behind NAT) so the device can initiate the management connection. See **System** > **Configuration** > **Manager Remote Access** . You can also configure the public IP address/FQDN in Security Cloud Control during this procedure.
- DHCP server for either Management or Ethernet 1/1 that provides an IP address and default gateway.

- Network access to the OpenDNS public DNS servers. IPv4: 208.67.220.220 and 208.67.222.222; IPv6: 2620:119:35::35. DNS servers obtained from DHCP are never used.

  The following names need to be resolved:

  Table 2: FQDNs for zero-touch provisioning

FQDNs
*.cisco.com (many FQDNs)
*.defenseorchestrator.com (many FQDNs)
*.defenseorchestrator.eu (for the EU, many FQDNs)
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

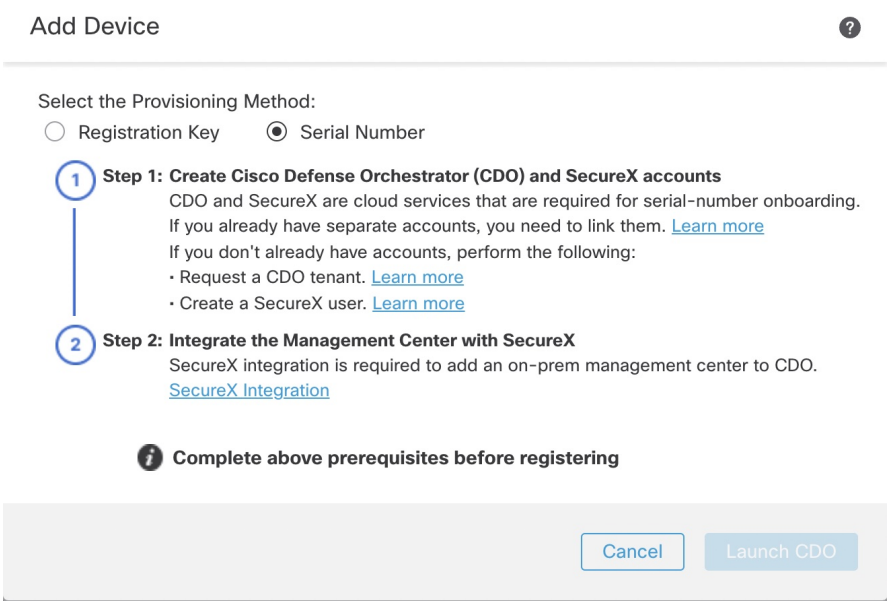
- The Firewall Management Center must be registered to the Smart Software Manager. A valid evaluation license is sufficient, but if it expires, you will not be able to add new devices until you successfully register.
- If you registered a device using IPv4 and want to convert it to IPv6, you must delete and reregister the device.

Procedure

Step 1 The first time you add a device using a serial number, you need to complete the following prerequisites. After the first time, you can skip to adding the devices directly in Security Cloud Control .

a) In the Firewall Management Center , choose **Devices** > **Device Management** .
b) From the **Add** drop-down menu, choose **Device** .
c) Click **Serial Number** for the provisioning method.

Figure 11: Add Device by Serial Number



d) Create a Security Cloud Control account.

Note If you already have preexisting but separate SecureX and Security Cloud Control accounts, you need to link them. See https://cisco.com/go/cdo-securex-link for more information about linking accounts.

If you don't already have accounts, perform the following:

- Create a Cisco Security Cloud (formerly SecureX) account. See the Security Cloud Control documentation for information about how to create one.
- Request a Security Cloud Control tenant. See the Security Cloud Control documentation for information about requesting a new Security Cloud Control tenant.

e) Integrate the Firewall Management Center with Cisco Security Cloud (formerly SecureX). Click the link to open the **SecureX Integration** page in the Firewall Management Center .

Click the **Enable SecureX** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code. Make sure this page is not blocked by a pop-up blocker.

For detailed information, see the "Enable SecureX Integration " section in the *Cisco Secure Firewall Management Center Administration Guide* .

Security Cloud Control onboards the on-prem Firewall Management Center after you integrate the Firewall Management Center with Cisco Security Cloud. Security Cloud Control needs the Firewall Management Center in its inventory for zero-touch provisioning to operate. Security Cloud Control 's Firewall Management Center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the Firewall Management Center , and cross-launching the Firewall Management Center .

Note For a Firewall Management Center high-availability pair, you also need to integrate the secondary Firewall Management Center with Cisco Security Cloud.

f) Click **Launch** Security Cloud Control if you do not already have it open, or log in here: https://www.defenseorchestrator.com/ .

Make sure Security Cloud Control is not blocked by a pop-up blocker.

Step 2 On the Security Cloud Control **Dashboard** (https://www.defenseorchestrator.com/), click **Onboard** (+ Onboard).

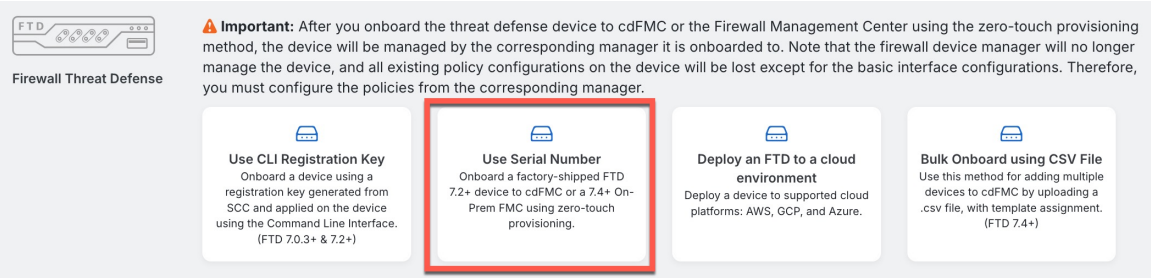
Click the **FTD** tile.

Figure 12: FTD Tile



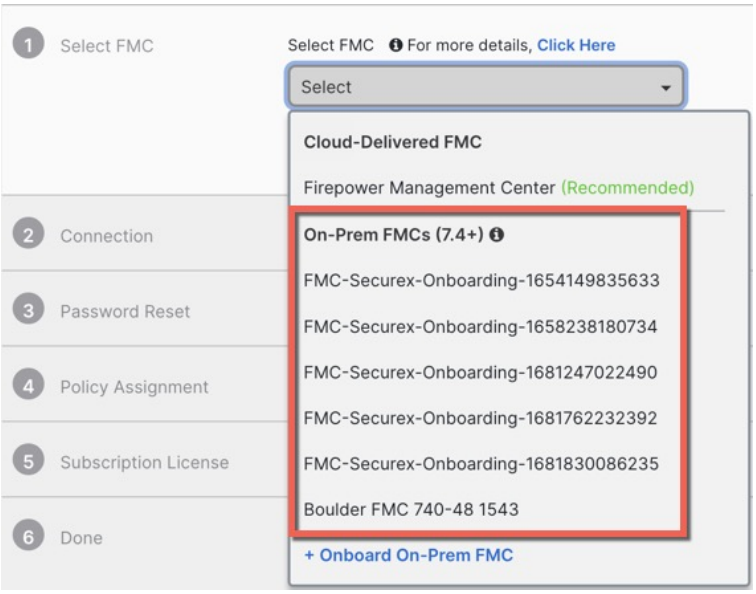
Step 3 On the **Onboard FTD Device** screen, click **Use Serial Number** .

Figure 13: Use Serial Number



Step 4 In **Select FMC** , choose an **On-Prem FMC** from the list, and click **Next** .

Figure 14: Select FMC



If the Firewall Management Center has a public IP address or FQDN set, it will show after you choose it.

Figure 15: Public IP Address/FQDN



The Firewall Management Center needs a public IP address/FQDN if the device does not have a public IP address/FQDN or if you use the Management interface for zero-touch provisioning . You can set the Firewall Management Center public IP address/FQDN by clicking the **FMC Public IP** link. You see the following dialog box.

Figure 16: Configure FMC Public IP/FQDN



Note For a Firewall Management Center high-availability pair, you also need to set the public IP address/FQDN on the secondary Firewall Management Center . You can't set value this using Security Cloud Control ; you need to set it in the secondary Firewall Management Center . See **System** > > **Configuration** > **Manager Remote Access** .

Step 5 In **Connection** , enter the device's serial number and device name. Click **Next** .

Figure 17: Connection

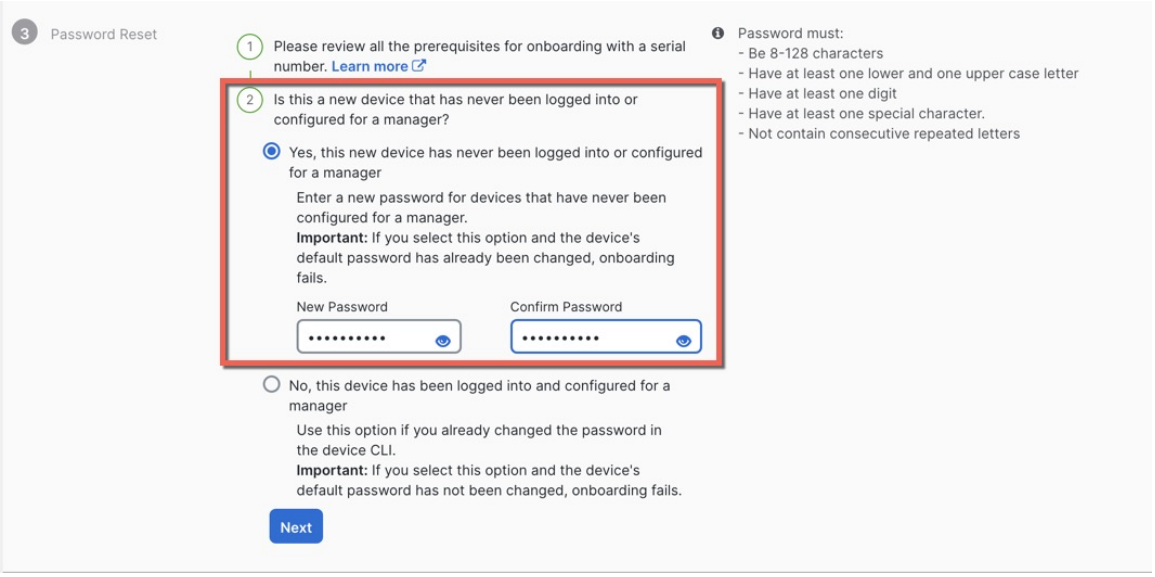


Step 6 In **Password Reset** , click **Yes...** . Enter a new password and confirm the new password for the device, then click **Next** .

For zero-touch provisioning , the device must be brand new or has been reimaged.

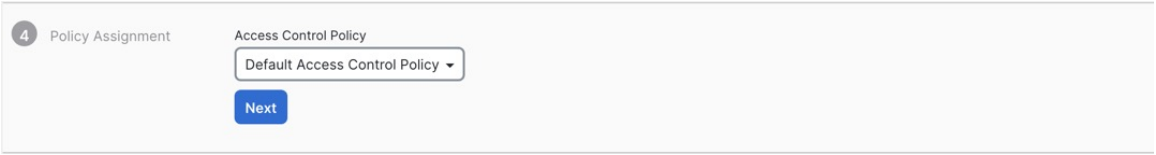
Note If you did log into the device and reset the password, and you did not change the configuration in a way that would disable zero-touch provisioning , then you should choose the **No...** option. There are a number of configurations that disable zero-touch provisioning , so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 18: Password Reset



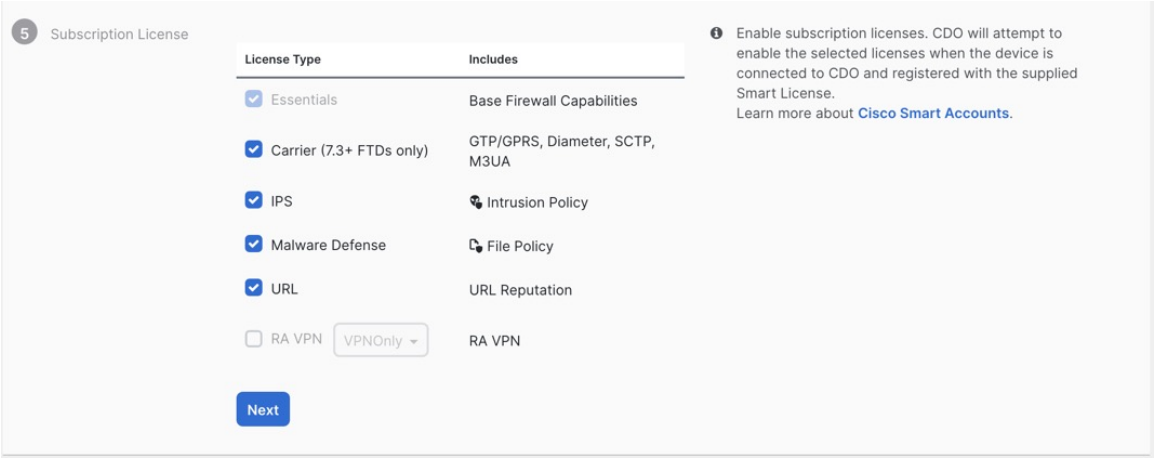
Step 7 In **Policy Assignment** , use the drop-down menu to select an access control policy for the device. If you have not added a policy on the Firewall Management Center , you should go to the Firewall Management Center and add one now. Click **Next** .

Figure 19: Policy Assignment



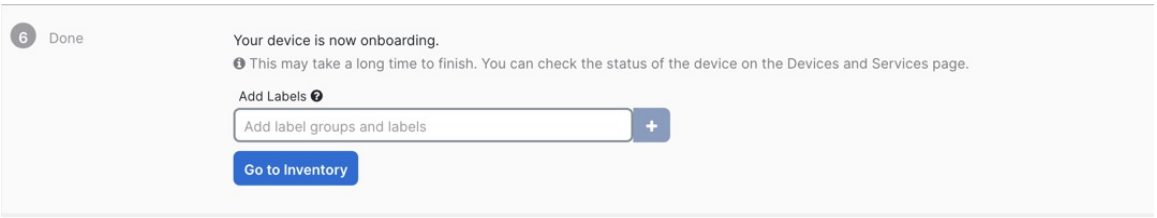
Step 8 In **Subscription License** , select the licenses for the device. Click **Next** .

Figure 20: Subscription License



Step 9 In **Done** , you can add labels to the device that show in Security Cloud Control ; they are not used on the Firewall Management Center .

Figure 21: Done



In the Firewall Management Center , the device is added to the **Device Management** page. You can also click **Go to Inventory** to see the devices in Security Cloud Control . On-prem Firewall Management Center devices are viewable in Security Cloud Control inventory for information purposes.

When using zero-touch provisioning on the outside interface, Security Cloud Control acts as a DDNS provider and does the following:

- Enables DDNS on outside using the "fmcOnly" method. This method is only supported for zero-touch provisioning devices.
- Maps the outside IP address with the following hostname: *serial-number* **.local** .

- Provides the IP address/hostname mapping to the Firewall Management Center so it can resolve the hostname to the correct IP address.
- Informs the Firewall Management Center if the IP address ever changes, for example, if the DHCP lease renews.

If you use zero-touch provisioning on the Management interface, DDNS is not supported. The Firewall Management Center must be publicly reachable so the device can initiate the management connection.

You can continue to use Security Cloud Control as the DDNS provider, or you can later change the DDNS configuration in the Firewall Management Center to a different method. See Configure Dynamic DNS, on page 838 for more information.

If the device fails to register, see Resolve serial number (zero-touch provisioning) registration issues, on page 47 .

Add a chassis

This task allows you to add a Firepower 4100/9300 chassis to the Firewall Management Center for chassis-level health monitoring and management.

You can add a Firepower 4100/9300 chassis to the Firewall Management Center. The management center and the chassis share a separate management connection using the chassis MGMT interface. The Firewall Management Center offers chassis-level health alerts. For configuration, you still need to use the Secure Firewall Chassis Manager or FXOS CLI.

Note For other models that support multi-instance mode, the manager configuration is completed as part of the conversion to multi-instance mode. See Enable multi-instance mode, on page 175. After you enable multi-instance mode, see Add a multi-instance chassis to the Firewall Management Center, on page 177.

Procedure

Step 1 Connect to the chassis FXOS CLI, either using the console port or SSH.

Step 2 Configure the Firewall Management Center.

create device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**NAT-ID** *nat_id*]

You are prompted for the registration key.

You can enter this command from any scope. This command is accepted immediately without using **commit-buffer**.

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the Firewall Management Center. At least one of the devices, either the Firewall Management Center or the chassis, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices. If you do not specify a **hostname**, then the chassis must have a reachable IP address or hostname and you must specify the **NAT-ID**.

- **NAT-ID** *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center when you register the chassis when one side does not specify a reachable IP address or hostname. It is required if you do not specify a **hostname**, however we recommend that you always set the NAT ID even when you specify a hostname or IP address. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.
- **Registration Key:** *reg_key*—You will be prompted for a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the chassis. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

Example:

```
firepower# create device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

Step 3 In the Firewall Management Center, add the chassis using the chassis management IP address or hostname.

a) Choose **Devices** > **Device Management**, and then from **Add** drop-down list, choose **Chassis**.

Figure 22: Add chassis

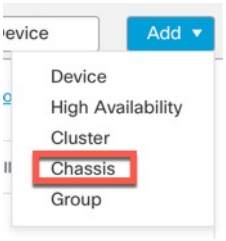
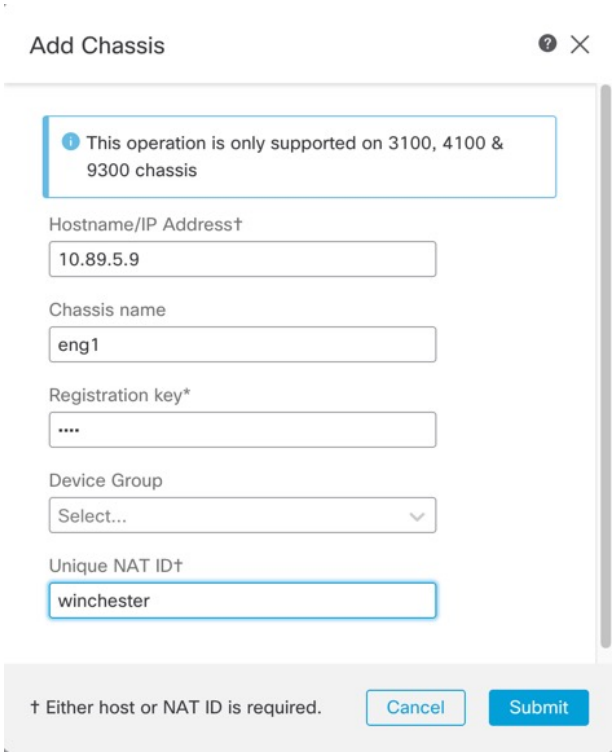


Figure 23: Add chassis



b) In the **Hostname/IP Address** field, enter the IP address or the hostname of the chassis you want to add.

If you don't know the hostname or IP address, you can leave this field blank specify the **Unique NAT ID**.

c) In the **Chassis Name** field, enter a name for the chassis as you want it to display in the Firewall Management Center.

d) In the **Registration Key** field, enter the same registration key that you used when you configured the chassis to be managed by the Firewall Management Center.

The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

e) In a multidomain deployment, regardless of your current domain, assign the chassis to a leaf **Domain**.

If your current domain is a leaf domain, the chassis is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the chassis. A chassis can only belong to one domain.

f) (Optional) Add the chassis to a **Device Group**.

g) If you used a NAT ID during chassis setup, expand enter the same NAT ID in the **Unique NAT ID** field.

The NAT ID can include alphanumeric characters and hyphens (-).

h) Click **Submit**.

The chassis is added to the **Devices** > **Device Management** page.

The chassis is successfully registered with the Firewall Management Center and appears in the device management interface for monitoring and management.

Register with a new management center

This procedure shows how to register with a new Firewall Management Center . You should perform these steps even if the new Firewall Management Center uses the old Firewall Management Center 's IP address.

Procedure

Step 1 On the old Firewall Management Center , if present, delete the managed device. See Delete (Unregister) a Device from the Firewall Management Center , on page 54 .

You cannot change the Firewall Management Center IP address if you have an active connection with the Firewall Management Center .

Step 2 Connect to the device CLI, for example using SSH.

Step 3 Configure the new Firewall Management Center .

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

- { *hostname* | *IPv4_address* | *IPv6_address* }—Sets the Firewall Management Center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE** —If the Firewall Management Center is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the Firewall Management Center , make sure that you specify both the device IP address and the *nat_id* ; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
- *regkey* —Make up a registration key to be shared between the Firewall Management Center and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the Firewall Management Center when you add the Firewall Threat Defense .
- *nat_id* —Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the Firewall Management Center and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the Firewall Management Center when you add the Firewall Threat Defense .
- *display_name* —Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying Security Cloud Control as the primary manager and an on-prem Firewall Management Center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
  - *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword)
  - **manager-** *timestamp*

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

Step 4 Add the device to the Firewall Management Center.

Resolve serial number (zero-touch provisioning) registration issues

If the device fails to register using the serial number after 2-3 minutes, see the common causes for failure. If you have physical access to the device, Check the LED status, on page 48

If you want to bypass any serial number troubleshooting, you can always use Add a Device Using a Registration Key , on page 32.

For other requirements for serial number registration, see Add a Device Using the Serial Number (Zero-Touch Provisioning) , on page 36.

"Waiting for Device to come Online" in Firewall Management Center

- **Cause**: You performed initial configuration at the CLI and unintentionally disabled zero-touch provisioning.

  Workaround: See Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning, on page 50.

- **Cause**: You performed initial configuration in the Firewall Device Manager and disabled zero-touch provisioning.

  Workaround: See Restart Zero-Touch Provisioning Using the Firewall Device Manager, on page 50.

- **Cause**: Zero-Touch Provisioning is disabled, and you don't have access to the CLI.

  Workaround: See Reset the Device, on page 52.

"A device with serial number <serial-number> already exists in the Security Cloud Control tenant" in Firewall Management Center

Cause: The serial number was already claimed by another manager in your tenant.

Workaround: If you already unregistered the device or you're unsure which Firewall Management Center has claimed it, then see Check for Changes in Security Cloud Control, on page 51. If the Firewall Management Center is offline, and you need to remove its claim, see Remove a Serial-Number Claim at the CLI, on page 48.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

"A device with serial number <serial-number> already exists in another Security Cloud Control tenant" in Firewall Management Center

Cause: The serial number was already claimed by another manager in another tenant.

Workaround: See Remove a Serial-Number Claim at the CLI, on page 48.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

Check the LED status

The LED status tells you about zero-touch provisioning readiness.

Firepower 1010, 1100

Table 3: Zero-Touch Provisioning: System (S) LED behavior

S LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00

Secure Firewall 1200, 3100

Table 4: Zero-Touch Provisioning: Managed (M) LED behavior

M LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00
Solid green	Onboarded	20:00 - 45:00

Remove a Serial-Number Claim at the CLI

If the device was claimed previously, but the management connection is not active, you can clear the claim. In the Firewall Management Center , you will see an error message such as **A device with serial number <serial-number> already exists in the Security Cloud Control tenant**.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

Procedure

Step 1 Connect to the FXOS CLI using SSH or the console port. See Log into the Command-Line Interface on the device, on page 13 for more information.

If you used SSH, you connect to the Firewall Threat Defense CLI. In this case, enter **connect fxos** .

Note If you are accessing the Firewall Threat Defense CLI for the first time and have to run through the setup script, answer **n** when prompted: `Do you want to configure IPv4? (y/n) [y]:` and `Do you want to configure IPv6? (y/n) [y]:` . You also must accept the default local manager: `Manage the device locally? (yes/no) [yes]:` . These settings will preserve zero-touch provisioning capability.

If you used the console port, you connect directly to FXOS.

If this is the first time you connect to the CLI using either SSH or the console, you are prompted to change the password. For zero-touch provisioning when you onboard the device, for the **Password Reset** area, be sure to choose **No** because you already set the password.

```
> connect fxos
firepower#
```

Step 2 Enter local management.

connect local-mgmt

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

Step 3 Deregister the device from the Cisco cloud.

cloud deregister

```
firepower(local-mgmt)# cloud deregister
Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Step 4 Erase the configuration to restore cloud connectivity.

erase configuration

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

What to do next

-

Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning

-

If you performed initial CLI setup and set the device to remote management, you can re-enable zero-touch provisioning by deleting the manager and re-adding the local manager. This setting doesn't mean you are intending to use the local manager; it just restores functionality required for zero-touch provisioning . Even if you set the manager to local, if you logged into Firewall Device Manager and completed initial setup, you may have disabled zero-touch provisioning . Deleting and re-adding the local manager will restore zero-touch provisioning .

Note You can only delete the manager if there is no current Firewall Management Center management connection.

Before you begin

-

Procedure

Step 1 Check the management status.

show managers

```
> show managers
No managers configured.
```

In this case, you opted for remote management but did not configure a Firewall Management Center . You need to set the manager to local.

```
> show managers
Managed locally.
```

This output shows you are already running the local manager. Even in this case, deleting the manager restores necessary services for zero-touch provisioning .

Step 2 Delete the manager.

configure manager delete

Step 3 Add the local manager.

configure manager local

What to do next

-

Restart Zero-Touch Provisioning Using the Firewall Device Manager

You can unintentionally disable low-touch provisioning if you log into the Firewall Device Manager and complete the initial setup in Firewall Device Manager . In this case, you can restart zero-touch provisioning

within the Firewall Device Manager . If you have access to the CLI, you can alternatively Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning, on page 50 .

Procedure

Step 1 In the Firewall Device Manager , click **Device** , then click the **System Settings** > **Cloud Services** .

Step 2 Check **Auto-enroll with** Security Cloud Control **or Secure Firewall Management Center** .

Step 3 Click **Register** .

Check for Changes in Security Cloud Control

If you unregister the device from a Firewall Management Center , the claim on the serial number should be removed automatically. However, in rare cases if the claim is still active, you can force Security Cloud Control to remove the device from your inventory.

Before you begin

-

Procedure

Step 1 Log into Security Cloud Control at https://security.cisco.com.

Step 2 Choose **Security Devices** , and then search for your serial number.

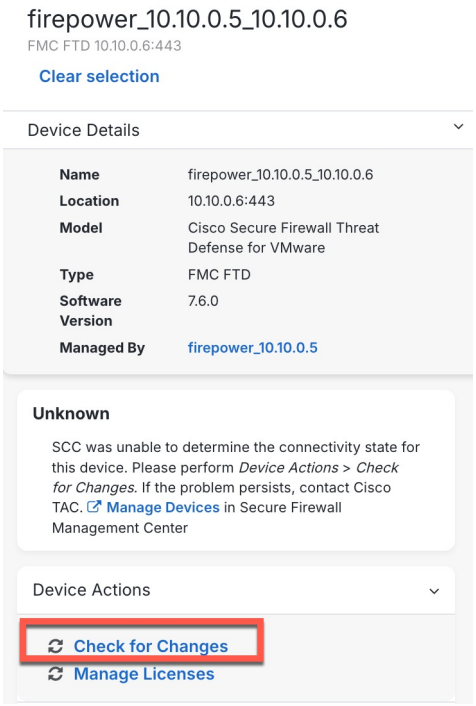
Figure 24: Search by Serial Number



If the device did not appear in the search results, it may be registered to a different tenant. In this case, see Remove a Serial-Number Claim at the CLI, on page 48.

Step 3 Select the device and click **Check for Changes** on the right.

Figure 25: Check for Changes



If the device was unregistered, it will disappear from the list and the device will attempt to connect to the cloud again.

If the device does not disappear, that means it's registered to another manager in the tenant. The name of the device includes the manager it is registered to, for example, **firepower_10.89.5.36**_1010-1. If you still want to register the device to a different manager, and you don't have access to the Firewall Management Center to unregister it, you can Remove a Serial-Number Claim at the CLI, on page 48 , but only if there is not an active management connection.

Reset the Device

Supported for the following models:

- Firepower 1010
- Firepower 1100
- Secure Firewall 3100

If you do not have access to the CLI and want to make sure your device is unconfigured and ready for zero-touch provisioning , reset the device to its default state.

Procedure

Step 1 Press the small, recessed Reset button for longer than five seconds.

See your hardware installation guide for more information. It can take a long time to start Firewall Threat Defense for the first time after a reset.

Step 2 Check the LED status, on page 48 to monitor when the device is zero-touch provisioning -ready.

Register with a new management center

This procedure shows how to register with a new Firewall Management Center . You should perform these steps even if the new Firewall Management Center uses the old Firewall Management Center 's IP address.

Procedure

Step 1 On the old Firewall Management Center , if present, delete the managed device. See Delete (Unregister) a Device from the Firewall Management Center , on page 54 .

You cannot change the Firewall Management Center IP address if you have an active connection with the Firewall Management Center .

Step 2 Connect to the device CLI, for example using SSH.

Step 3 Configure the new Firewall Management Center .

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

- { *hostname* | *IPv4_address* | *IPv6_address* }—Sets the Firewall Management Center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE** —If the Firewall Management Center is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the Firewall Management Center , make sure that you specify both the device IP address and the *nat_id* ; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
- *regkey* —Make up a registration key to be shared between the Firewall Management Center and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the Firewall Management Center when you add the Firewall Threat Defense .
- *nat_id* —Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the Firewall Management Center and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the Firewall Management Center when you add the Firewall Threat Defense .
- *display_name* —Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying Security Cloud Control as the primary manager and an on-prem Firewall Management Center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
  - *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword)

- **manager-** *timestamp*

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

Step 4 Add the device to the Firewall Management Center.

Delete (Unregister) a Device from the Firewall Management Center

If you no longer want to manage a device, you can unregister it from the Firewall Management Center .

To unregister a cluster, cluster node, or high availability pair, see the chapters for those deployments.

Unregistering a device:

- Severs all communication between the Firewall Management Center and the device.
- Removes the device from the **Device Management** page.
- Returns the device to local time management if the device's platform settings policy is configured to receive time from the Firewall Management Center using NTP.
- Leaves the configuration intact, so the device continues to process traffic.

  Policies, such as NAT and VPN, ACLs , and the interface configurations remain intact.

Registering the device again to the same or a different Firewall Management Center causes the configuration to be removed, so the device will stop processing traffic at that point.

Before you delete the device, be sure to export the configuration so you can re-apply the device-level configuration (interfaces, routing, and so on) when you re-register it. If you do not have a saved configuration , you will have to re-configure device settings.

After you re-add the device and either import a saved configuration or re-configure your settings, you need to deploy the configuration before it starts passing traffic again.

Before you begin

To re-apply the device-level configuration if you re-add it to the Firewall Management Center :

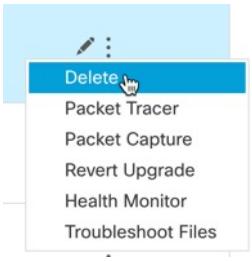
- Export the device configuration. See Export and import the device configuration, on page 751 .

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 Next to the device you want to unregister, click **More** (⋮) , and then click **Delete** .

Figure 26: Delete



Step 3 Confirm that you want to unregister the device.

Step 4 You can now change your manager.

- Re-register the device to this Firewall Management Center —If you know the registration key and NAT ID, refer to Add a Device Using a Registration Key , on page 32 . If you need to reset them, you can reconfigure the manager as though it's new. See Register with a new management center, on page 46 .
- Register to a new Firewall Management Center — Register with a new management center, on page 46 .
- Change to the Firewall Device Manager — Switch from Firewall Management Center to Firewall Device Manager , on page 65 .
- Delete the manager without specifying a new one—To sever the management connection on the Firewall Threat Defense without identifying a new manager (no manager mode), from the Firewall Threat Defense CLI use the **configure manager delete** command.

Shut down or restart the device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall.

See the following task to shut down or restart your system properly.

Note After restarting your device, you may see an error that the management connection could not be reestablished. In some cases, the connection is attempted before the Management interface on the device is ready. The connection will be retried automatically and should come up within 15 minutes.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that you want to restart, click **Edit** ( ) .

Step 3 Click **Device**.

Step 4 To restart the device:

a) Under **System**, click **Restart Device** ( ) .
b) When prompted, confirm that you want to restart the device.

Step 5 To shut down the device:

a) Under **System**, click **Shut Down Device** ( ) in the **System** section.
b) When prompted, confirm that you want to shut down the device.
c) If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

For the ISA 3000, when shutdown is complete, the System LED will turn off. Wait at least 10 seconds before you remove the power.

Download the managed device list

You can download a report of all the managed devices.

Before you begin

To perform the following task, you must be an Admin user.

Procedure

Step 1 Choose **Devices** > **Device Management** .

Step 2 Click the **Download Device List Report** link.

Step 3 You can download the device list in CSV or PDF format. Choose **Download CSV** or **Download PDF** to download the report.

Migrate Firewall Threat Defense devices

The Secure Firewall Threat Defense model migration wizard enables you to migrate configurations from an earlier Firewall Threat Defense model. After the migration, all routing and interface configurations from the source Firewall Threat Defense device are available in the target Firewall Threat Defense.

Supported devices and capabilities

The wizard supports multiple models as source and target devices, for more information see Supported Devices for Migration, on page 57.

Supported Devices for Migration

Documents the supported migration paths and device compatibility for Cisco Firepower and Secure Firewall models.

License for Firewall Threat Defense migration

You must meet licensing requirements for Firewall Threat Defense migration.

- Your Smart Licensing account must have the license entitlements for the target device.
- You must register and enroll the device with the Smart Licensing account. The migration copies the source device licenses to the target device.

Prerequisites for migration

This reference provides comprehensive prerequisites that must be satisfied to successfully migrate configurations from a source device to a target device in Secure Firewall Management Center environments.

General device prerequisites

- Register the source and the target devices to the Firewall Management Center.
- Ensure that the target device is a newly registered device without any configurations.
- Source and target devices must be in the same state and modes:
  - Domain
  - Firewall mode: Routed or Transparent
  - Compliance mode (CC or UCAPL)
- Ensure that you have permission for modifications on the devices.
- Ensure that the configurations on the source device are valid and have no errors.
- Deployment, import, or export tasks must not run on either of the devices during the migration. The source device can have pending deployments.

Prerequisites for HA devices

Configurations that the wizard migrates

The migration wizard copies configurations from the source device to the target device, including licenses, interfaces, policies, routing settings, and other essential device configurations.

General configurations

The migration wizard copies these configurations from the source device to the target device:

- Licenses
- Interface configurations
- Inline sets configurations
- Routing configurations
- DHCP and DDNS configurations
- Policies
- Associated objects and object overrides
- Platform settings
- Remote branch deployment configurations

Policy configurations

The migration wizard copies these policy configurations from the source device to the target device:

- Health policy
- NAT and QoS policy
- Remote access VPN policy
- FlexConfig policy
- Access control and prefilter policy
- IPS and DNS policy
- Malware and File policy
- SSL and Identity policy

Routing configurations

The migration wizard copies these routing configurations from the source device to the target device:

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- Policy Based Routing
- Static and Multicast Route
- Virtual Router

Interface configurations

The migration wizard copies these interfaces from the source device to the target device:

- Physical interfaces
- Sub-interfaces
- EtherChannel interfaces
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces

The migration wizard retains the device group of the target device.

Guidelines and limitations for migration

Follow these guidelines to ensure successful migration of secure firewall threat defense models:

- **For devices in multi-instance mode**:

  During migration, ensure that you map the interfaces according to the table below:

Source Device	Target Device
Physical interface	Physical interface
EtherChannel interface	EtherChannel interface
Supervisor-provisioned subinterface	Supervisor-provisioned subinterface
Tagged interface	Tagged interface
Untagged interface	Untagged interface
Shared interface	Shared and dedicated interface
Dedicated interface	Dedicated interface

  You cannot map a supervisor-provisioned subinterface to a subinterface created by an instance.

- **For HA devices**, you can migrate:
  - Source HA device to target HA device.
  - Source HA device to target standalone device.

- **For devices in remote branch deployment**:
  - Map the source manager access interface to the target manager access interface.
  - Ensure that the manager access interfaces of the source and target Firewall Management Centers are of the same IP address type (static or DHCP).
  - Both manager access interfaces must have IPv4 or IPv6 addresses.

    - If the manager access interfaces have static IP addresses, ensure that they are in the same subnet.

- **For Snort**:
- **For devices using diagnostic interfaces**:

  Only merged management interfaces are available on the target devices after migration.

Limitations

Be aware of these limitations when using the migration wizard:

- The migration wizard does not migrate:
    - Site-to-site VPN policies
- You can perform only one migration at a time.
- Remote access VPN trustpoint certificates are not enrolled after migration.
- For HA devices:
    - Target device: You cannot migrate a standalone device to an HA device.

Best practices for Threat Defense device migration

After a successful migration, perform these actions before deployment to ensure proper device configuration and functionality.

- IP addresses of the interfaces are copied to the target device from the source device. Change the IP addresses of the target device interfaces if the source device is live
- Ensure that you update your NAT policies with the modified IP addresses.
- Configure the interface speeds if they are set to default values after migration.
- Re-enroll the device certificates, if any, on the target device.
- (Optional) Configure SNMP for Firepower 1100 and 2100 using the platform settings for the device.
- (Optional) Configure remote branch deployments.

  If the source or target device had manager access through a data interface, after the migration, the manager access will be lost. Update the manager access configuration on the target device. For more information, see the *Change the Manager Access Interface from Management to Data* topic in the Cisco Secure Firewall Management Center Device Configuration Guide or the Online Help.
- Configure site-to-site VPN, if required. These configurations are not migrated from the source device.
- View the deployment preview before the deployment. From the **Deploy** drop-down menu, click **Advanced Deploy**, and then click the **Preview** ( ) icon for the device.
- Monitor the health of the device in the health monitor (choose **System** ( ) > **Health** > **Monitor**). After migration, the health policy of the source device becomes the health policy of the target device. You can also configure a new health policy for the device.

After migration, the device monitoring dashboard may temporarily display redundant colored lines because the device has different UUIDs before and after migration. This redundancy appears only during the migration time. An hour after migration, the dashboard will show a single line per metric.

Switch managers

You can change between managers as needed.

Switch from the Firewall Device Manager to the Firewall Management Center

When you switch from the Firewall Device Manager to the Firewall Management Center, all interface configuration is retained, in addition to the Management interface and the manager access settings. Note that other configuration settings, such as the access control policy or security zones, are not retained.

After you switch to the Firewall Management Center , you can no longer use the Firewall Device Manager to manage the Firewall Threat Defense device.

Procedure

Step 1 In the Firewall Device Manager, unregister the device from the Cisco Smart Software Manager.

Step 2 (Might be required) Configure the Management interface.

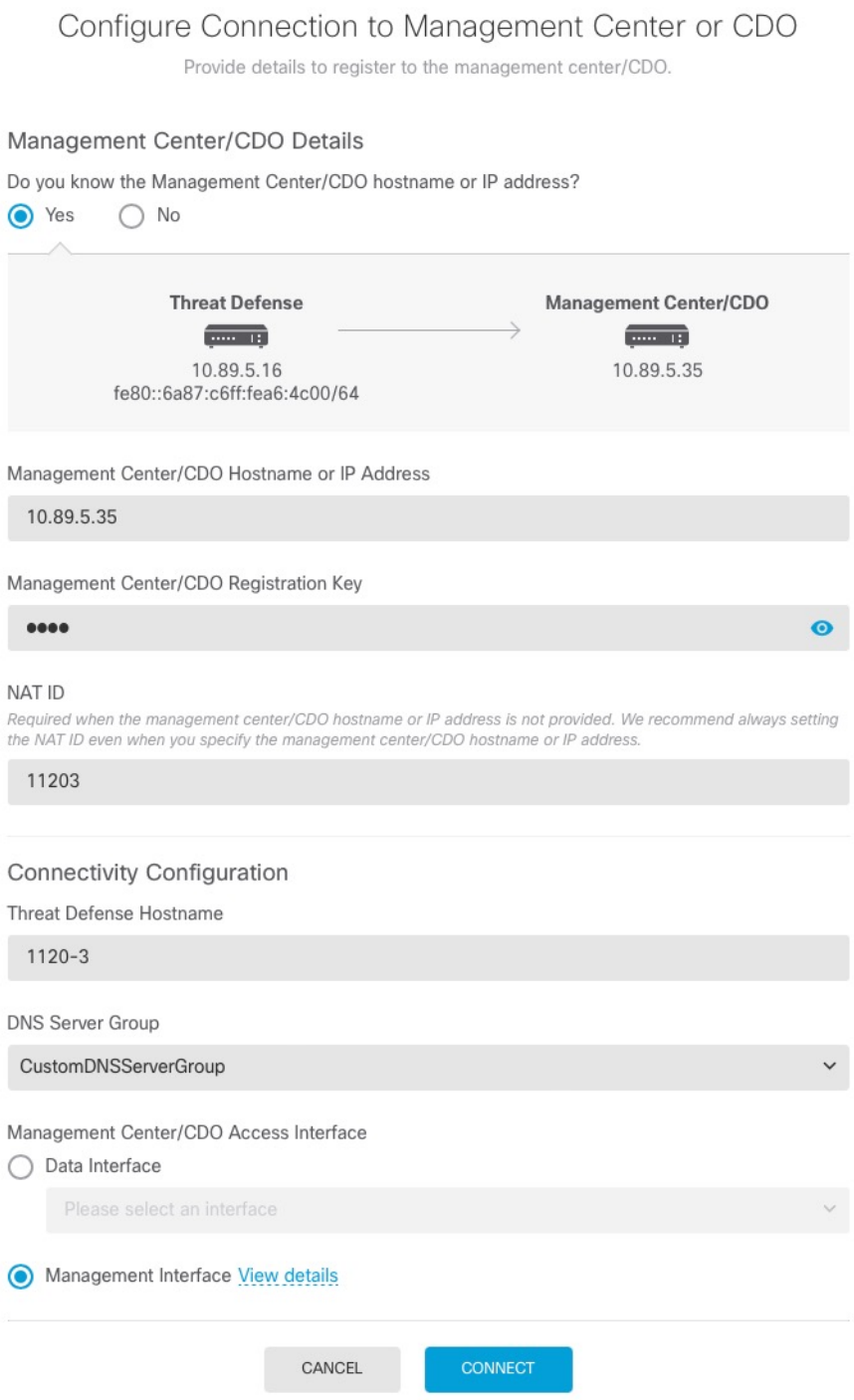
You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

Step 3 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

Step 4 Configure the **Management Center/CDO Details**.

Figure 27: Management Center/Security Cloud Control Details



a) For **Do you know the Management Center/CDO hostname or IP address?**, click **Yes** if you can reach the Firewall Management Center using an IP address or hostname, or **No** if the Firewall Management CenterSecurity Cloud Control is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/CDO Hostname or IP Address**.

c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

Step 5 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/CDO Access Interface** access, then this FQDN will be used for this interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/CDO Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall Management Center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense device that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/CDO Access InterfaceFMC Access Interface**, then this setting configures the Management DNS server.

c) For the **Management Center/CDO Access Interface**, choose any configured interface.

You can change the manager interface after you register the Firewall Threat Defense device to the Firewall Management Center, to either the Management interface or another data interface.

Step 6 (Optional) If you chose a data interface, and it was not the outside interface, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the Firewall Management Center.

If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.

Step 7 (Optional) If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

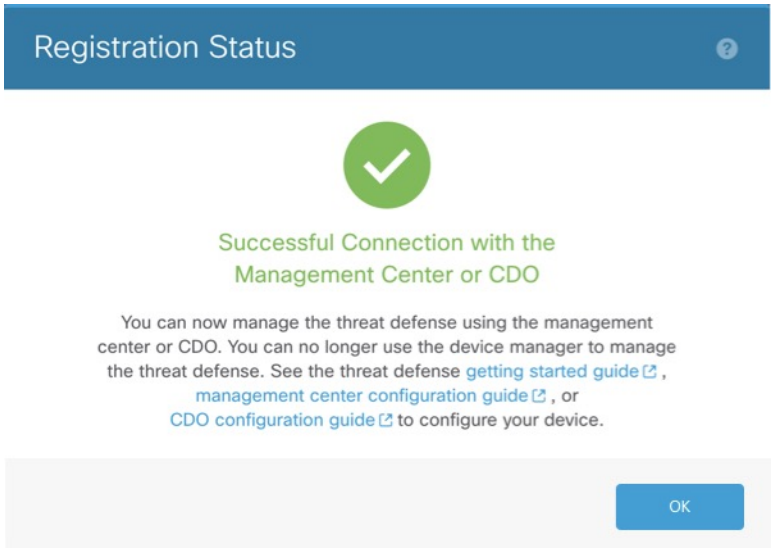
DDNS is not supported when using the Management interface for manager access.

Step 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/CDO Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall Device Manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center/CDO** dialog box, after which you will be disconnected from the Firewall Device Manager.

Figure 28: Successful Connection



Switch from Firewall Management Center to Firewall Device Manager

You can configure the Firewall Threat Defense device currently being managed by the on-premises or cloud-delivered Firewall Management Center to use the Firewall Device Manager instead.

You can switch from the Firewall Management Center to the Firewall Device Manager without reinstalling the software. Before switching from the Firewall Management Center to the Firewall Device Manager, verify that the Firewall Device Manager meets all of your configuration requirements. If you want to switch from the Firewall Device Manager to the Firewall Management Center, see Switch from the Firewall Device Manager to the Firewall Management Center , on page 61.

Caution Switching to the Firewall Device Manager erases the device configuration and returns the system to the default configuration. However, the Management IP address and hostname are preserved.

Procedure

Step 1 In the Firewall Management Center, delete the firewall from the **Devices** > **Device Management** page.

Step 2 Connect to the Firewall Threat Defense CLI using SSH or the console port. For SSH, open a connection to the **management IP address**, and log in to the Firewall Threat Defense CLI with the **admin** username (or any other user with admin privileges).

The console port defaults to the FXOS CLI. Connect to the Firewall Threat Defense CLI using the **connect ftd** command. The SSH session connects directly to the Firewall Threat Defense CLI.

If you cannot connect to the management IP address, do one of the following:

- Ensure that the management physical port is wired to a functioning network.
- Ensure that the management IP address and gateway are configured for the management network. Use the **configure network ipv4/ipv6 manual** command.

Step 3 Verify you are currently in remote management mode.

show managers

Example:

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Display name              : 10.89.5.35
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

Step 4 Delete the remote manager and go into no manager mode.

configure manager delete *uuid*

You cannot go directly from remote management to local management. If you have more than one manager defined, you need to specify the identifier (also known as the UUID; see the **show managers** command). Delete each manager entry separately.

Example:

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

Step 5 Configure the local manager.

configure manager local

You can now use a web browser to open the local manager at *https://management-IP-address*.

Example:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

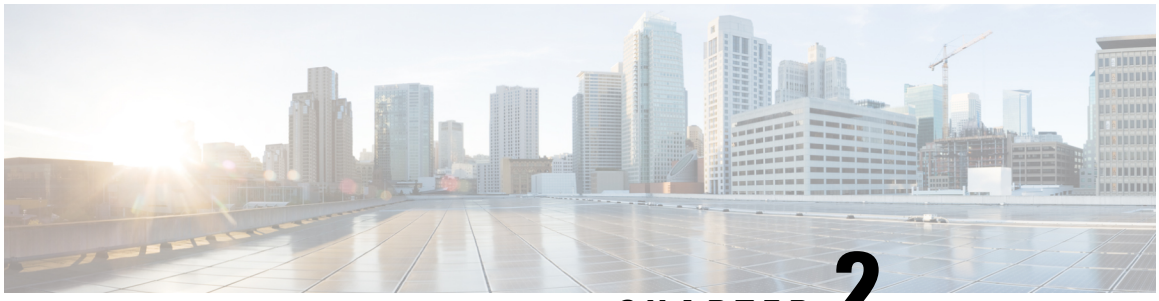
History for device registration

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	7.4.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the Firewall Management Center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the Firewall Management Center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Devices** > **Device Management** > **Add** > **Chassis**
Zero-Touch Provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the Firewall Management Center using a serial number.	7.4.0	Mgmt. center *is* publicly reachable: 7.2.0 Mgmt. center *is not* publicly reachable: 7.2.4/7.4.0	Zero-Touch Provisioning (also called low-touch provisioning) lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with SecureX and Security Cloud Control for this functionality. New/modified screens: **Devices** > **Device Management** > **Add** > **Device** > **Serial Number**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence**
Migrate Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E.
Download a report of all registered devices.	7.4.0	Any	You can now download a report of all registered devices. On **Devices** > **Device Management** , click the new **Download Device List Report** link, at the top right of the page.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Manage Firewall Threat Defense high availability pairs using a data interface.	7.4.0	7.4.0	Firewall Threat Defense high availability now supports using a regular data interface for communication with the Firewall Management Center. Previously, only standalone devices supported this feature. See: Device Management
ISA 3000 System LED support for shutting down.	7.0.5/7.3.0	7.0.5/7.3.0	When you shut down the ISA 3000, the System LED will turn off. You should wait at least 10 seconds before removing the power.
ISA 3000 support for shutting down.	7.0.2/7.2.0	7.0.2/7.2.0	You can now shut down the ISA 3000; previously, you could only reboot the device.
Multi-manager support.	7.2.0	7.2.0	We introduced the cloud-delivered management center. The cloud-delivered management center uses the Security Cloud Control (Security Cloud Control) platform and unites management across multiple Cisco security solutions. We take care of manager updates. Hardware or virtual management centers running Version 7.2+ can "co-manage" cloud-managed devices, but for event logging and analytics purposes only. You cannot deploy policy to these devices from the hardware or virtual management center. New/modified commands: **configure manager add** , **configure manager delete** , **configure manager edit** , **show managers** New/modified screens: • When you add a cloud-managed device to a hardware or virtual management center, use the new Security Cloud Control Managed Device check box to specify that it is analytics-only. • View which devices are analytics-only on **Devices** > **Device Management** . For more information, see Security Cloud Control documentation.
RAID support for SSDs on the Secure Firewall 3100.	7.1.0	7.1.0	The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. New/modified commands: **configure raid, show raid, show ssd**
Support for TLS 1.3 for the management connection.	7.1.0	7.1.0	The FMC-device management connection now uses TLS 1.3. Previously, TLS 1.2 was supported.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Use FDM to configure FTD for management by the FMC.	7.1.0	7.1.0	When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and manager access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FMC CLI, only the Management and manager access settings are retained (for example, the default inside interface configuration is not retained). After you switch to FMC, you can no longer use FDM to manage FTD. New/modified FDM screens: **System Settings** > **Management Center**
Filter devices by upgrade status.	6.7.0	6.7.0	The **Device Management** page now provides upgrade information about your managed devices, including whether a device is upgrading (and what its upgrade path is), and whether its last upgrade succeeded or failed. New/modified screens: **Devices** > **Device Management**
One-click access to the Firepower Chassis Manager.	6.4.0	6.4.0	For Firepower 4100/9300 series devices, the Device Management page provides a link to the Firepower Chassis Manager web interface. New/modified screens: **Devices** > **Device Management**
Filter devices by health and deployment status; view version information.	6.2.3	6.2.3	The Device Management page now provides version information for managed devices, as well as the ability to filter devices by health and deployment status. New/modified screens: **Devices** > **Device Management**



CHAPTER 2

Transparent or Routed Firewall Mode

This chapter describes how to set the firewall mode to routed or transparent, as well as how the firewall works in each firewall mode.

Note The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes. See Inline Sets and Passive Interfaces, on page 727 for more information about IPS-only interfaces. Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode described in this chapter or the firewall-type interfaces.

Caution

- Use FTD CLI commands to set "Firewall Mode."

- Firewall mode, on page 71
- Default settings, on page 81
- Guidelines for firewall mode, on page 81
- Set the firewall mode, on page 82

Firewall mode

A Firewall Threat Defense device supports two firewall modes for regular firewall interfaces:

- Routed Firewall mode
- Transparent Firewall mode

Routed firewall mode

In routed mode, the Firewall Threat Defense device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet.

Integrated routing and bridging features

With Integrated Routing and Bridging, you can use a "bridge group" where you group together multiple interfaces on a network, and the Firewall Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. The Firewall Threat Defense device routes between BVIs and regular routed interfaces. If you do not need clustering or EtherChannel member interfaces, you might consider using routed mode instead of transparent mode. In routed mode, you can have one or more isolated bridge groups like in transparent mode, but also have normal routed interfaces as well for a mixed deployment.

Transparent firewall mode

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.

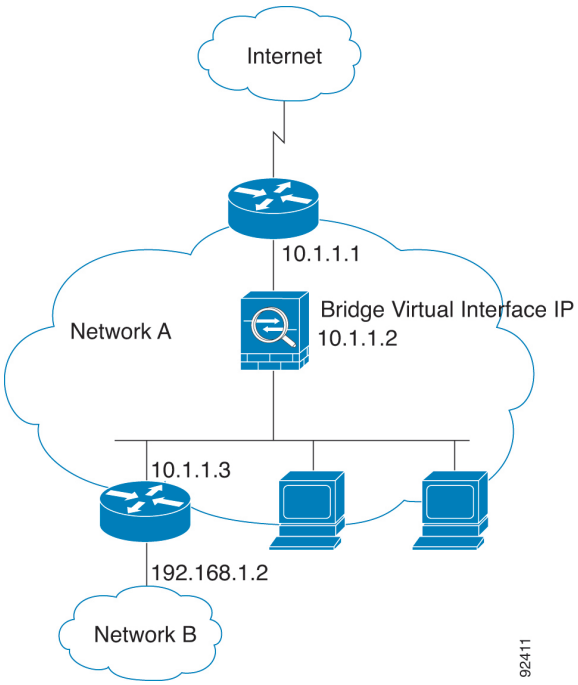
Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the Firewall Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

Transparent firewall network usage

The Firewall Threat Defense device connects the same network between its interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network.

The figure shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

Figure 29: Transparent firewall network



Passing traffic for routed-mode features

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality.

Supported traffic types

For example, by using an access rule, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV. You can also establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an access rule. Likewise, protocols like HSRP or VRRP can pass through the Firewall Threat Defense device.

Bridge groups

A bridge group is a group of interfaces that the Firewall Threat Defense device bridges instead of routes. Bridge groups are supported in both transparent and routed firewall mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Bridge virtual interfaces

Each bridge group includes a Bridge Virtual Interface (BVI). The Firewall Threat Defense device uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

BVI functionality by mode

In transparent mode: Only bridge group member interfaces are named and can be used with interface-based features.

In routed mode: The BVI acts as the gateway between the bridge group and other routed interfaces. To route between bridge groups/routed interfaces, you must name the BVI. For some interface-based features, you can use the BVI itself:

- DHCPv4 server—Only the BVI supports the DHCPv4 server configuration.
- Static routes—You can configure static routes for the BVI; you cannot configure static routes for the member interfaces.
- Syslog server and other traffic sourced from the Firewall Threat Defense device—When specifying a syslog server (or SNMP server, or other service where the traffic is sourced from the Firewall Threat Defense device), you can specify either the BVI or a member interface.

If you do not name the BVI in routed mode, then the Firewall Threat Defense device does not route bridge group traffic. This configuration replicates transparent firewall mode for the bridge group. If you do not need clustering or EtherChannel member interfaces, you might consider using routed mode instead. In routed mode, you can have one or more isolated bridge groups like in transparent mode, but also have normal routed interfaces as well for a mixed deployment.

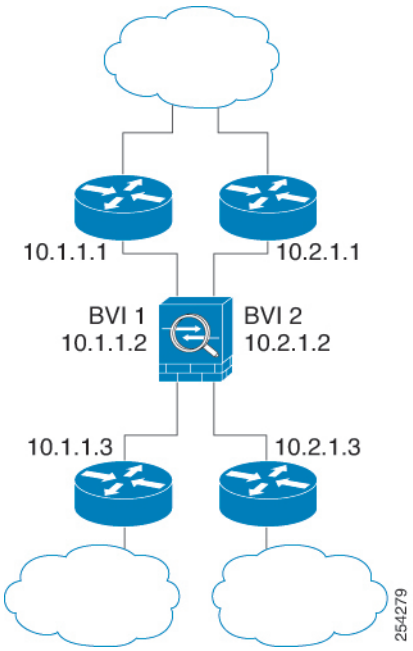
Bridge groups in transparent firewall mode

Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the Firewall Threat Defense device , and traffic must exit the Firewall Threat Defense device before it is routed by an external router back to another bridge group in the Firewall Threat Defense device. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration.

You can include multiple interfaces per bridge group. See Guidelines for firewall mode, on page 81 for the exact number of bridge groups and interfaces supported. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.

This figure shows two networks connected to the Firewall Threat Defense device, which has two bridge groups.

Figure 30: Transparent firewall network with two bridge groups



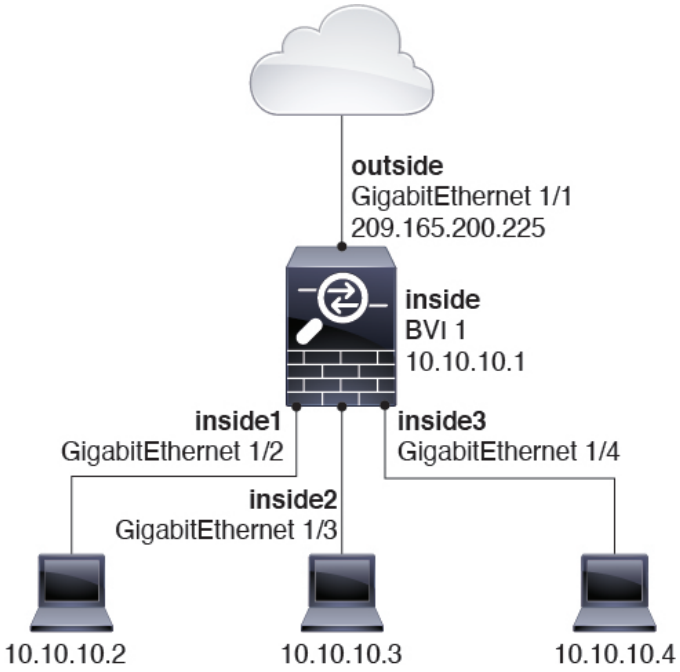
Bridge groups in routed firewall mode

Bridge group traffic can be routed to other bridge groups or routed interfaces. You can choose to isolate bridge group traffic by not assigning a name to the BVI interface for the bridge group. If you name the BVI, then the BVI participates in routing like any other regular interface.

Bridge group usage and configuration

One use for a bridge group in routed mode is to use extra interfaces on the Firewall Threat Defense instead of an external switch. For example, the default configuration for some devices include an outside interface as a regular interface, and then all other interfaces assigned to the inside bridge group. Because the purpose of this bridge group is to replace an external switch, you need to configure an access policy so all bridge group interfaces can freely communicate.

Figure 31: Routed firewall network with an inside bridge group and an outside routed interface



Allow layer 3 traffic

This topic describes how different types of Layer 3 traffic are handled through bridge groups and the access rule requirements for each traffic type.

- Unicast IPv4 and IPv6 traffic requires an access rule to be allowed through the bridge group.
- ARPs are allowed through the bridge group in both directions without an access rule. ARP traffic can be controlled by ARP inspection.
- IPv6 neighbor discovery and router solicitation packets can be passed using access rules.
- Broadcast and multicast traffic can be passed using access rules.

Allowed MAC addresses

These destination MAC addresses are allowed through the bridge group if allowed by your access policy (For more information, refer to Allow layer 3 traffic, on page 76). Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD

BPDUs handling

To prevent loops using the Spanning Tree Protocol, BPDUs are passed by default.

By default BPDUs are also forwarded for advanced inspection, which is unnecessary for this type of packet, and which can cause problems if they are blocked due to an inspection restart, for example. We recommend that you always exempt BPDUs from advanced inspection. To do so, use FlexConfig to configure an EtherType ACL that trusts BPDUs and exempts them from advanced inspection on each member interface.

The FlexConfig object should deploy the following commands, where you replace <if-name> with an interface name. Add as many access-group commands as needed to cover each bridge group member interface on the device. You can also choose a different name for the ACL.

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC address and route lookups

For traffic within a bridge group, the outgoing interface of a packet is determined by performing a destination MAC address lookup instead of a route lookup.

Route lookups, however, are necessary for these situations:

- Traffic originating on the Firewall Threat Defense device—Add a default/static route on the Firewall Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- SSL policy enabled in transparent firewall mode—
  - TLS 1.3 traffic passes through the Firewall Threat Defense device device.
  - Firewall Threat Defense device acts as a TCP proxy. It terminates the client-side TCP connection and initiates a separate server-side connection. The Firewall Threat Defense device TCP stack owns the session state.
  - For idle proxied sessions, Firewall Threat Defense device generates TCP ACK keepalive probes to preserve the connection state. These are not passthrough packets—the firewall originates them and sends them toward the client or server depending on the state of the TLS transit connection.
  - Because the Firewall Threat Defense device originates these keepalives, it must perform an adjacency table lookup (next-hop or egress MAC resolution) even in transparent mode.
  - If the adjacency lookup fails for one of these proxy-generated packets, the Firewall Threat Defense device logs syslog 110003.

    To prevent these syslog messages, configure routes on the Firewall Threat Defense device for the transit connection endpoints (client and server IP addresses). Proper routing enables successful adjacency lookups for keepalive packets.

    If the Firewall Threat Defense device successfully sends a TCP keepalive and receives a reply, it keeps the transit connection active. If the device cannot send the keepalives, or receives no reply, it removes the transit connection after approximately 240 seconds.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away—Add a static route on the Firewall Threat Defense device for traffic destined for the remote endpoint so that secondary connections are successful. The Firewall Threat Defense device creates a temporary "pinhole" in the access control policy to allow the secondary connection; and because the connection might use a different set of IP addresses than the primary connection, the Firewall Threat Defense device needs to perform a route lookup to install the pinhole on the correct interface.

Affected applications include:

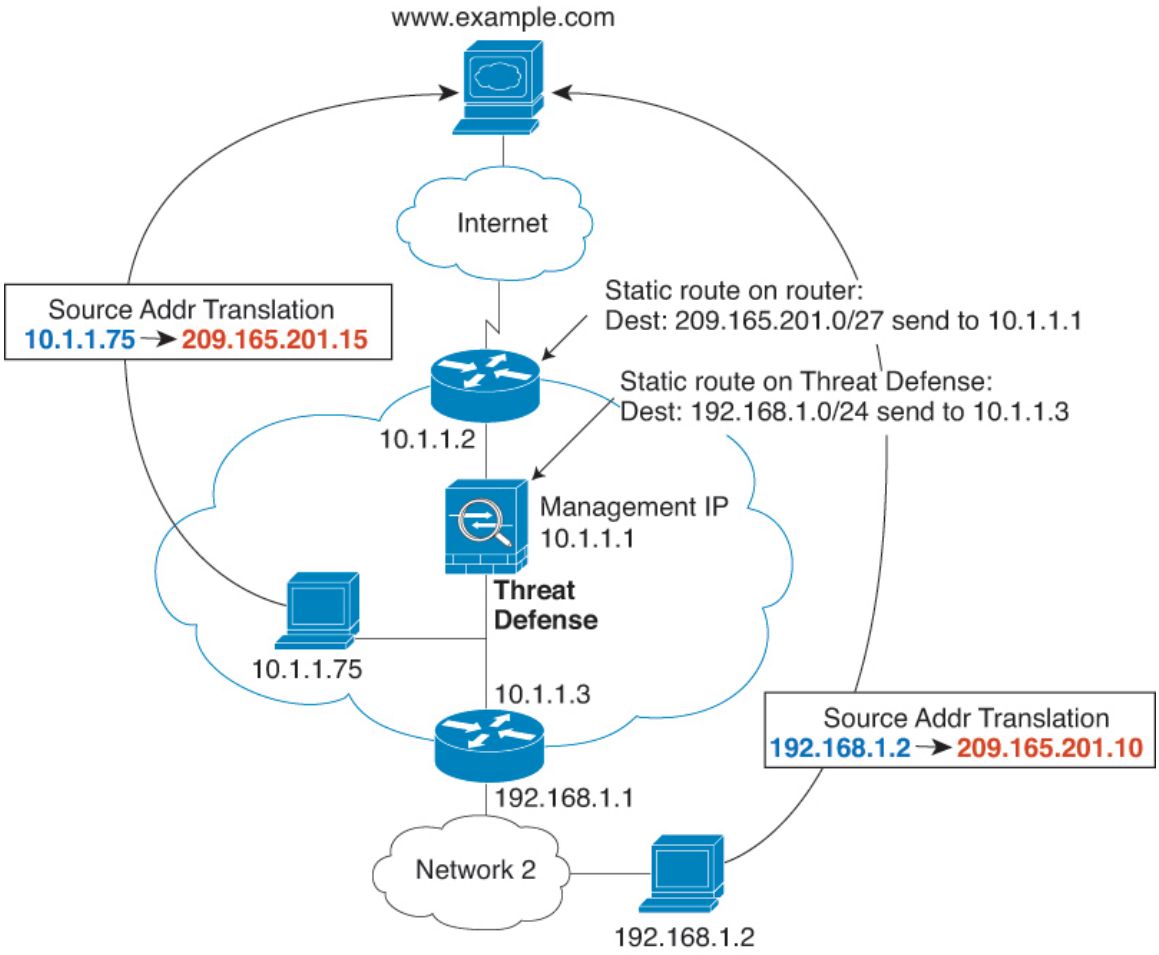
- H.323
- RTSP
- SIP and Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- Traffic at least one hop away for which the Firewall Threat Defense device performs NAT—Configure a static route on the Firewall Threat Defense device for traffic destined for the remote network. You also need a static route on the upstream router for traffic destined for the mapped addresses to be sent to the Firewall Threat Defense device.

  This routing requirement is also true for embedded IP addresses for VoIP and DNS with NAT enabled, and the embedded IP addresses are at least one hop away. The Firewall Threat Defense device needs to identify the correct egress interface so it can perform the translation.

NAT within a bridge group

Figure 32: NAT example: NAT within a bridge group



Unsupported features for bridge groups in transparent mode

This table lists the features that are not supported in bridge groups in transparent mode.

Table 5: Unsupported features in transparent mode

Feature	Description
Dynamic DNS	—
DHCPv6 stateless server	Only the DHCPv4 server is supported on bridge group member interfaces.

Feature	Description
DHCP relay	The transparent firewall can act as a DHCPv4 server, but it does not support DHCP relay. DHCP relay is not required because you can allow DHCP traffic to pass through using two access rules: one that allows DCHP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.
Dynamic routing protocols	You can, however, add static routes for traffic originating on the Firewall Threat Defense device for bridge group member interfaces. You can also allow dynamic routing protocols through the Firewall Threat Defense device using an access rule.
Multicast IP routing	You can allow multicast traffic through the Firewall Threat Defense device by allowing it in an access rule.
QoS	—
VPN termination for through traffic	The transparent firewall supports site-to-site VPN tunnels for management connections only on bridge group member interfaces. It does not terminate VPN connections for traffic through the Firewall Threat Defense device. You can pass VPN traffic through the Firewall Threat Defense device using an access rule, but it does not terminate non-management connections.

Unsupported features for bridge groups in routed mode

This table lists the features are not supported in bridge groups in routed mode.

Table 6: Unsupported features in routed mode

Feature	Description
EtherChannel member interfaces	Only physical interfaces, redundant interfaces, and subinterfaces are supported as bridge group member interfaces. Management interfaces are also not supported.
Clustering	Bridge groups are not supported in clustering.
Dynamic DNS	—
DHCPv6 stateless server	Only the DHCPv4 server is supported on BVIs.
DHCP relay	The routed firewall can act as a DHCPv4 server, but it does not support DHCP relay on BVIs or bridge group member interfaces.
Dynamic routing protocols	You can, however, add static routes for BVIs. You can also allow dynamic routing protocols through the Firewall Threat Defense device using an access rule. Non-bridge group interfaces support dynamic routing.
Multicast IP routing	You can allow multicast traffic through the Firewall Threat Defense device by allowing it in an access rule. Non-bridge group interfaces support multicast routing.

Feature	Description
QoS	Non-bridge group interfaces support QoS.
VPN termination for through traffic	You cannot terminate a VPN connection on the BVI. Non-bridge group interfaces support VPN. Bridge group member interfaces support site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the Firewall Threat Defense device. You can pass VPN traffic through the bridge group using an access rule, but it does not terminate non-management connections.

Default settings

Lists the default settings for firewall mode.

Bridge group defaults

By default, all ARP packets are passed within the bridge group.

Guidelines for firewall mode

Review these guidelines for firewall mode.

Bridge group limits and network requirements

- You can create up to 250 bridge groups, with 64 interfaces per bridge group.
- Each directly-connected network must be on the same subnet.
- The Firewall Threat Defense device does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

BVI IP address requirements

- An IP address for the BVI is required for each bridge group for to-the-device and from-the-device management traffic, as well as for data traffic to pass through the Firewall Threat Defense device. For IPv4 traffic, specify an IPv4 address. For IPv6 traffic, specify an IPv6 address.
- You can only configure IPv6 addresses manually.
- The BVI IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).

Unsupported bridge group members

- Management interfaces are not supported as bridge group members.

- For multi-instance mode, shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode).
- For the Firewall Threat Defense Virtual on VMware with bridged ixgbevf interfaces, transparent mode is not supported, and bridge groups are not supported in routed mode.
- For the Firepower 2100 series, bridge groups are not supported in routed mode.
- For the / 1010/ , you cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.
- For the Firepower 4100/9300, data-sharing interfaces are not supported as bridge group members.

Transparent mode requirements and limitations

- In transparent mode, you must use at least 1 bridge group; data interfaces must belong to a bridge group.
- In transparent mode, do not specify the BVI IP address as the default gateway for connected devices; devices need to specify the router on the other side of the Firewall Threat Defense as the default gateway.
- In transparent mode, the default route, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a regular static route that identifies the network from which you expect management traffic.
- Transparent mode is not supported on threat defense virtual instances deployed on Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure.

Routed mode requirements and limitations

- In routed mode, to route between bridge groups and other routed interfaces, you must name the BVI.
- In routed mode, Firewall Threat Defense-defined EtherChannel interfaces are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.

Traffic handling limitation

- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firewall Threat Defense when using bridge group members. If there are two neighbors on either side of the Firewall Threat Defense running BFD, then the Firewall Threat Defense will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

Set the firewall mode

You can set the firewall mode when you perform the initial system setup at the CLI. We recommend setting the firewall mode during setup because changing the firewall mode erases your configuration to ensure you do not have incompatible settings. If you need to change the firewall mode later, you must do so from the CLI.

Procedure

Step 1 Unregister the Firewall Threat Defense device from the Firewall Management Center.

You cannot change the mode until you unregister the device.

a) Performance profiles are retained across firewall mode changes and can't be changed after you re-register. You must set the performance profile to Default. See the **Performance Profile** page in your platform settings policy (choose **Devices** > **Platform Settings**, and then click **Edit** (✎) for your policy).

Deploy the configuration to make these changes.

b) Choose **Devices** > **Device Management**.

c) Next to the device you want to unregister, click **More** (⋮), and then click **Delete**.

Step 2 Access the Firewall Threat Defense device CLI, preferably from the console port.

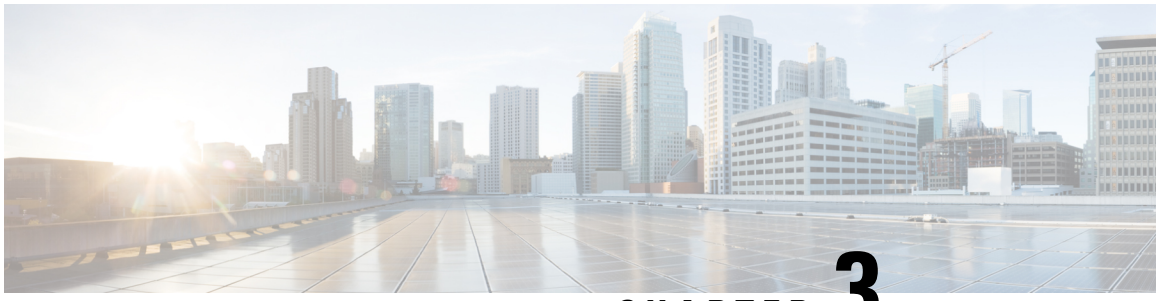
Step 3 Change the firewall mode:

configure firewall [**routed** | **transparent**]

Example:

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

Step 4 Re-register with the Firewall Management Center.



CHAPTER 3

CLI Users

Managed devices include a default **admin** account for CLI access. This chapter discusses how to create custom user accounts.

- CLI users, on page 85
- Guidelines for CLI users, on page 87
- Add an internal user at the CLI, on page 87
- External authentication for the Firewall Threat Defense, on page 90
- Troubleshoot LDAP authentication connections, on page 103
- History for CLI users, on page 105

CLI users

A CLI user is a user account that

- can be added as internal users or as external users on a LDAP or RADIUS server,
- is maintained separately on each managed device, and
- requires separate configuration for access to the Firewall Management Center versus managed devices.

User account separation

When you add a user to the Firewall Management Center, that user only has access to the Firewall Management Center; you cannot then use that username to log directly into a managed device. You must separately add a user on the managed device.

Internal and external users

Managed devices support two categories of users—internal and external—for user access control.

Internal users authenticate through a local database on the device. External users authenticate through LDAP or RADIUS servers when they are not found in the local database. Both user types enable secure access management for network devices.

User authentication types

Managed devices support these user authentication methods:

- Internal user: The device checks a local database for user authentication.
- External user: If the user is not present in the local database, the system queries an external LDAP or RADIUS authentication server.

CLI access

CLI access is a command-line interface capability that

- provides a Firepower CLI running on top of Linux for device administration
- enables creation of internal users on devices using the CLI, and
- supports establishment of external users on Firewall Threat Defense devices using the Firewall Management Center.

Security considerations for CLI access

Users with CLI Config level access can access the Linux shell using the **expert** command, and obtain `sudoers` privileges in the Linux shell, which can present a security risk.



Caution Users with CLI Config level access can access the Linux shell using the **expert** command, and obtain `sudoers` privileges in the Linux shell, which can present a security risk. For system security reasons, we strongly recommend:

- Only use the Linux shell under TAC supervision or when explicitly instructed by Firepower user documentation.
- Make sure that you restrict the list of users with CLI access appropriately.
- When granting CLI access privileges, restrict the list of users with Config level access.
- Do not add users directly in the Linux shell; only use the procedures in this chapter.
- Do not access Firepower devices using CLI expert mode unless directed by Cisco TAC or by explicit instructions in the Firepower user documentation.

CLI user roles

A CLI user role is an access control mechanism that

- determines the level of command access a user has on managed devices,
- controls whether users can execute configuration or non-configuration commands, and
- provides security by restricting unauthorized access to critical system functions.

Role types and permissions

On managed devices, user access to commands in the CLI depends on the role you assign.

- **None**: The user cannot log into the device on the command line.
- **Config**: The user can access all commands, including configuration commands. Exercise caution in assigning this level of access to users.
- **Basic**: The user can access non-configuration commands only. Only internal users and Firewall Threat Defense external RADIUS users support the Basic role.

Guidelines for CLI users

This reference provides essential guidelines for CLI users, including username requirements, default account information, and user account limits for different device models.

Usernames

- You cannot add the same username for both internal and external users. If the external server uses a duplicate username, the deployment to the device fails.
- The username must be Linux-valid:
  - Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
  - All lowercase
  - Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Defaults

All devices include an **admin** user as a local user account; you cannot delete the **admin** user. The default initial password is **Admin123**; the system forces you to change this during the initialization process. The agent stores the modified credentials in the Windows registry and uses the same encryption as the Firewall Management Center, which is Cipher Block Chaining (CBC). See the getting started guide for your model for more information about system initialization.

Number of user accounts

You can create a maximum of 43 user accounts for the Firepower 1000 and 2100.

Add an internal user at the CLI

Create internal users to provide authorized access to the Firewall Threat Defense system with appropriate privilege levels.

Use the CLI to create internal users on the Firewall Threat Defense.

Procedure

Step 1 Log into the device CLI using an account with Config privileges.

The **admin** user account has the required privileges, but any account with Config privileges will work. You can use an SSH session or the Console port.

For certain Firewall Threat Defense models, the Console port puts you into the FXOS CLI. Use the **connect ftd** command to get to the Firewall Threat Defense CLI.

Step 2 Create the user account.

configure user add *username* {**basic** | **config**}

- *username*—Sets the username. The username must be Linux-valid:
  - Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
  - All lowercase
  - Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)
- **basic**—Gives the user basic access. This role does not allow the user to enter configuration commands.
- **config**—Gives the user configuration access. This role gives the user full administrator rights to all commands.

Example:

This example adds a user account named johncrichton with Config access rights. The password is not shown as you type it.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Note Tell users they can change their own passwords using the **configure password** command.

Step 3 (Optional) Adjust the characteristics of the account to meet your security requirements.

You can use these commands to change the default account behavior.

- **configure user aging** *username max_days warn_days*

  Sets an expiration date for the user's password. Specify the maximum number of days for the password to be valid followed by the number of days before expiration the user will be warned about the upcoming expiration. Both values are 1 to 9999, but the warning days must be less than the maximum days. When you create the account, there is no expiration date for the password.

- **configure user forcereset** *username*

  Forces the user to change the password on the next login.

- **configure user maxfailedlogins** *username number*

Sets the maximum number of consecutive failed logins you will allow before locking the account, from 1 to 9999. Use the **configure user unlock** command to unlock accounts. The default for new accounts is 5 consecutive failed logins. The admin account is exempt from being locked out after a maximum number of failed logins unless you enable security certification compliance.

- **configure user minpasswdlen** *username number*

  Sets a minimum password length, which can be from 1 to 127.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  Enables or disables password strength checking, which requires a user to meet specific password criteria when changing their password. When a user's password expires or if the **configure user forcereset** command is used, this requirement is automatically enabled the next time the user logs in.

Step 4 Manage user accounts as necessary.

Users can get locked out of their accounts, or you might need to remove accounts or fix other issues. Use these commands to manage the user accounts on the system.

- **configure user access** *username* {**basic** | **config**}

  Changes the privileges for a user account.

- **configure user delete** *username*

  Deletes the specified account.

- **configure user disable** *username*

  Disables the specified account without deleting it. The user cannot log in until you enable the account.

- **configure user enable** *username*

  Enables the specified account.

- **configure user password** *username*

  Changes the password for the specified user. Users should normally change their own password using the **configure password** command.



Caution Do not use the Linux **passwd** command in Expert Mode to change the admin user password. This command can cause file system corruption. Only use the regular Firewall Threat Defense CLI **configure user password admin** command (if you are not admin) or **configure password** command (if you are admin). If you do not know the password and can't log in at all, refer to the password recovery procedure.

- **configure user unlock** *username*

  Unlocks a user account that was locked due to exceeding the maximum number of consecutive failed login attempts.

Note Firewall Threat Defense uses the Pluggable Authentication Module (PAM) framework for user authentication. Within this framework, the pam_unix.so module handles password hashing and verification using the SHA-512 algorithm

Passwords are hashed using the SHA-512 algorithm.

External authentication for the Firewall Threat Defense

External authentication for the Firewall Threat Defense is a security configuration that enables Firewall Threat Defense devices to authenticate users through external authentication servers by adding one or more external authentication objects.

External authentication for the Firewall Threat Defense

External authentication for the Firewall Threat Defense is a security feature that

- verifies user credentials with an LDAP or RADIUS server as specified in an external authentication object
- can be used by both the Firewall Management Center and Firewall Threat Defense devices, and
- allows only one external authentication object to be activated in the platform settings for the Firewall Threat Defense.

Authentication object sharing and user privileges

You can share the same object between the different appliance/device types or create separate objects.

Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1-30 seconds for LDAP, and 1-300 seconds for RADIUS). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Only a subset of fields in the external authentication object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for other device types, those fields will be used.

User privilege levels:

- LDAP users always have Config privileges
- RADIUS users can be defined as either Config or Basic users

User definition options:

- For RADIUS: Define users on the RADIUS server (with the Service-Type attribute) or pre-define the user list in the external authentication object
- For LDAP: Specify a filter to match CLI users on the LDAP server

Note Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you:

- Restrict the list of users with Linux shell access.
- Do not create Linux shell users.

LDAP

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that allows you to set up a directory on your network that organizes objects, such as user credentials, in a centralized location. Multiple applications can then access those credentials and the information used to describe them. If you ever need to change a user's credentials, you can change them in one place.

LDAP binding information

Microsoft has announced that Active Directory servers will start enforcing LDAP binding and LDAP signing in 2020. Microsoft is making these a requirement because when using default settings, an elevation of privilege vulnerability exists in Microsoft Windows that could allow a man-in-the-middle attacker to successfully forward an authentication request to a Windows LDAP server. For more information, refer to 2020 LDAP channel binding and LDAP signing requirement for Windows on the Microsoft support site.

If you have not done so already, we recommend you start using TLS/SSL encryption to authenticate with an Active Directory server.

RADIUS

RADIUS is a network authentication protocol that

- provides centralized authentication and authorization for network access,
- operates using client-server architecture for user credential verification, and
- supports accounting functions to track user sessions and network usage.

Remote Authentication Dial In User Service (RADIUS) is an authentication protocol used to authenticate, authorize, and account for user access to network resources. You can create an authentication object for any RADIUS server that conforms to RFC 2865.

Secure Firewall devices support the use of SecurID tokens. When you configure authentication by a server using SecurID, users authenticated against that server append the SecurID token to the end of their SecurID PIN and use that as their password when they log in. You do not need to configure anything extra on the Secure Firewall device to support SecurID.

By default, RADIUS uses port 1812 for authentication and port 1813 for accounting.

If you change the RADIUS authentication port, the RADIUS accounting port changes accordingly. Ensure that the Firewall Management Center can connect to the RADIUS server on the new accounting port; otherwise, authentication delays may occur.

Although you cannot configure RADIUS accounting parameters, the Firewall Threat Defense uses port 1813 for RADIUS accounting on the same server used for authentication. If the RADIUS server is unreachable on port 1813, it can cause delays in logging in.

Add an LDAP external authentication object for Firewall Threat Defense

Create external authentication object to provide authorized access to the Firewall Threat Defense system via LDAP, with appropriate privilege levels.

Add an LDAP server to support external users for Firewall Threat Defense management.

In a multidomain deployment, external authentication objects are only available in the domain in which they are created.

Sharing External Authentication

External LDAP objects can be used by the Firewall Management Center and Firewall Threat Defense devices. You can share the same object between the Firewall Management Center and devices or create separate objects. Be sure that both the Firewall Threat Defense and the Firewall Management Center can reach the LDAP server, even if you are not sharing the object. The Firewall Management Center is essential to retrieving the user list and downloading it to the device.



Note For LDAP, the timeout range is different for the Firewall Threat Defense and the Firewall Management Center , so if you share an object, be sure not to exceed the Firewall Threat Defense 's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the deployment to the Firewall Threat Defense will fail.

Supported Fields

Only a subset of fields in the LDAP object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for the Firewall Management Center , those fields will be used. This procedure only covers the supported fields for the Firewall Threat Defense. For other fields, refer to "Add an LDAP External Authentication Object for Firewall Management Center " in the *Cisco Secure Firewall Management Center Administration Guide* .

Usernames

Usernames must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

You cannot add the **admin** or **sshd** users for external authentication.

You can only add external users (as part of the External Authentication object) in the Firewall Management Center ; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the Firewall Management Center.

If you previously configured the same username for an internal user using the **configure user add** command, the Firewall Threat Defense first checks the password against the internal user, and if that fails, it checks the LDAP server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported.

Privilege Level

LDAP users always have Config privileges.

Before you begin

You must specify DNS server(s) for domain name lookup on your device. Even if you specify an IP address and not a hostname for the LDAP server on this procedure, the LDAP server may return a URI for authentication that can include a hostname. A DNS lookup is required to resolve the hostname. Refer to Modify Firewall Threat Defense management interface settings at the CLI , on page 763 to add DNS servers.

Procedure

Step 1 Choose **System** (⚙) > **Users**. Click the **External Authentication** tab.

Step 2 Click (+) **Add External Authentication Object**.

Step 3 Set the **Authentication Method** to **LDAP**.

a) Enter a **Name** and optional **Description**.

b) Choose a **Server Type** from the drop-down list.

Step 4 For the **Primary Server** , enter a **Host Name/IP Address**.

a) Change the **Port** from the default

If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

Step 5 (Optional) Enter the **Backup Server** parameters.

Step 6 Enter **LDAP-Specific Parameters**.

a) Enter the **Base DN** for the LDAP directory you want to access. For example, to authenticate names in the Security organization at the Example company, enter `ou=security,dc=example,dc=com`. Alternatively click **Fetch DNs** , and choose the appropriate base distinguished name from the drop-down list.

b) (Optional) Enter the **Base Filter**.

For example, if the user objects in a directory tree have a `physicalDeliveryOfficeName` attribute and users in the New York office have an attribute value of `NewYork` for that attribute, to retrieve only users in the New York office, enter `(physicalDeliveryOfficeName=NewYork)`.

To retrieve all cn names, except for disallowed users admin and sshd, enter `(&(cn=*)(!(|(cn=sshd)(cn=admin))))`.

c) Enter a **User Name** for a user who has sufficient credentials to browse the LDAP server. For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute, and the object for the administrator in the Security division at your example company has a `uid` value of `NetworkAdmin` , you might enter `uid=NetworkAdmin,ou=security,dc=example,dc=com`.

d) Enter the user password in the **Password** and the **Confirm Password** fields.

e) (Optional) Click **Show Advanced Options** to configure the following advanced options.

- **Encryption** —Click **None** , **TLS** , or **SSL**.

If you change the encryption method after specifying a port, you reset the port to the default value for that method. For **None** or **TLS** , the port resets to the default value of 389. If you choose SSL encryption, the port resets to 636.

- **SSL Certificate Upload Path** —For SSL or TLS encryption, you must choose a certificate by clicking **Choose File**.

  If you previously uploaded a certificate and want to replace it, upload the new certificate and redeploy the configuration to your devices to copy over the new certificate.

Note TLS encryption requires a certificate on all platforms. For SSL, the Firewall Threat Defense also requires a certificate. For other platforms, SSL does not require a certificate. However, we recommend that you *always* upload a certificate for SSL to prevent man-in-the-middle attacks.

- (Not Used) **User Name Template** —Not used by the Firewall Threat Defense.
- **Timeout (Seconds)** —Enter the number of seconds before rolling over to the backup connection, between 1 and 30. The default is 30.

Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center , so if you share an object, be sure not to exceed the Firewall Threat Defense 's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the Firewall Threat Defense LDAP configuration will not work.

Step 7 Configure **Attribute Mapping** to retrieve users based on an attribute.

- Enter a **UI Access Attribute**.**Note** : This field is not used for device CLI access; however, it is a required field, so you need to enter a value. You can just enter the same value that you enter for the **CLI Access Attribute**.
- Set the **CLI Access Attribute** if you want to use a CLI access attribute other than the user distinguished type. For example, on a Microsoft Active Directory Server, use the `sAMAccountName` CLI access attribute to retrieve CLI access users by typing `sAMAccountName`.

Note Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you restrict the list of users with CLI or Linux shell access.

Note Deploying an external authentication object that allows a large number of users with CLI access may cause deployments to time out and fail while waiting for the users to be created.

Step 8 Set the **CLI Access Filter**.

Choose one of the following methods:

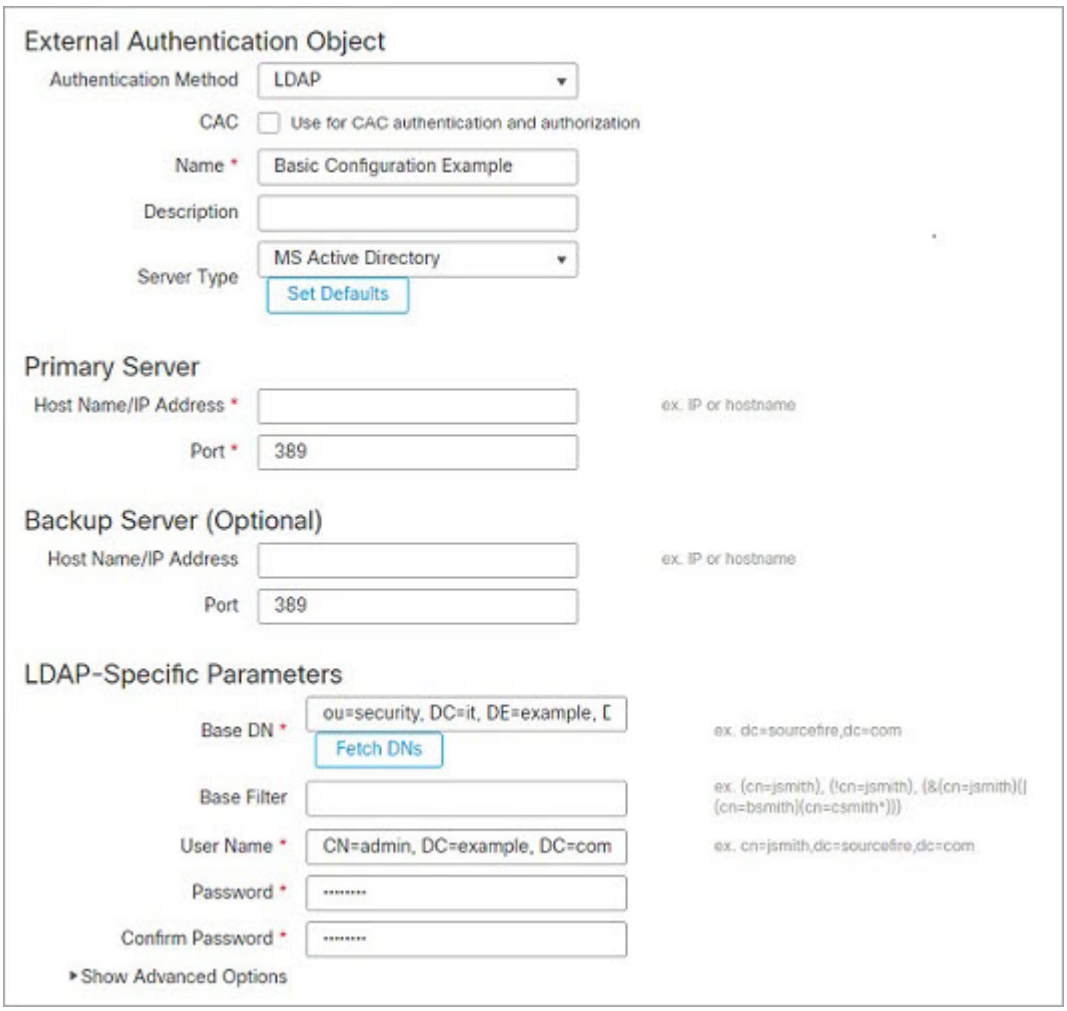
- To use the same filter you specified when configuring authentication settings, check the check box of **Same as Base Filter**.
- To retrieve administrative user entries based on attribute value, enter the attribute name, a comparison operator, and the attribute value you want to use as a filter, enclosed in parentheses. For example, if all network administrators have a `manager` attribute which has an attribute value of `shell` , you can set a base filter of `(manager=shell)`.

For username guidelines, refer to Usernames at the start of this procedure.

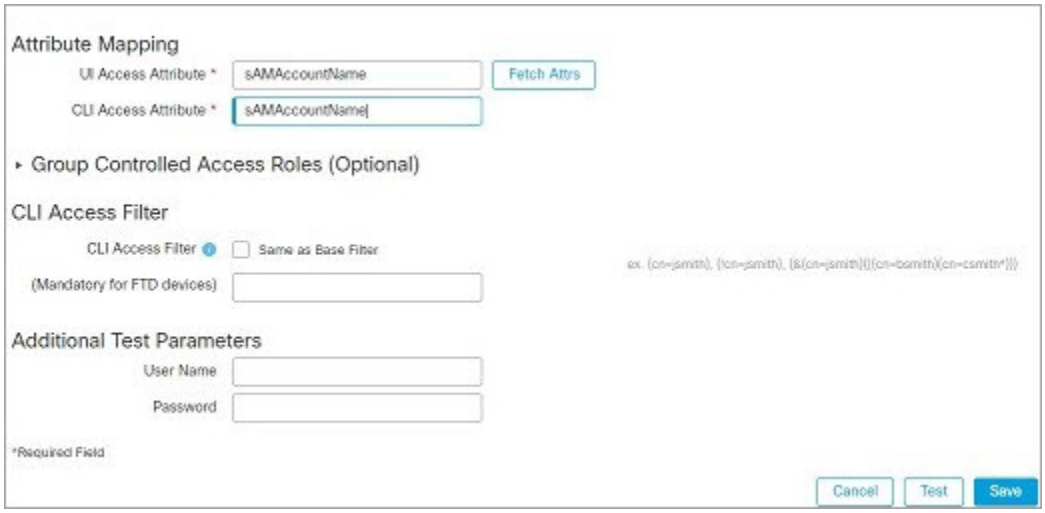
Step 9 Click **Save** and enable use of this server. For more information refer to Configure external authentication, on page 855.

Note If you later add or delete users on the LDAP server, you must redeploy the Platform Settings on managed devices. The Firewall Management Center redownloads the user list and deploys it to the device. For more information refer to Deploy configuration changes, on page 135.

The following figures illustrate a basic configuration of an LDAP login authentication object for a Microsoft Active Directory Server. The LDAP server in this example has an IP address of 10.11.3.4. The connection uses port 389 for access.



This example shows a connection using a base distinguished name of `OU=security,DC=it,DC=example,DC=com` for the security organization in the information technology domain of the Example company.

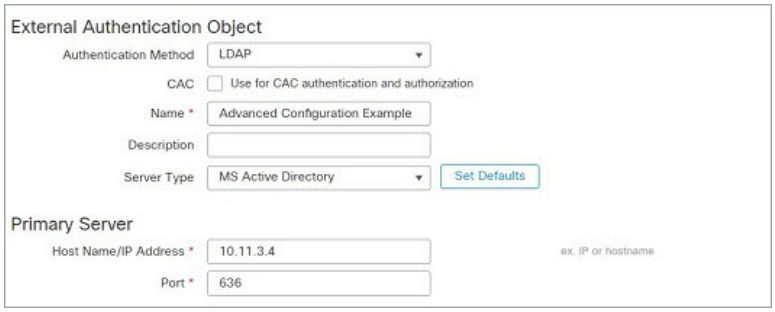


A **CLI Access Attribute** of `sAMAccountName` causes each `sAMAccountName` attribute to be checked for all objects in the directory for matches when a user logs into the Firewall Threat Defense.

Note that because no base filter is applied to this server, the Firewall Threat Defense checks attributes for all objects in the directory indicated by the base distinguished name. Connections to the server time out after the default time period (or the timeout period set on the LDAP server).

Advanced Example

This example illustrates an advanced configuration of an LDAP login authentication object for a Microsoft Active Directory Server. The LDAP server in this example has an IP address of 10.11.3.4. The connection uses port 636 for access.



This example shows a connection using a base distinguished name of `OU=security,DC=it,DC=example,DC=com` for the security organization in the information technology domain of the Example company. However, note that this server has a base filter of `(cn=*smith)`. The filter restricts the users retrieved from the server to those with a common name ending in `smith`.



The connection to the server is encrypted using SSL and a certificate named `certificate.pem` is used for the connection. In addition, connections to the server time out after 60 seconds because of the **Timeout (Seconds)** setting.

Because this server is a Microsoft Active Directory server, it uses the `sAMAccountName` attribute to store user names rather than the `uid` attribute.

The **CLI Access Attribute** of `sAMAccountName` causes each `sAMAccountName` attribute to be checked for all objects in the directory for matches when a user logs into the Firewall Threat Defense.

In the following example, the CLI access filter is set to be the same as the base filter.



Add a RADIUS external authentication object for Firewall Threat Defense

Configure a RADIUS server on the Firewall Threat Defense

Add a RADIUS server to support external users for the Firewall Threat Defense

Sharing External Authentication Objects

You can share the same object between the Firewall Management Center and devices or create separate objects. Note that the Firewall Threat Defense supports defining users on the RADIUS server, while the Firewall Management Center requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the Firewall Threat Defense , but if you want to define users on the RADIUS server, you must create separate objects for the Firewall Threat Defense and the Firewall Management Center.

Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center , so if you share an object, be sure not to exceed the Firewall Threat Defense 's smaller timeout range (1-300 seconds). If you set the timeout to a higher value, the Firewall Threat Defense RADIUS configuration will not work.

Firewall Threat DefenseFirewall Threat Defense

Only a subset of fields in the RADIUS object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for the Firewall Management Center , those fields will be used. This procedure only covers the supported fields for the Firewall Threat Defense. For other fields, refer to Add a RADIUS External Authentication Object for Firewall Management Center in the *Cisco Secure Firewall Management Center Administration Guide*.

Firewall Threat Defense

You cannot add the **admin** user for external authentication. You can only add external users (as part of the External Authentication object) in the Firewall Management Center ; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the Firewall Management Center.

If you previously configured the same username for an internal user using the **configure user add** command, the Firewall Threat Defense first checks the password against the internal user, and if that fails, it checks the RADIUS server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported. For users defined on the RADIUS server, be sure to set the privilege level to be the same as any internal users; otherwise you cannot log in using the external user password.

Before you begin

Define users on the RADIUS server using the Service-Type attribute.

These are supported values for the Service-Type attribute:

- Administrator (6)—Provides Config access authorization to the CLI. These users can use all commands in the CLI.
- NAS Prompt (7) or any level other than 6—Provides Basic access authorization to the CLI. These users can use read-only commands, such as **show** commands, for monitoring and troubleshooting purposes.

The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a sign (@) or slash (/)

Alternatively, you can predefine users in the external authentication object (refer to Step 6, on page 100). To use the same RADIUS server for the Firewall Threat Defense and Firewall Management Center while using the Service-Type attribute method for the Firewall Threat Defense , create two external authentication objects that identify the same RADIUS server: one object includes the predefined **CLI Access Filter** users (for use with the Firewall Management Center), and the other object leaves the **CLI Access Filter** empty (for use with Firewall Threat Defense s).

Procedure

Step 1 In the Firewall Management Center , choose **System** (⚙) > **Users**.

Step 2 Click **External Authentication** and select (+) **Add External Authentication Object**.

a) Set the **Authentication Method** to **RADIUS**.

b) Enter a **Name** and optional **Description**.

Step 3 For the **Primary Server** , enter a **Host Name/IP Address**.

a) Change the **Port** from the default.

b) Enter the **RADIUS Secret Key**.

Only IPv4 is supported.



Note If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field.

Step 4 (Optional) Enter the **Backup Server** parameters.

Step 5 (Optional) Enter **RADIUS-Specific Parameters**.

a) Enter the **Timeout (Seconds)** in seconds before retrying the primary server, between 1 and 300. The default is 30.



Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center , so if you share an object, be sure not to exceed the Firewall Threat Defense 's smaller timeout range (1-300 seconds). If you set the timeout to a higher value, the Firewall Threat Defense RADIUS configuration will not work.

b) Enter the **Retries** before rolling over to the backup server. The default is 3.

Step 6 (Optional) Instead of using RADIUS-defined users, in the **CLI Access Filter** area **Administrator CLI Access User List** field, enter the user names that should have CLI access, separated by commas. For example, enter `jchrichton, aerynsun, rygel`.

You may want to use the **CLI Access Filter** method for Firewall Threat Defense so you can use the same external authentication object with Firewall Threat Defense and other platform types.



Note If you want to use RADIUS-defined users, you must leave the **CLI Access Filter** empty.

Make sure that these usernames match usernames on the RADIUS server. The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)



Note Users with CLI access can gain Linux shell access with the **expert** command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you restrict the list of users with CLI or Linux shell access.

Note Deploying an external authentication object that allows a large number of users with CLI access may cause deployments to time out and fail while waiting for the users to be created.

Step 7 (Optional) Click **Test** to test Firewall Management Center connectivity to the RADIUS server.

This function can only test Firewall Management Center connectivity to the RADIUS server; there is no test function for managed device connectivity to the RADIUS server.

Step 8 (Optional) You can also enter **Additional Test Parameters** to test user credentials for a user who should be able to authenticate: enter a **User Name** and **Password** , and then click **Test**.

Tip If you mistype the name or password of the test user, the test fails even if the server configuration is correct. To verify that the server configuration is correct, click **Test** without entering user information in the **Additional Test Parameters** field first. If that succeeds, supply a user name and password to test with the specific user.

Example:

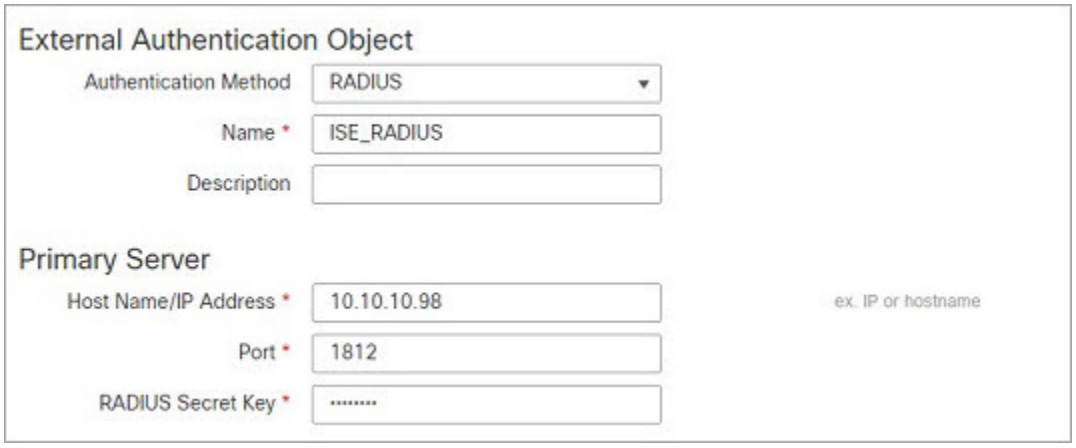
To test if you can retrieve the `JSmith` user credentials at the Example company, enter `JSmith` and the correct password.

Step 9 Click **Save** and enable use of this server. For more information refer to Configure external authentication, on page 855

Examples

Simple User Role Assignments

This figure illustrates a sample RADIUS login authentication object for a server running Cisco Identity Services Engine (ISE) with an IP address of 10.10.10.98 on port 1812. No backup server is defined.



This example shows RADIUS-specific parameters, including the timeout (30 seconds) and number of failed retries before the system attempts to contact the backup server, if any.

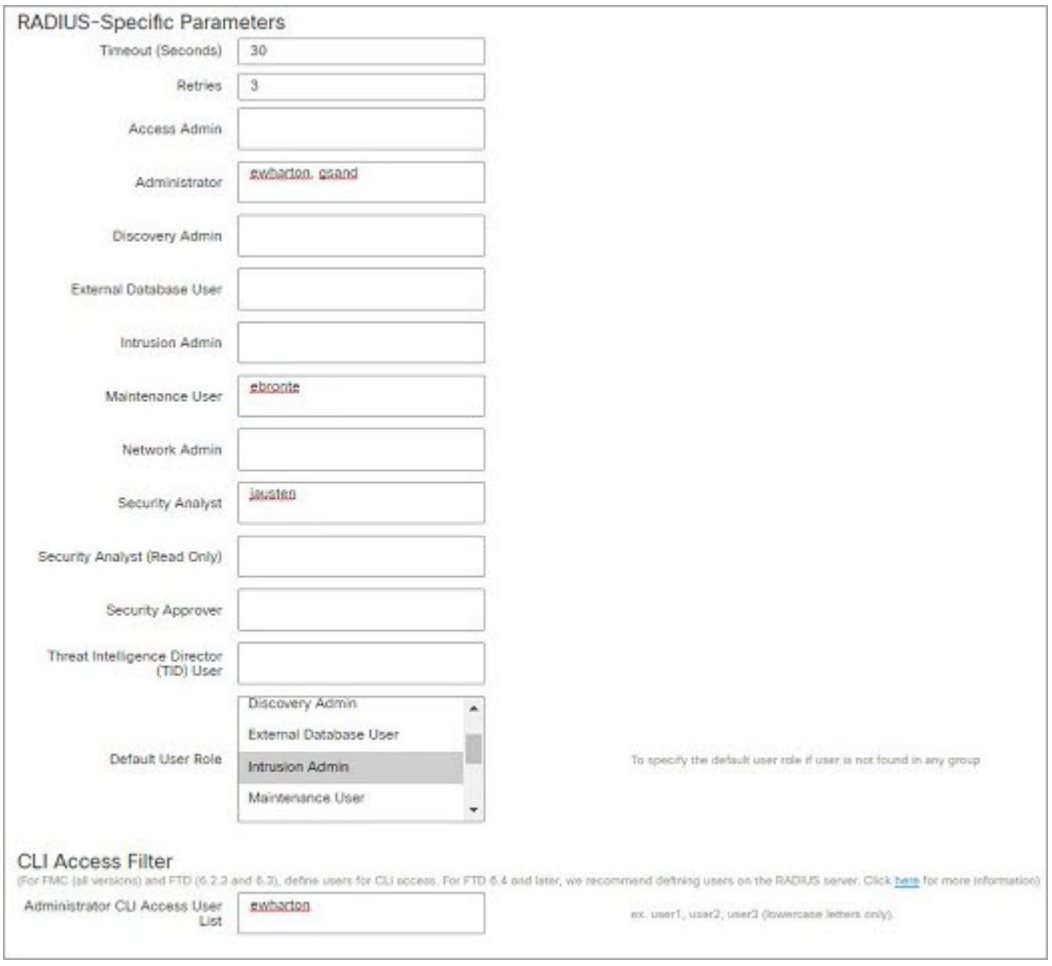
This example illustrates important aspects of RADIUS user role configuration:

Users `ewharton` and `gsand` are granted web interface Administrative access.

The user `cbronte` is granted web interface Maintenance User access.

The user `jausten` is granted web interface Security Analyst access.

The user `ewharton` can log into the device using a CLI account.



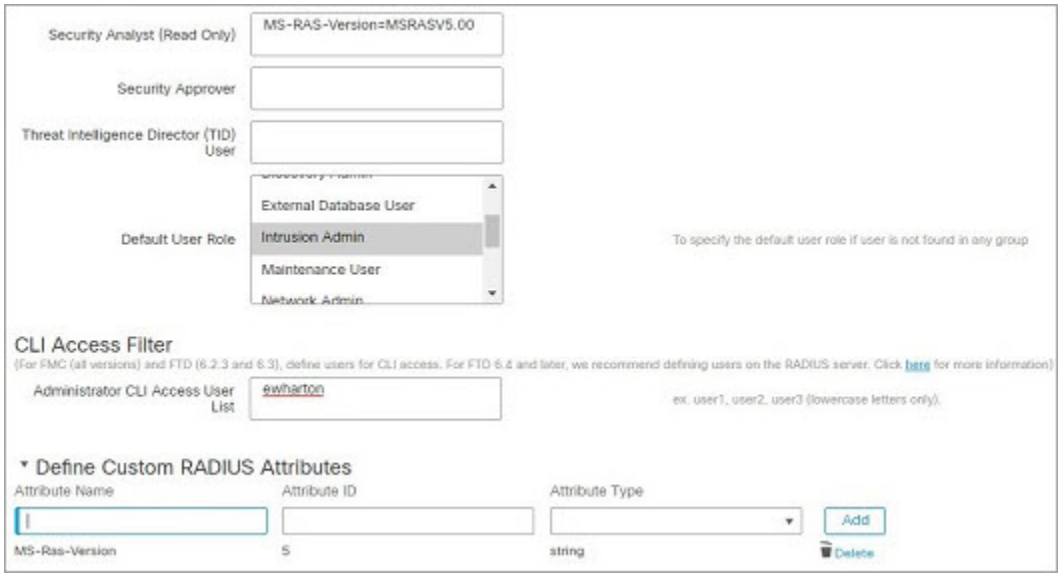
This graphic depicts the role configuration for the example:

Roles for Users Matching an Attribute-Value Pair

You can use an attribute-value pair to identify users who should receive a particular user role. If the attribute you use is a custom attribute, you must define the custom attribute.

This figure illustrates the role configuration and custom attribute definition in a sample RADIUS login authentication object for the same ISE server as in the previous example.

In this example, however, the `MS-RAS-Version` custom attribute is returned for one or more of the users because a Microsoft remote access server is in use. Note the `MS-RAS-Version` custom attribute is a string. In this example, all users logging in to RADIUS through a Microsoft v. 5.00 remote access server should receive the Security Analyst (Read Only) role, so you enter the attribute-value pair of `MS-RAS-Version=MSRASV5.00` in the **Security Analyst (Read Only)** field.



External authentication for users on Firewall Threat Defense devices

External authentication for users on Firewall Threat Defense devices is a security configuration that enables authentication through external authentication servers rather than local device credentials.

Configuration process

Enable External Authentication in the Threat Defense Platform Settings, and then deploy the settings to the managed devices. Refer to Configure external authentication, on page 855 for more information.

Troubleshoot LDAP authentication connections

This reference provides troubleshooting information for resolving LDAP authentication connection problems in your system configuration.

If you create an LDAP authentication object and it either does not succeed in connecting to the server you select or does not retrieve the list of users you want, you can tune the settings in the object.

If the connection fails when you test it, try the following suggestions to troubleshoot your configuration:

- Use the messages displayed at the top of the web interface screen and in the test output to determine which areas of the object are causing the issue.
- Check that the user name and password you used for the object are valid:
  - Check that you have the rights to browse to the directory indicated in your base-distinguished name by connecting to the LDAP server using a third-party LDAP browser.
  - Check that the user name is unique to the directory information tree for the LDAP server.
  - If you see an LDAP bind error 49 in the test output, the user binding for the user failed. Try authenticating to the server through a third-party application to see if the binding fails through that connection as well.

- When configuring LDAP authentication, avoid using a backslash ("\") in the binding password. The presence of a backslash in the password causes the LDAP binding process to fail, resulting in unsuccessful external authentication.

- Check that you have correctly identified the server:
  - Check that the server IP address or host name is correct.
  - Check that you have TCP/IP access from your local appliance to the authentication server where you want to connect.
  - Check that access to the server is not blocked by a firewall and that the port you have configured in the object is open.
  - If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used for the server.
  - Check that you have not used an IPv6 address for the server connection if you are authenticating CLI access.
  - If you used server type defaults, check that you have the correct server type and click **Set Defaults** again to reset the default values.
- If you typed in your base-distinguished name, click **Fetch DNs** to retrieve all the available base distinguished names on the server, and select the name from the list.
- If you are using any filters, access attributes, or advanced settings, check that each is valid and typed correctly.
- If you are using any filters, access attributes, or advanced settings, try removing each setting and testing the object without it.
- If you are using a base filter or a CLI access filter, make sure that the filter is enclosed in parentheses and that you are using a valid comparison operator (maximum 450 characters, including the enclosing parentheses).
- To test a more restricted base filter, try setting it to the base distinguished name for the user to retrieve just that user.
- If you are using an encrypted connection:
  - Check that the name of the LDAP server in the certificate matches the host name that you use to connect.
  - Check that you have not used an IPv6 address with an encrypted server connection.
- If you are using a test user, make sure that the user name and password are typed correctly.
- If you are using a test user, remove the user credentials and test the object.
- Test the query that you are using by connecting to the LDAP server and using this syntax:

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

For example, if you are trying to connect to the security domain on `myrtle.example.com` using the `domainadmin@myrtle.example.com` user and a base filter of (`cn=*`), you could test the connection using this statement:

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

If you can test your connection successfully but authentication does not work after you deploy a platform settings policy, check that authentication and the object you want to use are both enabled in the platform settings policy that is applied to the device.

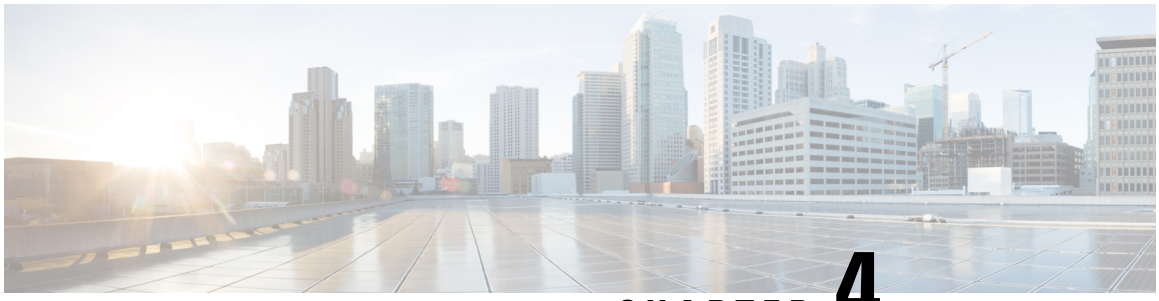
If you connect successfully but want to adjust the list of users retrieved by your connection, you can add or change a base filter or CLI access filter or use a more restrictive or less restrictive base DN.

While authenticating a connection to Active Directory (AD) server, rarely the connection event log indicates blocked LDAP traffic although the connection to AD server is successful. This incorrect connection log occurs when the AD server sends a duplicate reset packet. The Firewall Threat Defense device identifies the second reset packet as part of a new connection request and logs the connection with Block action.

History for CLI users

This reference provides version history information for CLI user features, including authentication enhancements and external authentication support for SSH access.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for the Service-Type attribute for Firewall Threat Defense users defined on the RADIUS server.	6.4.0	Any	For RADIUS authentication of Firewall Threat Defense CLI users, you used to have to pre-define the usernames in the RADIUS external authentication object and manually make sure that the list matched usernames defined on the RADIUS server. You can now define CLI users on the RADIUS server using the Service-Type attribute and also define both Basic and Config user roles. To use this method, be sure to leave the shell access filter blank in the external authentication object. New/modified screens: **System** > **Users** > **External Authentication** > **Add External Authentication Object** > **Shell Access Filter**
External authentication for Firewall Threat Defense SSH access.	6.2.3	Any	You can now configure external authentication for SSH access to the Firewall Threat Defense using LDAP or RADIUS. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**



CHAPTER 4

Change Management

You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.

- Change management, on page 107
- Requirements and prerequisites for change management, on page 111
- Guidelines and limitations for change management, on page 111
- Enabling or disabling change management, on page 112
- Manage tickets, on page 113
- History for change management, on page 118

Change management

Change management is a formal process that

- enforces an official approval process before configuration changes can be made to a device,
- requires administrators to open tickets before they can make configuration changes, and
- ensures that the right employees make the final decisions through submission and approval of tickets.

Change management characteristics

When using change management, the system implements these controls:

- Administrators can see their own changes within a ticket, but they cannot see changes anyone else has made within a ticket
- A policy is locked once a user makes a change within a ticket, preventing interfering changes
- Users cannot make changes while another user has made a change that is pending approval

Administrators can create multiple tickets so that a single ticket contains only logically-related policy changes. Tickets with a more limited scope are also easier to evaluate and approve quickly.

Make configuration changes in the change management workflow

This task enables configuration specialists to make configuration changes to supported policies and objects when change management is enabled.

When you enable change management, users who configure devices and shared policies need to change their approach slightly. Configuration specialists need to take the following approach when making configuration changes to supported policies and objects.

Procedure

Step 1 Create a ticket.

Step 2 Open the ticket.

Step 3 Make the configuration changes.

Note that the procedures explained in the online help and user guides assume that change management is not active, and omit any steps for creating, opening, or submitting tickets.

Step 4 Optionally, preview and validate the ticket to ensure the changes are complete and correct.

Step 5 Submit the ticket. At this point, the approver can either approve or reject the ticket.

- If the ticket is approved, deploy the changes.
- If the ticket is rejected, address the issues, and resubmit the ticket.

The configuration changes are successfully implemented through the change management workflow with proper approval and deployment processes.

Create separate approver and configuration roles

Separate approver and configuration roles are system-defined and custom roles that

- have permissions to modify (create/open/discard) and review (approve/reject) tickets,
- provide granular access control to separate ticket approval from configuration changes, and
- ensure that ticket approval is assigned only to users who have organizational authority to approve changes.

System-defined roles and permissions

Some system-defined roles have permissions to modify (create/open/discard) and review (approve/reject) tickets:

- To both modify and review tickets:
  - Admin
  - Network Admin
- To modify tickets only:
  - Access Admin
  - Intrusion Admin
- To review tickets only:

- Security Approver

If you need more granular roles to separate these activities due to your organizational requirements, you can create separate roles to ensure that ticket approval is assigned only to those users who have the organizational authority to approve changes. To create new user roles, go to **System** (⚙) > **Users** > **User Roles**.

These are the permissions, in the **System** (⚙) > **Configuration** > **Change Management** folder, relevant to ticket usage and approval. Note that these permissions are available only after you enable change management.

- Modify Tickets—To create tickets (for yourself), to use tickets for configuration changes, and to discard tickets.
- Review Tickets—To approve or reject tickets.
- Both Modify and Review Tickets—To create tickets for yourself and others, use tickets, and approve/reject tickets.

The approach you take depends on your precise requirements. For example:

- If your approvers should also be allowed to make configuration changes, you can simply assign them the system-defined roles, such as Administrator. Then, create custom configuration-only roles that include the same permissions but not the Review Tickets permission.
- If you need complete separation between approvers and those who make configuration changes, create custom roles for both, limiting the roles to either the Modify Tickets or the Review Tickets permission plus all other needed permissions for viewing or changing the supported policies and objects.

Policies and objects that support change management

If a policy or object supports the change management workflow, then creating, editing, or deleting the policy or object, including assigning a policy to a device, must be done in an open ticket.

Any action, policy, or object that does not support the change management workflow can be created, edited, or deleted, and so forth, without an open ticket. Even if a ticket is open, the changes made to unsupported policies are not included in the ticketed changes and are available for deployment immediately.

This information includes the policies and objects that are supported. Anything not listed is unsupported.

Supported policies

- Access control, including rules, references to other policies, and inheritance settings. Cloning access control policies is not included within a ticket. The clone is immediately accepted and available to all users.
- Device configuration policies:
  - Interfaces
  - Inline sets
  - DHCP
  - VTEP
  - All routing

- FlexConfig
- Intrusion policy and network analysis policy (NAP), Snort 3 only.
- Network address translation (NAT)
- Platform settings
- Prefilter policy
- QoS
- Umbrella SASE topology
- VPN policies, both site-to-site and remote access
- Zero trust access

Supported objects

- AAA server
- Access list
- Address pools
- AS path
- Community list
- DHCP IPv6 pools
- DNS server group
- FlexConfig objects
- Group policy
- Interface
- Key chain
- Network
- Policy list
- Port
- Prefix list
- Route map
- SLA monitor
- Time range
- Time zone
- Tunnel zone

- URL
- Variable set
- VLAN tag
- VPN objects (IKEv1, IKEv2 IPSec and policy, PKI enrollment, certificate map)

Requirements and prerequisites for change management

This reference provides the requirements and prerequisites necessary to configure change management functionality.

Model support

Management center

Supported domains

Any

User roles

- To enable or disable change management: Admin.
- To both modify and review tickets:
  - Admin
  - Network Admin
- To modify tickets only:
  - Access Admin
  - Intrusion Admin
- To review tickets only:
  - Security Approver

Guidelines and limitations for change management

When operating in change management mode, users can make changes to supported policies, but they cannot save the changes. For example, you could go through the dialog box to create a new platform settings policy without an open ticket, but when you click OK to actually create the policy, you will get an error and the policy will not be created.

The following activities require that all tickets be in a terminal state, that is, approved or discarded: backup/restore, moving a device between domains, upgrading Firewall Management Center.

Deleting a device from the inventory requires that all tickets involving that device be approved or discarded.

Some system processes prevent you from enabling or disabling change management. Wait until the following processes complete before you enable or disable change management:

- critical management center processes, including SRU updates, LSP updates, VDB updates, and management center upgrades
- pending or running background activities, including device registration; cluster auto-registration; Firewall Threat Defense high availability operations; high availability auto-registration; FlexConfig migration; cluster creation, break, edit, reconcile, or node changes; device-template creation or application; device-model migration; and EPM join or breakout
- system jobs, including backup or restore, device import or export, general import, and domain movement.

Your ability to create objects while configuring a feature is constrained based on whether the feature and objects are all supported by change management. For example, importing a configuration is not supported by change management. Therefore, you cannot create security zone objects, which are supported, during the import. On the other hand, you can create new objects while configuring access control rules, because both are supported.

When using Cloud-Delivered Firewall Management Center, a user defined in Security Cloud Control is available to be assigned tickets only after the user cross-launches cdFMC at least once. Until the first cross-launch, the user does not exist in cdFMC.

Enabling or disabling change management

Enable or disable change management to control whether users must open tickets and get approval when making configuration changes to the system.

The default is that the change management workflow is disabled. Users do not need to open tickets and get approval when making configuration changes. If you want to enforce the change management workflow, you must enable it globally for the system.

Before you begin

There are several system processes that prevent you from enabling/disabling change management. If any of the following are in process, you need to wait for them to complete before changing these settings: backup/restore; import/export; domain movement; upgrade; Flexconfig migration; device registration; high-availability registration, creation, break, or switch; cluster create, registration, break, edit, add or remove nodes; EPM break out or join.

An access control policy cannot be locked when you change these settings. If a policy is locked, you must wait for the lock to be released before enabling/disabling this feature.

Follow these steps to enable or disable change management:

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Click **Change Management**.

Step 3 Select **Enable Change Management**.

To disable the feature, deselect the option. All tickets must be approved or discarded to disable change management. You cannot disable change management if any ticket is in the In Progress, On Hold, Rejected, or Pending Approval state.

Step 4 Select the **Number of approvals required**, which is how many administrators must approve the change for the ticket to be approved and deployable. The default is 1, but you can require up to 5 approvers per ticket. Users can override this number when creating tickets.

Step 5 Select the **Ticket Purge Duration**, which is the number of days to keep approved tickets, from 1-100 days. The default is 5 days.

Step 6 (Optional.) Enter the **Reply to Address** and the email addresses for the **List of Approver Addresses**. You must also configure the email notification system settings for email to work.

Step 7 Click **Save**.

The system adds the **Ticket** ( ) shortcut to the menu bar, and the **System** ( ) > **Change Management Workflow** command. Users can manage tickets using these methods.

Change management is enabled or disabled according to your configuration. If enabled, the system adds ticket management shortcuts to the interface, and users must follow the change management workflow when making configuration changes.

Manage tickets

This task enables you to manage change management tickets for configuration changes to supported policies that require approval workflow.

When you enable change management, configuration changes for supported policies must be done within the context of a ticket. You open a ticket, make your changes, then submit the ticket for approval.

You can see a list of tickets, and create new ones, either on the change management page or through the ticket quick-access menu. All ticket changes are synchronized in each menu, so you can switch back and forth at your convenience and use whichever method you prefer.

Note When you open a ticket and make a change to a supported policy, that policy is locked from changes by other users or through other tickets. The policy remains locked until the ticket is approved or discarded.

Procedure

Step 1 Do any of these actions:

- Choose **System** ( ) > **Change Management Workflow** to open a page showing existing tickets.
- Click the **Ticket** ( ) quick-access menu. The icon can either be named Select a Ticket (if no ticket is opened), the ticket name if a ticket is opened, or unnamed if no tickets exist.

Both pages are organized the same. The **Ticket** tab lists all tickets, whereas the **Review** tab lists tickets that have been submitted for approval. The default view shows your tickets only.

Step 2 On the **Ticket** tab, take any of these actions:

- To create a new ticket, click **Add Ticket**.
- To view the details of a ticket, click the > next to the ticket name. The Details page includes UUID, name, description, user, last modified date, and comments. The History page includes the status changes for the ticket. The image at the top shows where the ticket stands in the overall workflow.
- To preview the configuration changes for an open ticket, click **Preview** ( ).
- To validate the configuration changes in an open ticket, click **Validate** ( ) or **More** ( ) > **Validate**. A dialog box opens showing error, warning, and informational messages, if there are any validation errors.
- To open a ticket, click **Open** ( ) or **More** ( ) > **Open**. To close an open ticket, click **Put Ticket on Hold (X)** or **More** ( ) > **Put Ticket on Hold**. Closing a ticket does not submit it for review, nor does it release any locks placed on edited policies.
- To submit an open ticket for review and approval, click **Submit for Approval** ( ) or **More** ( ) > **Submit for Approval**. The ticket must be open to be submitted.
- To discard a ticket, click **Discard** ( ) or **More** ( ) > **Discard**.
- To search for a ticket, type a string in the search box. The search looks at ticket name, description, and responsible user. To filter the list by ticket status (on the change management workflow page), click the status above the list: **New**, **Open**, **On Hold** (ticket was closed), **Rejected**, **Pending Approval**, **Approved**. Each status has a count of the number of tickets in that state. Click **All** under **My Tickets** to return to the default of showing all of your tickets, or **All** under **Tickets in System** to see everyone's tickets.

Step 3 On the **Reviews** tab, take any of these actions on submitted tickets.

The list is empty if there are no submitted tickets. In addition, only users with Review Ticket permissions can see this tab.

- To preview the configuration changes for a ticket, click **Preview** ( ).
- To validate the configuration changes in an open ticket, click **Validate** ( ) or **More** ( ) > **Validate**.
- To approve the ticket, click **Approve** ( ) or **More** ( ) > **Approve**.
- To disapprove the ticket, click **Reject** ( ) or **More** ( ) > **Reject**.

You have successfully managed your change management tickets. Approved tickets can proceed with configuration changes, while rejected tickets require revision before resubmission.

Create change management tickets

Create change management tickets to ensure all configuration changes are performed within the context of an approved workflow ticket.

When using the change management workflow, you must do all configuration changes within the context of an open ticket. If you do not already have a ticket, you must create a new one.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (📄) shortcut menu.

Step 2 Click **Add Ticket**.

Step 3 Configure the ticket options:

- **Name**—The name of the ticket. The name can include letters, numbers, spaces, and the following special characters: #-_!
- **Description**—An optional description of what you intend to configure using this ticket. For example, if you have a case number related to what you intend to fix using this ticket, that would be useful information in a description.
- **Number of Approvers**—How many administrators must approve the change for the ticket to be approved and deployable. You can specify 1-5.
- **Assign to**—Select the user who will own the ticket and be responsible for implementing the changes. Choose **self** to assign it to yourself.

Step 4 Click one of the following:

- **Create**—The ticket is added to the list of tickets, but it is not opened. You need to open it before you can work within the context of the ticket.
- **Create and Open**—The ticket is added to the list of tickets and also opened.

The change management ticket is created and available for use in the workflow. If you selected Create and Open, the ticket is immediately opened for configuration changes.

Opening a ticket for configuration changes

Open a ticket to enable configuration changes within the ticket management system.

Before you can make changes within a ticket, you must open the ticket.

If you have another ticket open, the system puts it on hold (closes it) for you before opening the new one.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (📄) shortcut menu.

Step 2 On the **Tickets** tab, click **Open** (📂) or **More** (⋮) > **Open** for the ticket.

Step 3 Optionally, enter a comment for the action.

Step 4 Click **Open**.

You can now start your configuration changes. The name of the ticket icon changes to the name of the open ticket.

The ticket is now open and ready for configuration changes. The ticket icon displays the name of the open ticket.

Preview a ticket

Preview a ticket to view all configuration changes made within the context of the ticket.

You can preview a ticket while making your configuration changes, or before approving it. The preview shows all configuration changes made within the context of the ticket.

Procedure

Step 1 Choose **System** ( ) > **Change Management Workflow**, or click the **Ticket** ( ) shortcut menu.

Step 2 Click **Preview** ( ) for the ticket.

The Preview dialog box opens. Changes are color coded according to the legend at the top of the dialog box.

Step 3 Select the policy whose changes you want to view in the Changed Policies list.

You are shown both the current version of the policy as it is defined in Secure Firewall Management Center (on the left) and the proposed changes defined within the ticket.

For policies that contain pages, such as platform settings, you can select the overall policy to see all changes, or specific pages within the policy, in the Changed Policies list.

You cannot alter the changes from within the preview. If you need to change something, you must close the preview and return to the policy you want to change.

Step 4 Optionally, click **Download as PDF** to save the preview to a PDF file for offline viewing or archival purposes.

Step 5 Click **OK**.

The ticket preview displays all configuration changes, allowing you to review them before approval or while making modifications.

Submit a ticket

Submit a ticket to apply changes made within the ticket after validation and review.

After you have completed the changes needed for a ticket, you can preview and validate the changes. Then, when you are satisfied with the changes, submit the ticket for review and approval.

Changes made within the ticket are not applied until you submit the ticket and the ticket is approved. Until approval happens, all policies modified within a ticket are locked to that ticket and cannot be changed by anyone else.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (📋) shortcut menu.

Step 2 Click **Submit for Approval** ( ) or **More** (⋮) > **Submit for Approval** for the open ticket.

Step 3 Optionally, enter a comment for your action.

Step 4 Click **Submit**.

The ticket is submitted for review and approval. Once approved, the changes made within the ticket are applied and the policies are unlocked.

Discard a ticket

Discard a ticket to remove any changes that were made within the ticket when you no longer need to proceed with those changes.

You cannot undo this action and retrieve a ticket with its changes. If you need them, you must create a new ticket and start over.

You cannot discard a ticket after you submit it. However, if the approver rejects the ticket, you can then discard it.



Note If you have permission to modify tickets, you can discard tickets that belong to another user. This makes it possible to deal with situations where an admin is on vacation or otherwise unavailable to manage an in-process ticket.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (📋) shortcut menu.

Step 2 Click **Discard** ( ) or **More** (⋮) > **Discard** for the ticket.

Step 3 Optionally, enter a comment for your action.

Step 4 Click **Discard**.

The ticket is discarded and any changes made within the ticket are removed.

Approving or rejecting a ticket

Approve or reject tickets to control which configuration changes become active and available for deployment in your network.

When a user submits a ticket, it must be approved for the changes made within the ticket to become active and available for deployment.

Whether you can approve your own tickets, or there is a separate approver, depends on your workplace policies and how user roles are assigned, not on the management software.

The Details view includes a summary of how many approvers are required for the ticket, and who has approved the ticket.

If the changes are inadequate or undesirable, you can reject the ticket. Rejected tickets go back to the submitter, who can then make additional changes and resubmit the ticket, or simply discard the ticket and the configuration changes it contains.

Procedure

Step 1 Choose **System** ( ) > **Change Management Workflow**, or click the **Ticket** ( ) shortcut menu.

Step 2 On the **Review** tab, click **Preview** ( ) for the ticket and evaluate the proposed changes.

You can also click **Validate** ( ) or **More** ( ) > **Validate** to check for errors.

Step 3 After completing your evaluation, do one of the following:

- To approve the ticket, click **Approve** ( ) or **More** ( ) > **Approve**.
- To disapprove the ticket, click **Reject** ( ) or **More** ( ) > **Reject**.

Step 4 Optionally, enter a comment for your action.

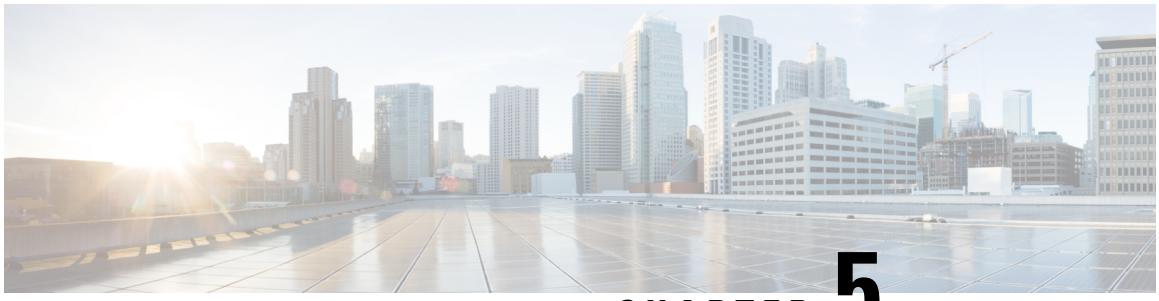
Step 5 Click **Approve** or **Reject**, as appropriate.

The ticket is approved or rejected based on your selection. Approved tickets become active and available for deployment. Rejected tickets return to the submitter for revision or disposal.

History for change management

The following table summarizes the feature changes by release for change management functionality.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Change management.	7.4.1	Any	You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. We added the **System**(⚙) > **Configuration** > **Change Management** page to enable the feature. When enabled, there is a **System**(⚙) > **Change Management Workflow** page, and a new **Ticket**(📄) quick access icon in the menu.



CHAPTER 5

Configuration Deployment

This chapter describes how to download configuration changes to one or more managed devices.

- Configuration deployment, on page 121
- Requirements and prerequisites for deployment management, on page 133
- Best practices for deploying configuration changes, on page 133
- Configuration deployment, on page 134
- Deployment management, on page 141
- History for configuration deployment, on page 154

Configuration deployment

Configuration deployment is a management process that enables centralized control and distribution of device settings from Firewall Management Center to managed devices.

Configuration changes that require deployment

Firewall Management Center marks out-of-date policies with red status text that indicates how many of its targeted devices need a policy update. Redeploy the policy to the devices to clear this status.

Deployment required

You must deploy changes after these configuration updates:

- Modifying an access control policy: any changes to access control rules, the default action, policy targets, Security Intelligence filtering, advanced options including preprocessing, and so on.
- Modifying any of the policies that the access control policy invokes: the SSL policy, network analysis policies, intrusion policies, file policies, identity policies, or DNS policies.
- Changing any reusable object or configuration used in an access control policy or policies it invokes:
  - network, port, VLAN tag, URL, and geolocation objects
  - Security Intelligence lists and feeds
  - application filters or detectors
  - intrusion policy variable sets

  - file lists
  - decryption-related objects and security zones

- Updating intrusion rules (SRU/LSP) or the vulnerability database (VDB).
- Upgrading managed devices.
- Upgrading the Firewall Management Center.

You can change some of these configurations from multiple places in the web interface. For example, you can modify security zones using the object manager (**Objects** > **Object Management**), but modifying an interface type in a device configuration (**Devices** > **Device Management**) can also change a zone and require a deployment.

Deployment not required

These updates do not require a deployment:

- Security Intelligence updates to feeds and the global Block or Do Not Block lists.
- URL filtering data updates.
- Geolocation database (GeoDB) updates.

Deployment preview

A deployment preview is a snapshot that provides all the policy and object changes to be deployed on the device.

The policy changes include the new policies, changes in the existing policies, and the deleted policies. The object changes include the added and modified objects which are used in policies. The unused object changes are not displayed because they are not deployed on the device.

Click the **Preview** icon next to a deployment job to view the configuration change log for that are pending to be deployed on the device. The change log includes:

- **Comparison View**: Displays a side-by-side comparison of all the device configuration changes made since your last deployment.
- **Advanced View**: Displays the pending CLI commands to be applied to the device.

For more information about viewing the deployment preview, refer to Deploy configuration changes, on page 135.

The preview shows all the default values, even when they are not altered, along with the other configured settings when an interface or a platform settings policy is added for the first time. Similarly, the high availability-related policies and default values for settings are shown, even when they are not altered, in the first preview after a high availability pair is configured or disrupted.

To view changes due to an auto rollback, refer to Edit deployment settings, on page 800.

Unsupported features:

- Object additions and attribute changes are displayed in the preview only if the objects are associated with any device or interface. Object deletions are not displayed.

- Preview is not supported for the policies:
  - High availability
  - Network discovery
  - Network analysis
  - Device settings
- User information at the rule level is not available for intrusion policies.
- The preview does not show the reordering of rules across policies.

  For DNS policies, reordered rules appear in the preview list as rule additions and deletions. For example, moving a rule from position 1 to position 3 in the rule order is displayed as if the rule was deleted from position 1 and added as a new rule in position 3. Similarly, when a rule is deleted, the rules under it are listed as edited rules as they have changed their positions. The changes are displayed in the final order in which they appear in the policy.
- Preview is not supported in these HA scenarios:
  - If a device was in standalone mode and if a chain is made, then an auto-deployment is triggered.

    For that particular job, preview is not supported. On hover over the **Preview** (), a message is displayed that it is a HA bootstrap deployment, and no preview is supported.
  - **Configuration groups** - Consider a flow in which a device was initially standalone. Subsequently, three deployments took place. In the fourth deployment, the device was a HA bootstrap deployment. After these, the user deploys devices 5, 6, and 7. The deployment 7 is an HA break deployment, and the user deploys devices 8, 9, and 10.

    In this flow, the preview between 3 and 5 is not supported because 4 was a HA deployment. Similarly, the preview between 8 and 3 is also not supported. Preview is supported only from 3 to 1, 7,6, 5, 4, and 10, 9, and 8.
  - If a device is broken (HA is broken) then the new device is considered as a fresh device.

Guidelines for selective policy deployment

The Firewall Management Center allows you to select a specific policy within the list of all the changes on the device that are due for deployment and deploy only the selected policy.

This table describes the policies that suppot selective deployment.

Table 7: Policies that support selective deployment

Type	Policy
Access control	• Access control policies • Prefilter policies • QoS policies

Type	Policy
Threat prevention and inspection	• Intrusion policies • Malware and file policies • DNS policies
Identity and discovery	• SSL / decryption policies • Identity policies • Network discovery
Device or network connectivity	• NAT policies • Routing policies • VPN policies

Use the this table to understand the constraints and conditions for applying selective policy deployment.

Table 8: Limitations for selective deployment

Type	Description	Scenarios
Full deployment	Full deployment is necessary for specific deploy scenarios, and the Firewall Management Center does not support selective deployment in such scenarios. If you encounter an error in such scenarios, you may choose to proceed by selecting all the changes for deployment on the device.	Full deployment is required for: • The first deployment after you upgrade the Firewall Management Center or its devices. • The first deployment after you restore a device. • The first deployment after modifications to a device's interface settings. • The first deployment after modifications in the virtual router settings. • When a device moves to a new domain (global to sub-domain or sub-domain to global).

Type	Description	Scenarios
Associated policy deployment	The Firewall Management Center identifies interdependent policies which are interlinked. When one of the interlinked policies is selected, the remaining interlinked policies are automatically selected.	Scenarios wherein an associated policy is automatically selected: • When a new object is associated with an existing policy. • When an existing policy's object is modified. Scenarios wherein multiple policies are automatically selected: • When a new object is associated with an existing policy, and the same object is already associated with other policies, all the associated policies are automatically selected. • When a shared object is modified, all the associated policies are automatically selected.
Interdependent policy changes (shown using color-coded tags)	The Firewall Management Center dynamically detects dependencies in-between policies, and between the shared objects and the policies. The interdependency of the objects or policies is shown using color-coded tags.	Scenarios wherein color-coded interdependent policies or objects are automatically selected: • When all the out-of-date policies have interdependent changes. For example, when an access control policy, an intrusion policy, and a NAT policy are out-of-date. Since access control policy and NAT policy share an object, all policies are selected together for deployment. • When all out-of-date policies share an object, and the object is modified.

Type	Description	Scenarios
Access Policy Group specifications	Access Policy Group policies are listed together in the preview window under **Access Policy Group** when you click **View** ( ).	The scenarios and the expected behavior for Access Policy Group policies are: • If the access control policy is out-of-date, all other out-of-date policies under this group, except file policy and intrusion policy, are selected when the access control policy is selected for deployment. However, if the access control policy is out-of-date, intrusion and file policies can be individually selected or deselected irrespective of whether the access control policy is selected or not, unless there are any dependent changes. For example, if a new intrusion policy is assigned to an access control rule, it indicates that there are dependent changes, then both the access control policy and the intrusion policy will be automatically selected when either of them is selected. • If no access control policy is out-of-date, other out-of-date policies in this group can be selected and deployed individually.

System username

The Firewall Management Center displays the username as **system** for specific management operations. This allows administrators to distinguish system-initiated actions from those performed by users.

The **system** username is applied to these operations:

- Rollback
- Upgrade
- Firewall Threat Defense backup and restore
- SRU update
- LSP update
- VDB update

Auto-enabling of application detectors

When you perform application control but disable required detectors, the Firewall Management Center automatically enables the appropriate system-provided detectors upon policy deployment. If no system-provided detector exists for the application, the Firewall Management Center enables the most recently modified user-defined detector.

Asset rediscovery with network discovery policy changes

When you deploy changes to a network discovery policy, the system deletes and then rediscovers MAC address, TTL, and hops information from the network map for the hosts in your monitored networks. Also, the affected managed devices discard any discovery data that has not yet been sent to the Firewall Management Center.

Snort restart scenarios

A Snort restart scenario is a situation that

- causes the traffic inspection engine, referred to as the `Snort process`, on a managed device to restart,
- interrupts inspection until the process resumesWhether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129., and
- may result in resource demands that cause a small number of packets to drop without inspection when you deploy.

Common snort restart triggers

Any of these scenarios cause the Snort process to restart:

- You deploy a specific configuration that requires the Snort process to restart. For more information, refer to Configurations that restart the snort process when deployed or activated, on page 131.
- You make a change that immediately restarts the Snort process. For more information, refer to Actions that immediately restart the snort process, on page 132.
- Traffic activates the currently deployed Automatic Application Bypass (AAB) configuration. For more information, refer Configure automatic application bypass, on page 797.
- Enabling or disabling **Logging connection events to RAM disk** feature. For more information, refer the section **Log to Ramdisk** in Troubleshoot Drain of FMC Unprocessed Events.

Inspection interruption warnings during deployment

When you deploy configurations, the **Inspect Interruption** column in the deploy page indicates if a deployed configuration will restart the Snort process on the Firewall Threat Defense device. When the traffic inspection engine referred to as the `Snort process` restarts, inspection is interrupted until the process resumes. Whether traffic is interrupted or passes without inspection during the interruption depends on how the traffic is handled by the device. You can proceed with the deployment, cancel the deployment and modify the configuration, or delay the deployment until a time when deploying would have the least impact on your network.

During deployment, when the **Inspect Interruption** column indicates **Yes** and you expand the device configuration listing, an icon will highlight any configuration type that may restart the Snort process. Moving your pointer over the icon displays a message saying that deployment may interrupt traffic.

This table summarizes how the deploy page displays inspection interruption warnings.

Table 9: Inspection interruption indicators

Type	Inspect interruption	Description
Firewall Threat Defense	**Inspect Interruption** ( )Yes	At least one configuration would interrupt inspection on the device if deployed, and might interrupt traffic depending on how the device handles traffic. You can expand the device configuration listing for more information.
	--	Deployed configurations will not interrupt traffic on the device.
	Undetermined	The system cannot determine if a deployed configuration may interrupt traffic on the device. Undetermined status is displayed before the first deployment after a software upgrade, or in some cases during a Support call.
	Errors ( )	The system cannot determine the status due to an internal error. Cancel the operation and click **Deploy** again to allow the system to redetermine the **Inspect Interruption** status. If the problem persists, contact Support.
sensor	--	The device identified as *sensor* is not the Firewall Threat Defense device; the system does not determine if a deployed configuration may interrupt traffic on this device.

For information on all configurations that restart the Snort process for all device types, see Configurations that restart the snort process when deployed or activated, on page 131.

Inspect traffic during policy apply

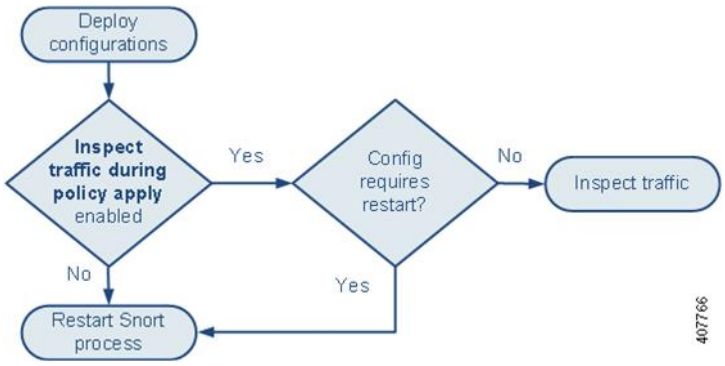
Inspect traffic during policy apply is an advanced access control policy general setting that enables managed devices to inspect traffic while configuration changes are applied, and allows inspection unless a deployed configuration requires the Snort process to restart.

Configuration options

You can configure this setting as follows:

- Enabled — Traffic is inspected during the deployment unless certain configurations require the Snort process to restart. When a Snort restart is not needed, the system first uses the currently deployed access control policy to inspect traffic, then switches to the policy being deployed.
- Disabled — Traffic is not inspected during the deployment. The Snort process always restarts when you deploy.

This graphic illustrates how Snort restarts can occur when you enable or disable **Inspect traffic during policy apply**.



Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. Refer to Snort restart traffic behavior, on page 129 and Configurations that restart the snort process when deployed or activated, on page 131.

Snort restart traffic behavior

This reference explains how different devices handle traffic when the Snort process restarts.

Table 10: The Firewall Threat Defense and the Firewall Threat Defense Virtual Restart Traffic Effects

Interface configuration	Restart traffic behavior
inline: **Snort Fail Open: Down**: disabled	dropped
inline: **Snort Fail Open: Down**: enabled	passed without inspection Some packets can be delayed in buffer for several seconds before the system recognizes that Snort is down. This delay can vary depending upon the load distribution. However, the buffered packets are eventually passed.

Interface configuration	Restart traffic behavior
routed, transparent (including EtherChannel, redundant, subinterface): **preserve-connection** enabled (**configure snort preserve-connection enable**; default) For more information, see *Cisco Secure Firewall Threat Defense Command Reference*.	existing TCP/UDP flows: passed without inspection so long as at least one packet arrives while Snort is down new TCP/UDP flows and all non-TCP/UDP flows: dropped Note that traffic drops even when **preserve-connection** is enabled for: • plaintext, passthrough prefilter tunnel traffic that matches an **Analyze** rule action or an **Analyze all tunnel traffic** default policy action • connections that do not match an access control rule and are instead handled by the default action • decrypted TLS/SSL traffic • a safe search flow • a captive portal flow
routed, transparent (including EtherChannel, redundant, subinterface): **preserve-connection** disabled (**configure snort preserve-connection disable**)	dropped
inline: tap mode	egress packet immediately, copy bypasses Snort
passive	uninterrupted, not inspected

Note In addition to traffic handling when the Snort process is down while it restarts, traffic can also pass without inspection or drop when the Snort process is busy, depending on the configuration of the Snort Fail Open **Busy** option (see Configure Inline Sets, on page 736). A device supports either the Failsafe option or the Snort Fail Open option, but not both.

Note When the Snort process is busy but not down during configuration deployment, some packets may drop on routed, switched, or transparent interfaces if the total CPU load exceeds 60 percent.

Warning Do not reboot the system while the Snort Rule Update is in progress.

Snort-busy drops happen when snort is not able to process the packets fast enough. Lina does not know whether Snort is busy due to processing delay, or if is stuck or due to call blocking. When transmission queue is full,

snort-busy drops occur. Based on Transmission queue utilization, Lina will try to access if the queue is being serviced smoothly.

Configurations that restart the snort process when deployed or activated

Deploying any of these configurations except AAB restarts the Snort process as described. Deploying AAB does not cause a restart, but excessive packet latency activates the currently deployed AAB configuration, causing a partial restart of the Snort process.

Access control policy advanced settings

- Deploy when **Inspect Traffic During Policy Apply** is disabled.
- Add or remove an SSL policy.

File policy

Deploy the first or last of any one of these configurations; note that while otherwise deploying these file policy configurations does not cause a restart, deploying non-file-policy configurations can cause restarts.

- Take either of these actions:
  - Enable or disable **Inspect Archives** when the deployed access control policy includes at least one file policy.
  - Add the first or remove the last file policy rule when **Inspect Archives** is enabled (note that at least one rule is required for **Inspect Archives** to be meaningful).
- Enable or disable **Store files** in a **Detect Files** or **Block Files** rule.
- Add the first or remove the last active file rule that combines the **Malware Cloud Lookup** or **Block Malware** rule action with an analysis option (**Spero Analysis or MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware, Unknown**, **Clean**, or **Custom**).

Note that access control rules that deploy these file policy configurations to security zones or tunnel zones cause a restart only when your configuration meets these conditions:

- Source or destination security zones in your access control rule must match the security zones associated with interfaces on the target devices.
- Unless the destination zone in you access control rule is *any*, a source tunnel zone in the rule must match a tunnel zone assigned to a tunnel rule in the prefilter policy.

Identity policy

- When SSL decryption is disabled (that is, when the access control policy does not include an SSL policy), add the first or remove the last active authentication rule.

  An active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

Network discovery

- Enable or disable non-authoritative, traffic-based user detection over the HTTP, FTP, or MDNS protocols, using the network discovery policy.

Device management

- MTU: Change the highest MTU value among all non-management interfaces on a device.
- Automatic Application Bypass (AAB): The currently deployed AAB configuration activates when a malfunction of the Snort process or a device misconfiguration causes a single packet to use an excessive amount of processing time. The result is a partial restart of the Snort process to alleviate extremely high latency or prevent a complete traffic stall. This partial restart causes a few packets to pass without inspection, or drop, depending on how the device handles traffic.

TLS server identity discovery

Enabling or disabling **TLS Server Identity Discovery** will result in a Snort 2 restart.

Note Snort 3 does not restart when **TLS Server Identity Discovery** is enabled or disabled.

Updates

- System update: Deploy configurations the first time after a software update that includes a new version of the Snort binary or data acquisition library (DAQ).
- For managed devices running Snort 3, deploying configurations the first time after installing a vulnerability database (VDB) update may temporarily interrupt application detection, but there will be no traffic interruptions.

Actions that immediately restart the snort process

These actions immediately restart the Snort process without requiring deployment. How the restart affects traffic depends on how the target device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Applications or application detectors

- Activate or deactivate a system or custom application detector.
- Delete an activated custom detector.
- **Save and Reactivate** an activated custom detector.
- Create a user-defined application.

When you perform any of these actions, a message warns you that continuing will restart the Snort process. The message allows you to cancel. The system restarts Snort on all managed devices in the current domain and any child domain.

High availability configuration

Create or break a Firewall Threat Defense high availability pair.

When you create or break a high availability pair, a message warns you that creating or breaking a high availability pair restarts the Snort process on the primary and secondary devices. The message allows you to cancel.

Requirements and prerequisites for deployment management

Before using the configuration deployment feature in the Firewall Management Center, ensure you meet these requirements.

- You must have **Administrator**, **Network Admin**, or **Security Approver** privileges to access the deployment features.
- Before deploying policy changes, you can compare the differences between the current device configuration and the pending policy, ensuring accuracy before you finalize the deployment. To use this feature, you must have the appropriate access rights, valid licenses for the specific policy, and be in the correct domain context.
-

Best practices for deploying configuration changes

Reliable management connection

The management connection between the Firewall Management Center and the device is a secure, TLS-1.3-encrypted communication channel between itself and the device.

To ensure reliable management connection, use a direct management path instead of routing management traffic through an additional encrypted tunnel, such as a Site-to-Site VPN. If the tunnel fails, you could lose management connectivity.

To maintain a reliable management connection, exclude management traffic from the VPN tunnel if it exits a VPN-terminating interface.



Caution Avoid routing a device's management connection through a VPN tunnel that terminates on the device itself. If a configuration update causes the tunnel to drop, you will lose the management connection and cannot recover the device configuration unless you connect directly to the device.

Maximum concurrent deployments

Avoid deploying to more than 25 percent of the maximum devices allowed for a Firewall Management Center in the same deployment task. For example, for the FMCv300, the maximum deployment task size is 75 devices (25 percent of 300). Deploying concurrently to more devices can cause performance issues.

Deployment of shared policies

For best performance, deploy to devices that use the same policies. Create a separate deployment task for each group of devices that share policies.

Time to deploy and memory limitations

Deployment time depends on multiple factors, including:

- The configurations you send to the device. For example, if you dramatically increase the number of Security Intelligence entries you block, deployment can take longer.
- Device model and memory. On devices with less memory, deployment can take longer.

Keep your configurations within the capability of your devices. If you exceed the maximum number of rules or policies supported by a target device, Firewall Management Center displays a warning. The maximum depends on a number of factors—not only memory and the number of processors on the device, but also on policy and rule complexity. For information on optimizing policies and rules, refer to Best practices for access control rules, on page 1625.

Use a maintenance window to lessen the impact of traffic interruptions

We *strongly* recommend you deploy in a maintenance window or at a time when interruptions will have the least impact.

- When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. Refer to Snort restart traffic behavior, on page 129 and Configurations that restart the snort process when deployed or activated, on page 131.
- For the Firewall Threat Defense devices, the **Inspect Interruption** column in the **Deploy** dialog warns you when deploying might interrupt traffic flow or inspection. You can proceed with, cancel, or delay deployment. For more information, refer to Inspection interruption warnings during deployment, on page 127.

Configuration deployment

Configuration deployment is the process of deploying configuration and policy updates to your Fireall Threat Defense devices after you make changes. This process allows you to apply changes to multiple components including device configurations, security policies, and network discovery settings.

Deployment components

Deploying updates applies to these components:

- Device and interface configurations
- Device-related policies, such as NAT, VPN, QoS, and platform settings policy
- Access control and related policies: DNS, file, identity, intrusion, network analysis, prefilter, SSL
- Network discovery policy
- Intrusion rule updates
- Configurations and objects associated with any of these elements

You can configure the system for automatic deployment by scheduling a deploy task or by setting the system to deploy when importing intrusion rule updates. Automating policy deployment is especially useful if you allow intrusion rule updates to modify system-provided base policies for intrusion and network analysis. Intrusion rule updates can also modify default values for the advanced preprocessing and performance options in your access control policies.

You can view deployment status in the **Notifications** pane.

Deploy configuration changes

Apply new or updated device configurations to managed devices.

After you change a device configuration, you must deploy the changes for them to take effect. Deploy during a maintenance window or off-peak hours to minimize potential traffic and inspection disruption.

Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. Refer to Snort restart traffic behavior, on page 129 and Configurations that restart the snort process when deployed or activated, on page 131.

Before you begin

- Confirm that all managed devices use the same revision of the Security Zones object. If you have edited security zone objects: Do not deploy configuration changes to any device until you edit the zone setting for interfaces on *all* devices you want to sync. You must deploy to all managed devices at the same time.
- To preview the deployment changes, enable REST API access. To enable the REST API access, follow the steps in *Enabling REST API Access* in the *Cisco Secure Firewall Management Center Administration Guide* .

Note The deployment process fails if the device configuration is being read at the device CLI during deployment. Do not execute commands such as **show running-config** during the deployment.

Procedure

Step 1 In the Firewall Management Center menu bar, click **Deploy**.

Step 2 For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all devices. For additional deployment options, click **Advanced Deploy**.

The rest of this procedure applies to the **Advanced Deploy** screen.

Step 3 Click **Expand Arrow** ( ) to view device-specific configuration changes to be deployed.

- The **Modified By** column lists the users who have modified the policies or objects. On expanding the device listing, you can view the users who have modified the policies against each policy listing. For

information about when the **System** user is shown (instead of the logged-in user), refer to System username, on page 126.

Note Usernames are not provided for deleted policies and objects.

- The **Inspect Interruption** column indicates if traffic inspection interruption may be caused in the device during deployment.

  When the status indicates (Yes) that deploying will interrupt inspection, and perhaps traffic, on the Firewall Threat Defense device, the expanded list indicates the specific configurations causing the interruption with the **Inspect Interruption** ( ).

  If the entry is blank in this column for a device, then it indicates that there will be no traffic inspection interruptions on that device during deployment.

  For information about identifying configurations that interrupt traffic inspection and might interrupt traffic when deployed to the Firewall Threat Defense devices, refer to Inspection interruption warnings during deployment, on page 127.

- The **Last Modified Time** column specifies when you last made the configuration changes.
- The **Preview** column allows you to preview the changes for the next deployment.
- The **Status** column provides the status for each deployment. For more information, see Deployment status, on page 141.

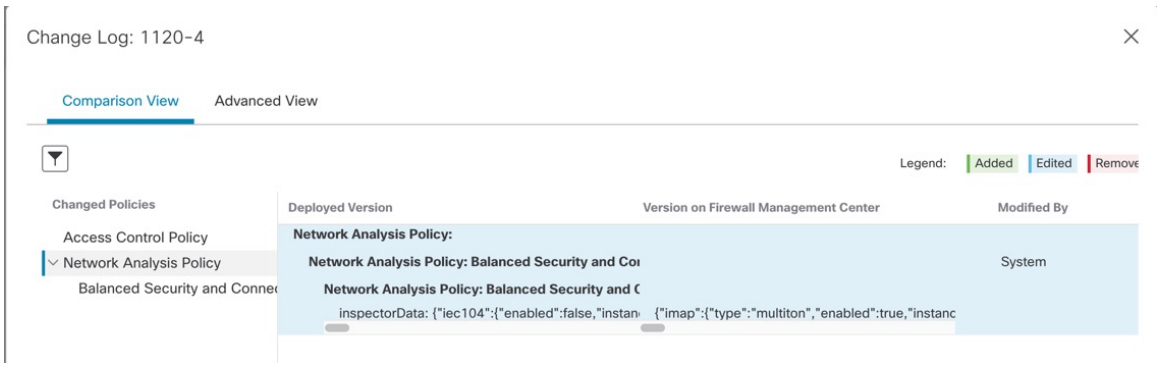
Step 4 In the **Preview** column, click **Preview** ( ) to see the configuration changes that you can deploy.

Note If you change the Firewall Management Center name in **System** ( ) > **Configuration** > **Information** , the deployment preview does not specify this change, yet it requires a deployment.

For unsupported features for Preview, see Deployment preview, on page 122.

The **Comparison View** tab lists all the policy and object changes. The left pane lists all the different policy types that have changed on the device, organized in a tree structure.

Figure 33: Comparison View



The **Filter**( ) lets you filter the policies at the user level and policy level.

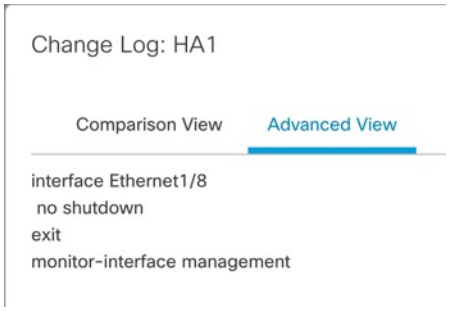
The right pane lists all the additions, changes, or deletions in the policy, or the object selected in the left pane. The two columns on the right pane provide the last deployed configuration settings (in the **Deployed Version** column) versus the changes that are due for deployment (in the **Version on Firewall Management Center** column). The last-deployed configuration settings are derived from a snapshot of the last saved deployment in the Firewall Management Center and not from the device. The background colors of the settings are color-coded as per the legend available on the top-right of the page.

The **Modified By** column lists the users who have modified, or added the configuration settings. At the policy level, the Firewall Management Center displays all the users who have modified the policy, and at the rule level, the Firewall Management Center displays only the last user who has modified the rule.

You can download a copy of the change log by clicking the **Download Report** button.

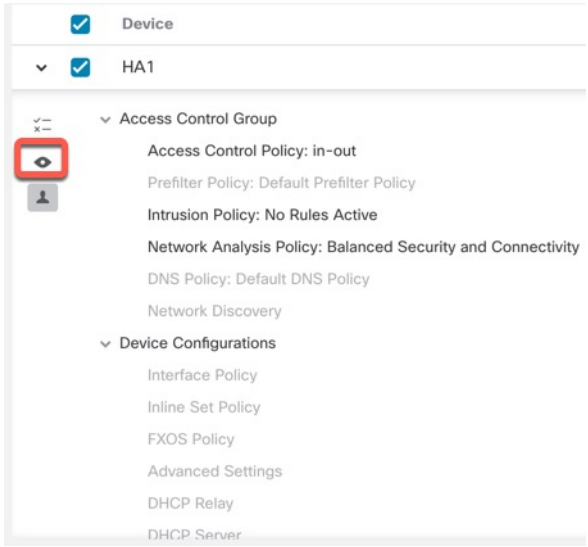
The **Advanced View** tab shows the CLI commands that will be applied. This view is useful if you are familiar with ASA CLI, which is used on the back end of the Firewall Threat Defense.

Figure 34: Advanced View



Step 5 Use **Show or Hide Policy** ( ) to selectively view or hide the associated unmodified policies.

Figure 35: Show or Hide Policy



Step 6 Check the box next to the device name to deploy all configuration changes, or click **Policy selection** ( ) to select individual policies or configurations to deploy while withholding the remaining changes without deploying them.

You can also view the interdependent changes for a certain policy or configuration using this option. The Firewall Management Center dynamically detects dependencies between policies (for example, between an access control policy and an intrusion policy), and between the shared objects and the policies. Interdependent changes are indicated using color-coded tags to identify a set of interdependent deployment changes. When one of the deployment changes is selected, the interdependent changes are automatically selected.

For more information, refer to Guidelines for selective policy deployment, on page 123.

Note

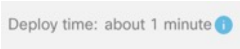
- When the changes in shared objects are deployed, the impacted policies should also be deployed along with them. When you select a shared object during deployment, the impacted policies are automatically selected.
- Selective deployment is not supported for scheduled deployments and deployments using REST APIs. You can only opt for complete deployment of all the changes in these cases.
- The pre-deployment checks for warnings and errors are performed not only on the selected policies, but on all the policies that are out-of-date. Therefore, the warnings or errors list shows the deselected policies as well.
- Similarly, the **Inspect Interruption** column indication on the Deployment page considers all out-of-date policies and not just the selected policies. For information on the **Inspect Interruption** column, refer to Inspection interruption warnings during deployment, on page 127.

Step 7 After you select the devices or policies to deploy, click **Estimate** to get a rough estimate of the deployment duration .

Figure 36: Estimate



Figure 37: Deploy Time



The time duration is a rough estimate (having around 70% accuracy), and the actual time taken for deployment may vary for a few scenarios. The estimate is dependable for deployments of up to 20 devices.

When an estimate is not available, it indicates that the data is not available, since the first successful deployment on the selected device is pending. This situation could occur after the Firewall Management Center reimage, version upgrade, or after a high availability failover.

Note The estimate is incorrect and unreliable for bulk policy changes (in case of bulk policy migrations), and selective deployments because the estimate is based on the heuristic technique.

Step 8 For more details about the Pre-readiness assessment states, refer to .

Step 9 Click **Deploy**.

Configuration changes are deployed to the selected devices. You receive confirmation messages regarding success, warnings, or errors.

What to do next

If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Messages** window. To view complete details, click the arrow icon before the warnings or errors.

You have the following choices:

- Deploy—Continue deploying without resolving warning conditions. Check the **Ignore warnings** checkbox, to ignore warnings and deploy the changes. You cannot proceed if the system identifies errors.
- Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.
- (Optional) Monitor deployment status; see *Viewing Deployment Messages* in the *Cisco Secure Firewall Management Center Administration Guide* .
- If the deployment fails, refer to Best practices for deploying configuration changes, on page 133 .
- During deployment, if there are specific configuration changes in the deployment, the deployment failure may lead to traffic being interrupted. For example, in a cluster environment, an erroneous configuration of an IP address that is not in the same subnet as the Site IPs is configured on the interface. Due to this error, deployment fails and the device attempts to clear the configuration while the rollback operation is being processed. These events collectively lead to a deployment failure that interrupts the traffic.

  See the following table to know what configuration changes may cause traffic interruption when deployment fails.

Table 11: Traffic interruption scenarios

Configuration Changes	Exists?	Traffic Impacted?
Threat Defense Service changes in an access control policy	Yes	Yes
VRF	Yes	Yes
Interface	Yes	Yes
QoS	Yes	Yes

Note The configuration changes interrupting traffic during deployment is valid only if both the Firewall Management Center and the Firewall Threat Defense are of version 6.2.3 or later.

Redeploy existing configurations to a device

Force-deploying existing configurations to a managed device ensures that its policy rules are fully regenerated and applied. This procedure is recommended during maintenance windows or when disruption to network traffic is minimal. Force-deploy takes longer than regular deployment because it generates all policy rules for the device.

Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. Refer to Snort restart traffic behavior, on page 129 and Configurations that restart the snort process when deployed or activated, on page 131.

Before you begin

- Review the guidelines described in Best practices for deploying configuration changes, on page 133.
- Plan to perform the redeployment during a maintenance window or low-impact period.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device where you want to force deployment.

Step 3 Click **Device**.

Step 4 Click **Edit** ( ) next to the **General** section heading.

Step 5 Click **Force Deploy** ( ).

Step 6 Click **Deploy**.

The system identifies any errors or warnings with the configurations you are deploying. You can click **Proceed** to continue without resolving warning conditions. However, you cannot proceed if the system identifies an error.

What to do next

- (Optional) Monitor deployment status; see *Viewing Deployment Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.
- If deploy fails, see Best practices for deploying configuration changes, on page 133.

Deployment management

Firewall Management Center provides a set of deployement management options to oversee configuration changes across your Firewall Threat Defense devices. These options enable you to monitor real-time deployment status, track historical records, and ensure configuration integrity through rollback capabilities. Additionally, you can utilize built-in reporting and policy comparison features to audit changes, verify compliance, and troubleshoot issues.

Deployment status

On the **Deployment** page, the **Status** column provides the deployment status for each device. If a deployment is in progress, a live progress indicator is displayed; otherwise, one of these deployment status values appears:

- **Pending**: Indicates that there are changes in the device that need be deployed.
- **Warnings or errors**: Indicates that the pre-deployment checks have identified warnings or errors for the deployment. You may continue deployment if there are warnings, but not if there are errors.

Note The status column provides the warning or error status only for a single user session on the **Deployment** page. If you navigate away or refresh the page, the status changes to **Pending**.

- **Failed**: Indicates that the previous deployment attempt failed. Click the status to view the details.
- **In queue**: Indicates that deployment is initiated, and the system is yet to start the deployment process.
- **Completed**: Indicates that deployment has completed successfully.

View deployment history

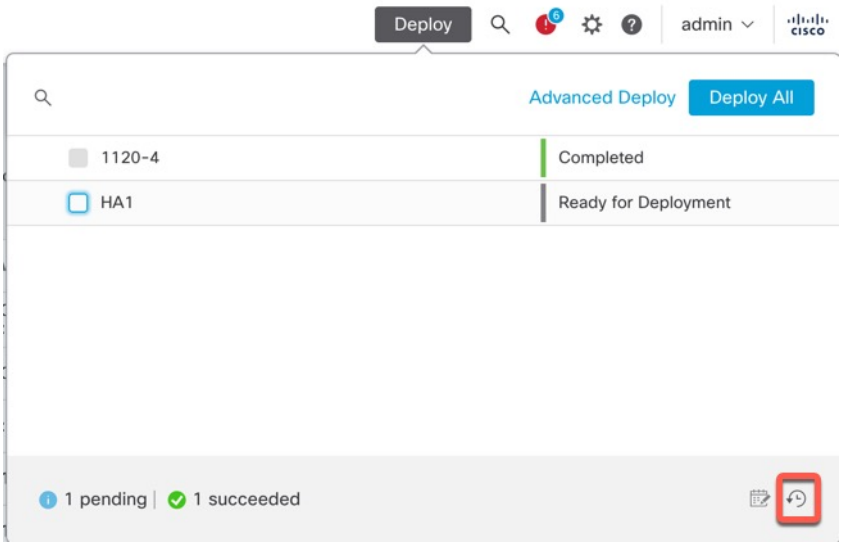
View deployment history to track and analyze past deployment activities, including successful deployments, failed deployments, and rollback operations.

In the deployment history, the last 10 successful deployments, the last 5 failed deployments, and last 5 rollback deployments are captured.

Procedure

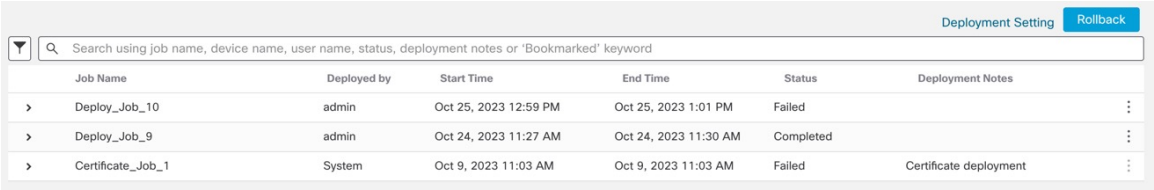
Step 1 On the Firewall Management Center menu bar, click **Deploy** and then click **Deployment History** ( ).

Figure 38: Deployment history icon



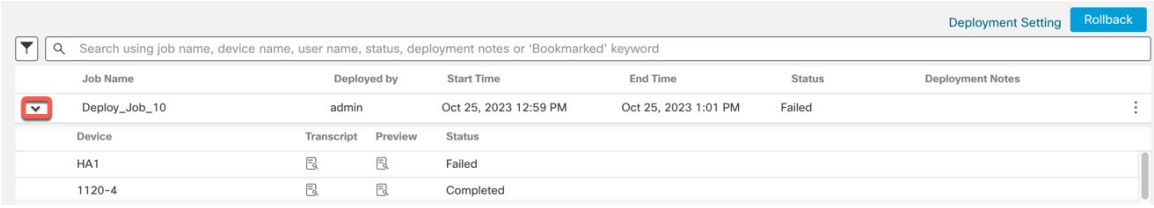
A list of all the previous deployment and rollback jobs is displayed in reverse chronological order.

Figure 39: Deployment history page



Step 2 Click **Expand Arrow** (›) next to the required deployment job to view the devices included in the job and their deployment statuses.

Figure 40: Expand



- View notes in the **Deployment Notes** column.

  Deployment notes are custom notes that a user can add as part of the deployment, and these notes are optional.

Step 3 (Optional) Click **Transcript Details** ( ) to view the commands sent to the device, and the responses received.

Figure 41: Transcript details icon

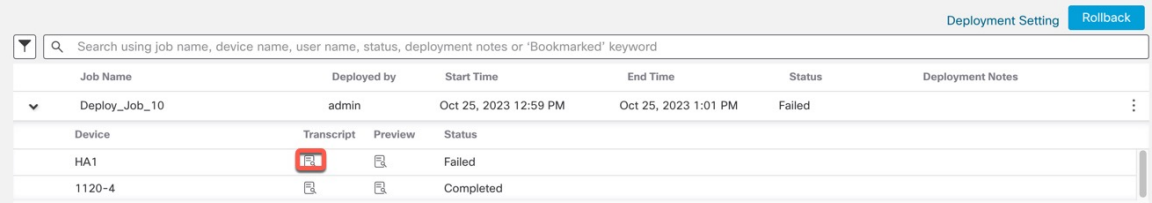
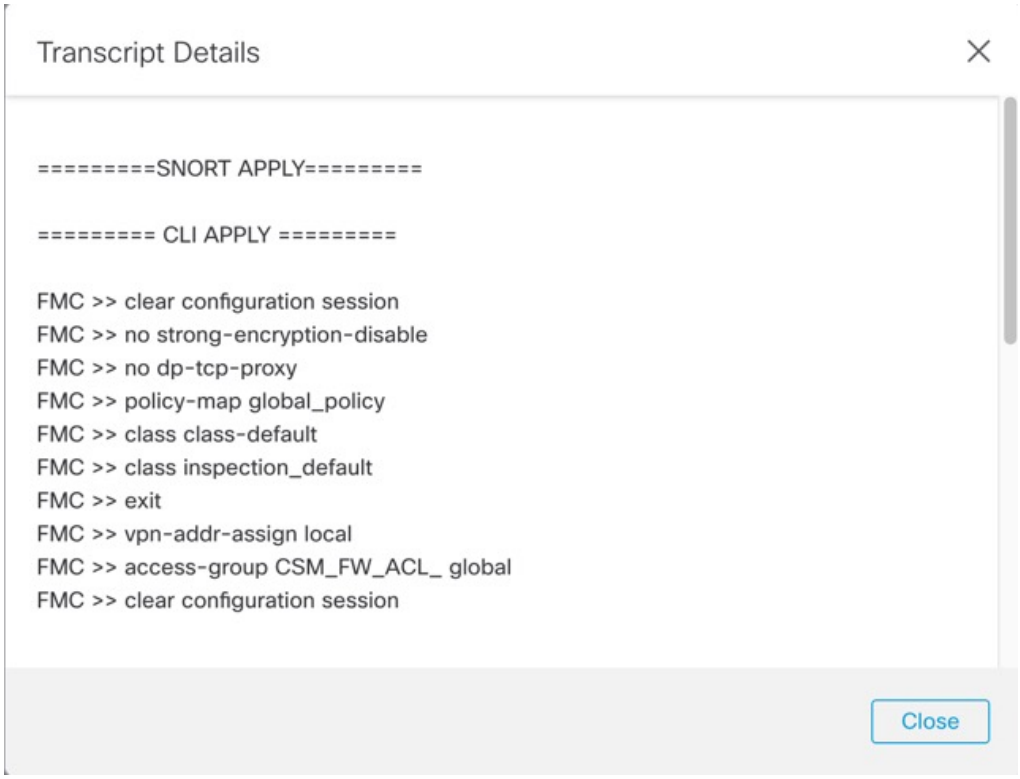


Figure 42: Transcript details



The transcript includes the following sections:

- **Snort Apply**—If there are any failures or responses from Snort-related policies, then the messages are displayed in this section. Normally, the section is empty.
- **CLI Apply**—This section covers features that are configured using commands that are sent to the device.

Note The transcript for the rollback operation does not provide the CLI commands information. To view the rollback commands, see View the deployment rollback transcript, on page 150.

- **Infrastructure Messages**—This section shows the status of different deployment modules.

In the **CLI Apply** section, the deployment transcript includes commands that are sent to the device, and any responses returned from the device. These responses can be informative messages or error messages. For failed deployments, look for messages that indicate errors with the commands. Examining these errors can be particularly helpful if you are using FlexConfig policies to configure customized features. These errors can help you correct the script in the FlexConfig object that is trying to configure the commands.

Note There is no distinction that is made in the transcript between commands that are sent for managed features and those generated from FlexConfig policies.

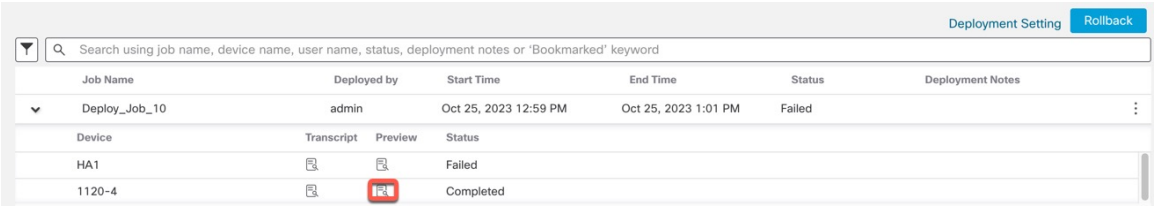
For example, the following sequence shows that Firewall Management Center sent commands to configure GigabitEthernet0/0 with the logical name **outside**. The device responded that it automatically set the security level to 0. Firewall Threat Defense does not use the security level for anything.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

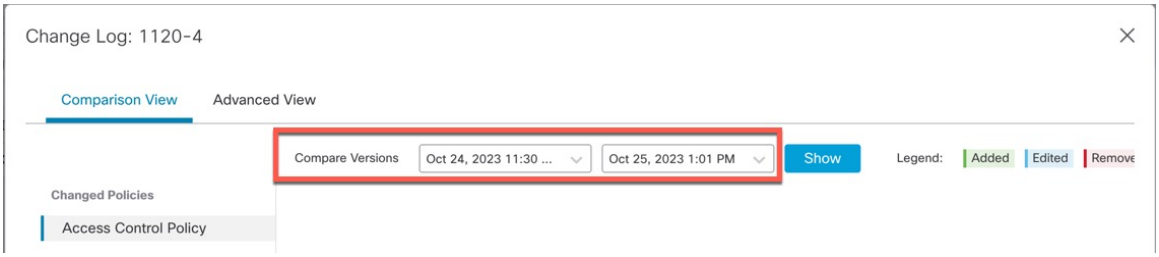
Step 4 (Optional) Click **Preview** ( ) to view the policy and object changes deployed on the device versus the previously deployed version.

Figure 43: Preview icon



a. To compare any two versions and view the change log, choose the required versions in the drop-down boxes and click the **Show** button. The drop-down boxes show the deployment job name and the end time of the deployment.

Figure 44: Compare versions



Note The drop-down boxes also show failed deployments.

b. The **Modified By** column lists the users who have modified the policies or objects.

1. At the policy level, Firewall Management Center displays all the user names who have modified the policy.
2. At the rule level, Firewall Management Center displays the last user who has modified the rule.

c. You can also download a copy of the change log by clicking **Download Report**.

Note

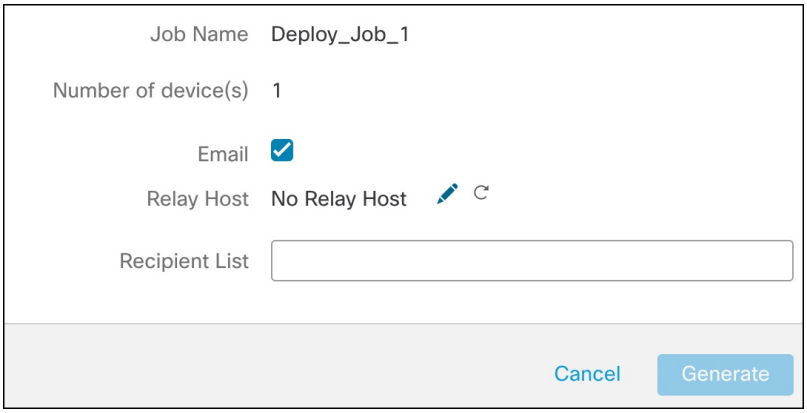
- Deployment history preview is not supported for certificate enrollments, HA operations, and failed deployments.
- When a device is registered, preview is not supported for the job history record that is created.

Step 5 (Optional) Against each deployment job, click the **More** (⋮) icon and execute other actions:

- **Bookmark**—To bookmark the deployment job.
- **Edit Deployment Notes**—To edit your custom deployment notes that you added for a deployment job.
- **Generate Report**—To generate a deployment report, which can be used for auditing. This report includes job properties with preview and transcript information, and the report can be downloaded as a PDF file.

a. Click **Generate Report** to generate a deployment report.

Figure 45: Generate report



b. In the **Generate Report** popup window, check the **Email** checkbox.

c. The report can also be sent through email if mail relay host is configured. If the mail relay host in not configured, use the **Edit** (✎) icon to configure or modify the mail relay host. For more information, see *Configuring a Mail Relay Host and Notification Address* in the *Cisco Secure Firewall Management Center Administration Guide*.

d. In the **Recipient List**, you can enter multiple email adddresses, separated by semicolons.

e. Click **Generate** to generate the report, and this report is emailed to the recipients.

f. In the Notifications task tab, you can track the progress. After the report generation is complete, click the link in the notification task tab to download the PDF report.

Set the number of configuration versions to retain

The Firewall Management Center stores device configuration history files as configuration versions. You can specify the number of configuration versions that you want to retain for a device. This setting allows you to estimate the size of the device configuration files on the disk and keep it within the allowed limit. Reducing the number of configuration versions can reduce the backup size and improve the high-availability synchronization speed of the Firewall Management Center.

Before you begin

- This feature is not supported in Version 7.4.0.
- In a high-availability deployment, configuration version settings are only available on the active Firewall Management Center.

Procedure

Step 1 Choose **Deploy** > **Deployment History** ( ).

Step 2 Click **Deployment Setting**.

Step 3 Choose the number of configuration versions that you want to retain for a device from the **Number of Versions to Retain** drop-down list.

Note Reducing the number of versions removes the oldest configuration versions to match the version size you have selected. You will not be able to preview or roll back to the removed versions.

- **Maximum Permitted Disk Size**: The maximum size for storing configuration versions is 20 GB. The Firewall Management Center calculates the size of configuration versions periodically and sends a health alert if the size of the configuration versions exceeds 20 GB. To resolve the health alert, choose a **Number of Versions to Retain** for which the estimated configuration version size is less than 20 GB.
- **Current Configuration Version Size**: The size of the configuration files on the Firewall Management Center for the previous deployment.
- **Estimated Configuration Version Size**: The approximate size of the configuration files on the Firewall Management Center. It is calculated based on the number of configuration versions you chose to retain.

Step 4 Click **Save**.

Deployment rollback

Deployment rollback is the process of reverting a device to a previously saved configuration state. This operation allows you to restore the device to its earlier state if a recent policy deployment results in unintended traffic behavior.

Note Rollback is a disruptive operation. Executing a rollback terminates all existing connections and resets routing tables, which will cause a temporary interruption of traffic.

Identifying the disruptive configuration

When a deployment has caused unintended traffic interruption, identify the specific change responsible for the condition. To compare current and previous deployments:

Before a rollback

1. Choose **Deploy** > **Deployment History**, expand the last deployed job that caused the traffic disruption, and click the **Preview** ( ).

   The preview page lets you compare deployments to identify specific changes from previous configurations.

2. After identifying the change causing the problem, rectify the configuration and redeploy it on the device.

After a rollback

1. After a successful rollback, choose **Deploy** > **Deployment**, and click the **Preview** icon next to the rolled back device.
2. View the changes between the rolled back configuration and the current changes in the Firewall Management Center that are pending deployment.
3. After identifying the change causing the problem, rectify the configuration, and redeploy it on the device.

Rollback reverts most configurations, but some exceptions apply. Refer the table below for details.

Rollback guidelines

Follow these guidelines to ensure successful configuration rollbacks.

- You have to perform a deployment before you can roll back again.
- After you perform a rollback, the rolled back devices are marked as out-of-date on the Firewall Management Center. The changes you made to the configuration are still pending for the next deployment. To see the pending changes, choose **Deploy** > **Deployment**, and click the **Preview** icon next to the rolled back device.
- For devices with very large access lists, if the **Object Group Search** setting is disabled, then the rollback operation may take a longer duration to complete. To verify the **Object Group Search** setting, choose **Devices** > **Device Management**, and then select the device and click **Edit Advanced Settings**.
- For the Firepower 4100/9300, make sure your current Firewall Chassis Manager interface configuration is the same for any rollback versions. Otherwise, the rollback interface configuration may not match your actual interfaces.

- Independent certificate enrollments are also listed as deployment jobs in the Deployment History page. However, you cannot roll back to these versions. A rollback from a deployment version created after certificate enrollments reverts the certificate associations as well. In the next deployment after a rollback, manually associate the certificates before proceeding with the deployment.
- If a deployment for a device with a FlexConfig object configured with a deployment frequency set to **Once** is rolled back, then you will not be able to redeploy the object even though it is displayed as out-of-date on the Preview page. After a rollback, you will have to manually unassign and then reassign the FlexConfig object to the device before the next deployment.

Rollback limitations

Observe these limitations that restrict the use of rollback functionality.

- You can roll back to any one of the last 10 versions before the currently deployed version. Rollback to versions prior to these are not supported. The rollback icon is greyed out for unsupported versions.
- Rollback is not supported if the manager access interface (Manager or data interface) is different between the rollback version and the current version.
- If you upgrade the Firewall Management Center, all rollback versions from the previous software release will no longer be available for devices, even if you did not upgrade the devices.
- If you upgrade the device, you can only roll back to versions on the current software release.
- For High Availability, rollback is not supported in these scenarios:
  - When the version you want to roll back to contains the high-availability bootstrap configuration. In other words, the deployment when you first formed high availability for the standalone devices.
  - When a device that is currently in standalone mode was part of a high availability pair in the previous deployment version.
- For clustering:
  - Rollback is not supported when a device that is currently in standalone mode was part of a cluster in the previous deployment version.
  - (Secure Firewall 3100/4200 and Firewall Threat Defense Virtual in a private cloud) If you change the clustering bootstrap configuration or add or delete nodes, you cannot roll back to a version prior to those changes.

Table 12: Configurations reverted and not reverted during rollback

Configurations that are reverted during a rollback	Configurations that are not reverted during a rollback
• All policy configurations • Interface configurations • SRU configurations • VDB configurations • LSP configurations • VPN configurations • FXOS configurations	• Snort binaries • Geo DB

Perform a rollback

Use rollback to revert a device to a previously deployed configuration when the traffic through the device is affected in an unintended way after a policy deployment.

You can roll back a device to a previously deployed configuration. After a policy deployment, if the traffic through the device is affected in an unintended way, rollback provides an option to revert the device to the earlier state, which existed before the faulty deployment.

Rollback reverts the configuration only on the selected devices.

Procedure

Step 1 Choose **Deploy >Deployment History** ( ).

A list of all the previous deployment jobs is displayed in reverse chronological order.

Step 2 Click **Rollback**.

Step 3 Filter the list of devices displayed by either clicking **Job** and choosing a job from the **Selected Job** drop-down list, or by clicking **Device List**.

Step 4 (Optional) Enter the device name in the **Search Device** search box to filter the device list.

Step 5 Check the box next to the devices you want to roll back and choose the version for each device from the **Rollback Version** drop-down list.

Figure 46: Selected job list

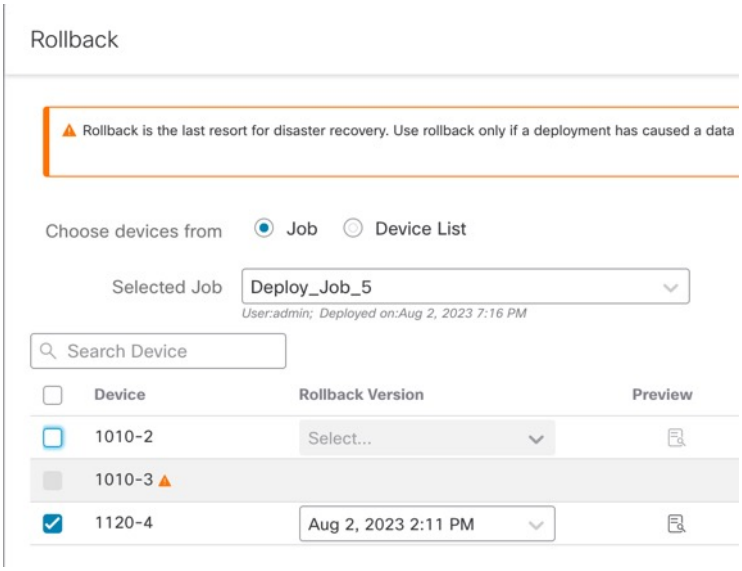
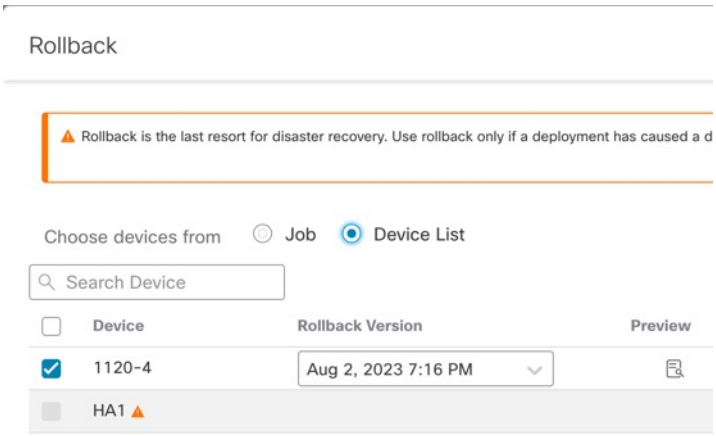


Figure 47: Device list



The job names and associated deployment notes are also listed for a particular rollback version.

Step 6 (Optional) Click the **Preview** ( ) to view the changes deployed in the selected version.

Step 7 Click **Rollback** to restore the selected devices to the chosen configuration version.

What to do next

To verify rollback status, go to **Deploy** > **Deployment** and check the rollback status next to the device name.

View the deployment rollback transcript

View the CLI commands that were executed during a successful rollback operation to understand what changes were made to the device configuration.

Rollback transcript is a written version of the commands that are sent to the device, along with the responses returned from the device. If a rollback operation has failed, the reason for the failure can be viewed by clicking **Deploy**, and then click the **Deployment History** (). However, to know the CLI commands executed for a successful rollback operation, follow the steps given below after a rollback operation has completed.

Note

- The CLI command information is available after a rollback is complete and is available only until the next deployment. The first deployment after a rollback operation erases all the rollback-related information.
- For any rollback deployment, the deployment notes are updated automatically as rollback job. In the **Deployment History** page, the user can filter the rollback jobs easily using the search option.

Procedure

Step 1 On the Secure Firewall Management Center menu bar, choose **System** () > **Health** > **Monitor**.
Step 2 Select the device, which was rolled back, from the left pane.
Step 3 Click **View System & Troubleshooting Details** link.
Step 4 Click **Advanced Troubleshooting**.
Step 5 Click **Threat Defense CLI**.
Step 6 Select **show** from the **Command** drop-down box.
Step 7 Enter `running` in the **Parameter** field.
Step 8 Click **Execute**.

Download policy changes report for multiple devices

Download reports on the policy and object changes made since your last deployment for multiple Firewall Threat Defense devices. Reports help you review pending changes before completing deployment. The reports are provided as a zip file containing:

- A pending changes report for each device, previewing modifications to policy or objects that are to be deployed on the device. For more information, refer to Deploy configuration changes, on page 135 and Deployment Preview.
- A consolidated report categorizing each device by report status.

Procedure

Step 1 Choose **Deploy** > **Advanced Deploy**.
Step 2 Check the check box next to the devices for which you want to generate a pending policy changes report, and then click **Pending Changes Reports**.
Step 3 Click **Pending Changes Reports**. Reports are generated in the background.

Step 4 On the Firewall Management Center menu bar, choose **Notifications** > **Tasks** to view the report generation task.

When the report request task is complete, the download link appears within the task notification.

Step 5 Click the **Download Report(s)** link to download the reports.

Compare policies

Policy comparison allows you to examine the differences between two policies or between a saved policy and the running configuration to review policy changes for compliance with your organization's standards or to optimize system performance.

You can compare these policy types:

- DNS
- File
- Health
- Identity
- Network Analysis
- SSL

The comparison view displays both policies in a side-by-side format. Differences between the two policies are highlighted:

- Blue indicates that the highlighted setting is different in the two policies, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy but not the other.

Before you begin

You can compare policies only if you have access rights and any required licenses for the specific policy, and you are in the correct domain for configuring the policy.

Procedure

Step 1 Access the management page for the policy you want to compare:

- DNS—**Policies** > **Access Control heading** > **DNS**
- File—**Policies** > **Access Control heading** > **Malware & File**
- Health—**System** (⚙) > **Health** > **Policy**
- Identity—**Policies** > **Access Control heading** > **Identity**
- Network Analysis—**Policies** > **Access Control heading** > **Access Control**, and then click **Network Analysis Policy** or **Policies** > **Access Control heading** > **Intrusion**, and then click **Network Analysis Policies**.

Note If your custom user role limits access to the first path listed here, use the second path to access the policy.

- SSL—**Policies** > **Access Control heading** > **Decryption**

Step 2 Click **Compare Policies**.

Step 3 From the **Compare Against** drop-down list, choose the type of comparison you want to make:

- To compare two different policies, choose **Other Policy**.
- To compare two revisions of the same policy, choose **Other Revision**.
- To compare another policy to the currently active policy, choose **Running Configuration**.

Step 4 Depending on the comparison type you choose, you have various choices:

- If you are comparing two different policies, choose the policies you want to compare from the **Policy A** and **Policy B** drop-down lists.
- If you are comparing the running configuration to another policy, choose the second policy from the **Policy B** drop-down list.

Step 5 Click **OK**.

Step 6 Review the comparison results:

- Comparison Viewer—To use the comparison viewer to navigate individually through policy differences, click **Previous** or **Next** above the title bar.
- Comparison Report—To generate a PDF report that lists the differences between the two policies, click **Comparison Report**.

Generate current policy reports

You can generate two types of reports for most policies: a single-policy report detailing the policy's current saved configuration, and a comparison report listing differences between two policies. You can generate a single-policy report for all policy types except health.

Note Intrusion policy reports combine the settings in the base policy with the settings of the policy layers, and make no distinction between which settings originated in the base policy or policy layer.

Before you begin

- Ensure you have the required access rights and licenses for the specific policy.
- Verify you are operating within the correct domain for the policy you wish to report.

Procedure

Step 1 Access the management page for the policy for which you want to generate a report:

- Access Control—**Policies** > **Access Control heading** > **Access Control**
- DNS—**Policies** > **Access Control heading** > **DNS**
- File—**Policies** > **Access Control heading** > **Malware & File**
- Health—**System** (⚙) > **Health** > **Policy**
- Identity—**Policies** > **Access Control heading** > **Identity**
- Intrusion—**Policies** > **Access Control heading** > **Intrusion**
- NAT—**Devices** > **NAT**
- Network Analysis—**Policies** > **Access Control heading** > **Access Control**, and then click **Network Analysis Policy** or **Policies** > **Access Control heading** > **Intrusion**, and then click **Network Analysis Policies**

Note If your custom user role limits access to the first path listed here, use the second path to access the policy.

- SSL—**Policies** > **Access Control heading** > **Decryption**

Step 2 Click **Report** (📄) next to the policy for which you want to generate a report.

History for configuration deployment

This reference provides a chronological history of configuration deployment features introduced across different software versions, including deployment rollback capabilities, advanced deployment views, report generation, and deployment preview functionality.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Set the number of deployment history files to retain for device rollback.	7.2.6 7.4.1	Any	You can now set the number of deployment history files to retain for device rollback, up to ten (the default). This can help you save disk space on the Firewall Management Center. New/modified screens: **Deploy** > **Deployment History** > **Deployment Setting** > **Configuration Version Setting**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	7.2.6 7.4.1	Any	You can generate, view, and download the reports as a zip file on configuration changes since your last deployment: • A *policy changes* report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A *consolidated* report that categorizes each device based on the status of policy changes report generation. This is especially useful after you upgrade either the Firewall Management Center or Firewall Threat Defense, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**.
Generate and email a report when you deploy configuration changes.	7.2	Any	You can now generate a report for any deployment. New/modified screens: **Deploy** > **Deployment History icon** > **More** > **Generate Report**
Deployment preview and user information in preview.	7.0	Any	The Deployment page has the following newly added features: • On the **Deployment** page, the **Modified By** column lists the users who have modified the policies against each policy listing. • Filter support for deployment – The Filter icon provided on the **Deployment** page provides an option to filter the device listings that are pending deployment. The Filter icon provides options to filter the listings based on selected devices and user names. • Deployment History Preview – Click **Preview** to view the policy and object changes deployed on the device versus the previously deployed version. In the deployment history, the last 10 successful deployments, the last five failed deployments, and last five rollback deployments are captured. • Deployment Notes – The **Deployment Notes** are custom and optional notes that a user can add as part of deployment. You can view the **Deployment Notes** column in the **Deployment History** page. • Deployment rollback is available for Snort 3 policies as well.
Roll back deployment on Firewall Threat Defense devices.	6.7	6.7	Rollback is a deployment functionality provided to remove the existing deployment on Firewall Threat Defense devices and to reconfigure the device with the previously deployed configuration. New/modified pages: The **Deploy** > **Deployment History** page provides a new Rollback column with the rollback icons. Similar rollback icons can also be found when the jobs are expanded, to initiate rollback at the device level.

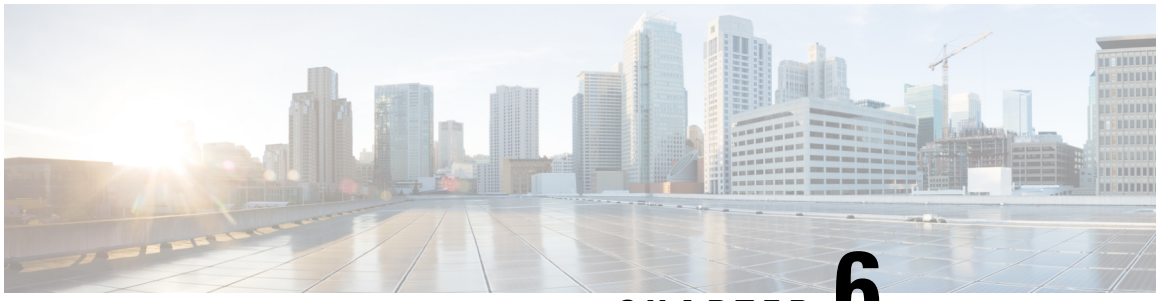
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New deployment web interface.	6.6	Any	The **Deploy** button on the Firewall Management Center menu bar is changed to **Deploy** menu. There are two new sub-menu options under it. These are **Deployment** and **Deployment History**. The Deployment page has undergone an improvement along with newly added features, and the new Deployment History page provides a legend of all the previous deployments. The Deployment page has the following newly added features: • Deployment status - On the Deployment page, the Status column provides the deployment status for each device. • Deployment estimate - The **Estimate** link is available on the Deployment page after you select a device, a policy, or a configuration. The **Estimate** link provides an estimate of the deployment duration once clicked. • Deployment preview - Preview provides a snapshot of all the policy and object changes to be deployed on the device. The policy changes include the new policies, changes in the existing policies, and the deleted policies. The object changes include the added and modified objects which are used in policies. • Selective policy deployment - Firewall Management Center allows you to select a specific policy within the list of all the changes on the device that are due for deployment and deploy only the selected policy.



PART II

High Availability and Scalability

- Multi-Instance Mode, on page 159
- Logical Devices on the Firepower 4100/9300, on page 223
- High Availability for Devices, on page 283
- Clustering: Secure Firewall 3100/4200, on page 323
- Clustering: Private Cloud , on page 385
- Clustering: Public Cloud, on page 437
- Clustering: Firepower 4100/9300, on page 529



CHAPTER 6

Multi-Instance Mode

You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). This chapter describes how to deploy the device in multi-instance mode.

- Multi-instance mode, on page 159
- Licenses for instances, on page 171
- Requirements and prerequisites for instances, on page 171
- Guidelines and limitations for instances, on page 172
- Instance configuration, on page 175
- Multi-instance mode, on page 219
- Multi-instance mode feature and version history, on page 222

Multi-instance mode

Multi-instance mode is a deployment mode that enables multiple container instances on a single chassis that act as completely independent devices.

Multi-instance modes and appliance modes

A multi-instance mode and an appliance mode are deployment types for network devices that

- determine whether the device operates as a single instance or supports multiple, independent instances,
- offer distinct management and configuration options at both the chassis and instance levels, and
- provide different approaches to resource allocation, interface assignment, and monitoring.

You can run the device in either appliance mode or multi-instance mode.

Appliance mode

Appliance mode is the default. The device runs the native Firewall Threat Defense image and acts as a single device. The only chassis-level configuration available (on the **Chassis Manager** page) is for network module management (breakout ports or enabling/disabling a network module).

Multi-instance mode

If you change to multi-instance mode, the device runs the Secure Firewall eXtensible Operating System (FXOS) on the chassis, while each instance runs separate Firewall Threat Defense images. You can configure the mode using the FXOS CLI.

Because multiple instances run on the same chassis, you need to perform chassis-level management of:

- CPU and memory resources using resource profiles.
- Interface configuration and assignment.
- Deployment and monitoring of instances.

For a multi-instance device, you add the *chassis* to the Firewall Management Center and configure chassis-level settings on the **Chassis Manager** page.

Chassis management interface

A chassis management interface is a network hardware feature that

- provides a dedicated pathway for device management and control,
- supports multi-instance modes by allowing each software instance its own management IP address, and
- separates management, eventing, and application access to streamline security, access, and monitoring.

Chassis management

The chassis uses the dedicated Management interface on the device. Multi-instance mode does not support using a data interface for chassis management or DHCP addressing for the Management interface.

You can only configure the chassis Management interface at the Firewall Threat Defense CLI (at initial setup) or FXOS CLI (after you convert to multi-instance mode). Refer to Enable multi-instance mode, on page 175 for initial setup. Refer to Change chassis management settings at the FXOS CLI, on page 216 to change Management interface settings in multi-instance mode.

Note By default, SSH is not allowed to this interface in multi-instance mode unless you enable the SSH server and an SSH access list. This difference means that you can connect to the application-mode threat defense Management interface using SSH, but after you convert to multi-instance mode, you can no longer connect using SSH by default. For more information, refer to Configure SSH and SSH access list, on page 201.

Instance management

All instances share the chassis management interface, and each instance has its own IP address on the Management network. After you add the instance and specify the IP address, you can make changes to the network settings at the Firewall Threat Defense CLI.

The instance Management IP address allows SSH by default.

Instance interfaces

A chassis interface is a network connection point that

- allows flexible assignment to instances through physical connections or VLAN subinterfaces,
- enables sharing (physical or VLAN) between multiple instances for efficient resource use, and
- restricts certain interface features (like subinterfaces or sharing) in multi-instance clusters, except for control links.

To provide flexible physical interface use for instances, you can create VLAN subinterfaces on the chassis and also share interfaces (VLAN or physical) between multiple instances. Refer to Shared interface scalability, on page 163 and Configure a subinterface, on page 187.

Note This chapter discusses *chassis* VLAN subinterfaces only. You can separately create subinterfaces within the Firewall Threat Defense instance. For more information, refer to Chassis interfaces vs. instance interfaces, on page 161.

Interface types

An interface type is a network configuration element that

- determines how physical interfaces, VLAN subinterfaces, and EtherChannel interfaces are used in deployment, and
- defines whether interfaces can be shared among instances or dedicated to specific traffic.

Physical interfaces, VLAN subinterfaces, and EtherChannel interfaces can be one of these types:

- Data: Use for regular data or the failover link. Data interfaces cannot be shared between instances, and instances cannot communicate over the backplane to other instances. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another instance. You can add VLAN subinterfaces to a data interface to provide separate failover links per High Availability pair.
- Data-sharing: Use for regular data. These data interfaces can be shared by one or more instances. Each instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

Chassis interfaces vs. instance interfaces

Chassis interfaces vs. instance interfaces is an interface management model that

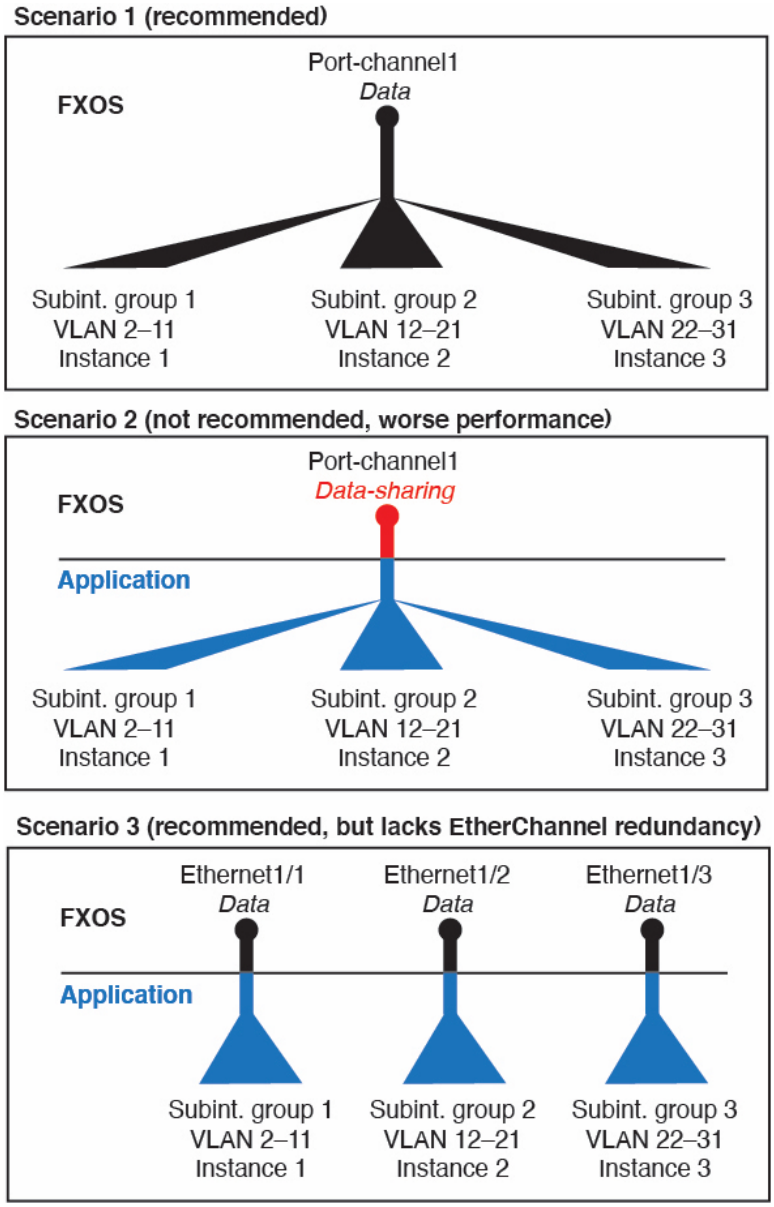
- manages basic Ethernet settings of physical interfaces, VLAN subinterfaces for instances, and EtherChannel interfaces at the chassis level,
- configures higher level settings within the instance, such as IP addresses for EtherChannels, and
- allows independent administrative control of interface states in both chassis and instance locations.

VLAN subinterfaces

You can create VLAN subinterfaces within the instance, just as you would for any device.

You can *also* create VLAN subinterfaces in the chassis. The instance-defined subinterfaces are not subject to the chassis limit. Choosing in which location to create subinterfaces depends on your network deployment and personal preference. For example, to share a subinterface, you must create the subinterface on the chassis. Another scenario that favors chassis subinterfaces comprises allocating separate subinterface groups on a single interface to multiple instances. For example, you want to use Port-channel1 with VLAN 2–11 on instance A, VLAN 12–21 on instance B, and VLAN 22–31 on instance C. If you create these subinterfaces in the instance, then you would have to share the parent interface in the chassis, which may not be desirable. See this illustration that shows the three ways you can accomplish this scenario:

Figure 48: VLANs in the chassis vs. the instance



Independent interface states in the chassis and in the instance

You can administratively enable and disable interfaces in both the chassis and in the instance. For an interface to be operational, the interface must be enabled in both locations. Because the interface state is controlled independently, you may have a mismatch between the chassis and instance.

The default state of an interface within the instance depends on the type of interface. For example, the physical interface or EtherChannel is disabled by default within the instance, but a subinterface is enabled by default.

Shared interface scalability

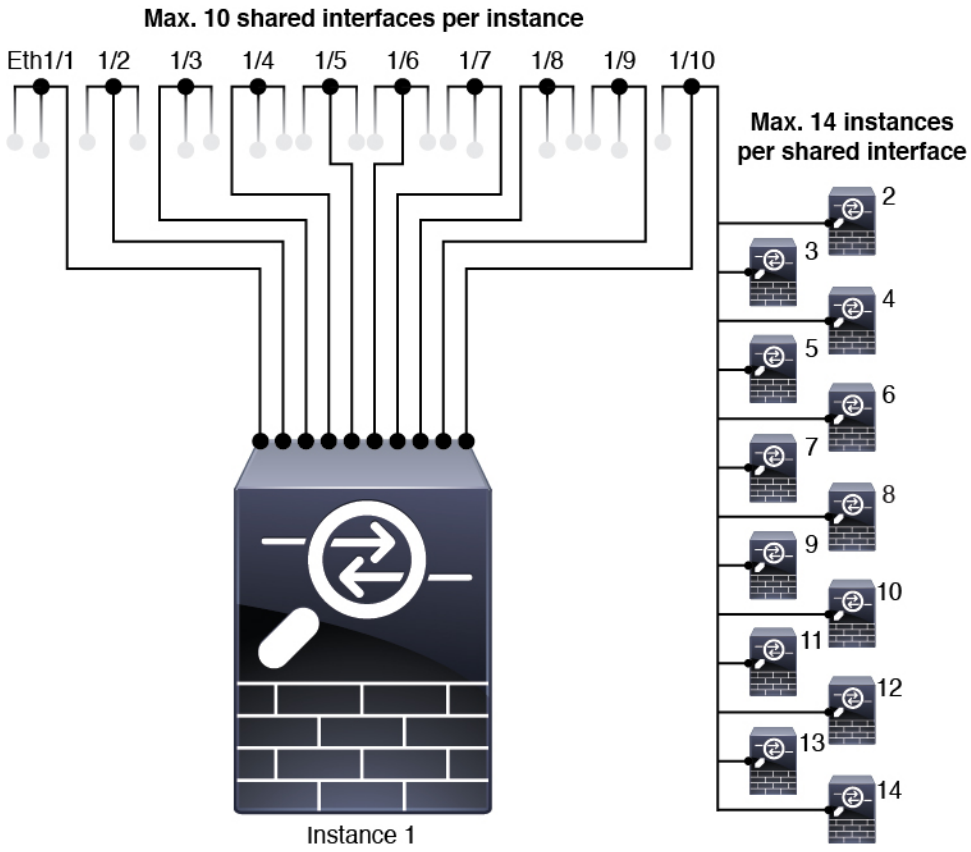
A shared interface is a network resource that

- allows multiple logical connections to transmit data concurrently,
- adapts bandwidth allocation based on real-time demand, and
- enhances scalability to support growing numbers of devices and traffic flows.

Instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. You can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:



Shared interface best practices

This topic outlines the best practices to follow when configuring shared interfaces to maximize performance and security.

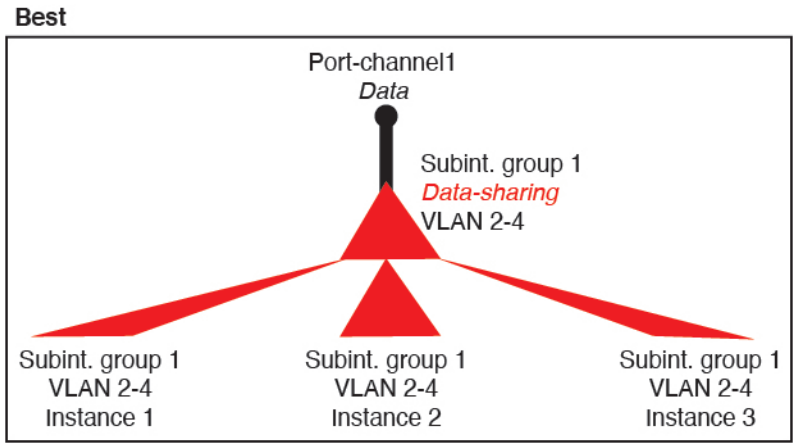
For optimal scalability of the forwarding table, share as few interfaces as possible. Instead, you can create up to 500 VLAN subinterfaces on one or more physical interfaces and then divide the VLANs among the container instances.

When sharing interfaces, follow these practices in the order of most scalable to least scalable:

1. Best: Share subinterfaces under a single parent, and use the same set of subinterfaces with the same group of instances.

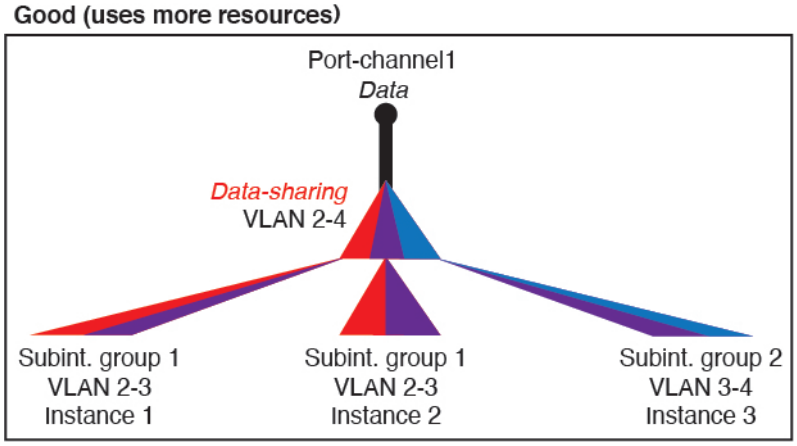
   For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel: Port-Channel1.2, 3, and 4 instead of Port-Channel2, Port-Channel3, and Port-Channel4. When you share subinterfaces from a single parent, the VLAN group table provides better scaling of the forwarding table than when sharing physical/EtherChannel interfaces or subinterfaces across parents.

Figure 49: Best: Shared Subinterface Group on One Parent



If you do not share the same set of subinterfaces with a group of instances, your configuration can cause more resource usage (more VLAN groups). For example, share Port-Channel1.2, 3, and 4 with instances 1, 2, and 3 (one VLAN group) instead of sharing Port-Channel1.2 and 3 with instances 1 and 2, while sharing Port-Channel1.3 and 4 with instance 3 (two VLAN groups).

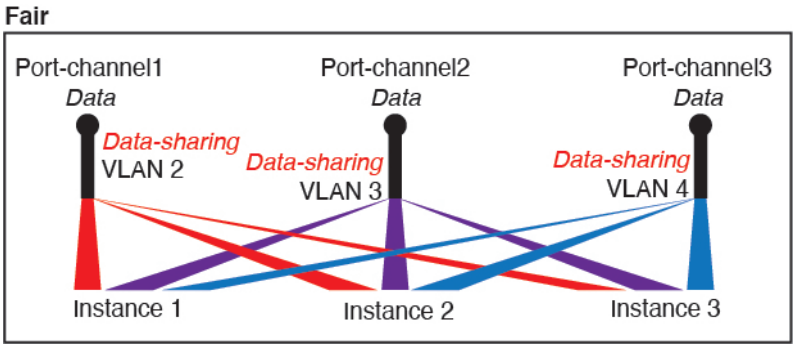
Figure 50: Good: Sharing Multiple Subinterface Groups on One Parent



2. Fair: Share subinterfaces across parents.

   For example, share Port-Channel1.2, Port-Channel2.3, and Port-Channel3.4 instead of Port-Channel2, Port-Channel4, and Port-Channel4. Although this usage is not as efficient as only sharing subinterfaces on the same parent, it still takes advantage of VLAN groups.

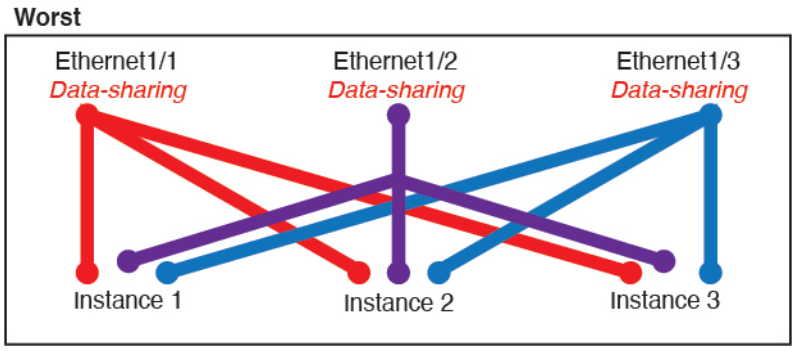
Figure 51: Fair: Shared Subinterfaces on Separate Parents



3. Worst: Share individual parent interfaces (physical or EtherChannel).

   This method uses the most forwarding table entries.

Figure 52: Worst: Shared Parent Interfaces



How the chassis classifies packets

The chassis processes incoming and outgoing packets as they pass through a device, ensuring that each packet is handled according to its type, destination, and security requirements.

Each packet that enters the chassis must be classified so that the chassis can determine to which instance to send a packet.

- Unique Interfaces: If only one instance is associated with the ingress interface, the chassis classifies the packet into that instance. For bridge group member interfaces (in transparent mode or routed mode), inline sets, or passive interfaces, this method is used to classify packets at all times.
- Unique MAC Addresses: The chassis automatically generates unique MAC addresses for all interfaces, including shared interfaces. If multiple instances share an interface, then the classifier uses unique MAC addresses assigned to the interface in each instance. An upstream router cannot route directly to an instance without unique MAC addresses. You can also set the MAC addresses manually when you configure each interface within the application.

Note If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each instance.

Classification examples

This reference provides examples to help you understand different classification scenarios and their implementation.

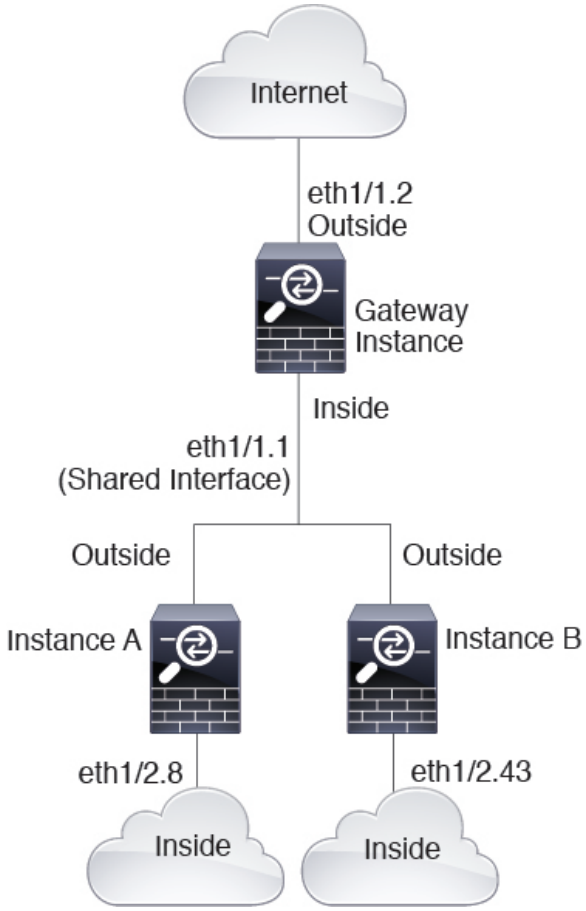
Cascading container instances

Cascading instances connect one instance's outside interface to another's inside interface, simplifying configuration by sharing parameters in the top instance. Avoid using shared interfaces with High Availability to prevent MAC address conflicts; use unique interfaces and an external switch instead.

Placing an instance directly in front of another instance is called *cascading instances*; the outside interface of one instance is the same interface as the inside interface of another instance. You might want to cascade instances if you want to simplify the configuration of some instances by configuring shared parameters in the top instance.

The following figure shows a gateway instance with two instances behind the gateway.

Figure 53: Cascading Instances



Note Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.

Typical multi-instance deployments

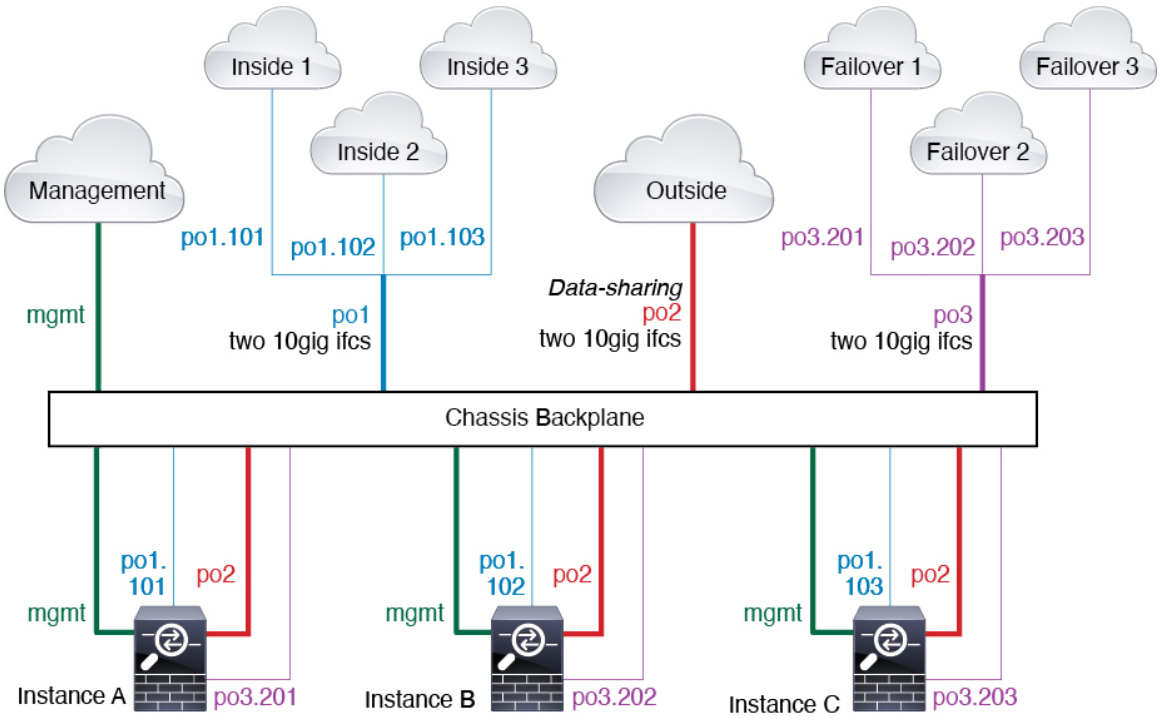
A typical multi-instance deployment is a firewall configuration that

- supports multiple container instances operating simultaneously,
- configures distinct interfaces for management, inside, outside, and failover connectivity, and
- utilizes dedicated subinterfaces and EtherChannels to enhance performance and reliability.

The following example includes three container instances in routed firewall mode. They include the following interfaces:

- Management: All instances and the chassis use the dedicated Management interface. Within each instance (and the chassis), the interface uses a unique IP address on the same management network.
- Inside: Each instance uses a subinterface on Port-Channel1 (data type). This EtherChannel includes two 10 Gigibit Ethernet interfaces. Each subinterface is on a separate network.
- Outside: All instances use the Port-Channel2 interface (data-sharing type). This EtherChannel includes two 10 Gigibit Ethernet interfaces. Within each application, the interface uses a unique IP address on the same outside network.
- Failover: Each instance uses a subinterface on Port-Channel3 (data type). This EtherChannel includes two 10 Gigibit Ethernet interfaces. Each subinterface is on a separate network.

Figure 54: Typical multi-instance deployment



Automatic MAC addresses for instance interfaces

An automatic MAC address for instance interfaces is a network identifier that is automatically generated and assigned to instance interfaces in multi-instance deployments.

The chassis automatically generates MAC addresses for instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the instance, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the instance.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

The chassis generates the MAC address using the following format:

A2*xx.yyzz.zzzz*

Where *xx.yy* is a user-defined prefix or a system-defined prefix, and *zz.zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the chassis native form:

A2**4D.00***zz.zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1.03***zz.zzzz*

Performance scaling factors for multi-instance modes

A performance scaling factor is a throughput adjustment metric that

- enables calculation of effective throughput in multi-instance appliance modes,
- considers the percentage of CPU cores assigned to each instance, and
- accounts for efficiency reductions compared to single-instance (appliance mode) operation.

The maximum throughput (connections, VPN sessions) for a platform is calculated for an appliance mode device's use of memory and CPU (and this value is shown in **show resource usage**). If you use multiple instances, then you need to calculate the throughput based on the percentage of CPU cores that you assign to the instance. For example, if you use an instance with 50% of the cores, then you should initially calculate 50% of the throughput. Moreover, the throughput available to an instance may be less than that available to an appliance.

For detailed instructions on calculating the throughput for instances, refer to https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html.

Instances and high availability

A high availability pair is a deployment option that

- uses two instances on separate chassis to ensure service continuity,
- allows for multiple high availability pairs to be created from available instances, and
- permits standalone instances to exist alongside high availability pairs within the same chassis.

You can use High Availability using an instance on 2 separate chassis; for example, if you have 2 chassis, each with 10 instances, you can create 10 High Availability pairs. You can also have standalone instances on the same chassis as High Availability instances. For more information about the requirements, refer to Requirements and prerequisites for instances, on page 171.

Note Clustering is not supported.

Licenses for instances

This reference provides information about how licenses are assigned and consumed for chassis and feature instances.

All licenses are consumed per chassis and not per instance. Refer to these details.

- Essentials licenses are assigned to the chassis as a whole, one per chassis.
- Feature licenses are assigned to each instance, but you only *consume* one license per feature per chassis.

Requirements and prerequisites for instances

This reference provides the requirements and prerequisites for deploying instances on Secure Firewall models, including supported models, upgrade paths, resource limitations per model, software requirements, high availability requirements, and management center requirements.

Model support

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140

Note The Secure Firewall 3105 is not supported.

Maximum container instances and resources per model

For each container instance, you can specify the number of CPU cores (or more specifically, threads) to assign to the instance. We use the term "core" generically to account for different hardware architecture. RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

Table 13: Maximum container instances and resources per model

Model	Max. Container Instances	Available CPU Cores (Threads)
Secure Firewall 3110	3	22
Secure Firewall 3120	5	30

Model	Max. Container Instances	Available CPU Cores (Threads)
Secure Firewall 3130	7	46
Secure Firewall 3140	10	62

Software requirements

- You can run different versions of Firewall Threat Defense software on each instance as long as they are all compatible with the version of FXOS running on the chassis.
- You cannot deploy an instance with a patch version of the Firewall Threat Defense software because it is not a complete bundle. You need to first deploy the major or maintenance version, and then patch it after deployment.

High availability requirements

- The two instances in a High Availability configuration must:
  - Be on separate chassis.
  - Be on the same model.
  - Have the same interfaces assigned. All interfaces must be preconfigured in the chassis identically before you enable High Availability.
  - Use the same resource profile attributes. The profile names can be different, but the definitions need to match.

Firewall Management Center requirements

For chassis management and all instances on the chassis, you must use the same Firewall Management Center due to the licensing implementation.

Guidelines and limitations for instances

This reference provides guidelines and limitations for managing instances on chassis, including general requirements, interface configurations, VLAN subinterfaces, EtherChannels, data-sharing interfaces, and MAC address considerations.

General guidelines

- A single Firewall Management Center must manage all instances on a chassis, as well as manage the chassis itself.
- For instances, these features are not supported:
  - TLS crypto acceleration
  - Clustering
  - Firewall Management Center UCAPL/CC mode

- Flow offload to hardware
- LLDP

- Primary management of the chassis by Security Cloud Control cloud-delivered Firewall Management Center and separate analytics-only management of the chassis by an on-prem Firewall Management Center is not supported. You can however add Security Cloud Control-managed instances to an analytics-only on-prem Firewall Management Center.

Management interface

- No support for a data interface for chassis management; only the dedicated Management interface can be used
- No DHCP addressing for the Management interface
- The management connection requires TCP port 8305; do not change the value from the default.

VLAN subinterfaces

- This document discusses *chassis* VLAN subinterfaces only. You can separately create subinterfaces within the instance.
- If you assign a parent interface to an instance, it only passes untagged (non-VLAN) traffic. Do not assign the parent interface unless you intend to pass untagged traffic.
- Subinterfaces are supported on Data or Data-sharing type interfaces.
- You can create up to 500 VLAN IDs.
- You cannot use subinterfaces for an inline set or as a passive interface.
- If you use a subinterface for the failover link, then all subinterfaces on that parent, and the parent itself, are restricted for use as failover links. You cannot use some subinterfaces as failover links, and some as regular data interfaces.

EtherChannels

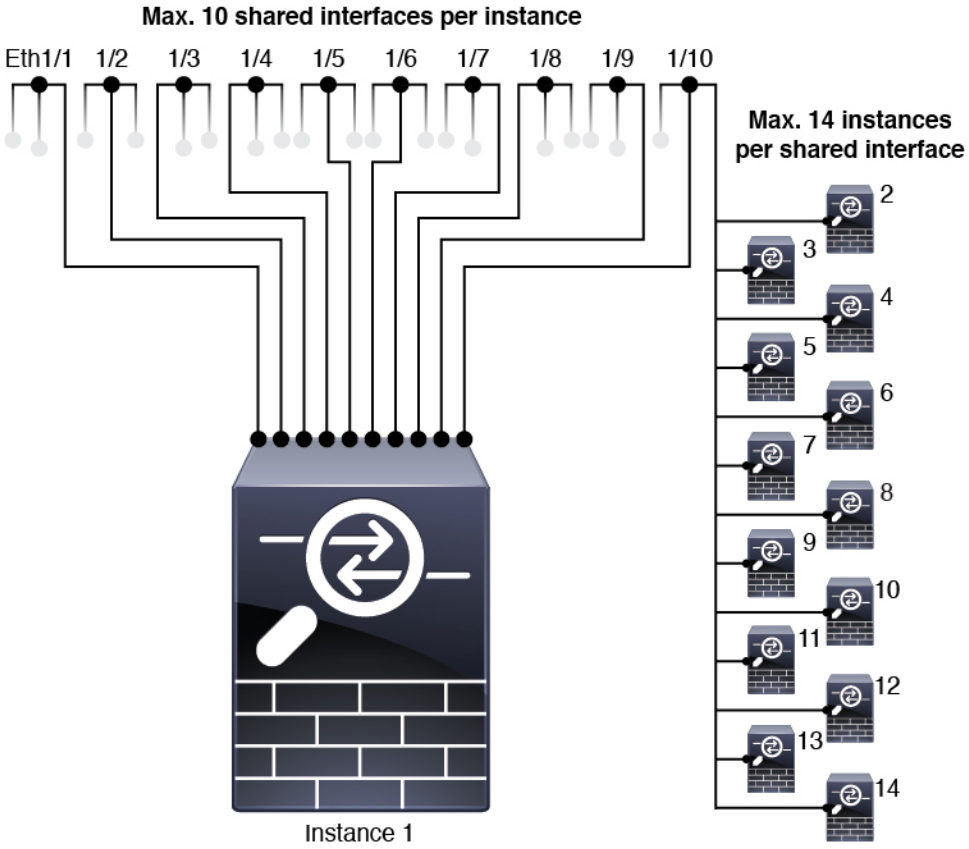
- You can configure up to 48 EtherChannels, limited by the number of physical interfaces.
- The EtherChannel can have up to 8 active interfaces.
- All interfaces in the EtherChannel must be the same media type and speed capacity. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, unless you set the speed to **Detect SFP**; in this case, you can use different interface capacities, and the lowest common speed is used.
- The chassis does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS **VLAN dot1Q tag native** command, then the chassis will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- In Cisco IOS software versions earlier than 15.1(1)S2, the chassis did not support connecting an EtherChannel to a switch stack. With default switch settings, if the chassis EtherChannel is connected cross stack, and if the primary switch is powered down, then the EtherChannel connected to the remaining

switch will not come up. To improve compatibility, set the **stack-MAC persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

Data-sharing interfaces

- Maximum 14 instances per shared interface. For example, you can allocate Ethernet1/1 to Instance1 through Instance14.

  Maximum 10 shared interfaces per instance. For example, you can allocate Ethernet1/1.1 through Ethernet1/1.10 to Instance1.



- You cannot use a data-sharing interface with a transparent firewall mode instance.
- You cannot use a data-sharing interface with inline sets or passive interfaces.
- You cannot use a data-sharing interface for the failover link.

Default MAC addresses

- MAC addresses for all interfaces are taken from a MAC address pool. For subinterfaces, if you decide to manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification. For more information, refer to Automatic MAC addresses for instance interfaces, on page 169.

Instance configuration

Prepare the chassis and management environment to enable instance configuration on your device.

Before you configure instances, you need to enable multi-instance mode, add the chassis to the Firewall Management Center, and configure chassis interfaces. You can also customize the chassis settings.

Enable multi-instance mode

You need to connect to the Firewall Threat Defense CLI at the console port to enable multi-instance mode. After you configure the mode, you can add it to the Firewall Management Center.

Note Although you can connect to SSH on the management port, we recommend using the console port to avoid multiple disconnections. This procedure covers the console port.

Procedure

Step 1 Connect to the chassis console port.

The console port connects to the FXOS CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

The first time you log in to FXOS, you are prompted to change the password.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. Refer to the FXOS troubleshooting guide for the reimage procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3 Check your current mode, Native or Container. If the mode is Native, you can continue with this procedure to convert to multi-instance (Container) mode.

show system detail

Example:

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

Step 4 Connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 5 The first time you log in to the Firewall Threat Defense, you are prompted to accept the General Terms. You are then presented with the CLI setup script.

The setup script lets you set the Management interface IP address and other settings. However, when you convert to multi-instance mode, the only settings that are retained are the following:

- Admin password (that you set at initial login)
- DNS servers
- Search domains

You will reset the Management IP address and gateway as part of the multi-instance mode command. After you convert to multi-instance mode, you can change Management settings at the FXOS CLI. For more information, refer to Change chassis management settings at the FXOS CLI, on page 216.

Step 6 Enable multi-instance mode, set the chassis management interface settings, and identify the Firewall Management Center. You can use IPv4 and/or IPv6 static addressing; DHCP is not supported. After you enter the command, you will be prompted to erase the configuration and reboot. Enter **ERASE** (all caps). The system reboots and, as part of changing the mode, erases the configuration with the exception of the Management network settings you set in the command and the admin password. The chassis hostname is set to "firepower-*model*."

IPv4:

configure multi-instance network ipv4 *ip_address network_mask gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv4_address* | **DONTRESOLVE**} *registration_key nat_id*

IPv6:

configure multi-instance network ipv6 *ipv6_address prefix_length gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv6_address* | **DONTRESOLVE**} *registration_key nat_id*

See the following **manager** components:

- {*hostname* | *ipv4_address* | **DONTRESOLVE**}: Specifies either the FQDN or IP address of the Firewall Management Center. At least one of the devices, either the Firewall Management Center or the chassis, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you don't specify a manager hostname or IP address in this command, then enter **DONTRESOLVE**; in this case, the chassis must have a reachable IP address or hostname, and you must specify the *nat_id*.
- *registration_key*: Enter a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the chassis. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*: Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center when you register the chassis when one side does not specify a reachable IP address or hostname. It is required if you do not specify a manager address or hostname, however, we recommend that you always set the NAT ID even when you specify a hostname or IP address. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.

To change the mode back to appliance mode, you must use the FXOS CLI and enter **scope system** and then **set deploymode native**. For more information, refer to Change chassis management settings at the FXOS CLI, on page 216.

Example:

```
> configure multi-instance network ipv4 172.16.0.104 255.255.255.0 172.16.0.1 manager
fmc1 172.16.0.103 impala67 winchester1
WARNING: This command will discard any FTD configuration (except admin's credentials).
Make sure you back up your content. All previous content will be lost. System is going to
be re-initialized.
Type ERASE to confirm:ERASE
Exit...
>
```

Add a multi-instance chassis to the Firewall Management Center

Add the multi-instance chassis to the Firewall Management Center to enable centralized management and configuration of all chassis settings and instances.

The management center and the chassis share a separate management connection using the chassis MGMT interface.

You can use the Firewall Management Center to configure all chassis settings as well as instances. The Secure Firewall Chassis Manager or configuration at the FXOS CLI is not supported.

Before you begin

Convert the chassis to multi-instance mode. For more information, refer to Enable multi-instance mode, on page 175.

Procedure

Step 1 In the Firewall Management Center, add the chassis using the chassis management IP address or hostname.

a) Choose **Devices** > **Device Management**, and then from **Add** drop-down list, choose **Chassis**.

Figure 55: Add chassis

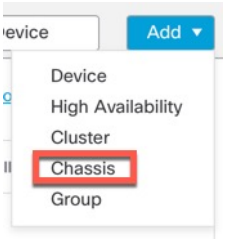
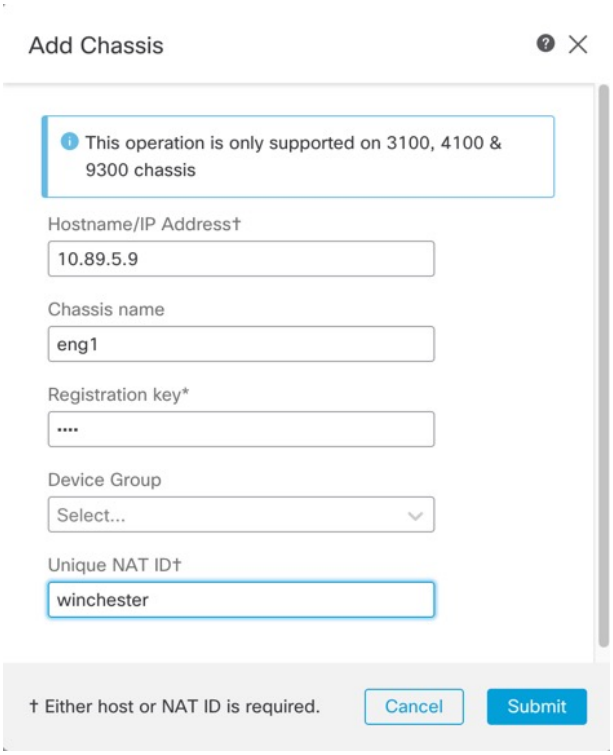


Figure 56: Add chassis



b) In the **Hostname/IP Address** field, enter the IP address or the hostname of the chassis you want to add.

If you don't know the hostname or IP address, you can leave this field blank specify the **Unique NAT ID**.

c) In the **Chassis Name** field, enter a name for the chassis as you want it to display in the Firewall Management Center.

d) In the **Registration Key** field, enter the same registration key that you used when you configured the chassis to be managed by the Firewall Management Center.

The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

e) In a multidomain deployment, regardless of your current domain, assign the chassis to a leaf **Domain**.

If your current domain is a leaf domain, the chassis is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the chassis. A chassis can only belong to one domain.

f) (Optional) Add the chassis to a **Device Group**.

g) If you used a NAT ID during chassis setup, expand enter the same NAT ID in the **Unique NAT ID** field.

The NAT ID can include alphanumeric characters and hyphens (-).

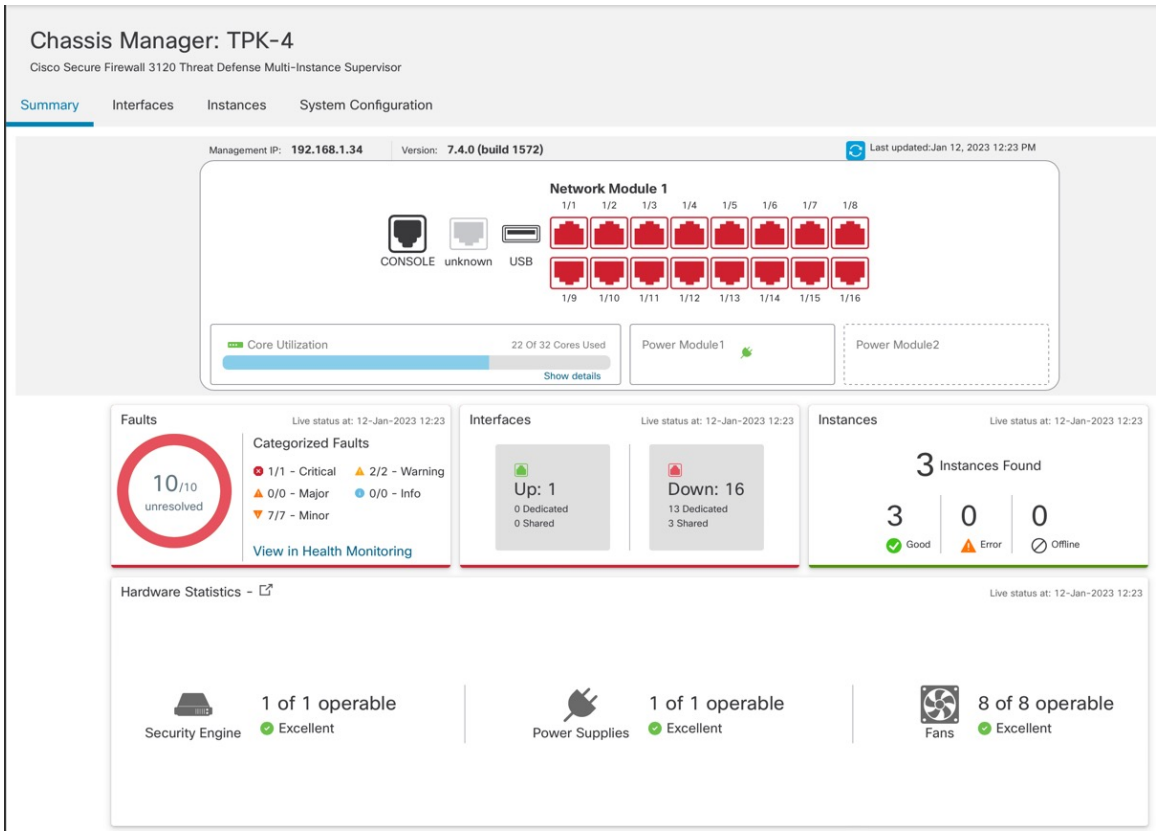
h) Click **Submit**.

The chassis is added to the **Devices** > **Device Management** page.

Step 2 To view and configure the chassis, click **Manage** in the **Chassis** column, or click **Edit** ( ).

The **Chassis Manager** page opens for the chassis to the **Summary** page.

Figure 57: Chassis summary



Chassis interface configuration

A chassis interface is a physical network interface that

- enables connection to the firewall's internal and external networks,
- supports configuration of basic Ethernet settings, VLAN subinterfaces, and EtherChannel grouping, and
- defaults to a disabled state until explicitly enabled by an administrator.

Additional information

Note To configure breakout ports and perform other network module operations, refer to Network module management for Secure Firewall 3100/4200, on page 625.

Note For information about the **Sync Device** button, refer to Sync Interface Changes with the Firewall Management Center, on page 622.

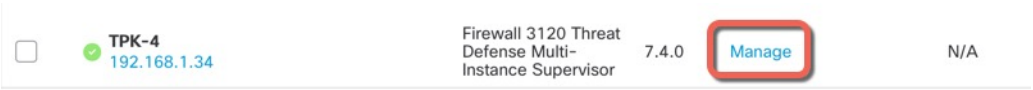
Configure a physical interface

You can physically enable and disable interfaces, as well as set the interface speed and duplex and other hardware settings. To use an interface, it must be physically enabled for the chassis and logically enabled in the instance. By default, physical interfaces are disabled. For VLAN subinterfaces, the admin state is inherited from the parent interface.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

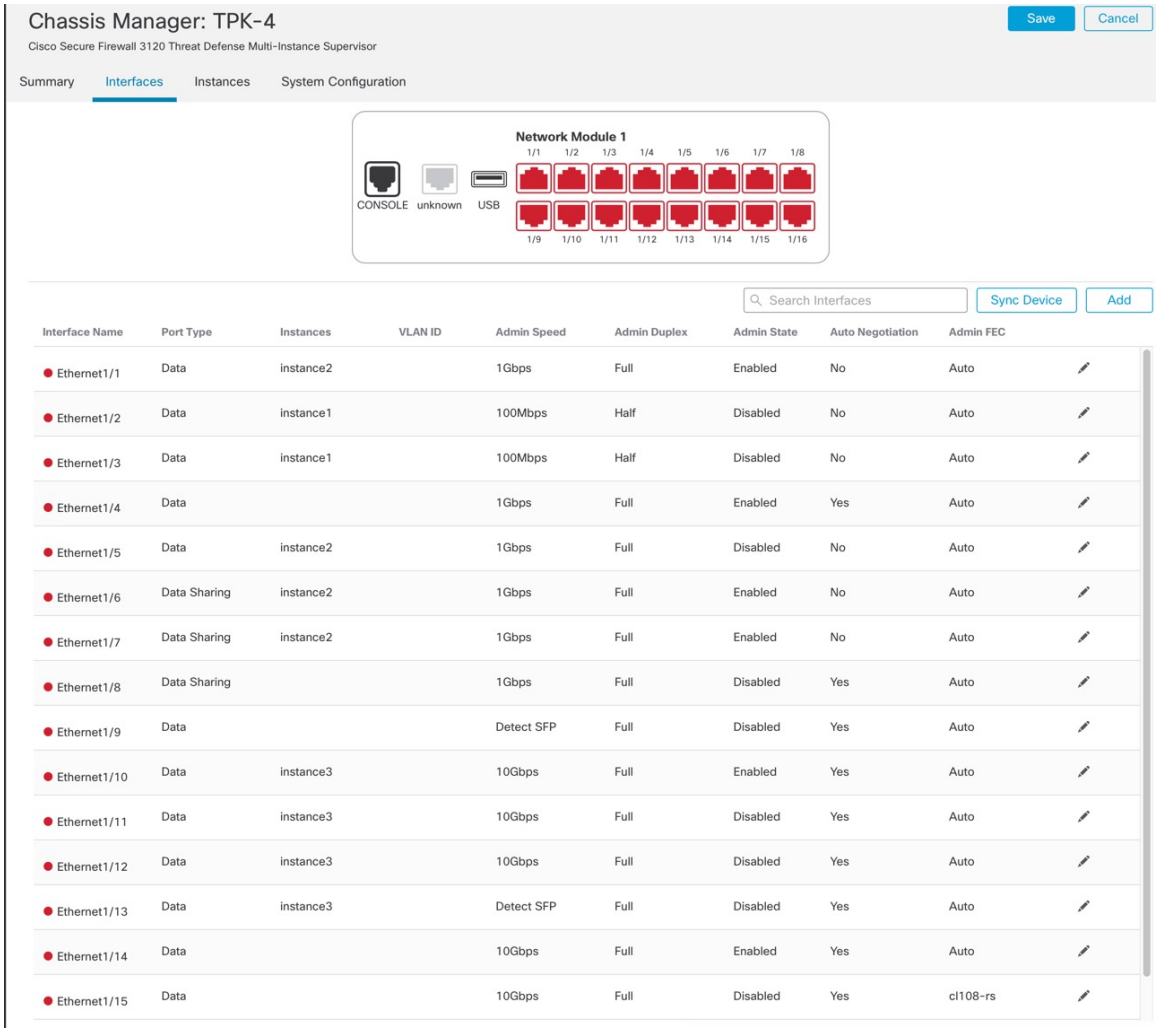
Figure 58: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

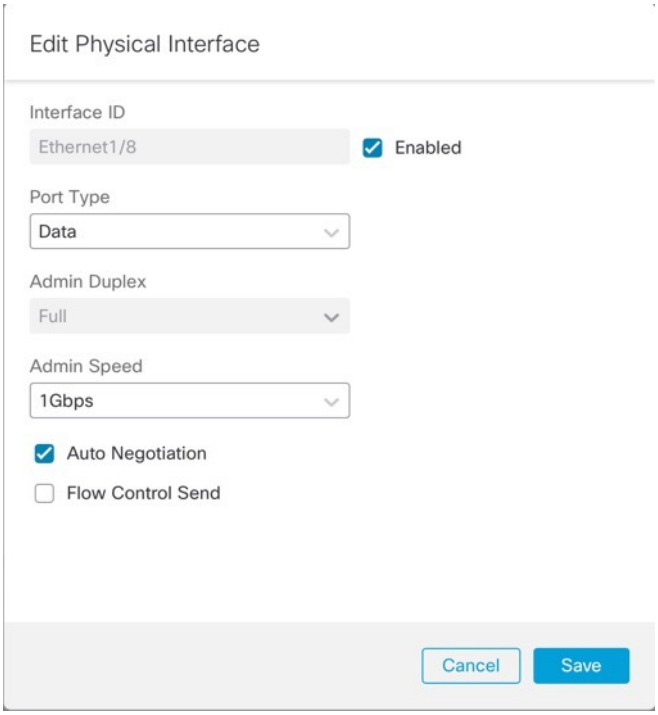
Step 2 Click **Interfaces**.

Figure 59: Interfaces



Step 3 Click **Edit** (✎) for the interface you want to edit.

Figure 60: Edit Physical Interface



Step 4 Enable the interface by checking the **Enabled** check box.

- For the **Port Type**, choose **Data** or **Data Sharing**.

  Figure 61: Port Type

- Set the **Admin Duplex**.

  Speeds of 1Gbps and higher only support **Full** duplex. SFP interfaces only support **Full** duplex.

- Set the **Admin Speed**.

  For SFPs, Choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always Full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically.

Step 5 (Optional) Check **Flow Control Send** to enable pause (XOFF) frames for flow control.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the threat defense port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note The Firewall Threat Defense supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flow control enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 6 (Optional) Check **Auto Negotiation** to set the interface to negotiate the speed, link status, and flow control. You cannot edit this setting for speeds lower than 1Gbps. For SFP interfaces, you can only disable auto-negotiation when the speed is set to 1Gbps.

Step 7 Click **Save** and then **Save** in the top right of the **Interfaces** page.

You can now **Deploy** the policy to the chassis. The changes are not active until you deploy them.

Configure an EtherChannel

An EtherChannel (also known as a port channel) can include up to 8 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, unless you set the speed to **Detect SFP**; in this case, you can use different interface capacities, and the lowest common speed is used.

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. "On" mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

When the chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state when it is added to an instance.

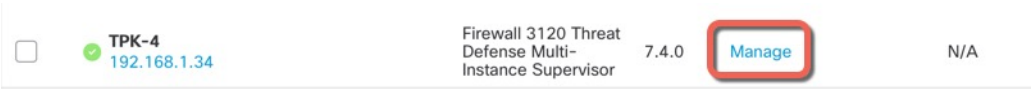
Before you begin

Enable physical interfaces and set hardware parameters. For more information, refer to Configure a physical interface, on page 180.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

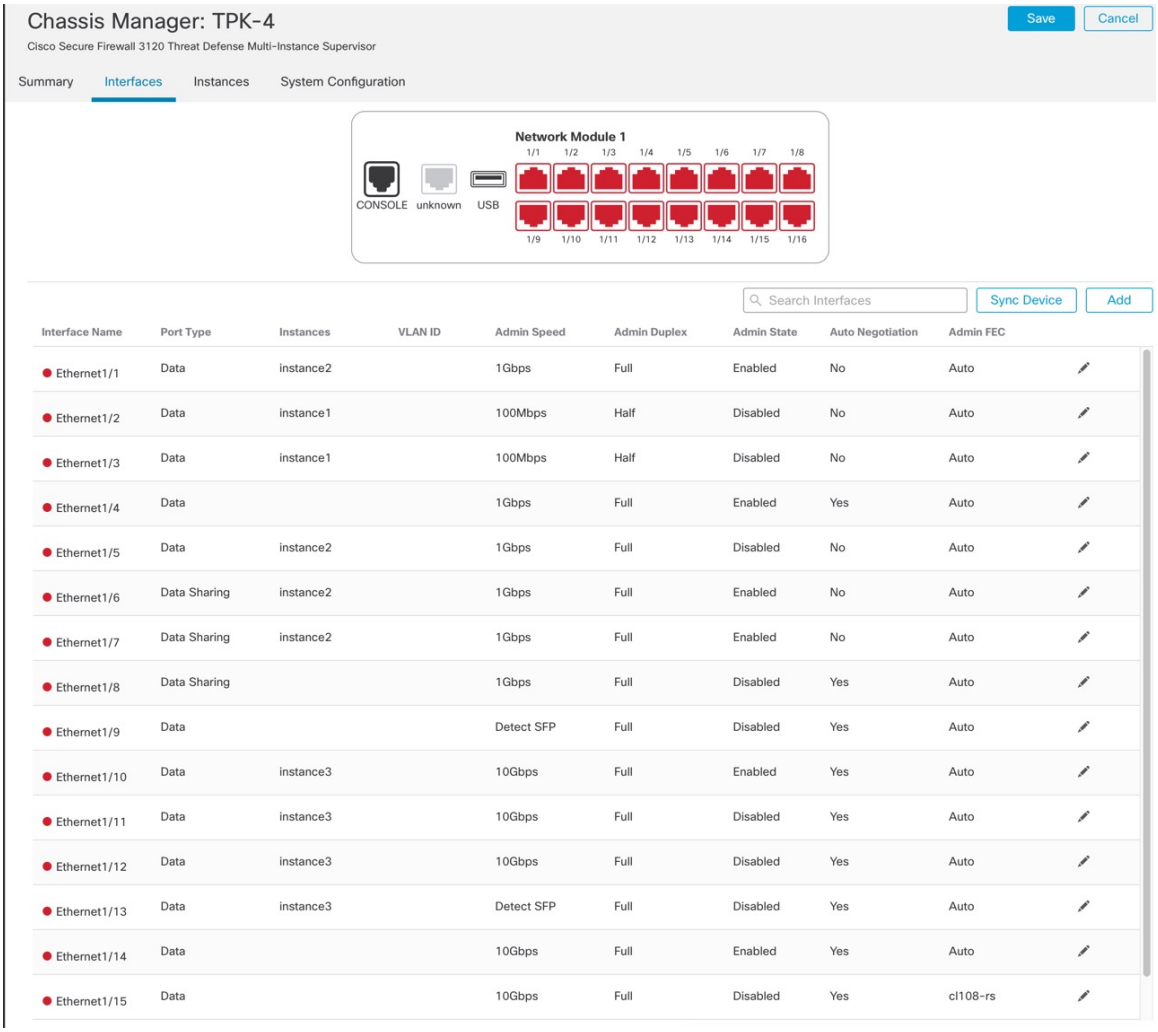
Figure 62: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

Step 2 Click **Interfaces**.

Figure 63: Interfaces



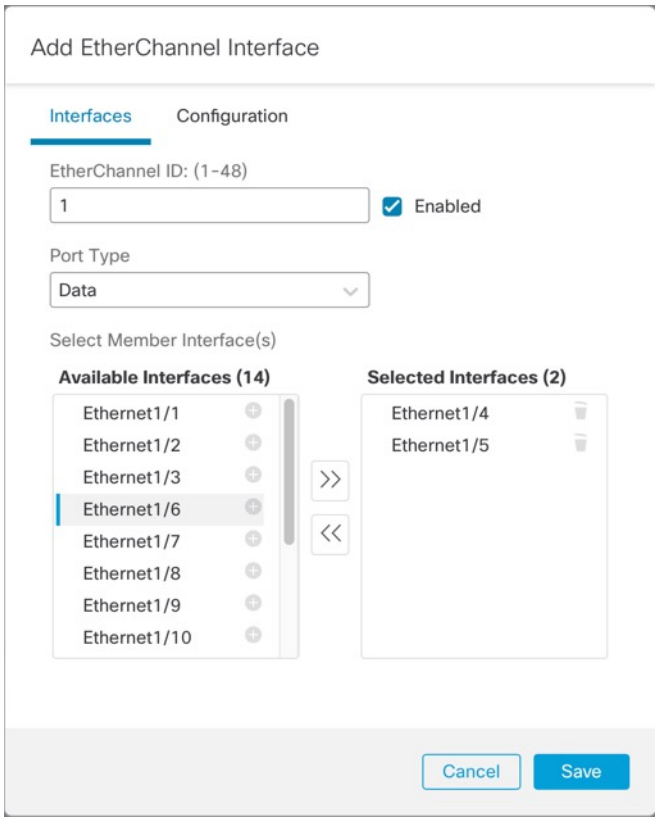
Step 3 Click **Add** > **EtherChannel Interface**.

Figure 64: Add EtherChannel



Step 4 Set the following **Interfaces** parameters.

Figure 65: Interfaces settings



a) For the **EtherChannel ID**, specify an ID between 1 and 48.
b) Check **Enabled**.
c) For the **Port Type**, choose **Data** or **Data Shared**.

   For information about the port type, refer to Interface types, on page 161.

d) To add a physical interface to the EtherChannel, select click **Add** (⊕) in the **Available Interfaces** list to move it to the **Selected Interfaces** list.

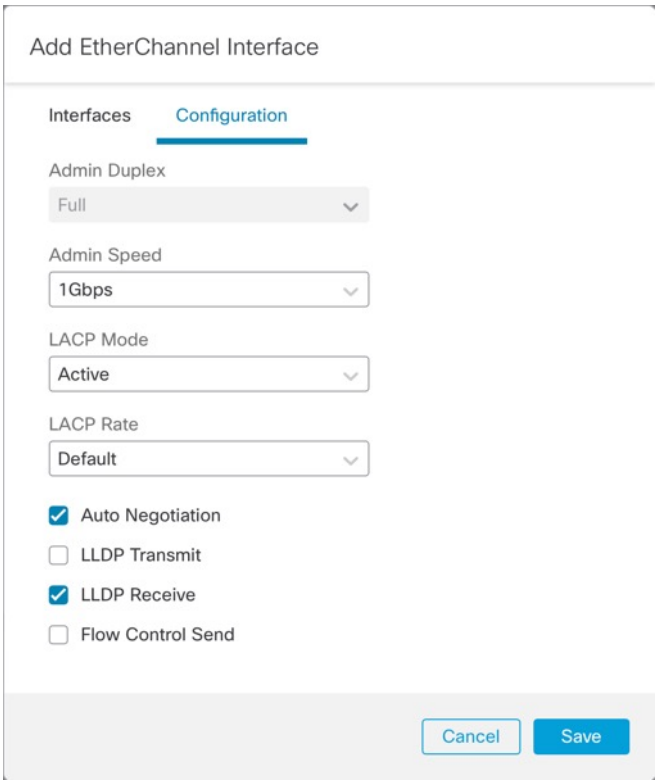
   To add or remove all interfaces, click the double arrow button.

Note You cannot add an interface that is already assigned to an instance.

Step 5 (Optional) Set the following **Configuration** parameters.

Many of these settings (excluding the LACP settings) set the requirements for interfaces to be included in the EtherChannel; they do not override the settings of member interfaces. So if you check **LLDP Transmit**, for example, you should only add interfaces that have that setting. If you set the **Admin Speed** to 1 Gbps, then only 1Gbps interfaces can be included.

Figure 66: Configuration settings



a) Choose the required **Admin Duplex** for the member interfaces, **Full Duplex** or **Half Duplex**.

If you add a member interface that is configured with the specified duplex, it will not successfully join the port channel.

b) Choose the required **Admin Speed** for the member interfaces from the drop-down list.

If you add a member interface that is not at the specified speed, it will not successfully join the port channel.

c) Choose the **LACP Mode**, **Active** or **On**.

- **Active**—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On**—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

Note It may take up to three minutes for an EtherChannel to come up to an operational state if you change its mode from On to Active or from Active to On.

d) Choose the **LACP Rate**, **Default**, **Fast**, or **Normal**.

The default is **Fast**.

e) Choose the required Link Layer Discovery Protocol (LLDP) settings for member interfaces by checking **LLDP Transmit** and/or **LLDP Receive**.

f) Check the required **Flow Control Send** setting for member interfaces.

Step 6 Click **Save** and then **Save** in the top right of the **Interfaces** page.

You can now **Deploy** the policy to the chassis. The changes are not active until you deploy them.

Configure a subinterface

You can add up to 500 subinterfaces to your chassis.

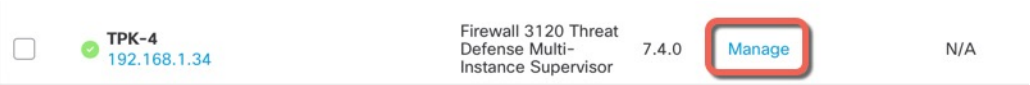
VLAN IDs per interface must be unique, and within an instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on *separate* interfaces as long as they are assigned to different instances. However, each subinterface still counts towards the limit even though it uses the same ID.

This section discusses *FXOS* VLAN subinterfaces only. You can separately create subinterfaces within the instance. For more information, refer to Chassis interfaces vs. instance interfaces, on page 161.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

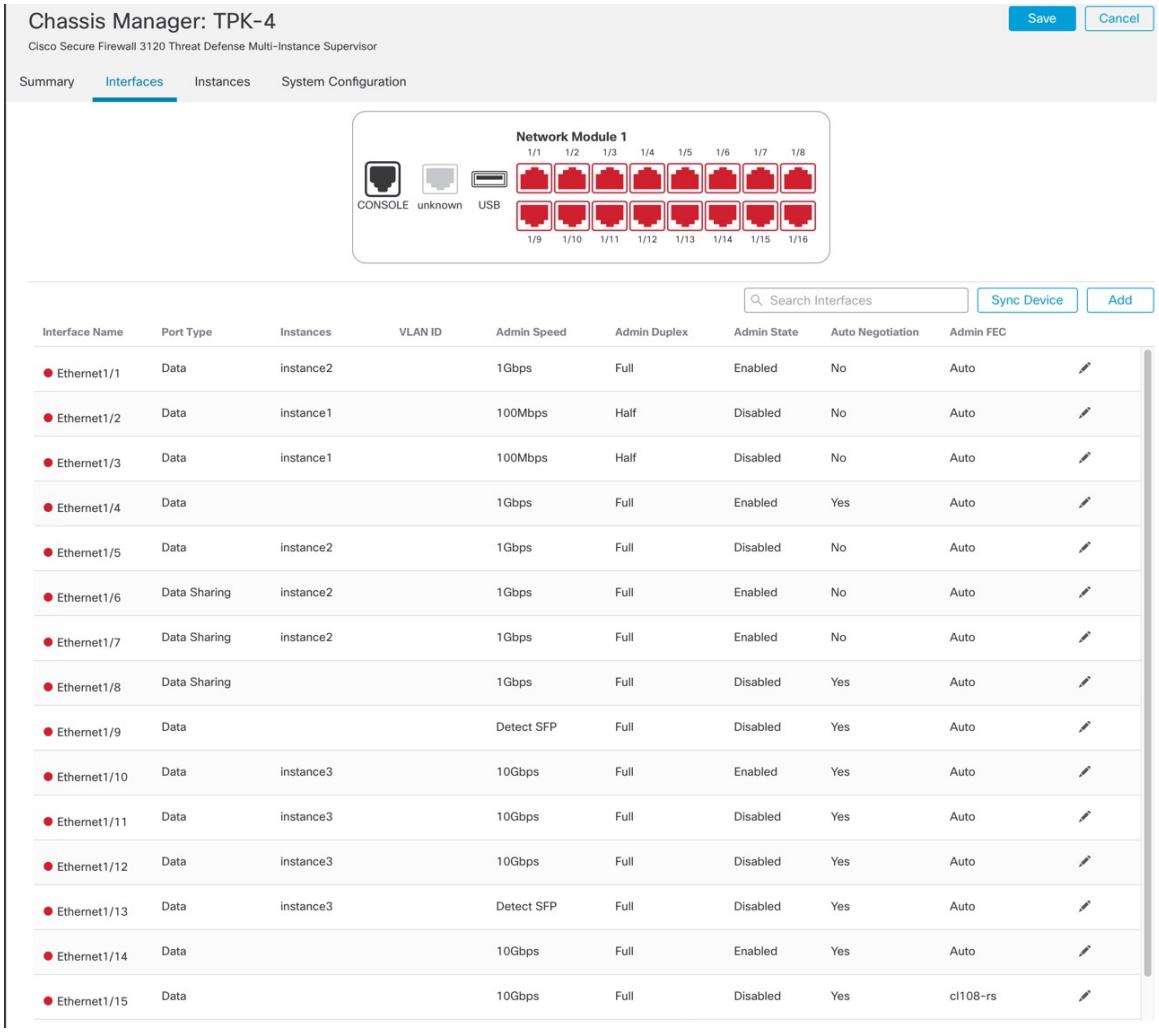
Figure 67: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

Step 2 Click **Interfaces**.

Figure 68: Interfaces



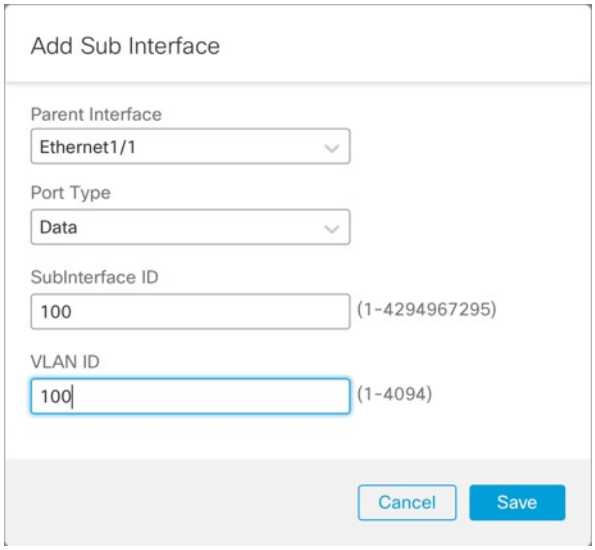
Step 3 Click **Add** > **Subinterface**.

Figure 69: Add subinterface



Step 4 Set the following parameters.

Figure 70: Subinterface settings



Step 5 Click **Save** and then **Save** in the top right of the **Interfaces** page.

You can now **Deploy** the policy to the chassis. The changes are not active until you deploy them.

Add an instance

Use this task when you need to add one or more instances to a chassis already in multi-instance mode. The number of supported instances depends on your model; refer to Requirements and prerequisites for instances, on page 171.

Before you begin

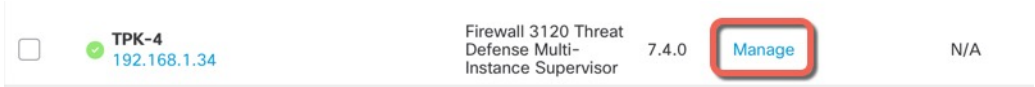
Enable multi-instance mode, on page 175 and Add a multi-instance chassis to the Firewall Management Center, on page 177.

Follow these steps to add an instance to a chassis in multi-instance mode:

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

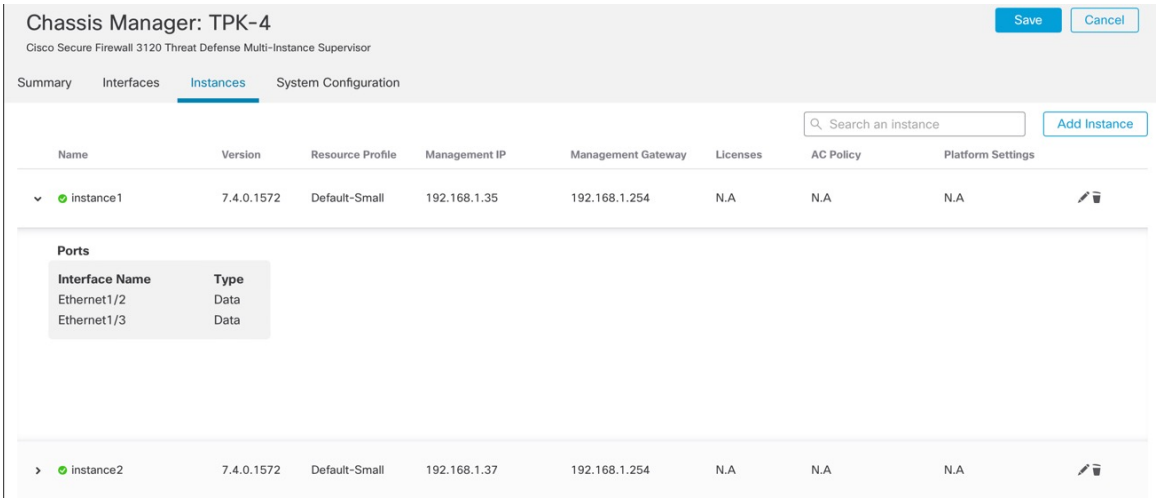
Figure 71: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

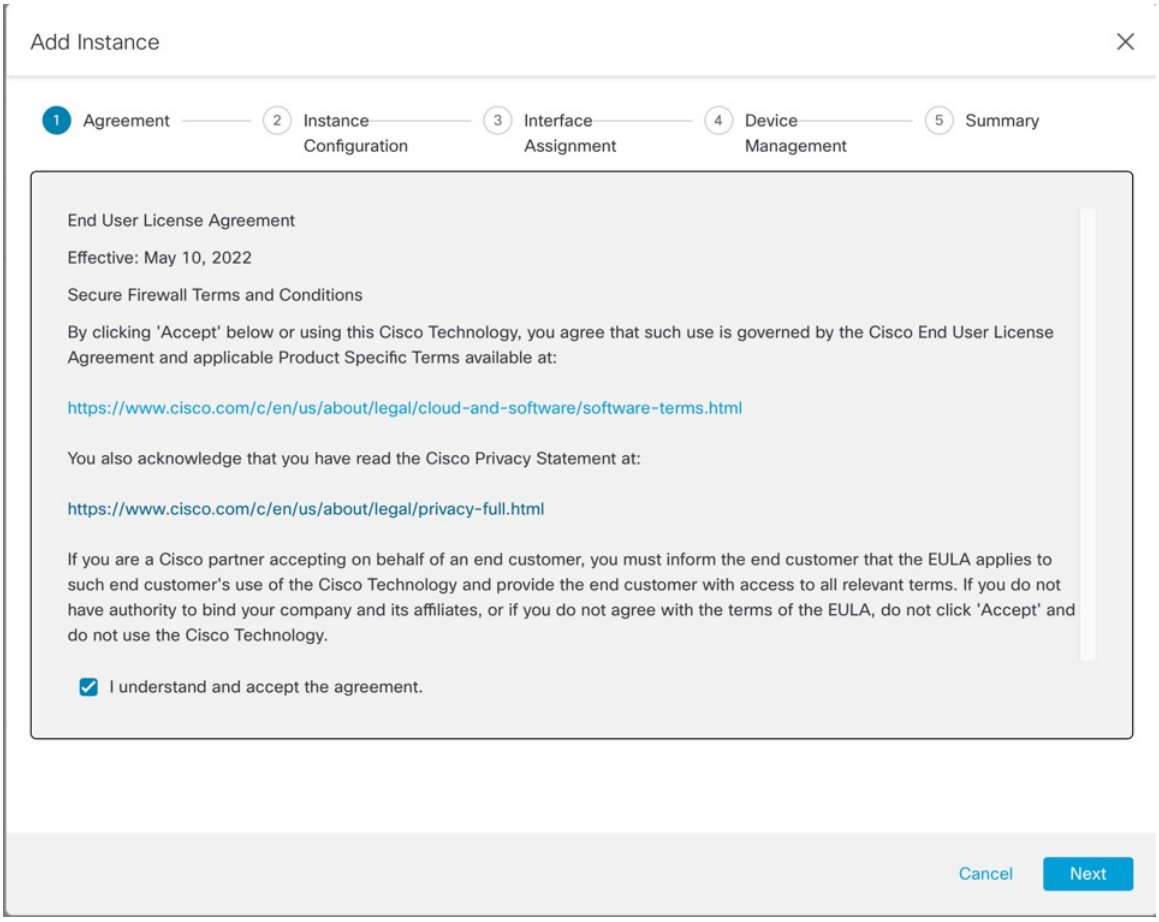
Step 2 Click **Instances**, and click **Add Instance**.

Figure 72: Instances



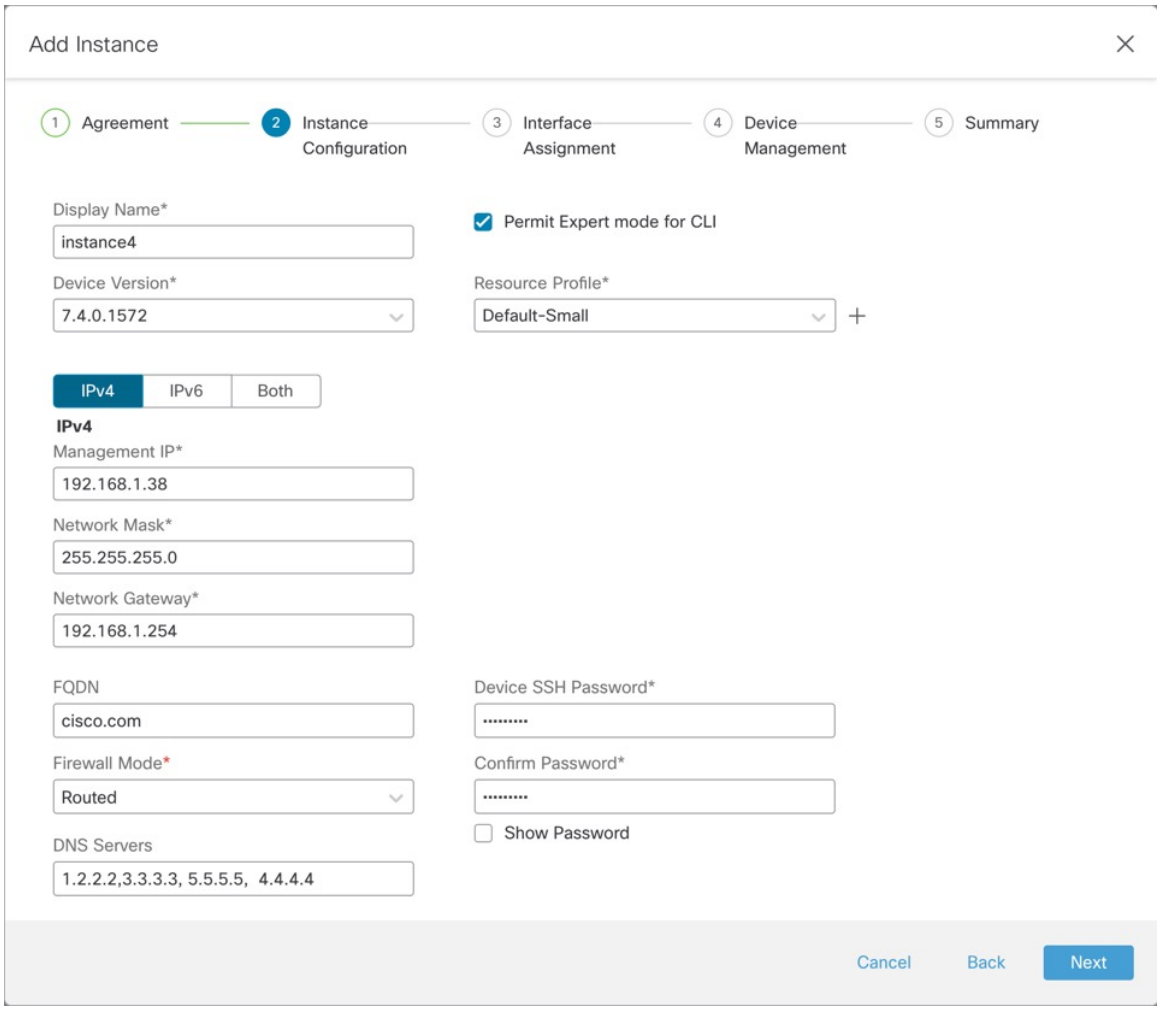
Step 3 On **Agreement**, check **I understand and accept the agreement**, then click **Next**.

Figure 73: Agreement



Step 4 On **Instance Configuration**, set the instance parameters, then click **Next**.

Figure 74: Instance configuration



- **Display Name**
- **Device Version**: Versions listed are packages currently downloaded to the chassis. Patch versions are not listed and cannot be used because they don't contain the entire bundle. To upgrade to a new package, refer to **Devices** > **Upgrade** > **Chassis Upgrade**. When you upgrade, both the old Firewall Threat Defense version and the new Firewall Threat Defense version will be listed in the menu. To download an older package, you need to use the FXOS CLI. Note: Both FXOS and Firewall Threat Defense images are included in the same package. For more information, refer to troubleshooting guide.

  For example:

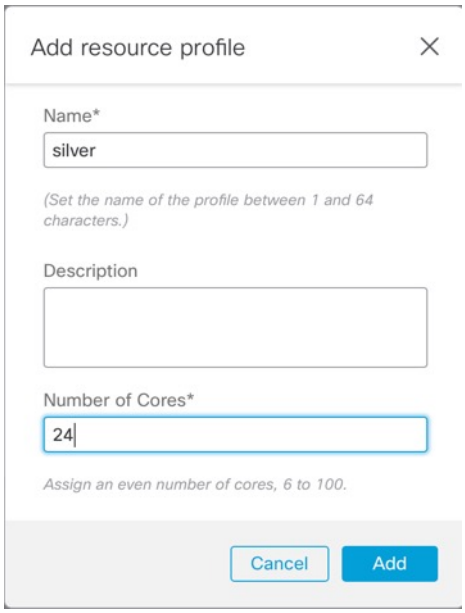
```
firepower-3110# scope firmware
firepower-3110# download image
https://10.10.7.89/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar : completed successfully.
```

- **IPv4**, **IPv6**, or **Both**: Set a **Management IP** address on the same network as the chassis Management interface. Set the **Network Mask** and gateway (likely the same gateway as the chassis). The chassis Management interface is shared with each instance, and each instance has its own IP address on the network. You can SSH to this IP address by default to reach the Firewall Threat Defense CLI.
- (Optional) **FQDN**
- **Firewall Mode**: **Routed** or **Transparent**. For more information about the firewall mode, refer to Transparent or Routed Firewall Mode, on page 71.
- **DNS Servers**: Enter a comma-separated list of DNS servers for management traffic only.
- (Optional) **Permit Expert Mode for CLI**: Expert Mode provides Firewall Threat Defense shell access for advanced troubleshooting.

  If you enable this option, then users who access the instance directly from an SSH session can enter Expert Mode. If you disable this option, then only users who access the instance from the FXOS CLI can enter Expert Mode. We recommend disabling this option to increase isolation between instances.

  Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the Firewall Threat Defense CLI.
- **Resource Profile**: The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance. The chassis includes these default resource profiles: Default-Small, Default-Medium, and Default-Large. You can add additional profiles for this chassis by clicking **Add** (+). You cannot later edit the resource profile.

Figure 75: Add resource profile



  - The minimum number of cores is 6.

Note Instances with a smaller number of cores might experience relatively higher CPU utilization than those with larger numbers of cores. Instances with a smaller number of cores are more sensitive to traffic load changes. If you experience traffic drops, try assigning more cores.

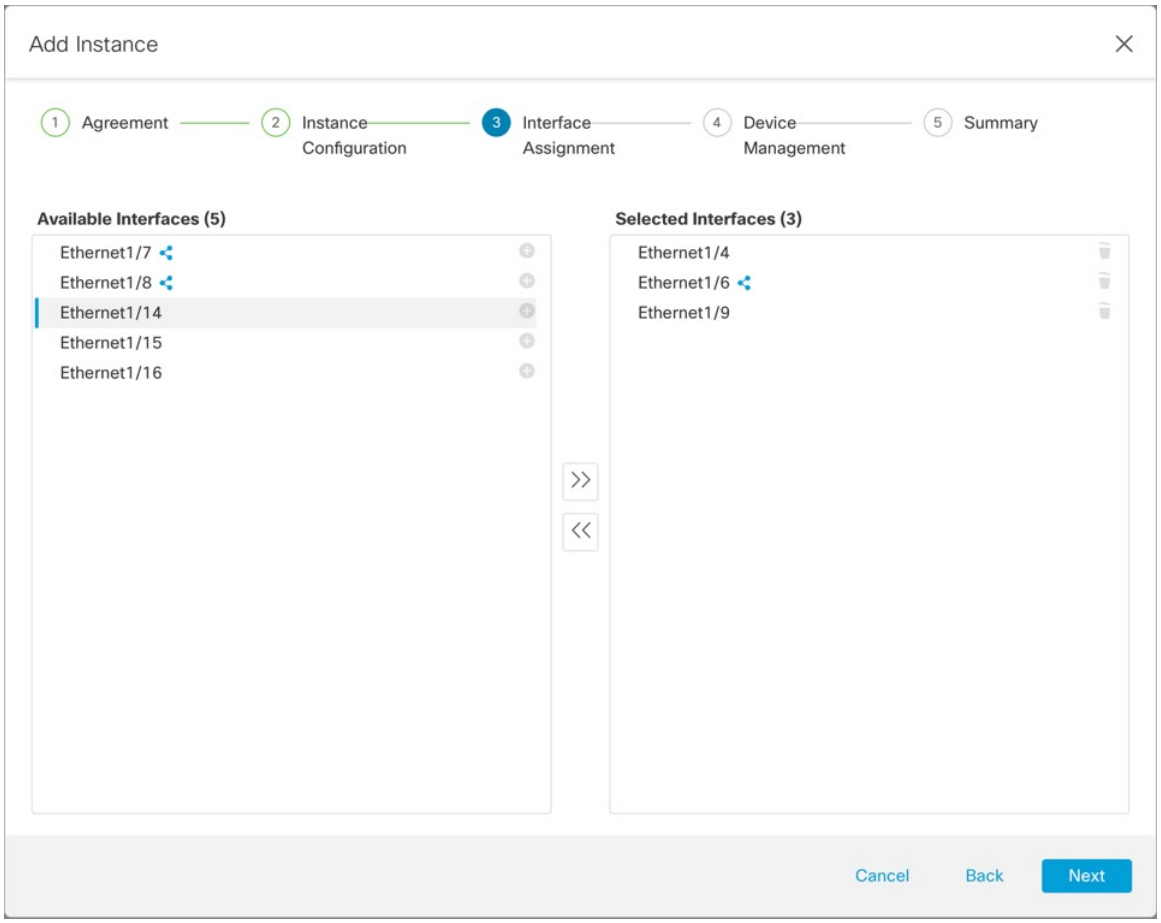
- You can assign cores as an even number (6, 8, 10, 12, 14 etc.) up to the maximum.
- The maximum number of cores available depends on the model; refer to Requirements and prerequisites for instances, on page 171.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for an established High Availability pair , if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.

- **Device SSH Password**: Set the Firewall Threat Defense admin user password for CLI access, either SSH or console. Repeat the password in the **Confirm Password** field.

Step 5 On **Interface Assignment**, assign the chassis interfaces to the instance, then click **Next**.

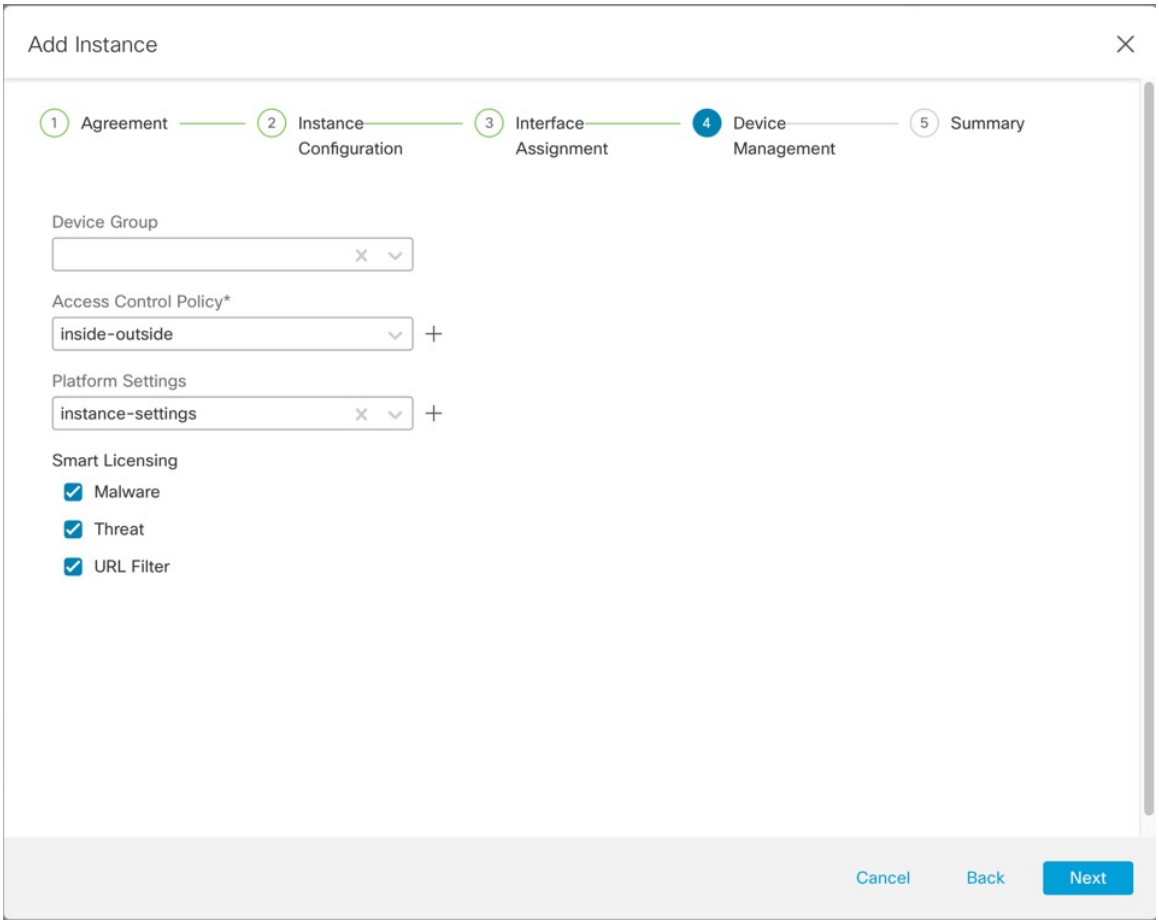
Figure 76: Interface assignment



Shared interfaces show the sharing icon ( ).

Step 6 On **Device Management**, set the device-specific settings, then click **Next**.

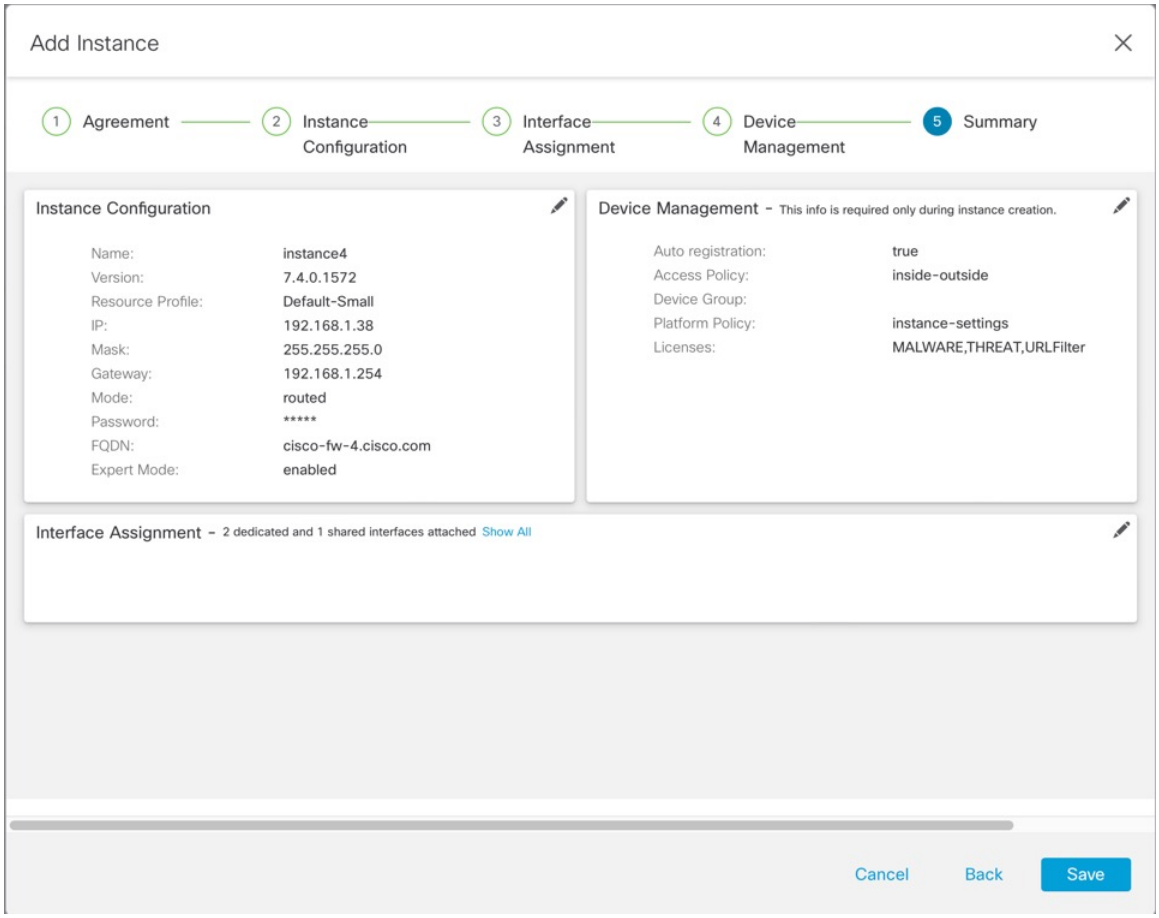
Figure 77: Device management



- **Device Group**
- **Access Control Policy**: Choose an existing access control policy, or create a new policy.
- **Platform Settings**: Choose an existing platform setting policy, or create a new policy.
- **Smart Licensing**

Step 7 On **Summary**, confirm your settings, then click **Save**.

Figure 78: Summary



You can edit any settings on this screen before saving the instance. After you save, the instance is added to the **Instances** screen.

Step 8 On the **Instances** screen, click **Save**.

Deploy the chassis configuration.

After deployment, the instance will be added as a device on the **Device Management** page.

Note Before you delete an instance, you must first unregister it on the **Device Management** page. If you delete the instance without unregistering it, the instance will remain as a stale entry in **Device Management**.

System configuration customization

You can configure chassis-level settings such as SNMP. You can also import or export the chassis FXOS configuration.

Configure SNMP

You can access chassis-level MIBs through the data interface of one of the instances, which you specify in the chassis system configuration. You can only use this instance for chassis SNMP information. You cannot access SNMP through the chassis Management interface.

Before you begin

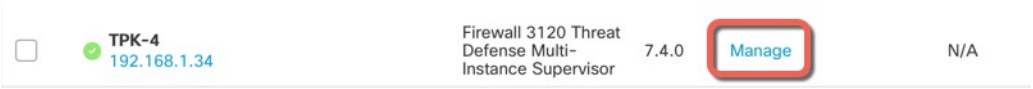
Configure SNMP for one of the instances. For more information, refer to Configure SNMP for a security device, on page 870.

Follow these steps to configure SNMP:

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

Figure 79: Manage Chassis

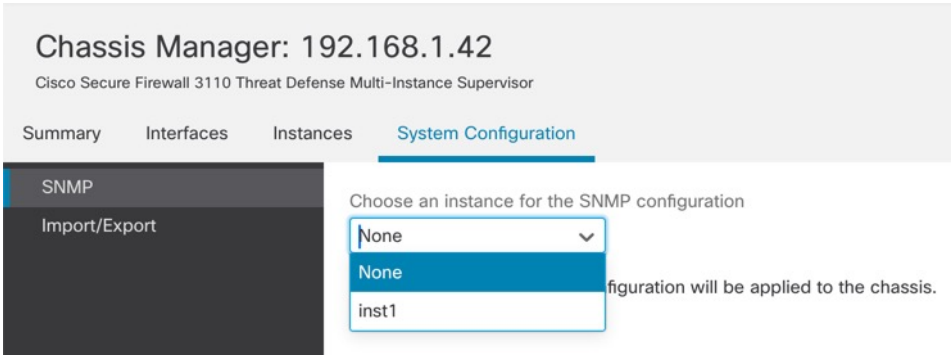


The **Chassis Manager** page opens for the chassis to the **Summary** page.

Step 2 Click **System Configuration**.

Step 3 Click **SNMP**, and choose the instance from the drop-down list.

Figure 80: SNMP



SNMP on the chassis will be accessible from the selected instance.

Step 4 Click **Save**.

Step 5 Deploy the chassis configuration.

Import or export the chassis configuration

You can use the configuration export feature to export an XML file containing chassis configuration settings to your local computer. You can later import that configuration file to quickly apply the configuration settings to your chassis to return to a known good configuration or to recover from a system failure.

Note You can't import the chassis configuration to a new chassis.

When exporting, only chassis configurations are exported; instance configuration settings are not exported. Instances need to be backed up separately using the device backup/restore feature.

When importing, all existing configurations on the chassis will be replaced by the configuration in the import file.

Before you begin

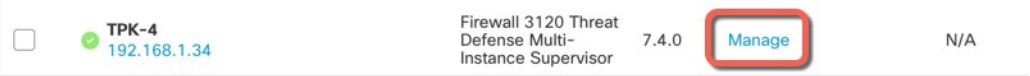
When you import the configuration to the same chassis, make sure the chassis matches for the following:

- Same chassis software version
- Same Firewall Threat Defense instance images
- Same network modules

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

Figure 81: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

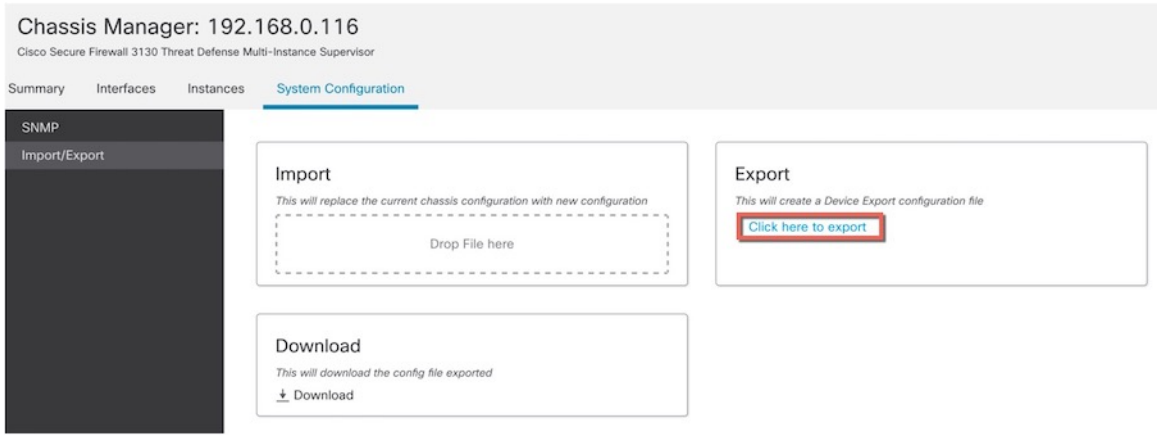
Step 2 Click **System Configuration**.

Step 3 Click **Import/Export**.

Step 4 To export the configuration, follow these steps.

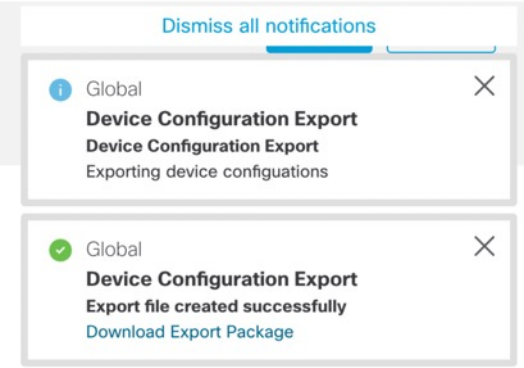
a) In the **Export** area, click **Click here to export**.

Figure 82: Create Export File



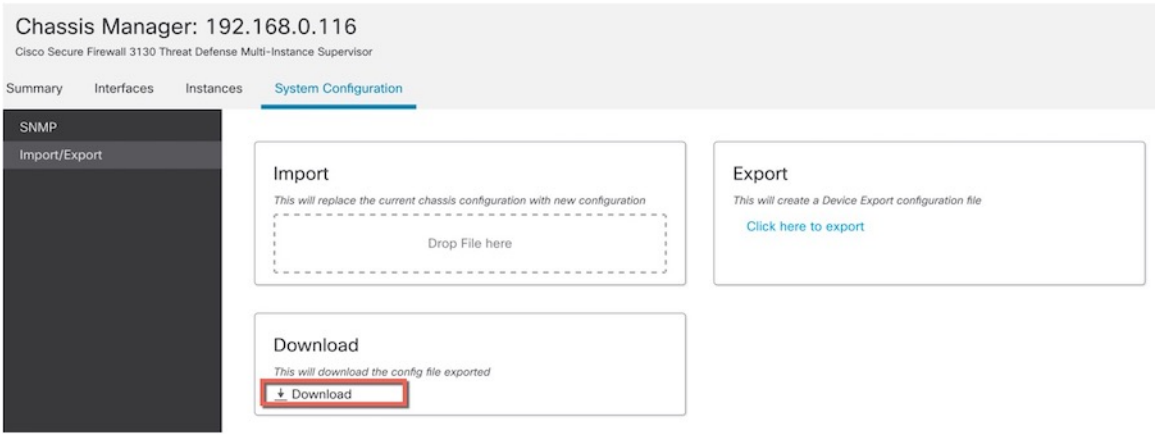
b) Monitor the notifications for the **Export file created successfully** message.

Figure 83: Export File Created Successfully



c) Download the export file by clicking the notification message (**Download Export Package**) or by clicking **Download**.

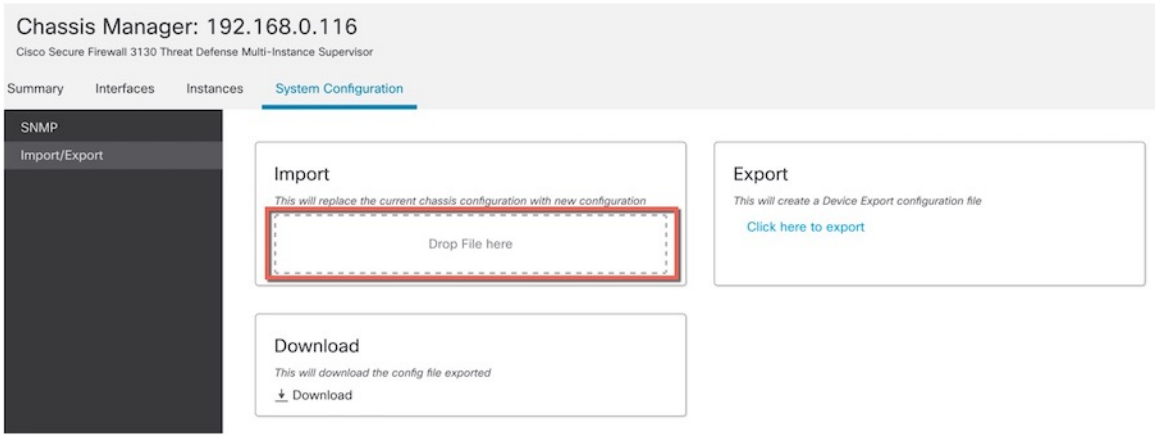
Figure 84: Download



The file is saved with the .sfo extension.

Step 5 To import a configuration, drag the **.sfo** file on the **Import** > **Drop File here** area.

Figure 85: Import



Chassis platform settings

Chassis platform settings are configuration features that configure a range of features for managing the chassis and can be shared among multiple chassis.

Chassis platform settings configure a range of features for managing the chassis. You can share the policy among multiple chassis. If you want different settings per chassis, you must create multiple policies.

Create a chassis platform settings policy

Use the **Platform Settings** page (**Devices** > **Platform Settings**) to manage platform settings policies. This page indicates the type of device for each policy. The **Status** column shows the device targets for the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 For an existing policy, you can **Copy** ( ), **Edit** ( ), or **Delete** ( ) the policy.

Caution You should not delete a policy that is the last-deployed policy on any of its target devices, even if it is out of date. Before you delete the policy completely, it is good practice to deploy a different policy to those targets.

Step 3 To create a new policy, click **New Policy**.

a) Choose **Chassis Platform Settings** from the drop-down list.
b) Enter a **Name** for the new policy and optionally, a **Description**.
c) Optionally, choose the **Available Chassis** where you want to apply the policy and click **Add** to add the selected chassis.
d) Click **Save**.

The system creates the policy and opens it for editing.

Step 4 To change the target chassis for a policy, click **Edit** ( ) next to the platform settings policy that you want to edit.

a) Click **Policy Assignment**.

b) To assign a chassis to the policy, select it in the **Available Chassis** list and click **Add**.

c) To remove a chassis assignment, click **Delete** ( ) next to a chassis in the **Selected Chassis** list.

d) Click **OK**.

Configure DNS

You need to specify a DNS server if the chassis requires resolution of hostnames to IP addresses. These chassis DNS settings are separate from the DNS settings per instance, which are configured in the device platform settings.

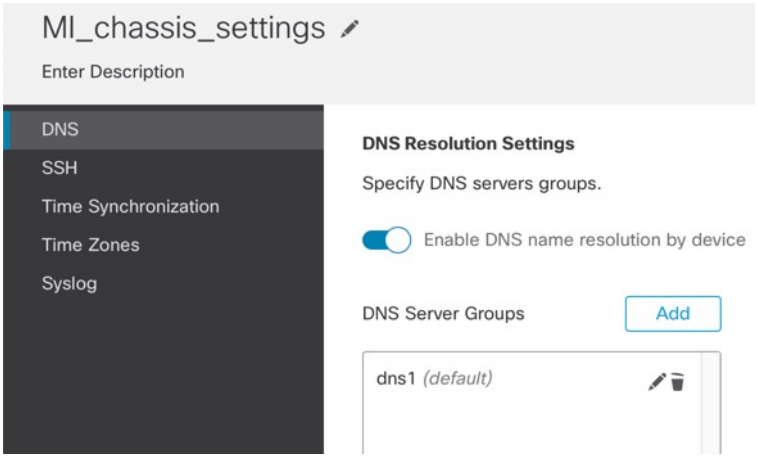
When you configure multiple DNS servers, the chassis uses servers in a random order. You can configure up to four servers across four DNS server groups. For example, you can configure a single server group with four servers, or you can configure four server groups with one server each.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the chassis policy.

Step 2 Choose **DNS**.

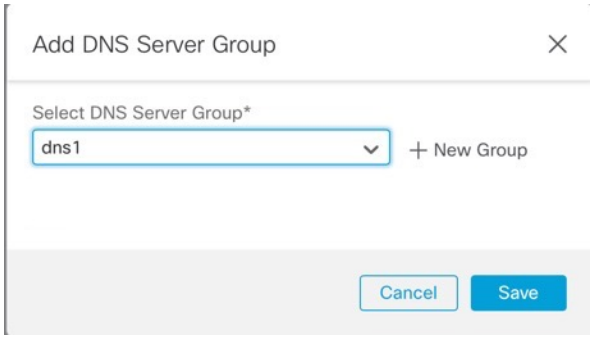
Figure 86: DNS



Step 3 Enable the **Enable DNS name resolution by device** slider.

Step 4 Click **Add** to add a DNS server group.

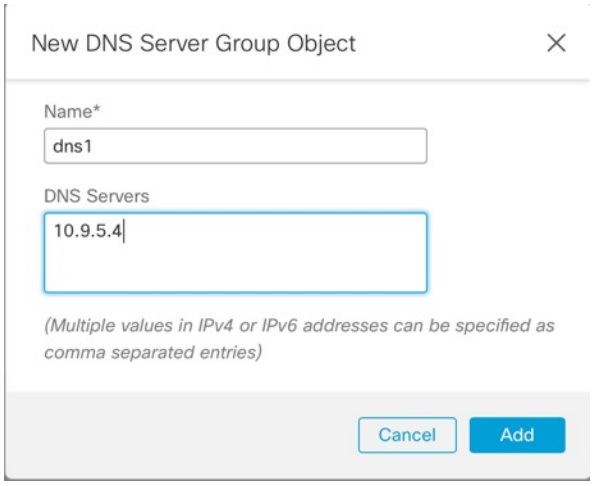
Figure 87: Add DNS server group



Step 5 Either select an existing DNS server group (refer to Create a DNS server group object, on page 2366), or click (+) **New Group**.

If you add a new group, you see this dialog box. Provide a name and up to four DNS server IP addresses as comma-separated values, and click **Add**.

Figure 88: New DNS server group object



Step 6 Click **Save** to add the DNS server to the list.

Step 7 Repeat these steps to add additional server groups.

Make sure you only identify a maximum of four DNS servers in all groups combined.

Step 8 Click **Save** to save all policy changes.

Configure SSH and SSH access list

To allow SSH sessions from the admin user to the chassis on the Management interface, enable the SSH server and configure the allowed networks.

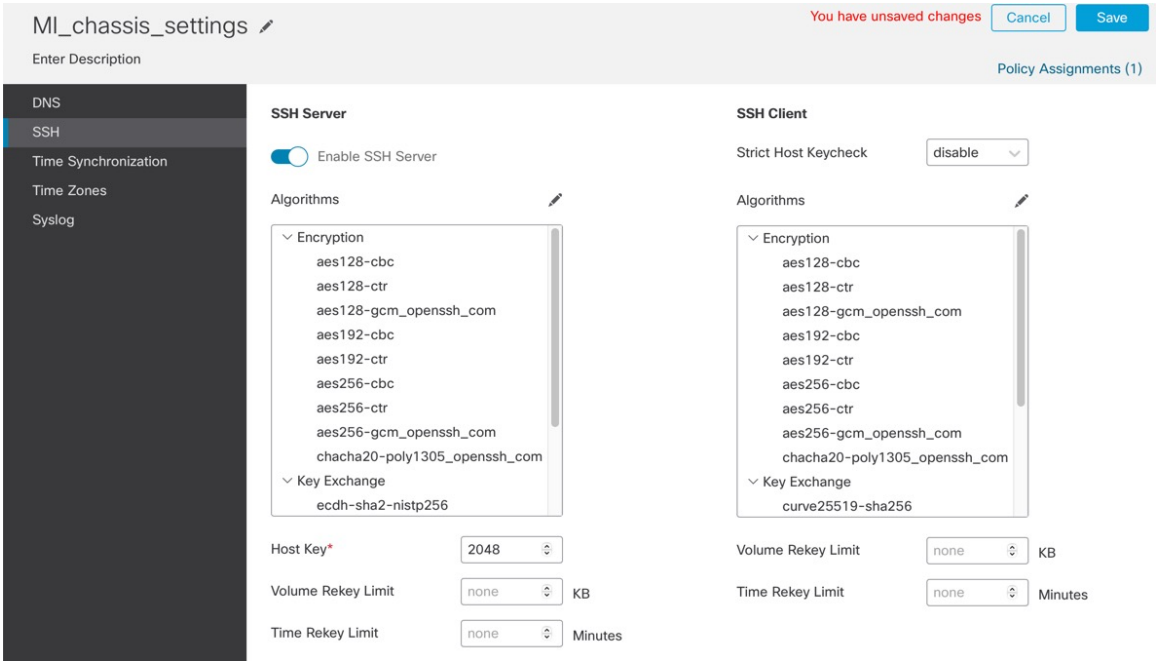
Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the chassis policy.

Step 2 Choose **SSH**.

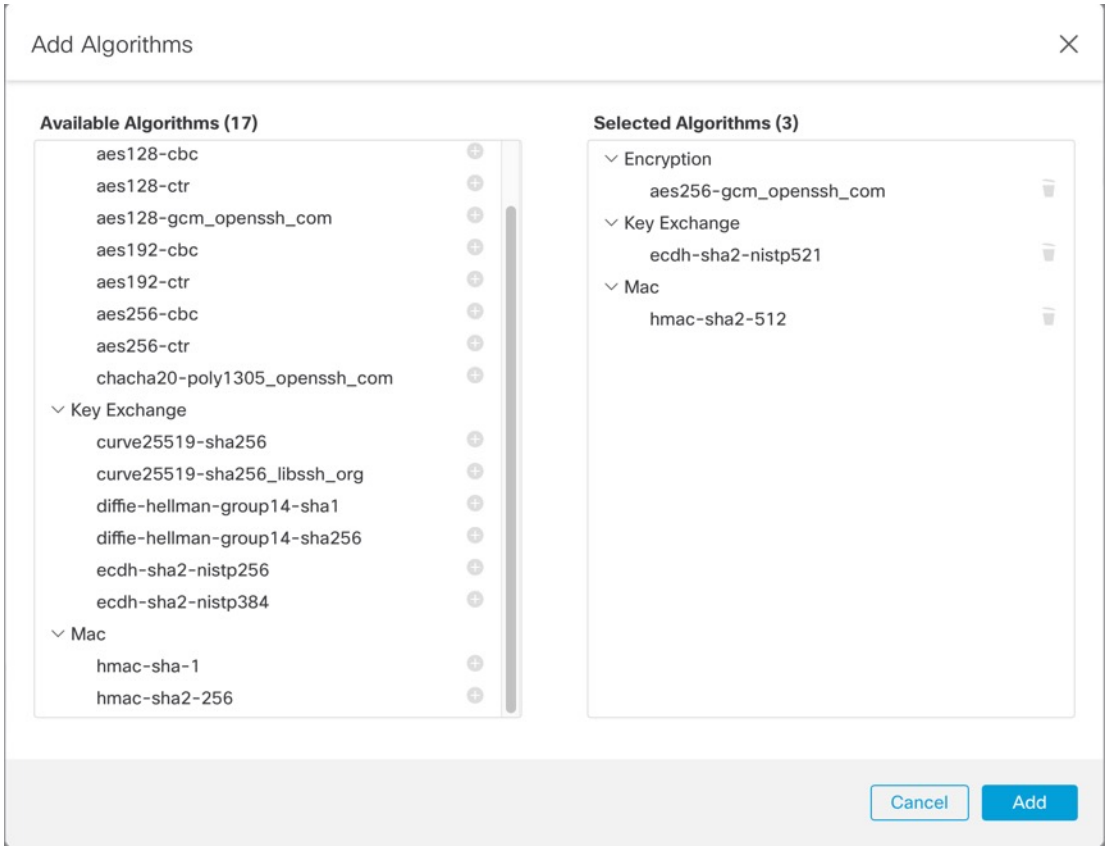
Step 3 To enable SSH access to the chassis, enable the **Enable SSH Server** slider.

Figure 89: SSH



Step 4 To set the allowed **Algorithms**, click **Edit** ( ).

Figure 90: Add Algorithms



a) Select the **Encryption** algorithms.
b) Select the **Key Exchange** algorithms.

   The key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication.

c) Select the **Mac** integrity algorithms.

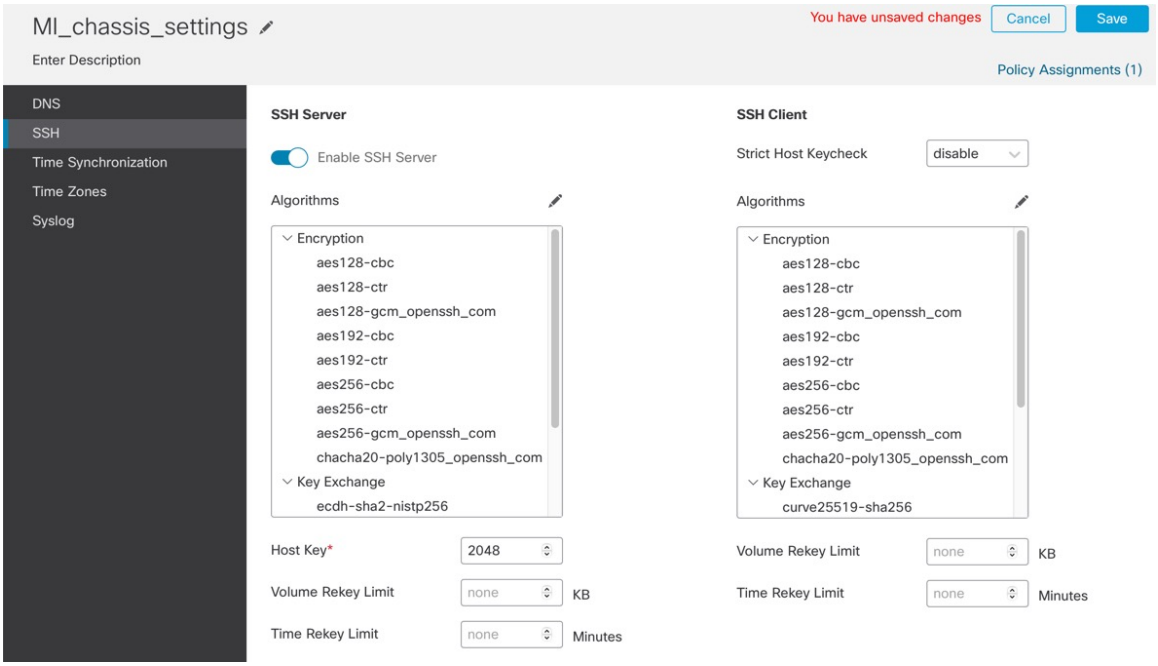
Step 5 For **Host Key**, enter the modulus size for the RSA key pairs.

The modulus value (in bits) is in multiples of 8 from 1024 to 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 2048.

Step 6 For the server **Volume Rekey Limit**, set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session.. For the server **Time Rekey Limit**, set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 7 For the **SSH Client**, configure the following settings.

Figure 91: SSH

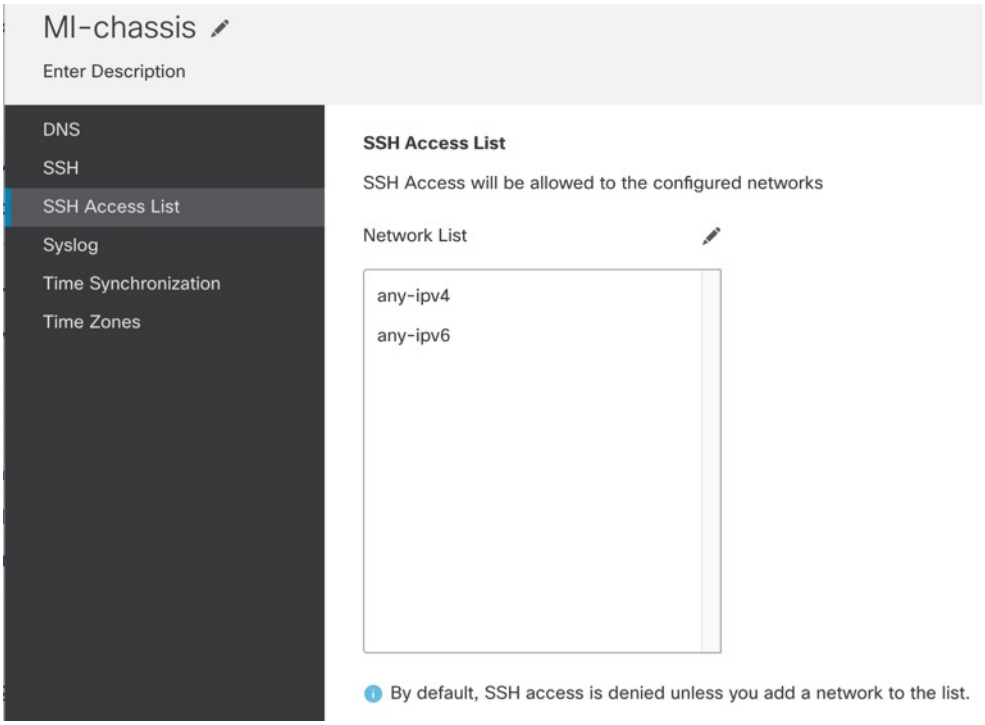


- **Strict Host Keycheck**—Choose **enable**, **disable**, or **prompt** to control SSH host key checking.
  - **enable**—The connection is rejected if the host key is not already in the FXOS known hosts file. You must manually add hosts at the FXOS CLI using the **enter ssh-host** command in the system/services scope.
  - **prompt**—You are prompted to accept or reject the host key if it is not already stored on the chassis.
  - **disable**—(The default) The chassis accepts the host key automatically if it was not stored before.
- **Algorithms**: Click **Edit** (✎). and select the **Encryption**, **Key Exchange**, and **Mac** algorithms.
- **Volume Rekey Limit**: Set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session.
- **Time Rekey Limit**: Set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 8 Choose **SSH Access List**. You need to allow access to IP addresses or networks before you can use SSH.

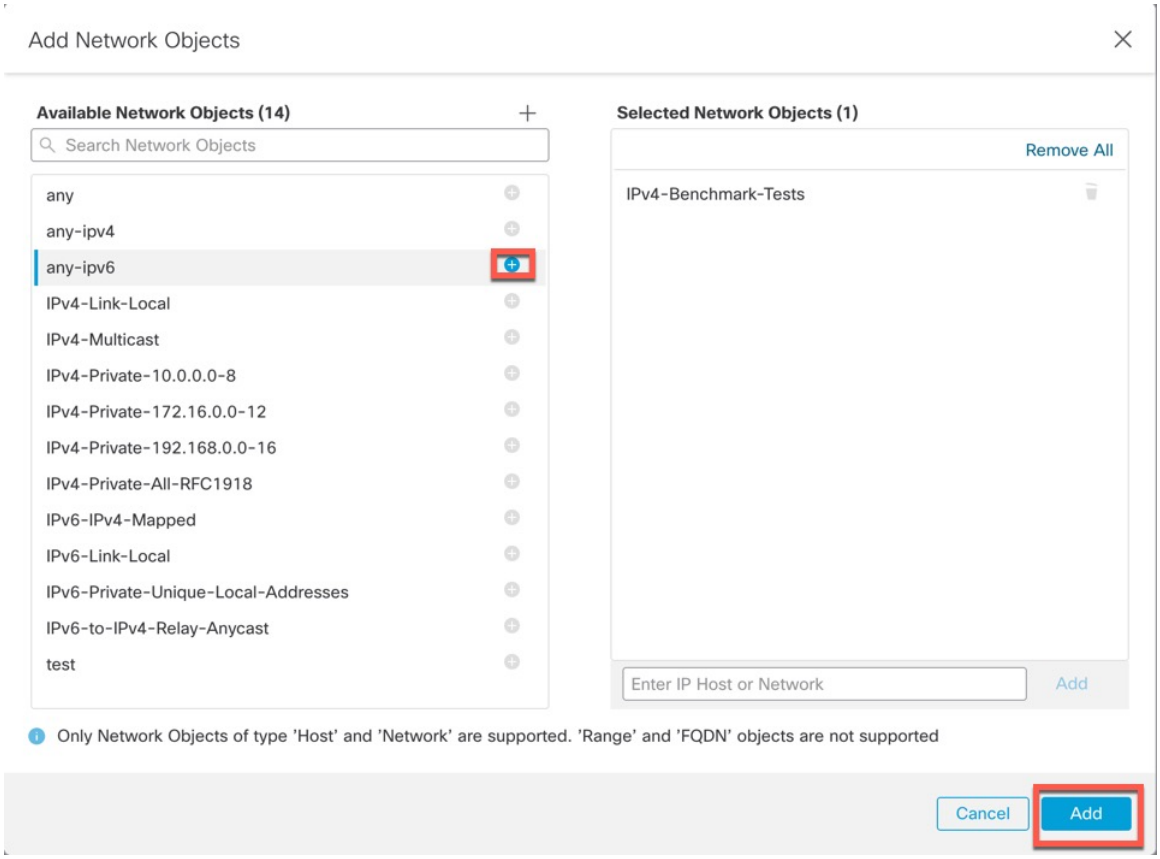
You can add up to 25 access lists.

Figure 92: SSH Access List



Step 9 Click **Edit** ( ) to add network objects and click **Save**. You can also manually enter IP addresses. Click **Save** to save all policy changes.

Figure 93: Network Objects



Configure syslog

You can enable syslogs from the chassis. These syslogs come from the chassis' FXOS operating system.

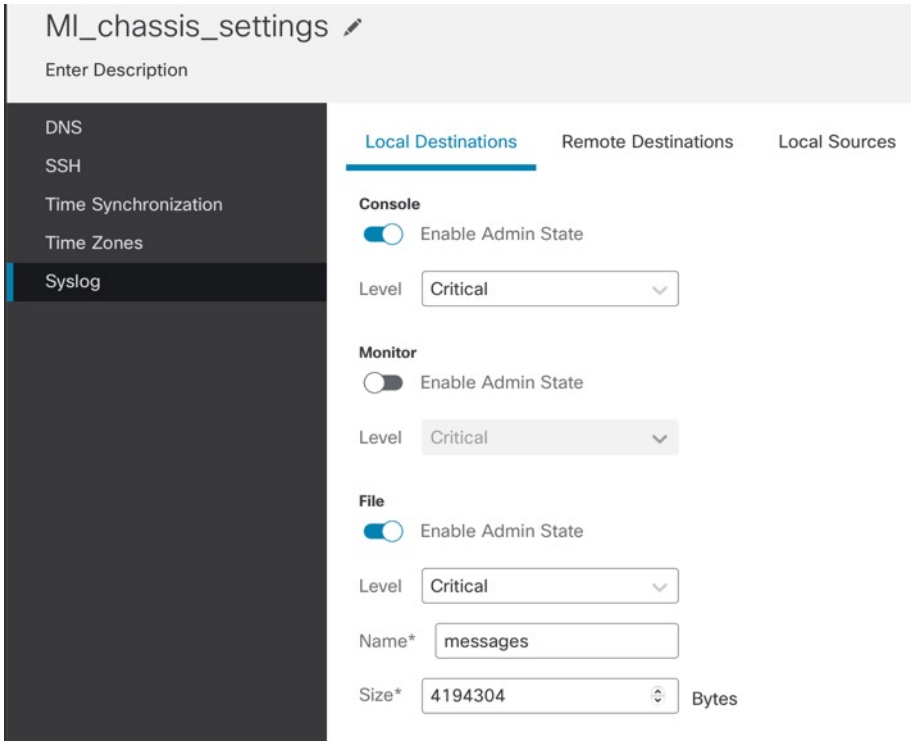
Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the chassis policy.

Step 2 Choose **Syslog**.

Step 3 Click the **Local Destinations** tab, and complete the following fields.

Figure 94: Syslog local destinations

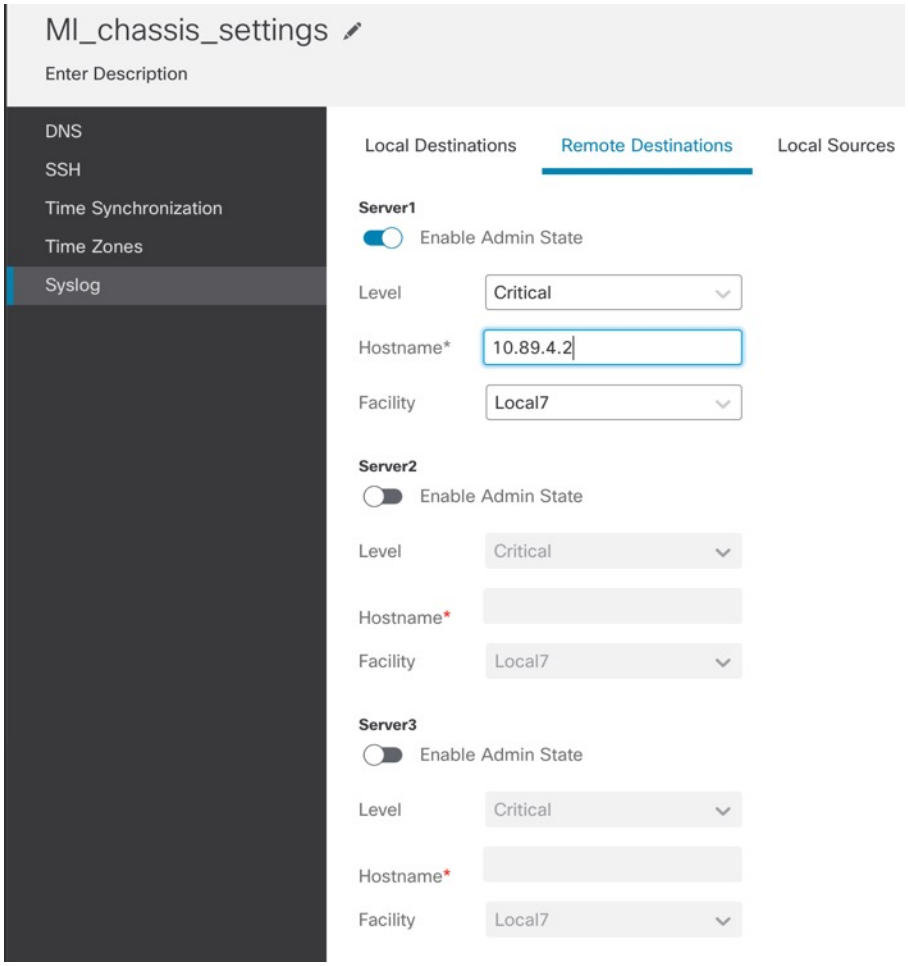


Name	Description
Console Section	
Admin State field	Whether the chassis displays syslog messages on the console. Check the **Enable** check box if you want to have syslog messages displayed on the console as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the console.
Level field	If you checked the **Enable** check box for **Console - Admin State**, select the lowest message level that you want displayed on the console. The chassis displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	

Name	Description
Admin State field	Whether the chassis displays syslog messages on the monitor. Check the **Enable** check box if you want to have syslog messages displayed on the monitor as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the monitor.
Level drop-down list	If you checked the **Enable** check box for **Monitor - Admin State**, select the lowest message level that you want displayed on the monitor. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Step 4 On the **Remote Destinations** tab, complete the following fields for up to three external logs that can store messages generated by the chassis:

Figure 95: Syslog remote destinations



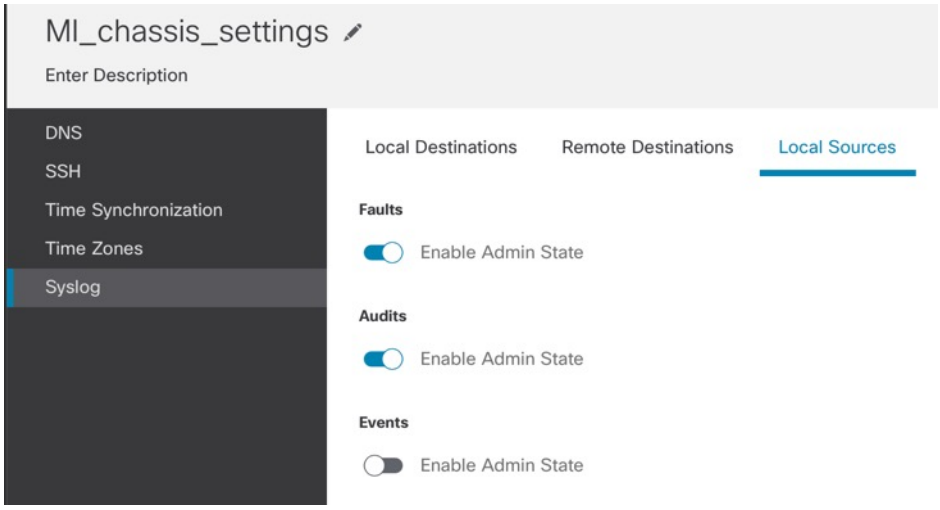
By sending syslog messages to a remote destination, you can archive messages according to the available disk space on the external syslog server, and manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

Name	Description
Admin State field	Check the **Enable** check box if you want to have syslog messages stored in a remote log file.

Name	Description
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname/IP Address field	The hostname or IP address on which the remote log file resides. **Note** You must configure a DNS server if you use a hostname rather than an IP address.
Facility drop-down list	Choose a system log facility for syslog servers to use as a basis to file messages. This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

Step 5 Click the **Local Sources** tab, and complete the following fields.

Figure 96: Syslog local sources



Name	Description
Faults > **Enable Admin State**	Enable system fault logging.
Audits > **Enable Admin State**	Enable audit logging.
Events > **Enable Admin State**	Enable system event logging.

Step 6 Click **Save** to save all policy changes.

Configure time synchronization

NTP is used to implement a hierarchical system of servers that provide precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure up to four NTP servers.

Note

- FXOS uses NTP version 3.
- If the stratum value of an external NTP server is 13 or greater, the application instance cannot sync to the NTP server on the FXOS chassis. Each time a NTP client syncs to a NTP server, the stratum value increases by one.

  If you have set up your own NTP server, you can find its stratum value in the /etc/ntp.conf file on the server. If the NTP server has stratum value of 13 or greater you can either change the stratum value in the ntp.conf file and restart the server, or use a different NTP server (for example: pool.ntp.org).

Before you begin

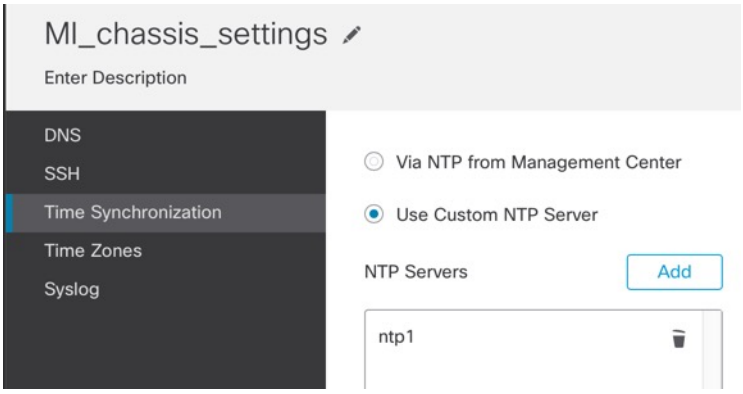
If you use a hostname for the NTP server, you must configure a DNS server. For more information, refer to Configure DNS, on page 200.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the chassis policy.

Step 2 Choose **Time Synchronization**.

Figure 97: Time synchronization



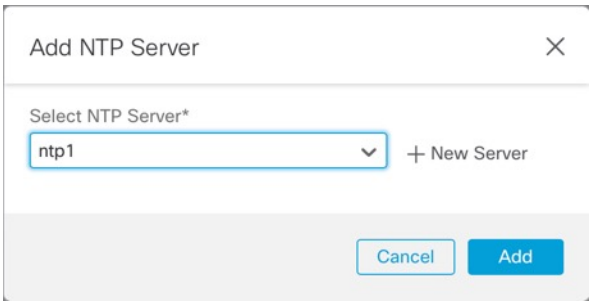
Step 3 If you want to obtain the time from the Firewall Management Center, click **Via NTP from Management Center**.

This option ensures both the chassis and the Firewall Management Center have the same time.

Step 4 To use an external NTP server, click **Use Custom NTP Server**.

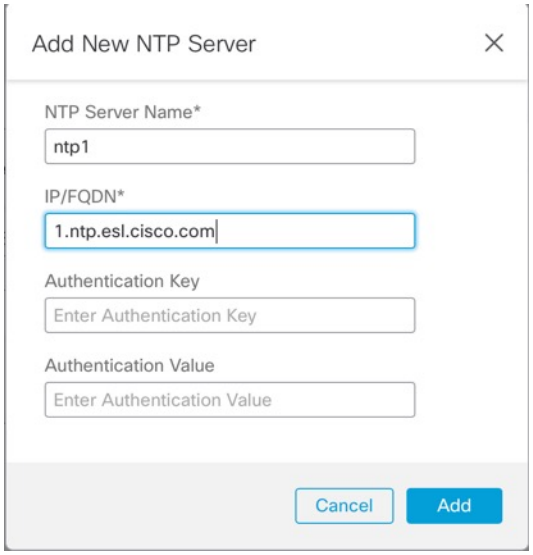
a) Click **Add** to add a server.

Figure 98: Add NTP server



b) Choose any already-defined servers from the drop-down menu and click **Add**, or click **New Server** to add a new server.

Figure 99: Add new NTP server



c) For a new server, enter the following fields, and click **Add**.

- **NTP Server Name**: A name to identify this server.
- **IP/FQDN**: The IP address or hostname of the server.
- **Authentication Key** and **Authentication Value**: Obtain the key ID and value from the NTP server. For example, to generate the SHA1 key on NTP server Version 4.2.8p8 or later with OpenSSL installed, enter the **NTP-keygen -M** command, and then view the key ID and value in the NTP.keys file. The key is used to tell both the client and server which value to use when computing the message digest.

  Only SHA1 is supported for NTP server authentication.

Step 5 Click **Save** to save all policy changes.

Configure time zones

Time zone configuration is essential for maintaining accurate timestamps in system logs and ensuring proper time-based functionality across the device.

Before you begin

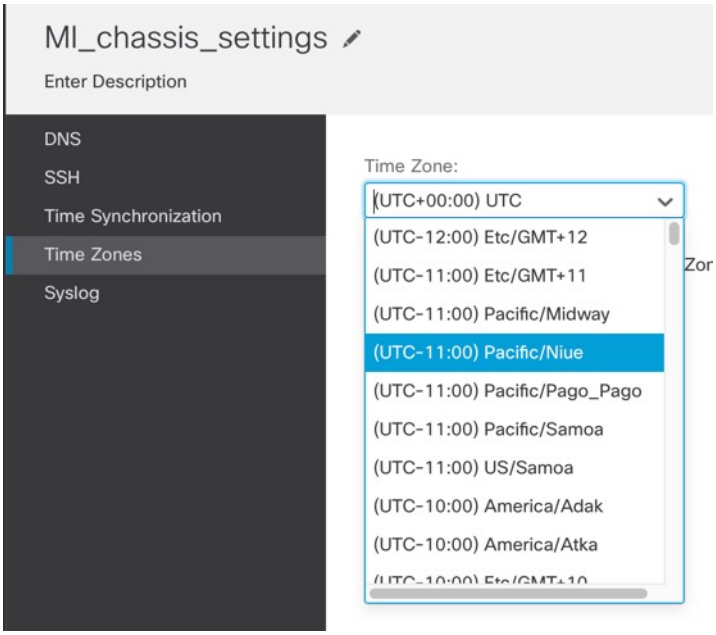
Follow these steps to configure the time zone for the chassis:

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the chassis policy.

Step 2 Choose **Time Zones**.

Figure 100: Time zones



Step 3 Choose your **Time Zone** from the drop-down menu.

Step 4 Click **Save** to save all policy changes.

Multi-instance mode management

This section describes less common tasks, including changing settings at the FXOS CLI or changing interfaces assigned to the chassis.

Change interfaces assigned to an instance

You can allocate or unallocate an interface on the instance. Adding a new interface, or deleting an unused interface, has minimal impact on the instance configuration. You can also edit the membership of an allocated EtherChannel without affecting the instance.

Deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the instance configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface.

Policies that refer to security zones are not affected.

Note For high availability, you need to make the same interface changes for the other unit. Otherwise, high availability might not operate correctly.

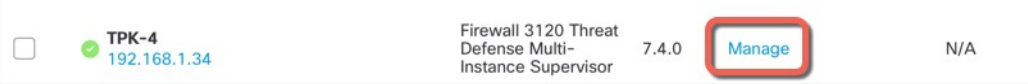
Before you begin

- Configure your interfaces according to Instance configuration, on page 175.
- If you plan to add an already-allocated interface to an EtherChannel, you need to unallocate the interface from the instance first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the instance.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column or click **Edit** ( ).

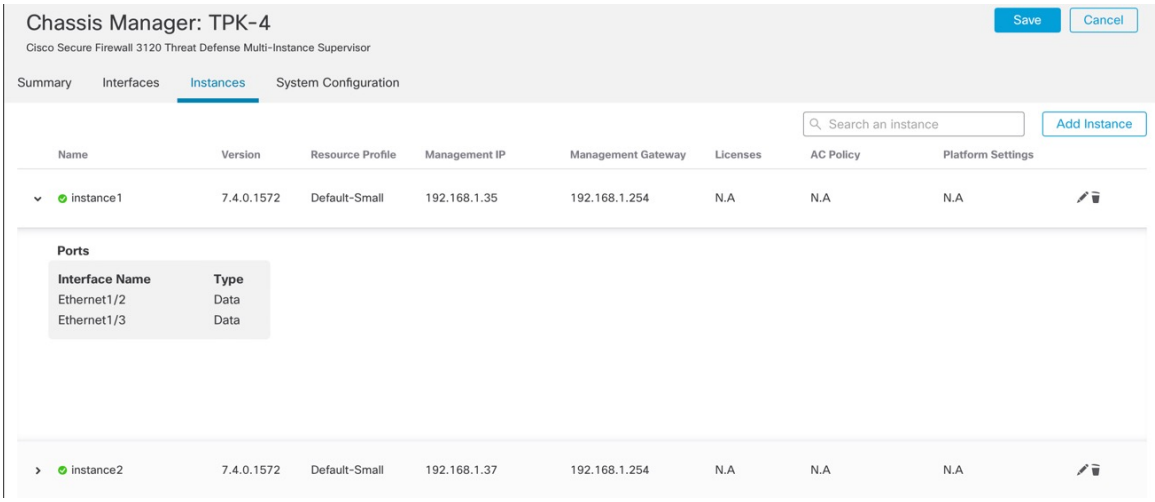
Figure 101: Manage Chassis



The **Chassis Manager** page opens for the chassis to the **Summary** page.

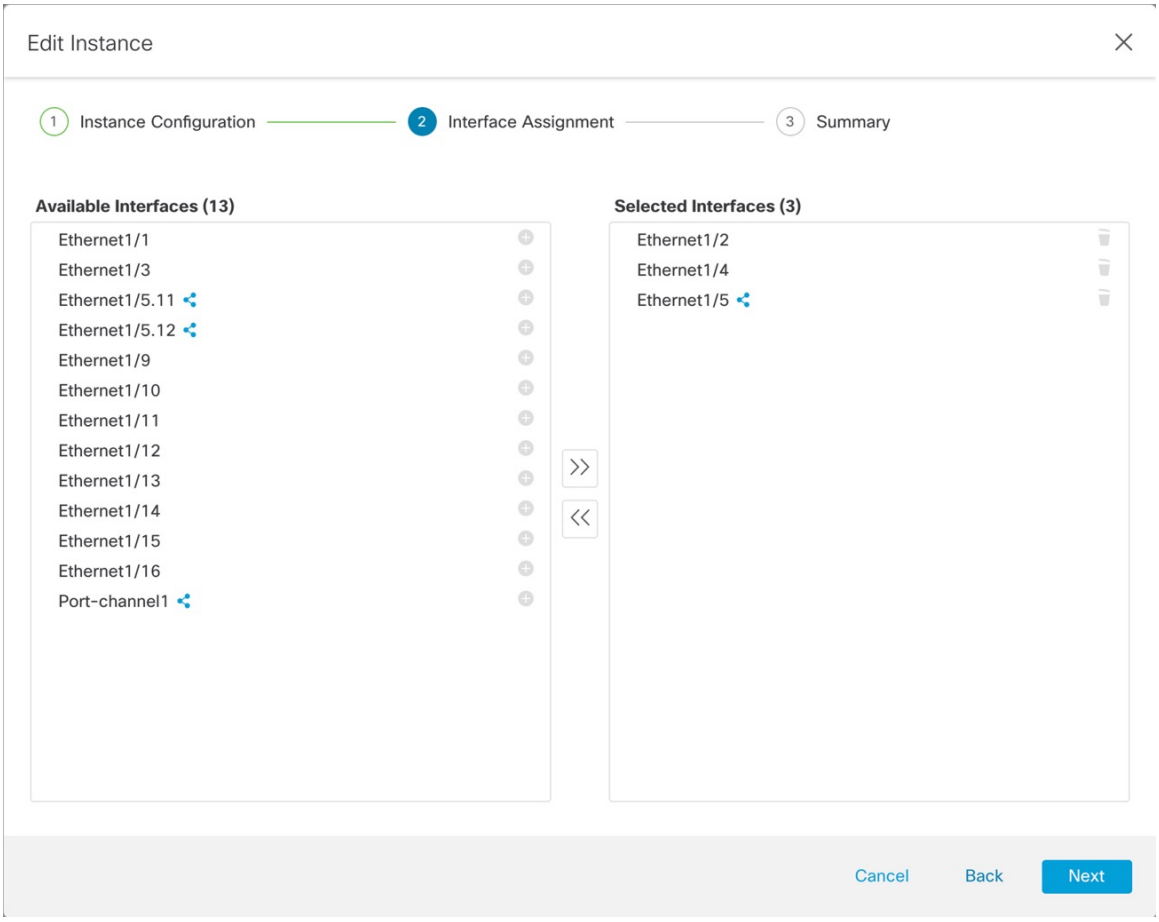
Step 2 Click **Instances**, and click **Edit** ( ) next to the instance for which you want to change interfaces.

Figure 102: Instances



Step 3 Click **Next** until you get to the **Interface Assignment** screen.

Figure 103: Interface assignment



Shared interfaces show the sharing icon ( ).

Step 4 Make your interface changes, and then click **Next**.

Step 5 Click **Save** on the **Summary** screen.

Step 6 For high availability, you need to make the same interface changes for the other unit. Otherwise, high availability might not operate correctly.

Change chassis management settings at the FXOS CLI

If you want to change the chassis management interface IP address and gateway, change the Firewall Management Center to a new manager, change the admin password, or disable multi-instance mode, you can do so from the FXOS CLI.

Procedure

Step 1 Connect to the chassis console port.

The console port connects to the FXOS CLI.

Note We recommend using the console port. You can also connect using SSH to the management interface, if configured in the chassis platform settings in the Firewall Management Center; however, if you change the management IP address, you will be disconnected.

Step 2 Log in with the username **admin** and the password you set during initial setup.

Step 3 Change the Management IP address. You can use a static IPv4 and/or IPv6 address.

IPv4:

scope fabric-interconnect

set out-of-band static IP *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

IPv6:

scope fabric-interconnect

scope ipv6-config

set out-of-band static ipv6 *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

Example:

IPv4:

```
firepower-3110# scope fabric-interconnect
firepower-3110 /fabric-interconnect # set out-of-band static ip 10.5.23.8 netmask
255.255.255.0
gw 10.5.23.1
```

IPv6:

```
firepower-3110# scope fabric-interconnect
firepower-3110 / fabric-interconnect # scope ipv6-config
firepower-3110 / fabric-interconnect /ipv6-config # set out-of-band static ipv6 2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

Step 4 Change the Firewall Management Center.

You should first unregister the chassis from the current Firewall Management Center.

enter device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**NAT-ID** *nat_id*]

You are prompted for the registration key.

You can enter this command from any scope.

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}: Specifies either the FQDN or IP address of the Firewall Management Center. At least one of the devices, either the Firewall Management Center or the chassis, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices. If you do not specify a **hostname**, then the chassis must have a reachable IP address or hostname and you must specify the **NAT-ID**.

- **NAT-ID** *nat_id*: Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center when you register the chassis when one side does not specify a reachable IP address or hostname. It is required if you do not specify a **hostname**, however we recommend that you always set the NAT ID even when you specify a hostname or IP address. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.
- **Registration Key:** *reg_key*: You will be prompted for a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the chassis. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

Example:

```
firepower-3110# enter device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

Step 5 Change the admin password.

scope security

set password

Enter a password: *password*

Confirm the password: *password*

Example:

```
firepower-3110# scope security
firepower-3110 /security # set password
Enter new password: Sw@nsong67
Confirm new password: Sw@nsong67
firepower-3110 /security #
```

Step 6 Disable multi-instance mode and set the system back to appliance mode.

scope system

set deploymode native

You are prompted to reboot.

Example:

```
firepower-3110# scope system
firepower-3110 /system # set deploymode native
All configuration and bootable images will be lost and system will reboot.
If there was out of band upgrade, it might reboot with the base version and
need to re-image to get the expected running version.
Do you still want to change deploy mode? (yes/no):yes
firepower-3110 /system #
```

To change the mode back to multi-instance mode, enter **set deploymode container**. You can check the current mode using the **show system detail** command.

Multi-instance mode

This section helps you troubleshoot and diagnose your multi-instance mode chassis and instances.

Multi-instance setups

A multi-instance setup is a system configuration approach that

- enables running multiple independent instances on a single hardware platform,
- allows flexible allocation of resources to each instance, and
- supports both container and native (appliance) operating modes.

show system detail

This FXOS command shows the current mode, Native or Container. If the mode is Native (also known as appliance mode), you can convert to multi-instance (Container) mode. Note that the prompt/name in multi-instance mode is generic "firepower-<model>" while the prompt in appliance mode is the hostname you set for the Firewall Threat Defense (by default "firepower")

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

scope system > show

This FXOS command shows the current mode in a table format. Note that the prompt/name in multi-instance mode is generic "firepower-<model>" while the prompt in appliance mode is the hostname you set for the Firewall Threat Defense.

```
firepower-3110# scope system
firepower-3110 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
```

```
    firepower-3110
               Stand Alone Container   10.89.5.42        ::

3110-1# scope system
3110-1 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
    3110-1     Stand Alone Native      10.89.5.41        ::
3110-1 /system #
```

Instance interfaces

An instance interface is a physical or virtual network interface on a device that

- enables connectivity between multiple logical instances within a system,
- facilitates assignment of interfaces to one or more instances, and
- supports configuration of forwarding rules using ECMP and multicast groups.

show portmanager switch forward-rules hardware mac-filter

This command shows the internal switch-forwarding rule for two instances with a dedicated physical interface assigned to each instance. Ethernet 1/2 is assigned to ftd1 and Ethernet 1/1 is assigned to ftd2.

ECMP group 1540 is assigned to ftd1 and ECMP group 1541 is assigned to ftd2.

```
secfw-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT      PKT_CNT       DMAC
1        0          17        0        17          19         29164  0:0:0:0:0:0
2        0          19        0        19          17         67588  0:0:0:0:0:0
3        0           1        0       101        1541             0  a2:5b:83:0:0:15
4        0           1        0       101        1541          8181  ff:ff:ff:ff:ff:ff
5        0           2        0       102        1540             0  a2:5b:83:0:0:18
6        0           2        0       102        1540           431  ff:ff:ff:ff:ff:ff
7        0          17        0         0           0         11133  0:0:0:0:0:0
8        0          17        0         0           0             0  0:0:0:0:0:0
```

This command shows the internal switch-forwarding rule for two instances with shared physical interfaces assigned to two instances. Ethernet 1/1 is shared between ftd1 and ftd2.

ECMP group 1540 is assigned to ftd1 and ECMP group 1541 is assigned to ftd2.

MCAST group 4096 is used for replicating broadcast traffic between ftd1 and ftd2.

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT      PKT_CNT       DMAC
1        0          17        0        17          19          2268  0:0:0:0:0:0
2        0          19        0        19          17          4844  0:0:0:0:0:0
3        0           1        0       101        1541             0  a2:5b:83:0:0:9
4        0           1        0       101        4096           546  ff:ff:ff:ff:ff:ff
5        0           1        0       101        1540             0  a2:5b:83:0:0:c
6        0          17        0         0           0          1263  0:0:0:0:0:0
7        0          17        0         0           0             0  0:0:0:0:0:0
```

This command shows the internal switch-forwarding rule for two instances with shared subinterfaces assigned to both instances. Ethernet 1/1.2452 is shared between ftd1 and ftd2.

ECMP group 1540 is assigned to ftd1 and ECMP group 1541 is assigned to ftd2.

MCAST group 4097 is used for replicating broadcast traffic between ftd1 and ftd2.

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19       21305  0:0:0:0:0:0
2        0         19       0       19         17       50976  0:0:0:0:0:0
3     2452          1       0      101       1541         430  a2:5b:83:0:0:f
4     2452          1       0      101       4097           0  ff:ff:ff:ff:ff:ff
5     2452          1       0      101       1540           0  a2:5b:83:0:0:12
6        0         17       0        0          0       11038  0:0:0:0:0:0
7        0         17       0        0          0           0  0:0:0:0:0:0
```

show portmanager switch ecmp-groups detail

Use this command to list each Instance Ecmp-Vport-Physical port mapping detail.

Note Physical-Port 18 is the backplane uplink interface between the internal switch and the instance.

```
firepower-3140(local-mgmt)# show portmanager switch ecmp-groups detail
       ECMP-GROUP  VPORT      PHYSICAL-PORT
1      1536        256        18
2      1537        257        18
3      1538        258        18
4      1539        259        18
5      1540        260        18
6      1541        261        18
7      1542        262        18
8      1543        263        18
9      1544        264        18
10     1545        265        18
```

show portmanager switch mcast-groups detail

Use this command to list MCAST group membership details.

```
firepower-3140(local-mgmt)# show portmanager switch mcast-groups detail
       MCAST-GROUP
1      4096
       Member-ports
       Ethernet 1/1
       ECMP-ID 1541
       ECMP-ID 1540
```

show portmanager counters mcast-group

Use this command to check the MCAST group packet counter.

```
firepower-3140(local-mgmt)# show portmanager counters mcast-group 4096
PKT_CNT: 8106
```

show portmanager counters ecmp

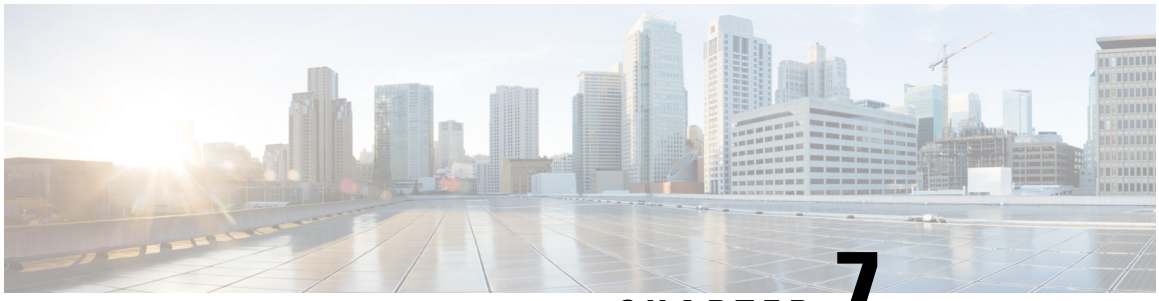
Use this command to check the ECMP group packet counter.

```
firepower-3140(local-mgmt)# show portmanager counters ecmp 1541
PKT_CNT: 430
```

Multi-instance mode feature and version history

This reference documents the history of multi-instance mode capabilities, including instance limit increases, platform support expansions, and management interface improvements for Secure Firewall devices.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multi-instance mode for the Secure Firewall 3100.	7.4.1	7.4.1	You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*Firewall Threat Defense upgrade*). New/modified screens: • **Devices** > **Device Management** > **Add** > **Chassis** • **Devices** > **Device Management** > **Device** > **Chassis Manager** • **Devices** > **Platform Settings** > **New Policy** > **Chassis Platform Settings** • **Devices** > **Chassis Upgrade** New/modified Firewall Threat Defense CLI commands: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** New/modified FXOS CLI commands: **create device-manager**, **set deploymode** Platform restrictions: Not supported on the Secure Firewall 3105.



CHAPTER 7

Logical Devices on the Firepower 4100/9300

The Firepower 4100/9300 is a flexible security platform on which you can install one or more *logical devices*. Before you can add the Firewall Threat Defense to the Firewall Management Center, you must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Secure Firewall Chassis Manager or the FXOS CLI. This chapter describes basic interface configuration and how to add a standalone or High Availability logical device using the Secure Firewall Chassis Manager. To use the FXOS CLI, see the FXOS CLI configuration guide. For more advanced FXOS procedures and troubleshooting, see the FXOS configuration guide.

- Supported interfaces, on page 223
- Logical devices, on page 238
- Licenses for container instances, on page 247
- Requirements and prerequisites for logical devices, on page 248
- Guidelines and limitations for logical devices, on page 255
- Configure interfaces, on page 259
- Configure logical devices, on page 264
- History for logical devices, on page 276

Supported interfaces

The Firepower 4100/9300 chassis supports physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces. EtherChannel interfaces can include up to 16 member interfaces of the same type.

Chassis management interface

A chassis management interface is a network interface that is used for management of the FXOS chassis by SSH or Firewall Chassis Manager.

The chassis management interface appears at the top of the **Interfaces** tab as **MGMT**. You can only enable or disable this interface on the **Interfaces** tab.

To configure parameters for this interface, you must configure them from the CLI. To view information about this interface in the FXOS CLI, connect to local management and show the management port:

Firepower # **connect local-MGMT**

Firepower(local-MGMT) # **show MGMT-port**

Note The chassis management interface does not support jumbo frames.

Interface types

Physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces are categorized into different types by their specific functions.

for different purposes.

These interface types are available, each defined by its specific function and configuration requirements:

- Data—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.
- Data-sharing—Use for regular data. These data interfaces are supported only with container instances and can be shared by one or more logical devices or container instances (Firewall Threat Defense using Firewall Management Center only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, clusters, or failover links.
- Mgmt—Use to manage application instances. These interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. You can only assign one management interface per logical device. Depending on your application and manager, you can later enable management from a data interface; but you must assign a management interface to the logical device even if you don't intend to use it after you enable data management. For information about the separate chassis management interface, see Chassis management interface, on page 223.

Note Changing the management interface will cause reboot of the logical device. For example, changing management interface from e1/1 to e1/2 causes the logical device to reboot so that the change can take effect.

- Eventing—Use as a secondary management interface for Firewall Threat Defense-using-Firewall Management Center devices. To use this interface, you must configure its IP address and other parameters at the Firewall Threat Defense CLI. For example, you can separate management traffic from events (such as web events). See the management center configuration guide for more information. Eventing interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical devices that share the interface. If you later configure a data interface for management, you cannot use a separate eventing interface.

Note A virtual Ethernet interface is allocated when each application instance is installed. If the application does not use an eventing interface, then the virtual interface will be in an admin down state.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. The Cluster type is only supported on EtherChannel interfaces. For multi-instance clustering, you cannot share a Cluster-type interface across devices. You can add VLAN subinterfaces to the Cluster EtherChannel to provide separate cluster control links per cluster. If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster. The Firewall Device Manager and Security Cloud Control do not support clustering.

Note This chapter discusses FXOS VLAN subinterfaces only. You can separately create subinterfaces within the Firewall Threat Defense application. For more information, refer to FXOS interfaces and application interfaces, on page 226.

Interface type support for the Firewall Threat Defense and ASA applications in standalone and cluster deployments is shown in the table.

Table 14: Interface type support

Application		Data	Data: Subinterface	Data-Sharing	Data-Sharing: Subinterface	Mgmt	Eventing	Cluster (EtherChannel only)	Cluster: Subinterface
Firewall Threat Defense	Standalone Native Instance	Yes	—	—	—	Yes	Yes	—	—
	Standalone Container Instance	Yes	Yes	Yes	Yes	Yes	Yes	—	—
	Cluster Native Instance	Yes (EtherChannel only for inter-chassis cluster)	—	—	—	Yes	Yes	Yes	—
	Cluster Container Instance	Yes (EtherChannel only for inter-chassis cluster)	—	—	—	Yes	Yes	Yes	Yes
ASA	Standalone Native Instance	Yes	—	—	—	Yes	—	Yes	—
	Cluster Native Instance	Yes (EtherChannel only for inter-chassis cluster)	—	—	—	Yes	—	Yes	—

FXOS interfaces and application interfaces

The Firepower 4100/9300 manages the basic Ethernet settings of physical interfaces, VLAN subinterfaces for container instances, and EtherChannel (port-channel) interfaces. Within the application, you configure higher-level settings. For example, you can only create EtherChannels in FXOS, but you can assign an IP address to the EtherChannel within the application.

These sections describe the interaction between FXOS and the application for interfaces.

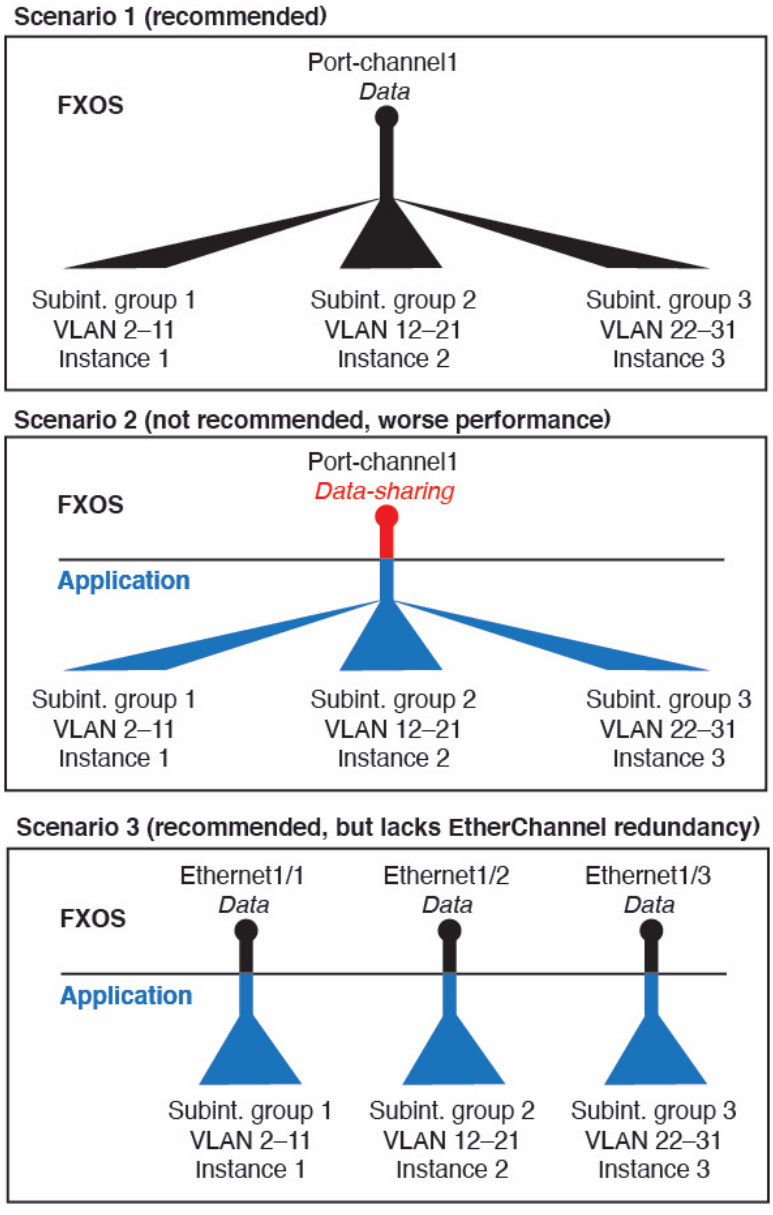
VLAN subinterfaces

For all logical devices, you can create VLAN subinterfaces within the application.

For container instances in standalone mode only, you can *also* create VLAN subinterfaces in FXOS. Multi-instance clusters do not support subinterfaces in FXOS except on the Cluster-type interface.

Application-defined subinterfaces are not subject to the FXOS limit. Choosing in which operating system to create subinterfaces depends on your network deployment and personal preference. For example, to share a subinterface, you must create the subinterface in FXOS. Another scenario that favors FXOS subinterfaces comprises allocating separate subinterface groups on a single interface to multiple instances. For example, you want to use Port-channel1 with VLAN 2–11 on instance A, VLAN 12–21 on instance B, and VLAN 22–31 on instance C. If you create these subinterfaces within the application, then you would have to share the parent interface in FXOS, which may not be desirable. See this illustration that shows the three ways you can accomplish this scenario:

Figure 104: VLANs in FXOS vs. the application for container instances



Independent interface states in the chassis and in the application

You can administratively enable and disable interfaces in both the chassis and the application. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and application.

The default state of an interface within the application depends on the type of interface. For example, the physical interface or EtherChannel is disabled by default within the application, but a subinterface is enabled by default.

Shared interface scalability

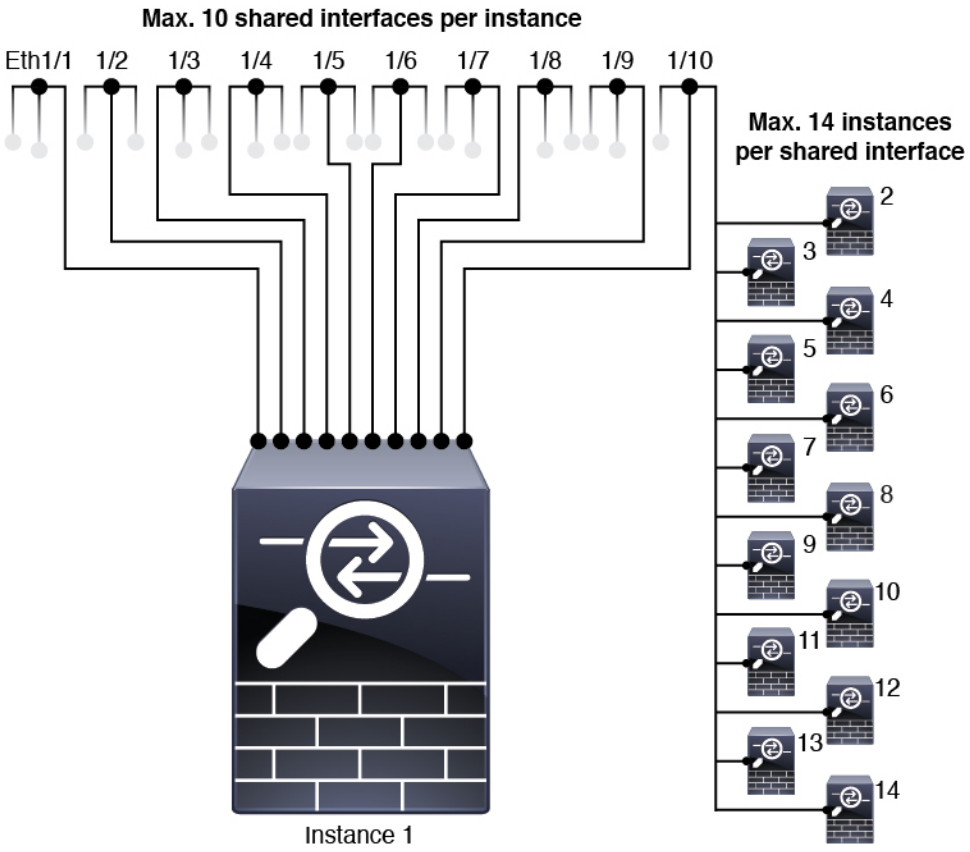
A shared interface is a network resource that

- allows multiple logical connections to transmit data concurrently,
- adapts bandwidth allocation based on real-time demand, and
- enhances scalability to support growing numbers of devices and traffic flows.

Instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. You can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:



Shared interface best practices

This topic outlines the best practices to follow when configuring shared interfaces to maximize performance and security.

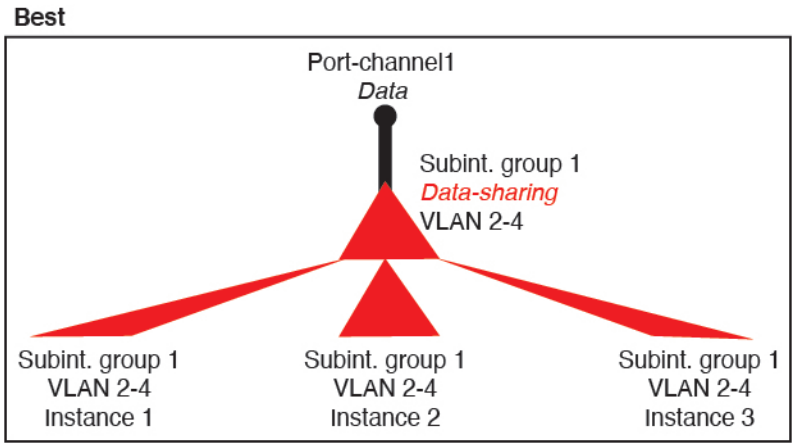
For optimal scalability of the forwarding table, share as few interfaces as possible. Instead, you can create up to 500 VLAN subinterfaces on one or more physical interfaces and then divide the VLANs among the container instances.

When sharing interfaces, follow these practices in the order of most scalable to least scalable:

1. Best: Share subinterfaces under a single parent, and use the same set of subinterfaces with the same group of instances.

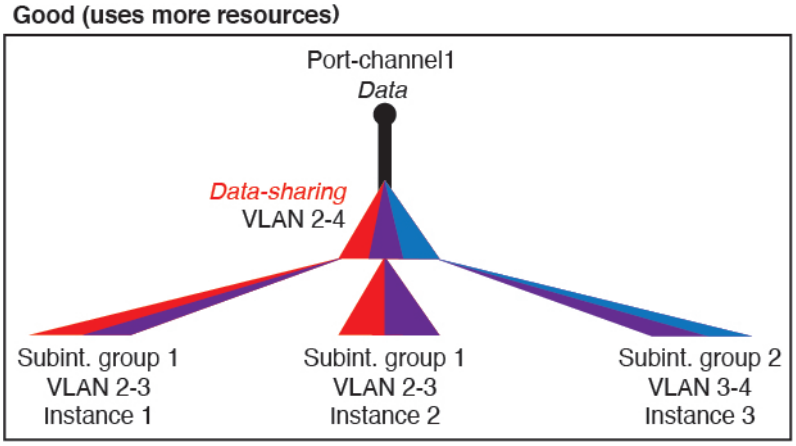
   For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel: Port-Channel1.2, 3, and 4 instead of Port-Channel2, Port-Channel3, and Port-Channel4. When you share subinterfaces from a single parent, the VLAN group table provides better scaling of the forwarding table than when sharing physical/EtherChannel interfaces or subinterfaces across parents.

Figure 105: Best: Shared Subinterface Group on One Parent



If you do not share the same set of subinterfaces with a group of instances, your configuration can cause more resource usage (more VLAN groups). For example, share Port-Channel1.2, 3, and 4 with instances 1, 2, and 3 (one VLAN group) instead of sharing Port-Channel1.2 and 3 with instances 1 and 2, while sharing Port-Channel1.3 and 4 with instance 3 (two VLAN groups).

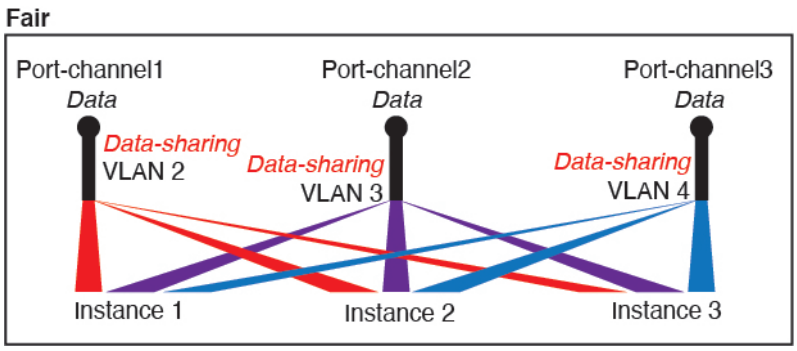
Figure 106: Good: Sharing Multiple Subinterface Groups on One Parent



2. Fair: Share subinterfaces across parents.

   For example, share Port-Channel1.2, Port-Channel2.3, and Port-Channel3.4 instead of Port-Channel2, Port-Channel4, and Port-Channel4. Although this usage is not as efficient as only sharing subinterfaces on the same parent, it still takes advantage of VLAN groups.

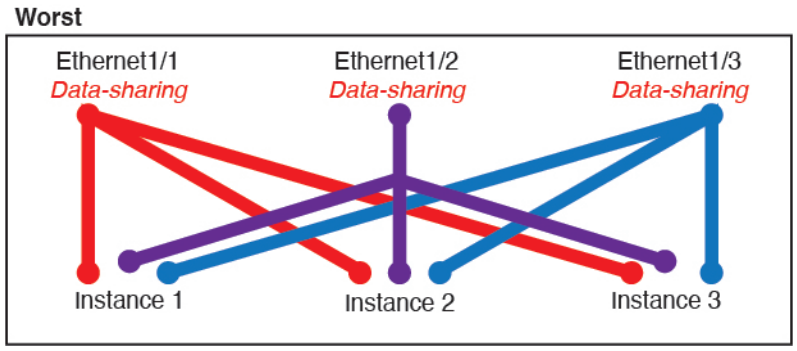
Figure 107: Fair: Shared Subinterfaces on Separate Parents



3. Worst: Share individual parent interfaces (physical or EtherChannel).

   This method uses the most forwarding table entries.

Figure 108: Worst: Shared Parent Interfaces



Shared Interface Usage Examples

See the following tables for examples of interface sharing and scalability. The below scenarios assume use of one physical/EtherChannel interface for management shared across all instances, and another physical or EtherChannel interface with dedicated subinterfaces for use with High Availability.

- Table 15: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with Three SM-44s, on page 232
- Table 16: Subinterfaces on One Parent and Instances on a Firepower 9300 with Three SM-44s, on page 233
- Table 17: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with One SM-44, on page 235
- Table 18: Subinterfaces on One Parent and Instances on a Firepower 9300 with One SM-44, on page 236

Firepower 9300 with Three SM-44s

The following table applies to three SM-44 security modules on a 9300 using only physical interfaces or EtherChannels. Without subinterfaces, the maximum number of interfaces are limited. Moreover, sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

Each SM-44 module can support up to 14 instances. Instances are split between modules as necessary to stay within limits.

Table 15: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with Three SM-44s

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: • 8 • 8 • 8 • 8	**0**	**4:** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16%
30: • 15 • 15	**0**	**2:** • Instance 1 • Instance 2	14%
14: • 14 (1 ea.)	**1**	**14:** • Instance 1-Instance 14	46%
33: • 11 (1 ea.) • 11 (1 ea.) • 11 (1 ea.)	**3:** • 1 • 1 • 1	**33:** • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33	98%
33: • *11 (1 ea.)* • *11 (1 ea.)* • *12 (1 ea.)*	***3:*** • *1* • *1* • *1*	***34:*** • *Instance 1-Instance 11* • *Instance 12-Instance 22* • *Instance 23-Instance 34*	*102%* DISALLOWED
30: • 30 (1 ea.)	**1**	**6:** • Instance 1-Instance 6	25%
30: • 10 (5 ea.) • 10 (5 ea.) • 10 (5 ea.)	**3:** • 1 • 1 • 1	**6:** • Instance 1-Instance2 • Instance 2-Instance 4 • Instance 5-Instance 6	23%

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
30: • 30 (6 ea.)	**2**	**5:** • Instance 1-Instance 5	28%
30: • 12 (6 ea.) • 18 (6 ea.)	**4:** • 2 • 2	**5:** • Instance 1-Instance2 • Instance 2-Instance 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • Instance 1 • Instance 2 • Instance 3 • Instance 4	44%
24: • 12 (6 ea.) • 12 (6 ea.)	**14:** • 7 • 7	**4:** • Instance 1-Instance2 • Instance 2-Instance 4	41%

The following table applies to three SM-44 security modules on a 9300 using subinterfaces on a single parent physical interface. For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel. Sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

Each SM-44 module can support up to 14 instances. Instances are split between modules as necessary to stay within limits.

Table 16: Subinterfaces on One Parent and Instances on a Firepower 9300 with Three SM-44s

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
168: • 168 (4 ea.)	**0**	**42:** • Instance 1-Instance 42	33%
224: • 224 (16 ea.)	**0**	**14:** • Instance 1-Instance 14	27%
14: • 14 (1 ea.)	**1**	**14:** • Instance 1-Instance 14	46%

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
33: • 11 (1 ea.) • 11 (1 ea.) • 11 (1 ea.)	**3:** • 1 • 1 • 1	**33:** • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33	98%
70: • 70 (5 ea.)	**1**	**14:** • Instance 1-Instance 14	46%
165: • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.)	**3:** • 1 • 1 • 1	**33:** • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33	98%
70: • 70 (5 ea.)	**2**	**14:** • Instance 1-Instance 14	46%
165: • 55 (5 ea.) • 55 (5 ea.) • 55 (5 ea.)	**6:** • 2 • 2 • 2	**33:** • Instance 1-Instance 11 • Instance 12-Instance 22 • Instance 23-Instance 33	98%
70: • 70 (5 ea.)	**10**	**14:** • Instance 1-Instance 14	46%
165: • *55 (5 ea.)* • *55 (5 ea.)* • *55 (5 ea.)*	***30:*** • *10* • *10* • *10*	***33:*** • *Instance 1-Instance 11* • *Instance 12-Instance 22* • *Instance 23-Instance 33*	*102%* DISALLOWED

Firepower 9300 with One SM-44

The following table applies to the Firepower 9300 with one SM-44 using only physical interfaces or EtherChannels. Without subinterfaces, the maximum number of interfaces are limited. Moreover, sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

The Firepower 9300 with one SM-44 can support up to 14 instances.

Table 17: Physical/EtherChannel Interfaces and Instances on a Firepower 9300 with One SM-44

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: • 8 • 8 • 8 • 8	**0**	**4:** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16%
30: • 15 • 15	**0**	**2:** • Instance 1 • Instance 2	14%
14: • 14 (1 ea.)	**1**	**14:** • Instance 1-Instance 14	46%
14: • 7 (1 ea.) • 7 (1 ea.)	**2:** • **1** • **1**	**14:** • Instance 1-Instance 7 • Instance 8-Instance 14	37%
32: • 8 • 8 • 8 • 8	**1**	**4:** • Instance 1 • Instance 2 • Instance 3 • Instance 4	21%
32: • 16 (8 ea.) • 16 (8 ea.)	**2**	**4:** • Instance 1-Instance 2 • Instance 3-Instance 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • Instance 1 • Instance 2 • Instance 3 • Instance 4	25%

Dedicated Interfaces	Shared Interfaces	Number of Instances	% Forwarding Table Used
32: • 16 (8 ea.) • 16 (8 ea.)	**4:** • 2 • 2	**4:** • Instance 1-Instance 2 • Instance 3-Instance 4	24%
24: • 8 • 8 • 8	**8**	**3:** • Instance 1 • Instance 2 • Instance 3	37%
10: • 10 (2 ea.)	**10**	**5:** • Instance 1-Instance 5	69%
10: • 6 (2 ea.) • 4 (2 ea.)	**20:** • 10 • 10	**5:** • Instance 1-Instance 3 • Instance 4-Instance 5	59%
14: • *12 (2 ea.)*	***10***	***7:*** • *Instance 1-Instance 7*	*109%* DISALLOWED

The following table applies to the Firepower 9300 with one SM-44 using subinterfaces on a single parent physical interface. For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel. Sharing multiple physical interfaces uses more forwarding table resources than sharing multiple subinterfaces.

The Firepower 9300 with one SM-44 can support up to 14 instances.

Table 18: Subinterfaces on One Parent and Instances on a Firepower 9300 with One SM-44

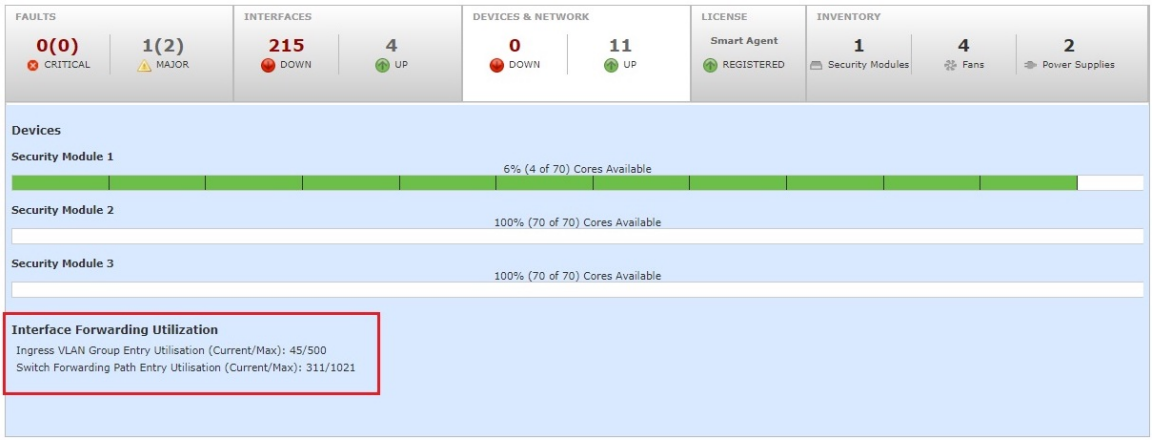
Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
112: • 112 (8 ea.)	**0**	**14:** • Instance 1-Instance 14	17%
224: • 224 (16 ea.)	**0**	**14:** • Instance 1-Instance 14	17%
14: • 14 (1 ea.)	**1**	**14:** • Instance 1-Instance 14	46%

Dedicated Subinterfaces	Shared Subinterfaces	Number of Instances	% Forwarding Table Used
14: • 7 (1 ea.) • 7 (1 ea.)	**2:** • 1 • 1	**14:** • Instance 1-Instance 7 • Instance 8-Instance 14	37%
112: • 112 (8 ea.)	**1**	**14:** • Instance 1-Instance 14	46%
112: • 56 (8 ea.) • 56 (8 ea.)	**2:** • 1 • 1	**14:** • Instance 1-Instance 7 • Instance 8-Instance 14	37%
112: • 112 (8 ea.)	**2**	**14:** • Instance 1-Instance 14	46%
112: • 56 (8 ea.) • 56 (8 ea.)	**4:** • 2 • 2	**14:** • Instance 1-Instance 7 • Instance 8-Instance 14	37%
140: • 140 (10 ea.)	**10**	**14:** • Instance 1-Instance 14	46%
140: • 70 (10 ea.) • 70 (10 ea.)	**20:** • 10 • 10	**14:** • Instance 1-Instance 7 • Instance 8-Instance 14	37%

View shared interface resources

To view forwarding table and VLAN group usage, see the **Devices & Network** > **Interface Forwarding Utilization** area.

For example:



Inline set link state propagation for the Firewall Threat Defense

Inline set link state propagation is a network feature that automatically synchronizes the link state between two paired interfaces in an inline set.

An inline set acts like a bump on the wire and binds two interfaces together to slot into an existing network. This function allows the system to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

When you configure an inline set in the Firewall Threat Defense application and enable link state propagation, the Firewall Threat Defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the chassis senses the change and updates the link state of the other interface to match it. Note that the chassis requires up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

Note Do not enable Hardware Bypass and link state propagation for the same inline set.

Logical devices

A logical device is a virtualization construct that lets you run one application instance (either ASA or Firewall Threat Defense) and also one optional decorator application (Radware DefensePro) to form a service chain.

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.

Note For the Firepower 9300, you can install different application types (ASA and Firewall Threat Defense) on separate modules in the chassis. You can also run different versions of an application instance type on separate modules.

Standalone and clustered logical devices

You can add these logical device types:

- Standalone—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.
- Cluster—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three modules must participate in the cluster, for both native and container instances. The Firewall Device Manager does not support clustering.

Logical device application instances

Application instances run in the following deployment types:

- Native instance—A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance.
- Container instance—A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances. Multi-instance capability is only supported for the Firewall Threat Defense using Firewall Management Center; it is not supported for the ASA or the Firewall Threat Defense using Firewall Device Manager.

Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full Firewall Threat Defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the Firewall Threat Defense.

For the Firepower 9300, you can use a native instance on some modules and container instances on the other modules.

Container instance interfaces

To provide flexible physical interface use for container instances, you can create VLAN subinterfaces in FXOS and also share interfaces (VLAN or physical) between multiple instances. Native instances cannot use VLAN subinterfaces or shared interfaces. A multi-instance cluster cannot use VLAN subinterfaces or shared

interfaces. An exception is made for the cluster control link, which can use a subinterface of the Cluster EtherChannel. For more information, refer to Shared interface scalability, on page 163 and Add a VLAN subinterface for container instances, on page 263.

Note This document discusses FXOS VLAN subinterfaces only. You can separately create subinterfaces within the Firewall Threat Defense application. For more information, refer to FXOS interfaces and application interfaces, on page 226.

How the chassis classifies packets

The chassis processes incoming and outgoing packets as they pass through a device, ensuring that each packet is handled according to its type, destination, and security requirements.

Each packet that enters the chassis must be classified so that the chassis can determine to which instance to send a packet.

- Unique Interfaces: If only one instance is associated with the ingress interface, the chassis classifies the packet into that instance. For bridge group member interfaces (in transparent mode or routed mode), inline sets, or passive interfaces, this method is used to classify packets at all times.
- Unique MAC Addresses: The chassis automatically generates unique MAC addresses for all interfaces, including shared interfaces. If multiple instances share an interface, then the classifier uses unique MAC addresses assigned to the interface in each instance. An upstream router cannot route directly to an instance without unique MAC addresses. You can also set the MAC addresses manually when you configure each interface within the application.

Note If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each instance.

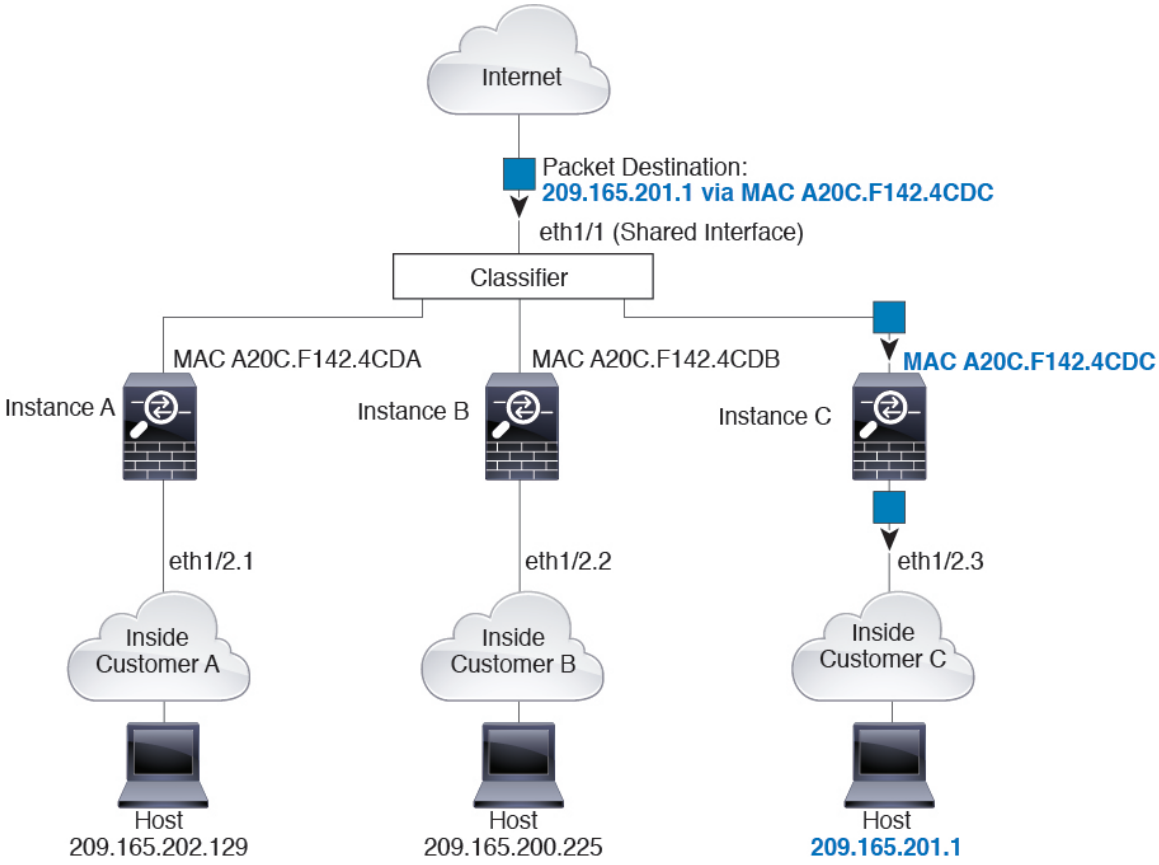
Classification examples

These examples demonstrate how packet classification works in various network configurations and firewall deployment scenarios.

Packet classification with a shared interface using MAC addresses

This figure shows multiple instances sharing an outside interface. The classifier assigns the packet to Instance C because Instance C includes the MAC address to which the router sends the packet.

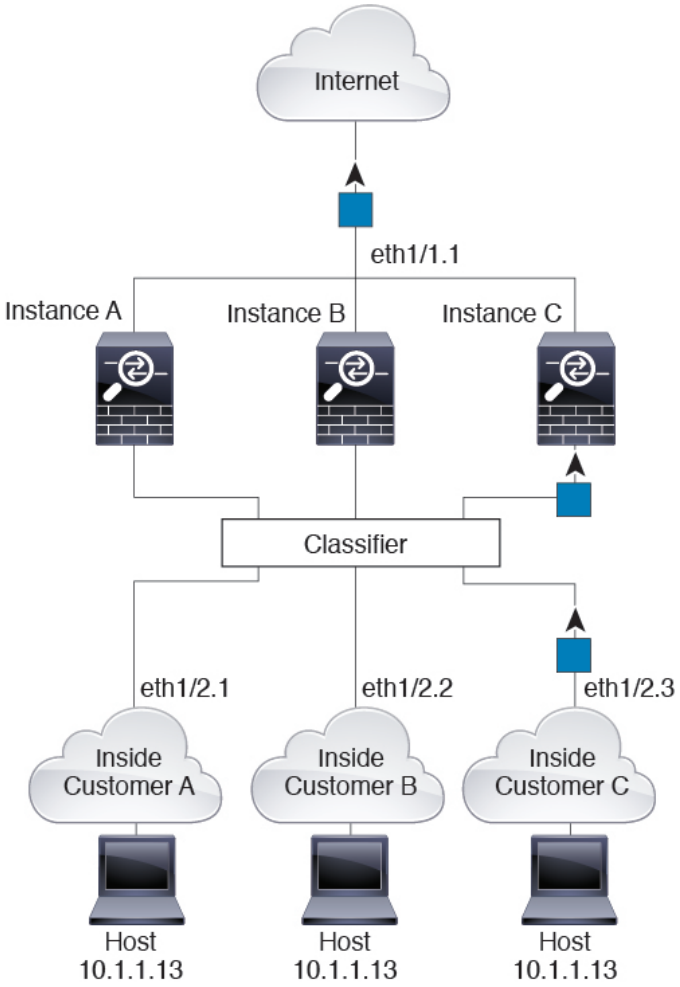
Figure 109: Packet classification with a shared interface using MAC addresses



Incoming traffic from inside networks

Note that all new incoming traffic must be classified, even from inside networks. This figure shows a host on the Instance C inside network accessing the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

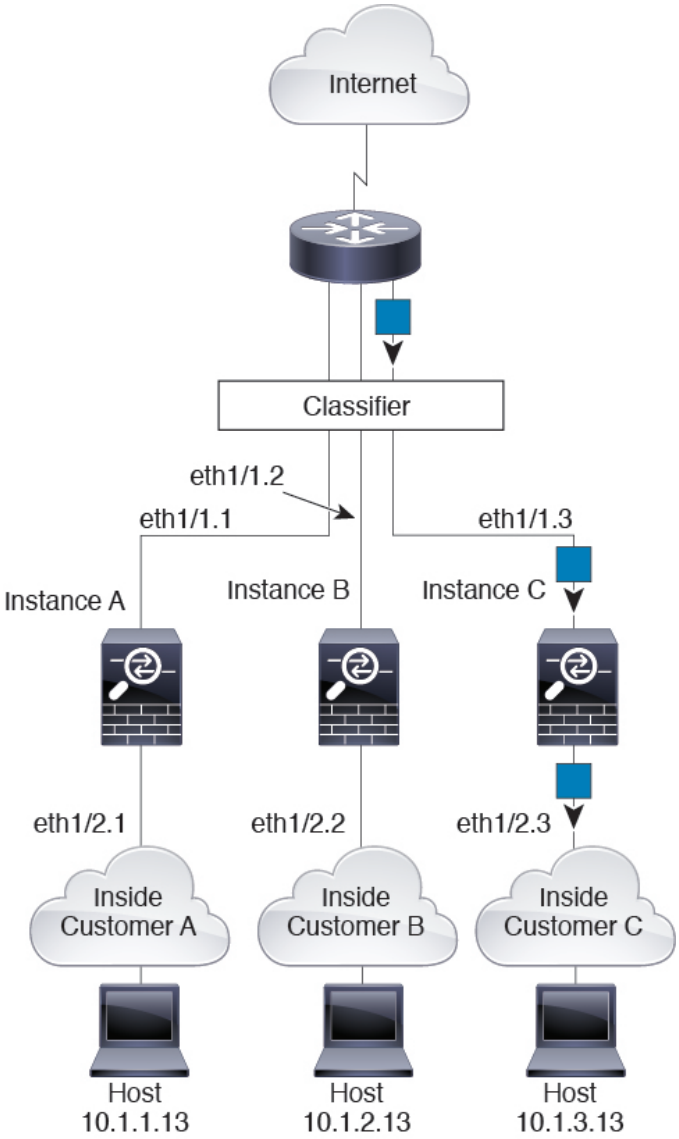
Figure 110: Incoming traffic from inside networks



Transparent firewall instances

For transparent firewalls, you must use unique interfaces. This figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

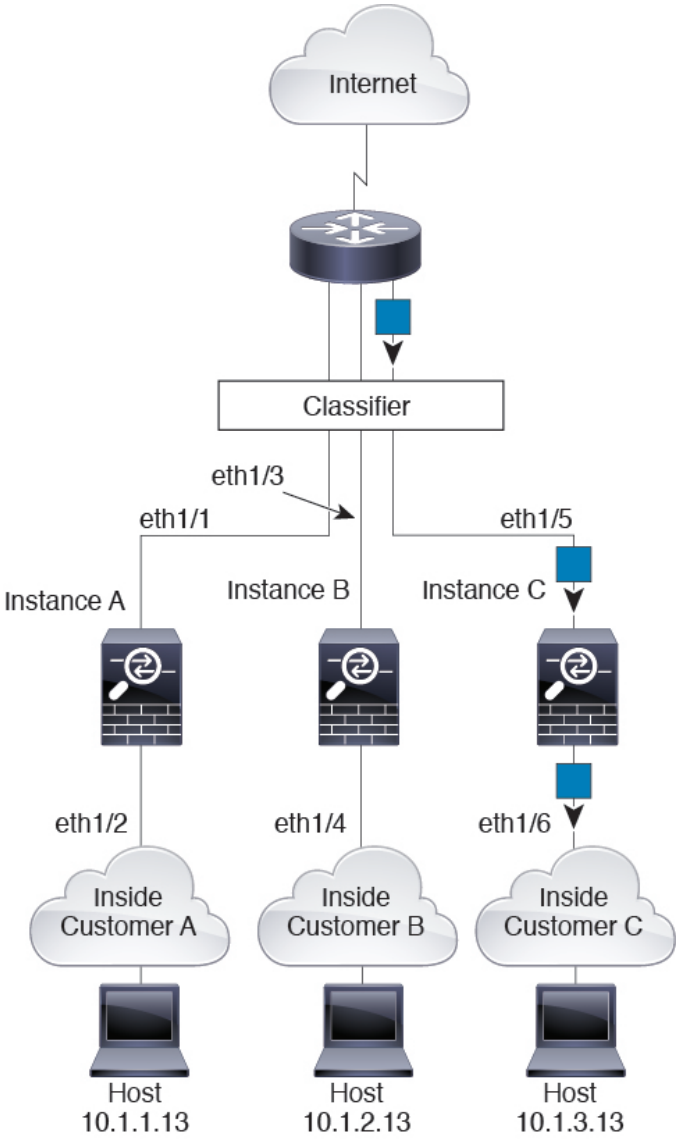
Figure 111: Transparent firewall instances



Inline sets

For inline sets, you must use unique interfaces and they must be physical interfaces or EtherChannels. This figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/5, which is assigned to Instance C.

Figure 112: Inline sets



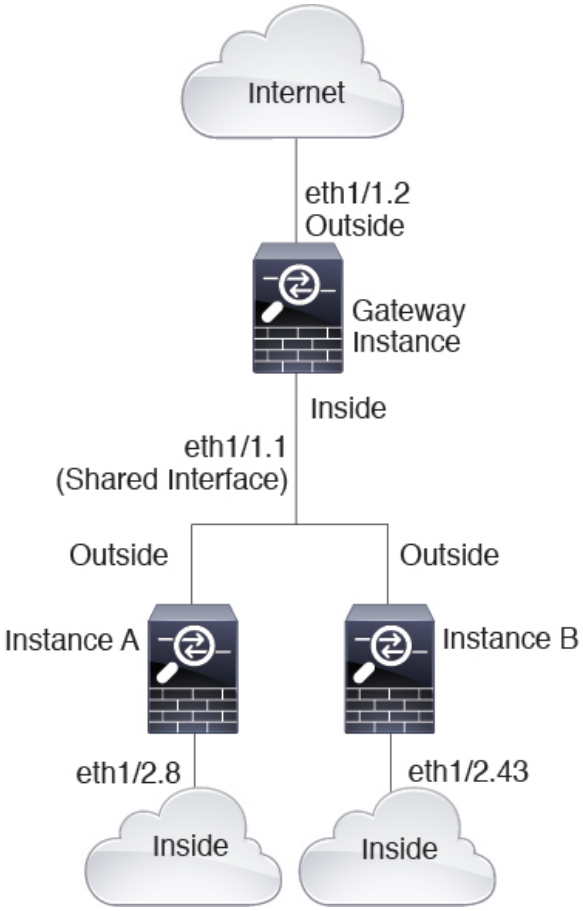
Cascading container instances

Cascading instances connect one instance's outside interface to another's inside interface, simplifying configuration by sharing parameters in the top instance. Avoid using shared interfaces with High Availability to prevent MAC address conflicts; use unique interfaces and an external switch instead.

Placing an instance directly in front of another instance is called *cascading instances*; the outside interface of one instance is the same interface as the inside interface of another instance. You might want to cascade instances if you want to simplify the configuration of some instances by configuring shared parameters in the top instance.

The following figure shows a gateway instance with two instances behind the gateway.

Figure 113: Cascading Instances



Note Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.

Typical multi-instance deployment

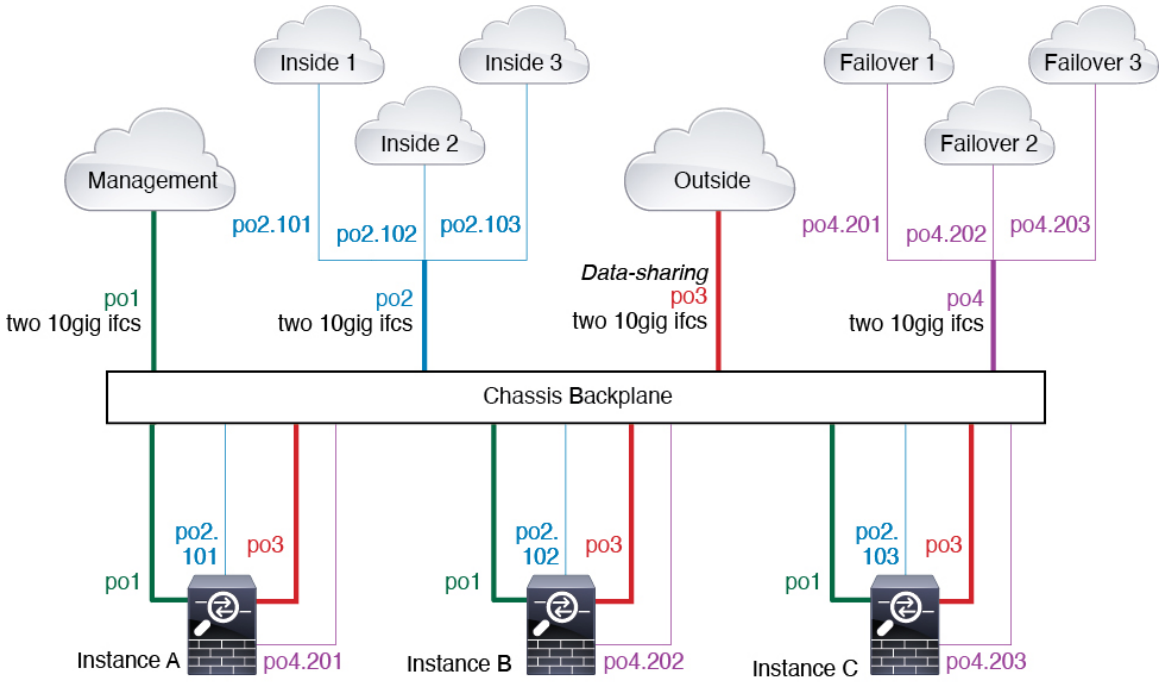
This example includes three container instances in routed firewall mode and their interface configurations.

The container instance include these interfaces:

- Management—All instances use the Port-Channel1 interface (management type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Within each application, the interface uses a unique IP address on the same management network.
- Inside—Each instance uses a subinterface on Port-Channel2 (data type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Each subinterface is on a separate network.

- Outside—All instances use the Port-Channel3 interface (data-sharing type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Within each application, the interface uses a unique IP address on the same outside network.
- Failover—Each instance uses a subinterface on Port-Channel4 (data type). This EtherChannel includes two 10 Gigabit Ethernet interfaces. Each subinterface is on a separate network.

Figure 114: Typical Multi-Instance deployment



Automatic MAC Addresses for Container Instance Interfaces

The chassis automatically generates MAC addresses for instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the instance, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the instance.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

The chassis generates the MAC address using the following format:

A2*xx.yyzz.zzzz*

Where *xx.yy* is a user-defined prefix or a system-defined prefix, and *zz.zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xxyy*) to match the chassis native form:

A2**4D.00***zz.zzzz*

For a prefix of 1009 (03F1), the MAC address is:

A2**F1.03***zz.zzzz*

Container instance resource management

To specify resource usage per container instance, create one or more resource profiles in FXOS. When you deploy the logical device or application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance. To view the available resources per model, refer to Requirements and prerequisites for container instances, on page 250. To add a resource profile, refer to Add a resource profile for container instances , on page 264.

Performance scaling factor for multi-instance capability

The maximum throughput (connections, VPN sessions, and TLS proxy sessions) for a platform is calculated for a native instance's use of memory and CPU (and this value is shown in **show resource usage**). If you use multiple instances, then you need to calculate the throughput based on the percentage of CPU cores that you assign to the instance. For example, if you use a container instance with 50% of the cores, then you should initially calculate 50% of the throughput. Moreover, the throughput available to a container instance may be less than that available to a native instance.

For detailed instructions on calculating the throughput for instances, refer to Firepower NGFW Multi-Instance Performance on 4100 and 9300 Series Appliances.

Container instances and high availability

You can configure high availability using a container instance on 2 separate chassis. For example, if you have 2 chassis, each with 10 instances, you can create 10 high availability pairs. Note that high availability is not configured in FXOS; configure each high availability pair in the application manager.

For detailed requirements, refer to Requirements and prerequisites for high availability configuration, on page 251 and Add a high availability pair, on page 271.

Container instances and clustering

You can create a cluster of container instances using one container instance per security module/engine. For details, see Requirements and prerequisites for clustering, on page 251.

Licenses for container instances

All licenses are consumed per security engine/chassis (for the Firepower 4100) or per security module (for the Firepower 9300), and not per container instance. See the details:

- Essentials licenses are automatically assigned: one per security module/engine.
- Feature licenses are manually assigned to each instance; but you only consume one license per feature per security module/engine. For example, for the Firepower 9300 with 3 security modules, you only need

one URL Filtering license per module for a total of 3 licenses, regardless of the number of instances in use.

For example:

Table 19: Sample license usage for container instances on a Firepower 9300

Firepower 9300	Instance	Licenses
Security Module 1	Instance 1	Essentials, URL Filtering, Malware Defense
	Instance 2	Essentials, URL Filtering
	Instance 3	Essentials, URL Filtering
Security Module 2	Instance 4	Essentials, IPS
	Instance 5	Essentials, URL Filtering, Malware Defense, IPS
Security Module 3	Instance 6	Essentials, Malware Defense, IPS
	Instance 7	Essentials, IPS

Table 20: Total number of licenses

Essentials	URL Filtering	Malware Defense	IPS
3	2	3	2

Requirements and prerequisites for logical devices

See the following sections for requirements and prerequisites.

Requirements and prerequisites for hardware and software combinations

Review these baseline requirements and prerequisites for FXOS hardware and software combinations.

The Firepower 4100/9300 supports multiple models, security modules, application types, and high availability and scalability features. See the following requirements for allowed combinations.

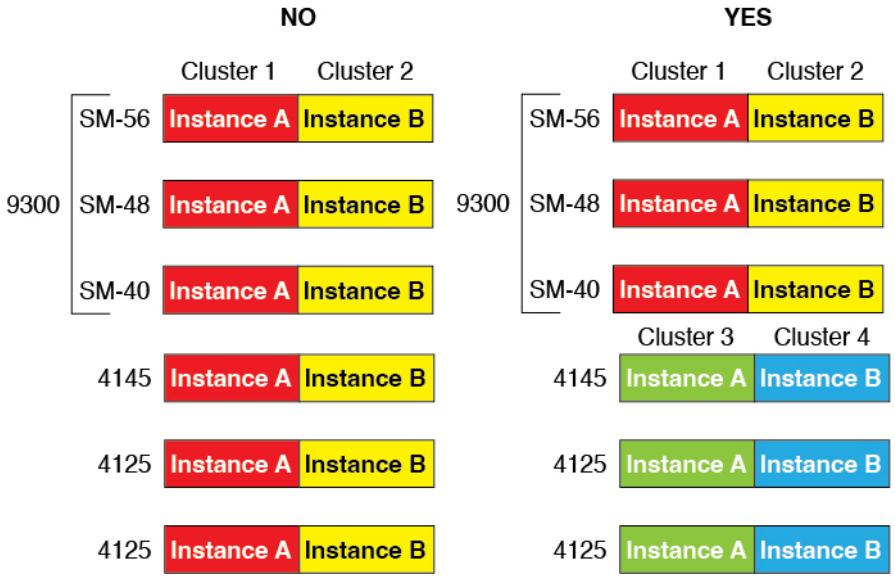
Firepower 9300 Requirements

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See these requirements:

- Security Module Types—You can install modules of different types in the Firepower 9300. For example, you can install the SM-48 as module 1, SM-40 as module 2, and SM-56 as module 3.
- Native instance Clustering—All security modules in the cluster, whether it is intra-chassis or inter-chassis, must be the same type. You can have different quantities of installed security modules in each chassis,

although all modules present in the chassis must belong to the cluster including any empty slots. For example, you can install 2 SM-40s in chassis 1, and 3 SM-40s in chassis 2. You cannot use clustering if you install 1 SM-48 and 2 SM-40s in the same chassis.

- Container instance Clustering—You can create a cluster using instances on different model types. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-48, and SM-40. You *cannot* mix the Firepower 9300 and the Firepower 4100 in the same cluster, however.

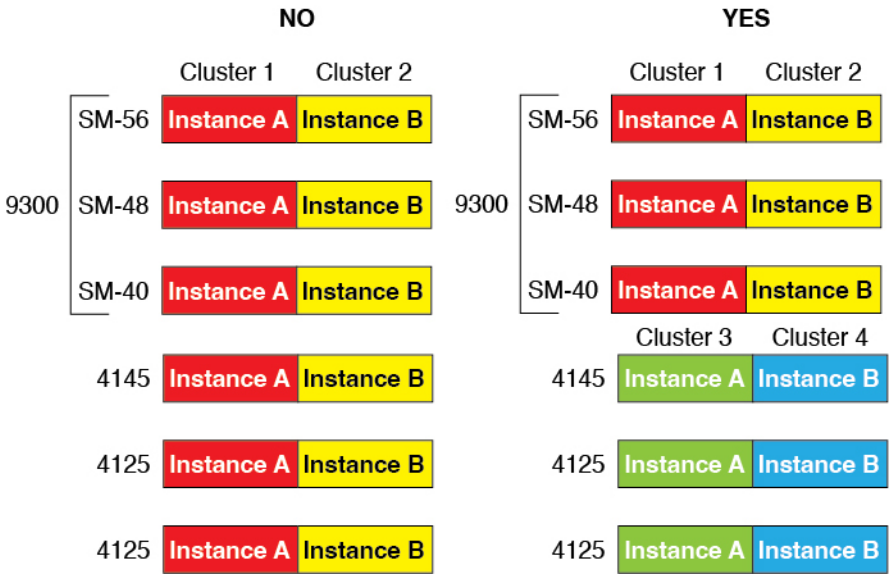


- High Availability—High Availability is only supported between same-type modules on the Firepower 9300. However, the two chassis can include mixed modules. For example, each chassis has an SM-40, SM-48, and SM-56. You can create High Availability pairs between the SM-40 modules, between the SM-48 modules, and between the SM-56 modules.
- ASA and Firewall Threat Defense application types—You can install different application types on separate modules in the chassis. For example, you can install ASA on module 1 and module 2, and Firewall Threat Defense on module 3.
- ASA or Firewall Threat Defense versions—You can run different versions of an application instance type on separate modules, or as separate container instances on the same module. For example, you can install the Firewall Threat Defense 6.3 on module 1, Firewall Threat Defense 6.4 on module 2, and Firewall Threat Defense 6.5 on module 3.

Firepower 4100 requirements

The Firepower 4100 comes in multiple models. See these requirements:

- Native and Container instances—When you install a container instance on a Firepower 4100, that device can only support other container instances. A native instance uses all of the resources for a device, so you can only install a single native instance on the device.
- Native instance Clustering—All chassis in the cluster must be the same model.
- Container instance Clustering—You can create a cluster using instances on different model types. For example, you can create a cluster using an instance on a Firepower 4145 and a 4125. You *cannot* mix the Firepower 9300 and the Firepower 4100 in the same cluster, however.



- High Availability—High Availability is only supported between same-type models.
- ASA and Firewall Threat Defense application types—The Firepower 4100 can only run a single application type.
- The Firewall Threat Defense container instance versions—You can run different versions of Firewall Threat Defense as separate container instances on the same module.

Requirements and prerequisites for container instances

For information about high-availability or clustering requirements with multi-instance, see Requirements and prerequisites for high availability configuration, on page 251 and see Requirements and prerequisites for clustering, on page 251.

Supported application types

The Firewall Threat Defense using Firewall Management Center

Maximum container instances and resources per model

For each container instance, you can specify the number of CPU cores to assign to the instance. RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

Table 21: Maximum container instances and resources per model

Model	Max. Container Instances	Available CPU Cores	Available RAM	Available Disk Space
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4125	10	62	162 GB	644 GB

Model	Max. Container Instances	Available CPU Cores	Available RAM	Available Disk Space
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 9300 SM-40 security module	13	78	334 GB	1359 GB
Firepower 9300 SM-48 security module	15	94	334 GB	1341 GB
Firepower 9300 SM-56 security module	18	110	334 GB	1314 GB

Firewall Management Center Requirements

For all instances on a Firepower 4100 chassis or Firepower 9300 module, you must use the same Firewall Management Center due to the licensing implementation.

Requirements and prerequisites for high availability configuration

The two units in a high availability configuration must meet these requirements:

- Be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not supported.
- Be the same model.
- Have the same interfaces assigned to the High Availability logical devices.
- Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.

High availability is only supported between same-type modules on the Firepower 9300; but the two chassis can include mixed modules. For example, each chassis has an SM-56, SM-48, and SM-40. You can create High Availability pairs between the SM-56 modules, between the SM-48 modules, and between the SM-40 modules.

For container instances, each unit must use the same resource profile attributes.

For container instances: Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.

For other high availability system requirements, see High availability system requirements, on page 284.

Requirements and prerequisites for clustering

This topic provides the necessary prerequisites and hardware support details for configuring clustering on supported security appliances.

Cluster model support

The Firewall Threat Defense supports clustering on the following models:

- Firepower 9300— You can include up to 16 nodes in the cluster. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules. Supports clustering with multiple chassis and clustering isolated to security modules within one chassis.
- Firepower 4100—Supported for up to 16 nodes using clustering with multiple chassis.

User roles

The following user roles are required to manage clustering configurations:

- Admin
- Access Admin
- Network Admin

Clustering hardware and software requirements

All chassis in a cluster:

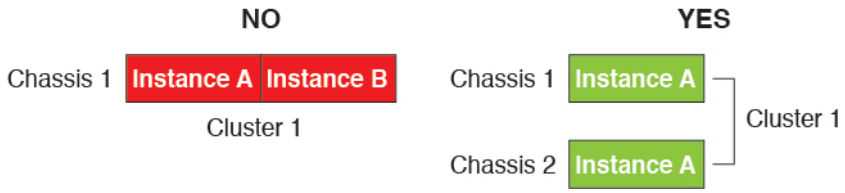
- Native instance clustering—For the Firepower 4100: All chassis must be the same model. For the Firepower 9300: All security modules must be the same type. For example, if you use clustering, all modules in the Firepower 9300 must be SM-40s. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.
- Container instance clustering—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-48, and SM-40. Or you can create a cluster on a Firepower 4145 and a 4125.



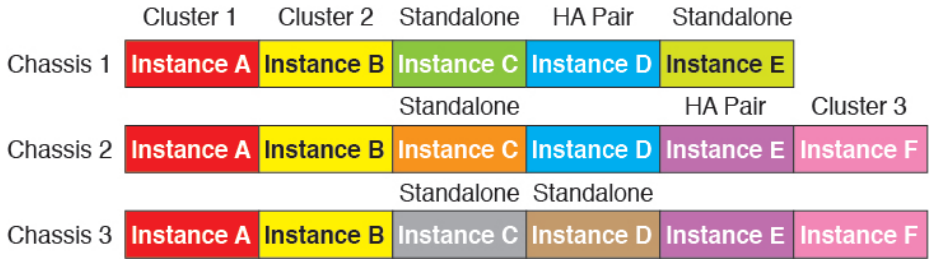
- Must run the identical FXOS and application software except at the time of an image upgrade. Mismatched software versions can lead to poor performance, so be sure to upgrade all nodes in the same maintenance window.
- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in clusters with multiple chassis. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the data nodes, and ending with the control node.
- Must use the same NTP server. For Firewall Threat Defense, the Firewall Management Center must also use the same NTP server. Do not set the time manually.

Multi-instance clustering requirements

- No intra-security-module/engine clustering—For a given cluster, you can only use a single container instance per security module/engine. You cannot add 2 container instances to the same cluster if they are running on the same module.



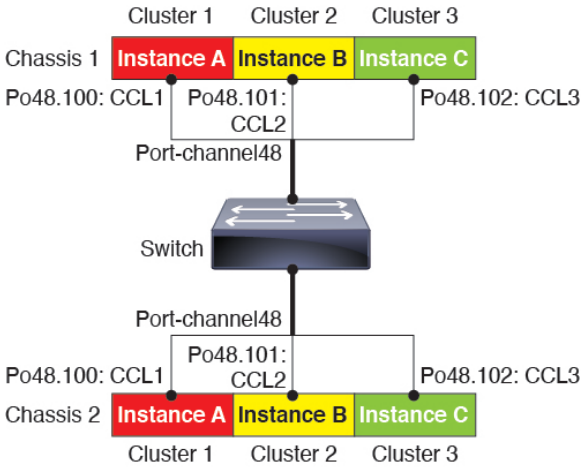
- Mix and match clusters and standalone instances—Not all container instances on a security module/engine need to belong to a cluster. You can use some instances as standalone or High Availability nodes. You can also create multiple clusters using separate instances on the same security module/engine.



- All 3 modules in a Firepower 9300 must belong to the cluster—For the Firepower 9300, a cluster requires a single container instance on all 3 modules. You cannot create a cluster using instances on module 1 and 2, and then use a native instance on module 3, or example.



- Match resource profiles—We recommend that each node in the cluster use the same resource profile attributes; however, mismatched resources are allowed when changing cluster nodes to a different resource profile, or when using different models.
- Dedicated cluster control link—For clusters with multiple chassis, each cluster needs a dedicated cluster control link. For example, each cluster can use a separate subinterface on the same cluster-type EtherChannel, or use separate EtherChannels.



- No shared interfaces—Shared-type interfaces are not supported with clustering. However, the same Management and Eventing interfaces can used by multiple clusters.
- No subinterfaces—A multi-instance cluster cannot use FXOS-defined VLAN subinterfaces. An exception is made for the cluster control link, which can use a subinterface of the Cluster EtherChannel.
- Mix chassis models—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-48, and SM-40. Or you can create a cluster on a Firepower 4145 and a 4125.



- Maximum 6 nodes—You can use up to six container instances in a cluster.

Switch requirements

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 4100/9300 chassis.
- For supported switch characteristics, see Cisco FXOS Compatibility.

Guidelines and limitations for logical devices

This section provides guidelines and limitations for configuring and managing logical devices.

Guidelines and limitations for interface configuration

VLAN subinterfaces

Consider these guidelines when configuring VLAN subinterfaces in your network deployment.

- This document discusses FXOS VLAN subinterfaces only. You can separately create subinterfaces within the Firewall Threat Defense application. For more information, refer to FXOS interfaces and application interfaces, on page 226.
- Subinterfaces can only be assigned to container instances.

Note If you assign a parent interface to a container instance, it only passes untagged (non-VLAN) traffic. Do not assign the parent interface unless you intend to pass untagged traffic. For Cluster type interfaces, the parent interface cannot be used.

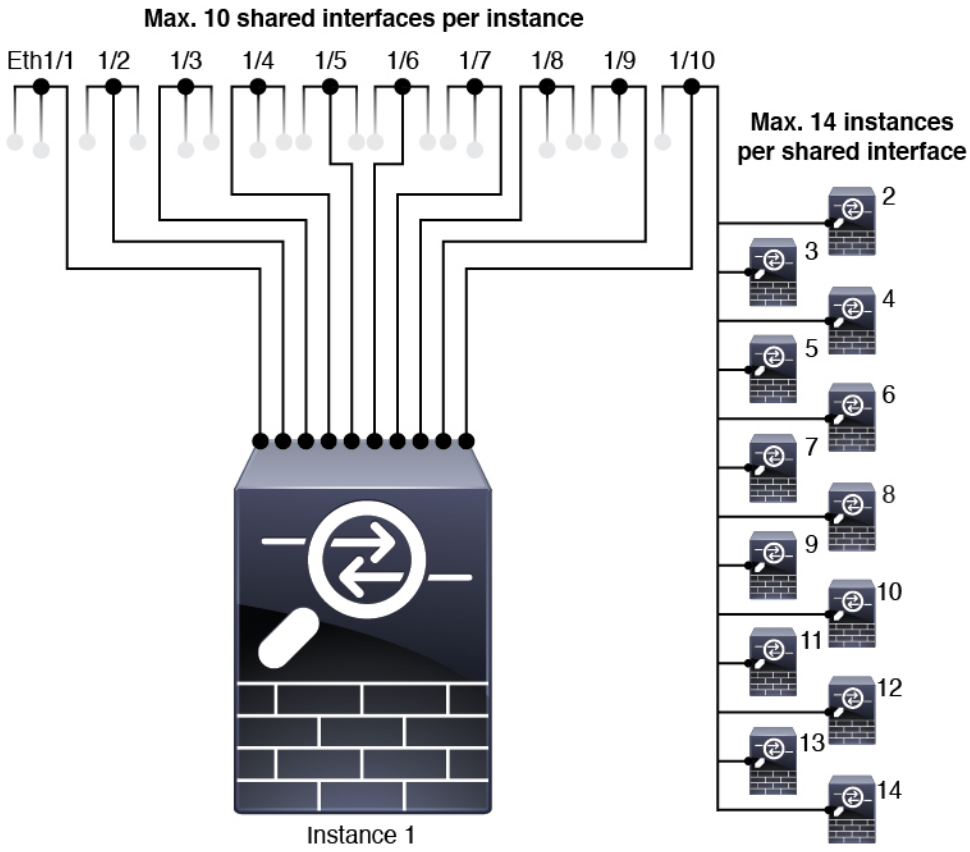
- Subinterfaces are supported on Data or Data-sharing type interfaces, as well as Cluster type interfaces. If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster.
- For multi-instance clustering, FXOS subinterfaces are not supported on Data interfaces. However, subinterfaces are supported for the cluster control link, so you can use either a dedicated EtherChannel or a subinterface of an EtherChannel for the cluster control link. Note that *application*-defined subinterfaces are supported for Data interfaces.
- You can create up to 500 VLAN IDs.
- See these limitations within the logical device application; keep these limitations in mind when planning your interface allocation.
  - You cannot use subinterfaces for an inline set or as a passive interface.
  - If you use a subinterface for the failover link, then all subinterfaces on that parent, and the parent itself, are restricted for use as failover links. You cannot use some subinterfaces as failover links, and some as regular data interfaces.

Data-sharing interfaces

Consider these limitations when configuring data-sharing interfaces.

- You cannot use a data-sharing interface with a native instance.
- Maximum 14 instances per shared interface. For example, you can allocate Ethernet1/1 to Instance1 through Instance14.

  Maximum 10 shared interfaces per instance. For example, you can allocate Ethernet1/1.1 through Ethernet1/1.10 to Instance1.



- You cannot use a data-sharing interface in a cluster.
- See these limitations within the logical device application; keep these limitations in mind when planning your interface allocation.
  - You cannot use a data-sharing interface with a transparent firewall mode device.
  - You cannot use a data-sharing interface with Firewall Threat Defense inline sets or passive interfaces.
  - You cannot use a data-sharing interface for the failover link.

Inline Sets for Firewall Threat Defense

Consider these guidelines when using inline sets for Firewall Threat Defense.

- Supported for physical interfaces (both regular and breakout ports) and EtherChannels. Subinterfaces are not supported.
- Link state propagation is supported.
- Do not enable Hardware Bypass and link state propagation for the same inline set.

Hardware bypass

Consider these limitations when configuring hardware bypass functionality.

- Supported for the Firewall Threat Defense; you can use them as regular interfaces for the ASA.

- The Firewall Threat Defense only supports Hardware Bypass with inline sets.
- Hardware Bypass-capable interfaces cannot be configured for breakout ports.
- You cannot include Hardware Bypass interfaces in an EtherChannel and use them for Hardware Bypass; you can use them as regular interfaces in an EtherChannel.
- Hardware Bypass is not supported with High Availability.
- Do not enable Hardware Bypass and link state propagation for the same inline set.

Default MAC addresses

For native instances:

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- EtherChannels—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.

For container instances:

- MAC addresses for all interfaces are taken from a MAC address pool. For subinterfaces, if you decide to manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification. See Automatic MAC Addresses for Container Instance Interfaces, on page 246.

General guidelines for firewall mode, HA, and multi-instance configurations

Firewall mode configuration

You can set the firewall mode to routed or transparent in the bootstrap configuration for the Firewall Threat Defense.

High availability configuration

Configure high availability within the application configuration and use appropriate interfaces for failover and state links.

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links. Data-sharing interfaces are not supported.

Multi-Instance configuration

Enable multiple context mode and multi-instance capabilities according to platform-specific requirements and limitations.

- Multi-instance capability with container instances is only available for the Firewall Threat Defense using Firewall Management Center.

- For Firewall Threat Defense container instances, a single Firewall Management Center must manage all instances on a security module/engine.
- For Firewall Threat Defense container instances, the following features are not supported:
  - Radware DefensePro link decorator
  - Firewall Management Center UCAPL/CC mode
  - Flow offload to hardware

Configure interfaces

By default, physical interfaces are disabled. You can enable interfaces, add EtherChannels, add VLAN subinterfaces, and edit interface properties.

Enable or disable an interface

You can change the **Admin State** of each interface to be enabled or disabled. By default, physical interfaces are disabled. For VLAN subinterfaces, the admin state is inherited from the parent interface.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The Interfaces page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 To enable the interface, click the disabled **Slider disabled** () so that it changes to the enabled **Slider enabled** ().

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from gray to green.

Step 3 To disable the interface, click the enabled **Slider enabled** () so that it changes to the disabled **Slider disabled** ().

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from green to gray.

Configure a physical interface

Configure physical interface settings including enable/disable state, speed, duplex, type, and auto-negotiation to ensure proper network connectivity.

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, it must be physically enabled in FXOS and logically enabled in the application.

Note

- For QSFPH40G-CUxM, auto-negotiation is enabled by default and you cannot disable it.
- If you replace an SFP on a port with a different SFP module, the speed, duplex, and auto-negotiation of the interface is not updated automatically. You must manually reconfigure the interface.

Before you begin

An interface that is already a member of an EtherChannel cannot be modified individually. Be sure to configure settings before you add it to the EtherChannel.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Edit** in the row for the interface you want to edit to open the **Edit Interface** dialog box.

Step 3 Configure the interface settings:

a) To enable the interface, check the **Enable** check box. To disable the interface, uncheck the **Enable** check box.

b) Choose the interface **Type**:

See Interface types, on page 224 for details about interface type usage.

- **Data**
- **Data-sharing**—For container instances only.
- **Mgmt**
- **Firepower-eventing**—For Firewall Threat Defense only.
- **Cluster**—Do not choose the **Cluster** type; by default, the cluster control link is automatically created on Port-channel 48.

c) Choose the speed of the interface from the **Speed** drop-down list.

d) If your interface supports **Auto Negotiation**, click the **Yes** or **No** radio button.

If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the platform interface as well. For example, N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, for the port to be connected you must disable the default auto-negotiation on the platform and the switch.

e) Choose the duplex of the interface from the **Duplex** drop-down list.

f) Choose a previously-configured **Network Control Policy**. For more information on how to configure a Network Control Policy, see Configure a Network Control Policy.

g) Explicitly configure **Debounce Time (ms)**. Enter a value between 0-15000 milli-seconds.

Note Configuring Debounce Time is not supported on 1G interfaces.

Step 4 Click **OK**.

Add an EtherChannel (port channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical Data or Data-sharing interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- On—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

Note It may take up to three minutes for an EtherChannel to come up to an operational state if you change its mode from On to Active or from Active to On.

Non-data interfaces only support active mode.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. "On" mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

When the Firepower 4100/9300 creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management interface for a standalone logical device
- The EtherChannel is added as a management interface or cluster control link for a logical device that is part of a cluster
- The EtherChannel is added as a data interface for a logical device that is part of a cluster and at least one unit has joined the cluster

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** or **Down** state.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Add Port Channel** above the interfaces table to open the **Add Port Channel** dialog box.

Step 3 Enter an ID for the port channel in the **Port Channel ID** field. Valid values are between 1 and 47.

Port-channel 48 is reserved for the cluster control link when you deploy a clustered logical device. If you do not want to use Port-channel 48 for the cluster control link, you can delete it and configure a Cluster type EtherChannel with a different ID.You can add multiple Cluster type EtherChannels and add VLAN subinterfaces for use with multi-instance clustering. For intra-chassis clustering, do not assign any interfaces to the Cluster EtherChannel.

Step 4 To enable the port channel, check the **Enable** check box. To disable the port channel, uncheck the **Enable** check box.

Step 5 Choose the interface **Type**:

See Interface types, on page 224 for details about interface type usage.

- **Data**
- **Data-sharing**—For container instances only.
- **Mgmt**
- **Firepower-eventing**—For Firewall Threat Defense only.
- **Cluster**

Step 6 Set the required **Admin Speed** for the member interfaces from the drop-down list.

If you add a member interface that is not at the specified speed, it will not successfully join the port channel.

Step 7 For Data or Data-sharing interfaces, choose the LACP port-channel **Mode**, **Active** or **On**.

For non-Data or non-Data-sharing interfaces, the mode is always active.

Step 8 Set the required **Admin Duplex** for the member interfaces, **Full Duplex** or **Half Duplex**.

If you add a member interface that is configured with the specified duplex, it will not successfully join the port channel.

Step 9 To add an interface to the port channel, select the interface in the **Available Interface** list and click **Add Interface** to move the interface to the Member ID list.

You can add up to 16 member interfaces of the same media type and capacity. The member interfaces must be set to the same speed and duplex, and must match the speed and duplex that you configured for this port channel. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.

Tip You can add multiple interfaces at one time. To select multiple individual interfaces, click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

Step 10 To remove an interface from the port channel, click the **Delete** button to the right of the interface in the Member ID list.

Step 11 Click **OK**.

Add a VLAN subinterface for container instances

You can add between 250 and 500 VLAN subinterfaces to the chassis, depending on your network deployment.You can add up to 500 subinterfaces to your chassis.

For multi-instance clustering, you can only add subinterfaces to the Cluster-type interface; subinterfaces on data interfaces are not supported.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on separate interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

This document discusses FXOS VLAN subinterfaces only. You can separately create subinterfaces within the Firewall Threat Defense application. For more information on when to use FXOS subinterfaces and application subinterfaces, refer to FXOS interfaces and application interfaces, on page 226.

Procedure

Step 1 Choose **Interfaces** to open the **All Interfaces** tab.

The **All Interfaces** tab provides both a visual representation and a tabular list of all currently installed interfaces.

Step 2 Click **Add New** > **Subinterface** to open the **Add Subinterface** dialog box.

Step 3 Do these steps to configure the subinterface:

a) Choose the interface **Type**:

See Interface types, on page 224 for details about interface type usage.

- **Data**
- **Data-sharing**
- **Cluster**—If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster.

For Data and Data-sharing interfaces: The type is independent of the parent interface type; you can have a Data-sharing parent and a Data subinterface, for example.

b) Choose the parent **Interface** from the drop-down list.

You cannot add a subinterface to a physical interface that is currently allocated to a logical device. If other subinterfaces of the parent are allocated, you can add a new subinterface as long as the parent interface itself is not allocated.

c) Enter a **Subinterface ID**, between 1 and 4294967295.

This ID will be appended to the parent interface ID as *interface_id.subinterface_id*. For example, if you add a subinterface to Ethernet1/1 with the ID of 100, then the subinterface ID will be: Ethernet1/1.100. This ID is not the same as the VLAN ID, although you can set them to match for convenience.

d) Set the **VLAN ID** between 1 and 4095.

Step 4 Click **OK**.

Expand the parent interface to view all subinterfaces under it.

Configure logical devices

Add a standalone logical device or a high-availability pair on the Firepower 4100/9300.

Add a resource profile for container instances

To specify resource usage per container instance, create one or more resource profiles. When you deploy the logical device/application instance, you specify the resource profile that you want to use. The resource profile sets the number of CPU cores; RAM is dynamically allocated according to the number of cores, and disk space is set to 40 GB per instance.

- The minimum number of cores is 6.

Note Instances with a smaller number of cores might experience relatively higher CPU utilization than those with larger numbers of cores. Instances with a smaller number of cores are more sensitive to traffic load changes. If you experience traffic drops, try assigning more cores.

- You can assign cores as an even number (6, 8, 10, 12, 14 etc.) up to the maximum.
- The maximum number of cores available depends on the security module/chassis model; see Requirements and prerequisites for container instances, on page 250.

The chassis includes a default resource profile called "Default-Small," which includes the minimum number of cores. You can change the definition of this profile, and even delete it if it is not in use. Note that this profile is created when the chassis reloads and no other profile exists on the system.

Changing the resource profile after you assign it is disruptive. See the following guidelines:

- You cannot change the resource profile settings if it is currently in use. You must disable any instances that use it, then change the resource profile, and finally reenable the instance.

- If you change the resource profile settings after you add the Firewall Threat Defense instance to the Firewall Management Center, then update the inventory for each unit on the Firewall Management Center.

  Choose **Devices** > **Device Management**, click **Edit** ( ) for the instance, then click **Refresh** ( ) on the **Device** > **Inventory Details** area.

- If you assign a different profile to an instance, it reboots.
- If you assign a different profile to instances in an established high-availability pair, which requires the profile to be the same on both units, you must:
  1. Break high availability.
  2. Assign the new profile to both units.
  3. Re-establish high availability.
- If you assign a different profile to instances in an established cluster, which allows mismatched profiles, then apply the new profile on the data nodes first; after they all come back up, you can apply the new profile to the control node.

Procedure

Step 1 Choose **Platform Settings** > **Resource Profiles**, and click **Add**.

The **Add Resource Profile** dialog box appears.

Step 2 Set the following parameters.

- **Name**: Sets the name of the profile between 1 and 64 characters. Note that you cannot change the name of this profile after you add it.
- **Description**: Sets the description of the profile up to 510 characters.
- **Number of Cores**: Sets the number of cores for the profile, between 6 and the maximum, depending on your chassis, as an even number.

Step 3 Click **OK**.

Add a Standalone Firewall Threat Defense

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can use native instances on some modules, and container instances on the other module(s).

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300.

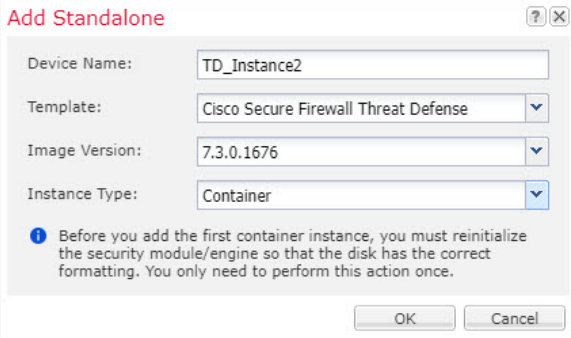
Note For the Firepower 9300, you can install different application types (ASA and Firewall Threat Defense) on separate modules in the chassis. You can also run different versions of an application instance type on separate modules.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).
- You can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management. See the **configure network management-data-interface** command in the FTD command reference for more information.
- You must also configure at least one Data type interface. Optionally, you can also create a firepower-eventing interface to carry all event traffic (such as web events). See Interface types, on page 224 for more information.
- For container instances, if you do not want to use the default profile, add a resource profile according to Add a resource profile for container instances , on page 264.
- For container instances, before you can install a container instance for the first time, you must reinitialize the security module/engine so that the disk has the correct formatting. Choose **Security Modules** or **Security Engine**, and click the **Reinitialize icon**. An existing logical device will be deleted and then reinstalled as a new device, losing any local application configuration. If you are replacing a native instance with container instances, you will need to delete the native instance in any case. You cannot automatically migrate a native instance to a container instance.
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - Firewall Management Center IP address and/or NAT ID of your choosing
  - DNS server IP address
  - Firewall Threat Defense hostname and domain name

Procedure

Step 1 Choose **Logical Devices**.

Step 2 Click **Add** > **Standalone**, and set the following parameters:



a) Provide a **Device Name**.

This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

Note You cannot change this name after you add the logical device.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

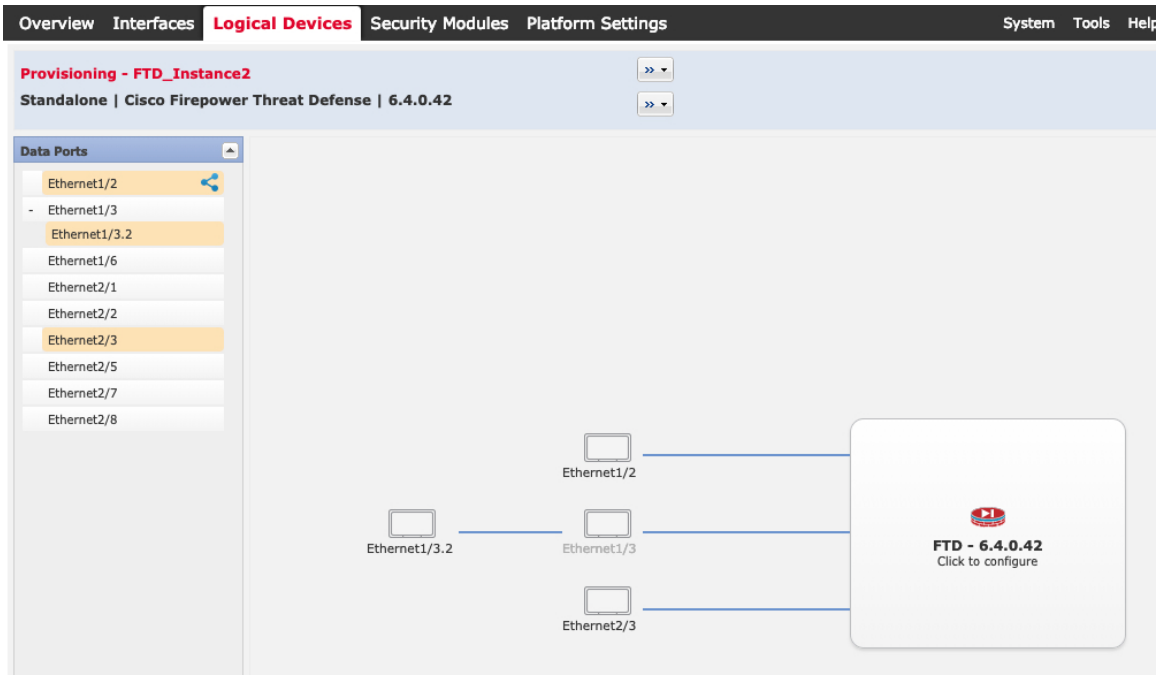
d) Choose the **Instance Type**: **Container** or **Native**.

A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.

e) Click **OK**.

You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each interface that you want to assign to the device.



You can only assign data and data-sharing interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in Firewall Management Center, including setting the IP addresses.

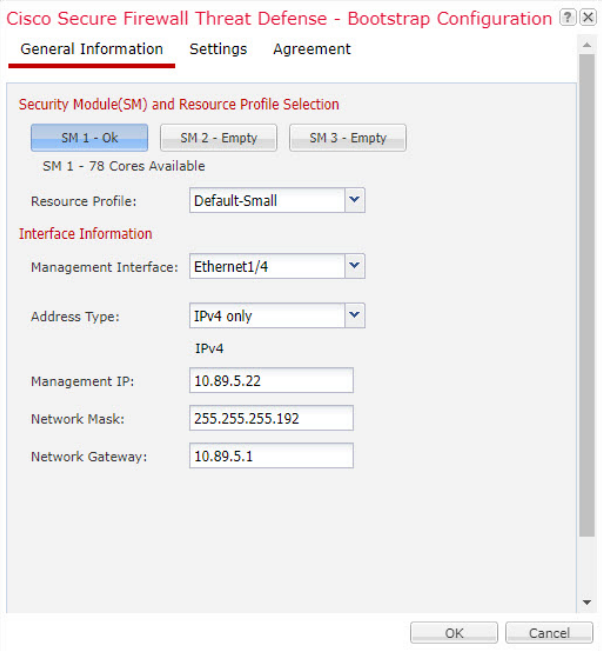
You can only assign up to 10 data-sharing interfaces to a container instance. Also, each data-sharing interface can be assigned to at most 14 container instances. A data-sharing interface is indicated by the sharing icon ( ).

Hardware Bypass-capable ports are shown with the following icon: . For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only (see the Firewall Management Center configuration guide). Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:



a) (For the Firepower 9300) Under **Security Module Selection** click the security module that you want to use for this logical device.

b) For a container instance, specify the **Resource Profile**.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes.

Note If you later assign a different profile to instances in an established high-availability pair, which requires the profile to be the same on both units, you must:

1. Break high availability.
2. Assign the new profile to both units.
3. Re-establish high availability.

c) Choose the **Management Interface**.

This interface is used to manage the logical device. This interface is separate from the chassis management port.

d) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.

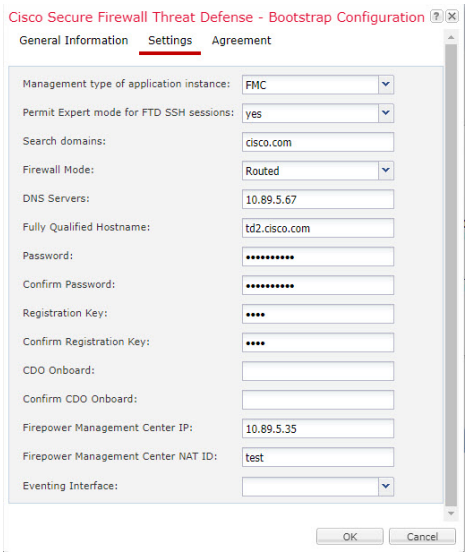
e) Configure the **Management IP** address.

Set a unique IP address for this interface.

f) Enter a **Network Mask** or **Prefix Length**.

g) Enter a **Network Gateway** address.

Step 6 On the **Settings** tab, complete the following:



a) For a native instance, in the **Management type of application instance** drop-down list, choose **FMC**.

   Native instances also support Firewall Device Manager as a manager. After you deploy the logical device, you cannot change the manager type.

b) Enter the **Firepower Management Center IP** of the managing Firewall Management Center. If you do not know the Firewall Management Center IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

c) For a container instance, **Permit Expert mode from FTD SSH sessions**: **Yes** or **No**. Expert Mode provides Firewall Threat Defense shell access for advanced troubleshooting.

   If you choose **Yes** for this option, then users who access the container instance directly from an SSH sesssion can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.

   Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the Firewall Threat Defense CLI.

d) Enter the **Search Domains** as a comma-separated list.

e) Choose the **Firewall Mode**: **Transparent** or **Routed**.

   In routed mode, the Firewall Threat Defense is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

   The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

f) Enter the **DNS Servers** as a comma-separated list.

   The Firewall Threat Defense uses DNS if you specify a hostname for the Firewall Management Center, for example.

g) Enter the **Fully Qualified Hostname** for the Firewall Threat Defense.

h) Enter a **Registration Key** to be shared between the Firewall Management Center and the device during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the Firewall Management Center when you add the Firewall Threat Defense.

i) Enter a **Password** for the Firewall Threat Defense admin user for CLI access.

j) Choose the **Eventing Interface** on which events should be sent. If not specified, the management interface will be used.

This interface must be defined as a Firepower-eventing interface.

k) For a container instance, set the **Hardware Crypto** as **Enabled** or **Disabled**.

This setting enables TLS crypto acceleration in hardware, and improves performance for certain types of traffic. This feature is enabled by default. You can enable TLS crypto acceleration for up to 16 instances per security module. This feature is always enabled for native instances. To view the percentage of hardware crypto resources allocated to this instance, enter the **show hw-crypto** command.

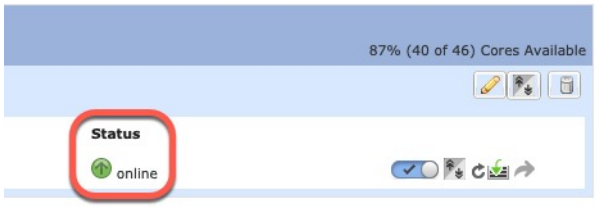
Step 7 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.





Step 10 See the Firewall Management Center configuration guide to add the Firewall Threat Defense as a managed device and start configuring your security policy.

Add a high availability pair

Firewall Threat Defense High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

Before you begin

Refer to Requirements and prerequisites for high availability configuration, on page 251.

Procedure

Step 1 Allocate the same interfaces to each logical device.

Step 2 Allocate 1 or 2 data interfaces for the failover and state link(s).

These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.

For container instances, data-sharing interfaces are not supported for the failover link. We recommend that you create subinterfaces on a parent interface or EtherChannel, and assign a subinterface for each instance to use as a failover link. Note that you must use all subinterfaces on the same parent as failover links. You cannot use one subinterface as a failover link and then use other subinterfaces (or the parent interface) as regular data interfaces.

Step 3 Enable High Availability on the logical devices. Refer to High Availability for Devices, on page 283.

Step 4 If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.

Change an Interface on a Firewall Threat Defense Logical Device

You can allocate or unallocate an interface, or replace a management interface on the Firewall Threat Defense logical device. You can then sync the interface configuration in the Firewall Management Center.

Adding a new interface, or deleting an unused interface has minimal impact on the Firewall Threat Defense configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the Firewall Threat Defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the Firewall Management Center.

Deleting an interface will delete any configuration associated with that interface.

Before you begin

- Configure your interfaces, and add any EtherChannels according to Configure a physical interface, on page 259 and Add an EtherChannel (port channel), on page 261.
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management or eventing interface with a management EtherChannel, then you need to create the EtherChannel with at least 1 unallocated data member interface, and then replace the current management interface with the EtherChannel. After the Firewall Threat Defense device reboots (management interface changes cause a reboot), and you sync the configuration in the Firewall

Management Center, you can add the (now unallocated) management interface to the EtherChannel as well.

- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the Firewall Management Center. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.
- In mult-instance mode, for changing a sub-interface with an another sub-interface with the same vlan tag, you must first remove all the configuration (including nameif config) of the interface and then unalloacte the interface from Firewall Chassis Manager. Once unallocated, add the new interface and then use sync interfaces from the Firewall Management Center.

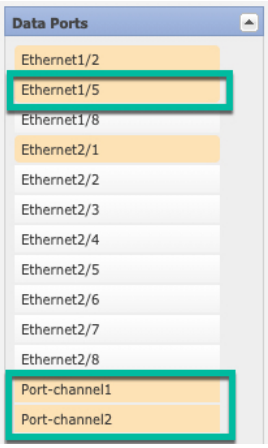
Procedure

Step 1 In the Firewall Chassis Manager, choose **Logical Devices**.

Step 2 Click the **Edit** icon at the top right to edit the logical device.

Step 3 Allocate a new data interface by selecting the interface in the **Data Ports** area.

Do not delete any interfaces yet.



Step 4 Replace the management or eventing interface:

For these types of interfaces, the device reboots after you save your changes.

a) Click the device icon in the center of the page.
b) On the **General** or **Cluster Information** tab, choose the new **Management Interface** from the drop-down list.
c) On the **Settings** tab, choose the new **Eventing Interface** from the drop-down list.
d) Click **OK**.

If you change the IP address of the Management interface, then you must also change the IP address for the device in the Firewall Management Center: go to **Devices** > **Device Management** > **Device/Cluster**. In the **Management** area, set the IP address to match the bootstrap configuration address.

Step 5 Click **Save**.

Step 6 Sync the interfaces in the Firewall Management Center.

a) Log into the Firewall Management Center.
b) Select **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.
c) Click the **Sync Device** button on the top left of the **Interfaces** page.
d) After the changes are detected, you will see a red banner on the **Interfaces** page indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.
e) If you plan to delete an interface, manually transfer any interface configuration from the old interface to the new interface.

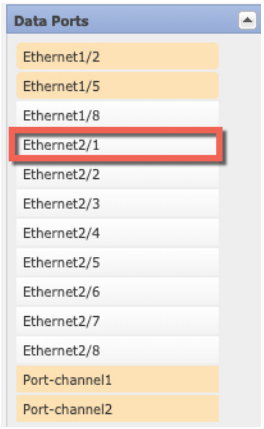
   Because you have not yet deleted any interfaces, you can refer to the existing configuration. You will have additional opportunity to fix the configuration after you delete the old interface and re-run the validation. The validation will show you all locations in which the old interface is still used.

f) Click **Validate Changes** to make sure your policy will still work with the interface changes.

   If there are any errors, you need to change your policy and rerun the validation.

g) Click **Save**.
h) Click **Deploy** > **Deployment**.
i) Select the devices and click **Deploy** to deploy the policy to the assigned devices. The changes are not active until you deploy them.

Step 7 In the Firewall Chassis Manager, unallocate a data interface by de-selecting the interface in the **Data Ports** area.



Step 8 Click **Save**.

Step 9 Sync the interfaces again in the Firewall Management Center.

Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

Procedure

Step 1 Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2 Connect to the application console.

connect ftd *name*

To view the instance names, enter the command without a name.

Example:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

Step 3 Exit the application console to the FXOS module CLI.

- Firewall Threat Defense—Enter **exit**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

History for logical devices

This table provides a chronological history of feature updates and improvements for logical devices, enabling you to track feature availability and requirements across different Firewall Management Center versions.

Table 22: Logical devices feature history

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Synchronization between the Firewall Threat Defense operational link state and the physical link state	6.7	Any	The chassis can now synchronize the Firewall Threat Defense operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The Firewall Threat Defense application interface admin state is not considered. Without synchronization from Firewall Threat Defense, data interfaces can be in an Up state physically before the Firewall Threat Defense application has completely come online, for example, or can stay Up for a period of time after you initiate Firewall Threat Defense shutdown. For inline sets, this state mismatch can result in dropped packets because external routers may start sending traffic to the Firewall Threat Defense before the Firewall Threat Defense can handle it. This feature is disabled by default and can be enabled per logical device in FXOS. **Note** This feature is not supported for clustering, container instances, or Firewall Threat Defense with a Radware vDP decorator. It is also not supported for the ASA. New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail**
Firewall Threat Defense configuration backup and restore using Firewall Management Center for container instances	6.7	Any	You can now use the Firewall Management Center backup/restore tool on Firewall Threat Defense container instances. New/Modified Firewall Management Center screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup** New/Modified Firewall Threat Defense CLI commands: **restore** Supported platforms: Firepower 4100/9300 **Note** Requires FXOS 2.9.

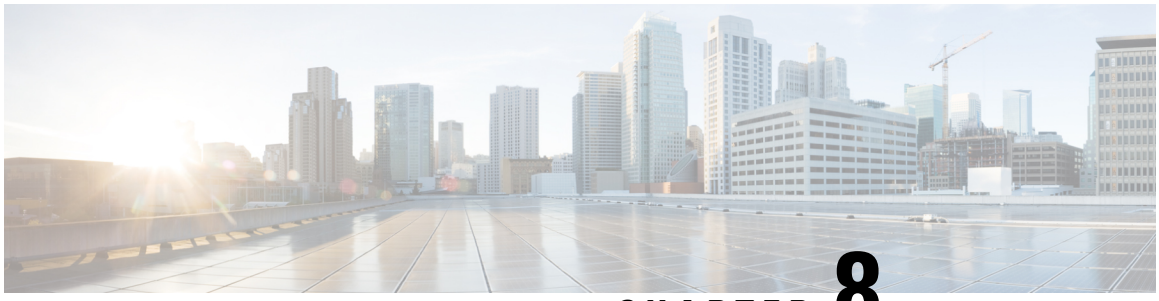
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for VLAN subinterfaces on a Cluster type interface (multi-instance use only)	6.6	Any	For use with multi-instance clusters, you can now create VLAN subinterfaces on cluster-type interfaces. Because each cluster requires a unique cluster control link, VLAN subinterfaces provide a simple method to fulfill this requirement. You can alternatively assign a dedicated EtherChannel per cluster. Multiple cluster interfaces are now allowed. New/Modified Firepower Chassis Manager screens: **Interfaces** > **All Interfaces** > **Add New** drop-down menu **Subinterface** > **Type** field New/Modified FXOS commands: **set port-type cluster** **Note** Requires FXOS 2.8.1.
Firewall Threat Defense on the Firepower 4112	6.6	Any	We introduced the Firepower 4112. **Note** Requires FXOS 2.8.1.
TLS crypto acceleration for multiple container instances	6.5	Any	TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only one container instance per module/security engine. New instances have this feature enabled by default. However, the upgrade does not enable acceleration on existing instances. Instead, run the **enter hw-crypto** and then the **set admin-state enabled** FXOS commands. New/Modified Firepower Chassis Manager screens: Click **Logical Devices** > **Add Device** > **Settings** and then click the **Hardware Crypto** drop-down list. **Note** Requires FXOS 2.7.1.
Firewall Threat Defense on the Firepower 4115, 4125, and 4145	6.4	Any	We introduced the Firepower 4115, 4125, and 4145. **Note** Requires FXOS 2.6.1.157.
Firepower 9300 SM-40, SM-48, and SM-56 support	6.4	Any	We introduced the following three security modules: SM-40, SM-48, and SM-56. **Note** Requires FXOS 2.6.1.157.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for ASA and Firewall Threat Defense on separate modules of the same Firepower 9300	6.4	Any	You can now deploy ASA and Firewall Threat Defense logical devices on the same Firepower 9300. **Note** Requires FXOS 2.6.1.157.
Support for SSL hardware acceleration on one Firewall Threat Defense container instance on a module/security engine	6.4	Any	You can now enable SSL hardware acceleration for one container instance on a module/security engine. SSL hardware acceleration is disabled for other container instances, but enabled for native instances. New/Modified FXOS commands: **config hwCrypto enable** No modified screens. **Note** Requires FXOS 2.6.1.157.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multi-instance capability for Firewall Threat Defense on the Firepower 4100/9300	6.3	Any	You can now deploy multiple logical devices, each with a Firewall Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance. You can configure High Availability using a container instance on 2 separate chassis. Clustering is not supported. **Note** Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available on the Firewall Threat Defense. New/Modified Firewall Management Center screens: • **Devices** > **Device Management** > **Edit** icon **Interfaces** tab New/Modified Firepower Chassis Manager screens: • **Overview** > **Devices** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **Subinterface** • **Interfaces** > **All Interfaces** > **Type** • **Logical Devices** > **Add Device** • **Platform Settings** > **Mac Pool** • **Platform Settings** > **Resource Profiles** New/Modified FXOS commands: **connect ftd name**, **connect module telnet**, **create bootstrap-key PERMIT_EXPERT_MODE**, **create resource-profile**, **create subinterface**, **scope auto-macpool**, **set cpu-core-count**, **set deploy-type**, **set port-type data-sharing**, **set prefix**, **set resource-profile-name**, **set vlan**, **scope app-instance ftd name**, **show cgroups container**, **show interface**, **show mac-address**, **show subinterface**, **show tech-support module app-instance**, **show version** Supported platforms: Firepower 4100/9300

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cluster control link customizable IP Address for the Firepower 4100/9300	6.3	Any	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2. *chassis_id*. *slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/modified Firepower Chassis Manager screens: • **Logical Devices** > **Add Device** > **Cluster Information** > **CCL Subnet IP** field New/Modified FXOS commands: **set cluster-control-link network** Supported platforms: Firepower 4100/9300
Support for data EtherChannels in On mode	6.3	Any	You can now set data and data-sharing EtherChannels to either to Active LACP mode or On mode. Other types of EtherChannels only support Active mode. New/Modified Firepower Chassis Manager screens: • **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode** New/Modified FXOS commands: **set port-channel-mode** Supported platforms: Firepower 4100/9300
Support for EtherChannels in Firewall Threat Defense inline sets	6.2	Any	You can now use EtherChannels in a Firewall Threat Defense inline set. Supported platforms: Firepower 4100/9300
Inter-chassis clustering for 6 Firewall Threat Defense modules	6.2	Any	You can now enable inter-chassis clustering for the Firewall Threat Defense. You can include up to 6 modules in up to 6 chassis. New/modified Firepower Chassis Manager screens: • **Logical Devices** > **Configuration** Supported platforms: Firepower 4100/9300
Hardware bypass support on the Firepower 4100/9300 for supported network modules	6.1	Any	Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. New/Modified screens: • **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 4100/9300

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Inline set link state propagation support for the Firewall Threat Defense	6.1	Any	When you configure an inline set in the Firewall Threat Defense application and enable link state propagation, the Firewall Threat Defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. New/Modified FXOS commands: **show fault |grep link-down**, **show interface detail** Supported platforms: Firepower 4100/9300
Support for intra-chassis clustering on the Firewall Threat Defense on the Firepower 9300	6.0.1	Any	The Firepower 9300 supports intra-chassis clustering with the Firewall Threat Defense application. New/Modified Firepower Chassis Manager screens: • **Logical Devices** > **Configuration** New/Modified FXOS commands: **enter mgmt-bootstrap ftd**, **enter bootstrap-key FIREPOWER_MANAGER_IP**, **enter bootstrap-key FIREWALL_MODE**, **enter bootstrap-key-secret REGISTRATION_KEY**, **enter bootstrap-key-secret PASSWORD**, **enter bootstrap-key FQDN**, **enter bootstrap-key DNS_SERVERS**, **enter bootstrap-key SEARCH_DOMAINS**, **enter ipv4 firepower**, **enter ipv6 firepower**, **set value**, **set gateway**, **set ip**, **accept-license-agreement** Supported platforms: Firepower 4100/9300



CHAPTER 8

High Availability for Devices

The following topics describe how to configure Active/Standby failover to accomplish high availability of the Firewall Threat Defense.

- Secure Firewall Threat Defense high availability, on page 283
- Config-sync optimization, on page 302
- Requirements and prerequisites for high availability, on page 303
- Guidelines for High availability, on page 303
- Add a high availability pair, on page 306
- Configure optional high availability parameters, on page 309
- Manage High availability, on page 311
- Monitoring High availability, on page 319
- Troubleshoot configuration sync failure, on page 320
- History for high availability, on page 320

Secure Firewall Threat Defense high availability

Secure Firewall Threat Defense high availability is a failover configuration that

- requires two identical Firewall Threat Defense devices connected through a dedicated failover link and optionally a state link
- supports Active/Standby failover where one unit passes traffic while the standby unit does not actively pass traffic synchronizes configuration and state information, and
- monitors the health of the active unit (hardware, interfaces, software, and environmental status) to determine if failover conditions are met.

Failover process details

When a failover occurs, the active unit fails over to the standby unit, which then becomes active. The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

Note High availability is not supported on Firewall Threat Defense Virtual running in the public cloud. See the Secure Firewall Threat Defense Virtual getting started guides for more information about configuring the Firewall Threat Defense Virtual device for high availability.

High availability system requirements

High availability system requirements are specifications that define the hardware, software, and license prerequisites for Firewall Threat Defense devices to function in a High availability configuration.

Hardware requirements

Hardware requirements are specifications that ensure two units in a High availability configuration can

- maintain identical hardware configurations including model, interfaces, modules, and RAM
- support proper synchronization and failover functionality, and
- ensure reliable high availability operation.

Hardware requirement specifications

The two units in a High availability configuration must meet these requirements:

- Be the same model. In addition, for container instances, they must use the same resource profile attributes.

  For the Firepower 9300, High Availability is only supported between same-type modules. However, the two chassis can include mixed modules. For example, each chassis has an SM-56, SM-48, and SM-40. You can create High Availability pairs between the SM-56 modules, between the SM-48 modules, and between the SM-40 modules.

  If you change the resource profile after you add the High Availability pair to the Firewall Management Center, update the inventory for each unit on the **Devices** > **Device Management** > **Device** > **System** > **Inventory** dialog box.

  If you assign a different profile to instances in an established high-availability pair, which requires the profile to be the same on both units, you must:

  1. Break high availability.
  2. Assign the new profile to both units.
  3. Re-establish high availability.

- Have the same number and types of interfaces.

  For the Firepower 4100/9300 chassis, all interfaces must be preconfigured in FXOS identically before you enable High availability. If you change the interfaces after you enable High availability, make the interface changes in FXOS on the Standby unit, and then make the same changes on the Active unit.

If you are using units with different flash memory sizes in your High availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the

configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

Software requirements

Software requirements are configuration specifications that High availability units must meet to function properly in a failover configuration.

Required software specifications

The two units in a High availability configuration must meet these requirements:

- Be in the same firewall mode (routed or transparent).
- Have the same software version.
- Be in the same domain or group on the Firewall Management Center.
- Have the same NTP configuration. See Synchronize time on FTD devices, on page 908.
- Configuration changes must be fully deployed to the devices.
- Not have DHCP or PPPoE configured in any of their interfaces.
- (Firepower 4100/9300) Have the same flow offload mode, either both enabled or both disabled.

License requirements for Firewall Threat Defense devices in a high availability pair

Both Firewall Threat Defense units in a high availability configuration must have the same licenses.

High availability configurations require two license entitlements: one for each device in the pair.

Before high availability is established, it does not matter which licenses are assigned to the secondary/standby device. During high availability configuration, the Firewall Management Center releases any unnecessary licenses assigned to the standby unit and replaces them with identical licenses assigned to the primary/active unit.

For example, if the active unit has a Essentials license and a IPS license, and the standby unit has only a Essentials license, the Firewall Management Center communicates with the Smart Software Manager to obtain an available IPS license from your account for the standby unit. If your license account does not include enough purchased entitlements, your account becomes Out-of-Compliance until you purchase the correct number of licenses.

Failover and stateful failover links

A failover link and stateful failover link are dedicated connections that

- establish communication between the two units in a failover configuration
- require the same interface to be used between corresponding devices for consistency, and
- transmit critical failover and state information between the paired units.

Configuration recommendations

Cisco recommends to use the same interface between two devices in a failover link or a stateful failover link. For example, in a failover link, if you have used eth0 in device 1, use the same interface (eth0) in device 2 as well.

Failover link

A failover link is a communication mechanism that enables two units in a failover pair to constantly communicate to determine the operating status of each unit.

Failover link data

This below information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

Interface for the failover link

A failover link interface is a dedicated communication channel that

- exists solely for failover communication between high availability units
- uses an unused data interface (physical, or EtherChannel)
- cannot be shared with normal networking interfaces or user data traffic, and
- requires specific interface sizing based on the device model.

Interface restrictions and requirements

You can use an unused data interface (physical, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. You also cannot use a subinterface with the exception of a subinterface defined on the chassis for multi-instance mode. The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and also for the state link).

The Firewall Threat Defense does not support sharing interfaces between user data and the failover link. You also cannot use separate subinterfaces on the same parent for the failover link and for data (multi-instance chassis subinterfaces only). If you use a chassis subinterface for the failover link, then all subinterfaces on that parent, and the parent itself, are restricted for use as failover links.



Note When using an EtherChannel as the failover or state link, you must confirm that the same EtherChannel with the same member interfaces exists on both devices before establishing high availability.

See these guidelines for the failover link:

- Firepower 4100/9300—You cannot use the management-type interface for the failover link.
- See these guidelines for sizing the link.

Table 23: Failover link size

Model	Interface Size for Combined Failover and State Link
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Secure Firewall 3100	Secure Firewall 3105—1 Gbps Secure Firewall 3110—1 Gbps Secure Firewall 3120—1 Gbps Secure Firewall 3130—10 Gbps Secure Firewall 3140—10 Gbps
Secure Firewall 4200	10 Gbps
Firepower 9300	10 Gbps

The alternation frequency is equal to the unit hold time.

Note If you have a large configuration and a low unit hold time, alternating between the member interfaces can prevent the secondary unit from joining/re-joining. In this case, disable one of the member interfaces until after the secondary unit joins.

For an EtherChannel used as the failover link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a failover link.

Connect the failover link

The failover link enables communication and coordination between units in a failover configuration.

You need to establish a physical connection between the failover units to enable proper failover functionality.

Procedure

Connect the failover link using one of the following methods:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the Firewall Threat Defense device.
- Using an Ethernet cable to connect the units directly, without the need for an external switch.

If you do not use a switch between the units and the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The failover link is physically connected and ready for failover configuration.

Stateful failover links

A stateful failover link is a network connection that

- passes connection state information between failover units, and
- must be configured to enable stateful failover functionality.

State link configuration requirements

To use Stateful Failover, you must configure a Stateful Failover link (also known as the state link) to pass connection state information.

Shared failover links

A shared failover link is an interface conservation method that enables multiple network functions to use the same failover connection, though dedicated interfaces for state and failover links should be considered for large configurations and high traffic networks.

Dedicated interface for the stateful failover link

A dedicated interface for the stateful failover link is a data interface configuration that uses a dedicated physical or EtherChannel interface specifically for the state link in failover deployments.

Performance considerations

You can use a dedicated data interface—such as a physical or EtherChannel interface—for the state link. For requirements about a dedicated state link, refer to Interface for the failover link, on page 286. See the section on connecting the state link for additional information Connect the failover link, on page 287.

For optimum performance with long-distance failover, the state link latency should be less than 10 milliseconds but no more than 250 milliseconds. If latency exceeds 10 milliseconds, performance might degrade due to retransmission of failover messages.

Failover and data link interruption avoidance

Failover and data link interruption avoidance is a network design practice that

- ensures failover links and data interfaces travel through different paths to decrease the chance that all interfaces fail at the same time
- prevents failover operation suspension when the failover link is down, and
- maintains network resilience by using proper connection scenarios.

Connection scenarios

We recommend that failover links and data interfaces travel through different paths to decrease the chance that all interfaces fail at the same time. If the failover link is down, the failover operation is suspended until the health of the failover link is restored.

These connection scenarios help design a resilient failover network.

Scenario 1—Not recommended

If a single switch or a set of switches are used to connect both failover and data interfaces between two Firewall Threat Defense devices, then when a switch or inter-switch-link is down, both Firewall Threat Defense devices become active. Therefore, the two connection methods shown in these figures are **not** recommended.

Figure 115: Connecting with a single switch—not recommended

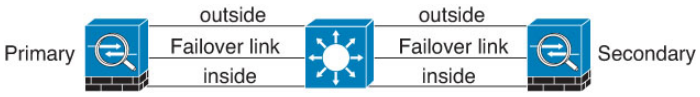
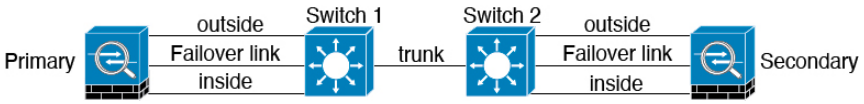


Figure 116: Connecting with a double-switch—not recommended



Scenario 2—Recommended

We recommend that failover links not use the same switch as the data interfaces. Instead, use a different switch or use a direct cable to connect the failover link, as shown in these figures.

Figure 117: Connecting with a different switch

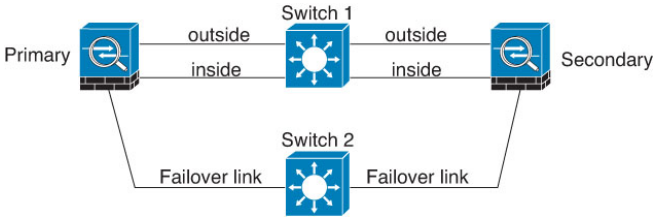
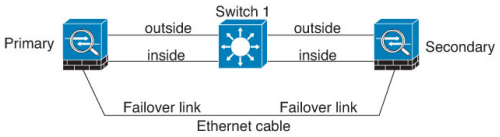


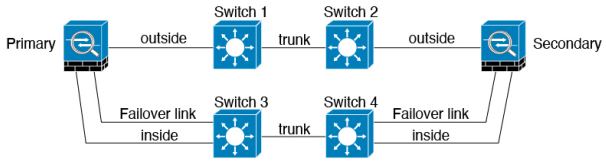
Figure 118: Connecting with a cable



Scenario 3—Recommended

If the Firewall Threat Defense data interfaces are connected to more than one set of switches, then a failover link can be connected to one of the switches, preferably the switch on the secure (inside) side of network, as shown in this figure.

Figure 119: Connecting with a secure switch



MAC addresses and IP addresses in High availability

MAC addresses and IP addresses in High availability are network addressing mechanisms that

- provide unique identification for network interfaces during failover scenarios
- maintain network connectivity when primary devices become unavailable, and
- ensure seamless traffic flow between active and standby configurations.

Address configuration types

When you configure your interfaces, you can specify an active IP address and a standby IP address on the same network. Generally, when a failover occurs, the new active unit takes over the active IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

Note Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state. You also cannot connect to the standby unit on that interface for management purposes.

The IP address and MAC address for the state link do not change at failover.

Active/standby configurations use specific address handling methods:

For Active/Standby High availability, see the following for IP address and MAC address usage during a failover event:

1. The active unit always uses the primary unit's IP addresses and MAC addresses.
2. When the active unit fails over, the standby unit assumes the IP addresses and MAC addresses of the failed unit and begins passing traffic.
3. When the failed unit comes back online, it is now in a standby state and takes over the standby IP addresses and MAC addresses.

However, if the secondary unit boots without detecting the primary unit, then the secondary unit becomes the active unit and uses its own MAC addresses, because it does not know the primary unit MAC addresses. When the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary unit, which can cause an interruption in your network traffic. Similarly, if you swap out the primary unit with new hardware, a new MAC address is used.

If you disable high availability and set the failover configurations to a disabled state, you will need to manually resume high availability, or reboot the device. It is recommended to use the command **configure**

high-availability resume and resume the high availability instead of rebooting the device. If you reload the standby unit with the failover configuration disabled, the standby unit boots up as the active unit and uses the primary unit's IP addresses and MAC addresses. This leads to duplicate IP addresses and causes network traffic disruptions. Use the command **configure high-availability resume** to enable failover and restore the traffic flow.



Note If you enable failover on a standalone device, the data interfaces go down at negotiation state of failover, interrupting traffic.

Virtual MAC addresses guard against this disruption, because the active MAC addresses are known to the secondary unit at startup, and remain the same in the case of new primary unit hardware. We recommend that you configure the virtual MAC address on both the primary and secondary units to ensure that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit. If you do not configure virtual MAC addresses, you might need to clear the ARP tables on connected routers to restore traffic flow. The Firewall Threat Defense does not send gratuitous ARPs for static NAT addresses when the MAC address changes, so connected routers do not learn of the MAC address change for these addresses.

For Active/Active failover, see the following for IP address and MAC address usage during a failover event:

1. The primary unit autogenerates active and standby MAC addresses for all interfaces in failover group 1 and 2 contexts. You can also manually configure the MAC addresses if necessary, for example, if there are MAC address conflicts.
2. Each unit uses the active IP addresses and MAC addresses for its active failover group, and the standby addresses for its standby failover group. For example, the primary unit is active for failover group 1, so it uses the active addresses for contexts in failover group 1. It is standby for the contexts in failover group 2, where it uses the standby addresses.
3. When a unit fails over, the other unit assumes the active IP addresses and MAC addresses of the failed failover group and begins passing traffic.
4. When the failed unit comes back online, and you enabled the preempt option, it resumes the failover group.

Virtual MAC addresses provide specialized functionality:

The Firewall Threat Defense has multiple methods to configure virtual MAC addresses. We recommend using only one method. If you set the MAC address using multiple methods, the MAC address used depends on many variables, and might not be predictable.

For multi-instance capability, the FXOS chassis autogenerates only primary MAC addresses for all interfaces. You can overwrite the generated MAC address with a virtual MAC address with both the primary and secondary MAC addresses, but predefining the secondary MAC address is not essential; setting the secondary MAC address does ensure that to-the-box management traffic is not interrupted in the case of new secondary unit hardware.

MAC address table updates occur during failover events:

During failover, the device that is designated as the new active device generates multicast packets for each MAC address entry in the MAC table and sends them to all the bridge group interfaces. This action prompts the upstream switches in the bridge group to update their routing tables with the new active device's interface to ensure accurate traffic forwarding.

The time taken to generate multicast packets and update the routing tables of the upstream switches depends on the number of entries in the MAC address table and the number of bridge group interfaces. Use the **show failover statistics state-switch-delay** command to display statistics related to the delays encountered during failover events.

Stateful failover

A stateful failover is a high availability mechanism that

- continuously passes per-connection state information from the active unit to the standby unit
- maintains connection information after a failover occurs, and
- allows supported end-user applications to continue communication sessions without reconnecting.

Stateful failover operation

During Stateful Failover, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

Supported features

Supported features are high availability capabilities that

- enable state information to be passed to the standby Firewall Threat Defense device during Stateful Failover
- maintain connection states and critical information for seamless traffic flow, and
- ensure minimal disruption during failover events.

State information types

For Stateful Failover, these state information types are passed to the standby device:

- NAT translation table.
- TCP and UDP connections and states, including HTTP connection states. Other types of IP protocols, and ICMP, are not parsed by the active unit, because they get established on the new active unit when a new packet arrives.
- Snort connection states, inspection results, and pin hole information, including strict TCP enforcement.
- The ARP table
- The Layer 2 bridge table (for bridge groups)
- The ISAKMP and IPsec SA table
- GTP PDP connection database
- SIP signaling sessions and pin holes.
- Static and dynamic routing tables—Stateful Failover participates in dynamic routing protocols, like OSPF and EIGRP, so routes that are learned through dynamic routing protocols on the active unit are maintained

in a Routing Information Base (RIB) table on the standby unit. Upon a failover event, packets travel normally with minimal disruption to traffic because the active secondary unit initially has rules that mirror the primary unit. Immediately after failover, the re-convergence timer starts on the newly active unit. Then the epoch number for the RIB table increments. During re-convergence, OSPF and EIGRP routes become updated with a new epoch number. Once the timer is expired, stale route entries (determined by the epoch number) are removed from the table. The RIB then contains the newest routing protocol forwarding information on the newly active unit.



Note Routes are synchronized only for link-up or link-down events on an active unit. If the link goes up or down on the standby unit, dynamic routes sent from the active unit may be lost. This is normal, expected behavior.

- DHCP Server—DHCP address leases are not replicated. However, a DHCP server configured on an interface will send a ping to make sure an address is not being used before granting the address to a DHCP client, so there is no impact to the service. State information is not relevant for DHCP relay or DDNS.
- Access control policy decisions—Decisions related to traffic matching (including URL, URL category, geolocation, and so forth), intrusion detection, malware, and file type are preserved during failover. However, for connections being evaluated at the moment of failover, there are the following caveats:
  - AVC—App-ID verdicts are replicated, but not detection states. Proper synchronization occurs as long as the App-ID verdicts are complete and synchronized before failover occurs.
  - Intrusion detection state—Upon failover, once mid-flow pickup occurs, new inspections are completed, but old states are lost.
  - File malware blocking—The file disposition must become available before failover.
  - File type detection and blocking—The file type must be identified before failover. If failover occurs while the original active device is identifying the file, the file type is not synchronized. Even if your file policy blocks that file type, the new active device downloads the file.
- User identity decisions from the identity policy, including the user-to-IP address mappings gathered passively through ISE Session Directory, and active authentication through captive portal. Users who are actively authenticating at the moment of failover might be prompted to authenticate again.
- Network AMP—Cloud lookups are independent from each device, so failover does not affect this feature in general. Specifically:
  - Signature Lookup—If failover occurs in the middle of a file transmission, no file event is generated and no detection occurs.
  - File Storage—If failover occurs when the file is being stored, it is stored on the original active device. If the original active device went down while the file was being stored, the file does not get stored.
  - File Pre-classification (Local Analysis)—If failover occurs in the middle of pre-classification, detection fails.
  - File Dynamic Analysis (Connectivity to the cloud)—If failover occurs, the system might submit the file to the cloud.

  - Archive File Support—If failover occurs in the middle of an analysis, the system loses visibility into the file/archive.
  - Custom Blocking—If failover occurs, no events are generated.
- Security Intelligence decisions. However, DNS-based decisions that are in process at the moment of failover are not completed.
- RA VPN—Remote access VPN end users do not have to reauthenticate or reconnect the VPN session after a failover. However, applications operating over the VPN connection could lose packets during the failover process and not recover from the packet loss.
- From all the connections, only established ones will be replicated on the Standby device.

Unsupported features

Unsupported features are device capabilities that

- are not passed to the standby Firewall Threat Defense in Stateful Failover
- do not maintain state information during failover events, and
- may require re-establishment after a failover occurs.

State information limitations

For Stateful Failover, the following state information is not passed to the standby Firewall Threat Defense:

- Sessions in plaintext tunnels other than GREv0 and IPv4-in-IP. Sessions inside tunnels are not replicated and the new active node will not be able to reuse existing inspection verdicts to match the correct policy rules.
- Decrypted TLS/SSL connections—The decryption states are not synchronized, and if the active unit fails, then decrypted connections will be reset. New connections will need to be established to the new active unit. Connections that are not decrypted (in other words, those that match a TLS/SSL Do Not Decrypt rule action) are not affected and are replicated correctly.
- Multicast routing.

Bridge group requirements for high availability

Bridge group requirements for high availability are special considerations that

- address traffic loss on bridge group member interfaces during failover
- prevent switch ports from entering blocking state for 30 to 50 seconds, and
- provide workarounds to maintain connectivity during topology changes.

High availability workarounds

There are special considerations for high availability when using bridge groups.

When the active unit fails over to the standby unit, the switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss on the

bridge group member interfaces while the port is in a blocking state, you can configure one of the following workarounds:

- Switch port is in Access mode—Enable the STP PortFast feature on the switch:

```
interface interface_id
  spanning-tree portfast
```

  The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, it eventually transitions into STP blocking mode.

- If the switch port is in Trunk mode, or you cannot enable STP PortFast, then you can use one of the following less desirable workarounds that impacts failover functionality or STP stability:
  - Disable interface monitoring on the bridge group and member interfaces.
  - Increase the interface hold time in the failover criteria to a high value that will allow STP to converge before the unit fails over.
  - Decrease the STP timers on the switch to allow STP to converge faster than the interface hold time.

Failover health monitoring

Failover health monitoring is a system capability that monitors each unit for overall health and interface health.

Health monitoring tests

The Firewall Threat Defense device performs tests to determine the state of each unit. This section includes information about how the Firewall Threat Defense device performs tests to determine the state of each unit.

Unit health monitoring

Unit health monitoring is a failover mechanism that

- determines the health of peer units by monitoring the failover link with hello messages
- sends LANTEST messages on each data interface when three consecutive hello messages are missed, and
- initiates appropriate failover actions based on peer unit responsiveness.

Unit health monitoring behavior

The Firewall Threat Defense device determines the health of the other unit by monitoring the failover link with hello messages. If a unit does not receive three consecutive hello messages on the failover link, the sends LANTEST messages on each data interface, including the failover link, to validate whether the peer is responsive. The action that the Firewall Threat Defense device takes depends on the response from the other unit. These are the possible actions:

- If the Firewall Threat Defense device receives a response on the failover link, then it does not fail over.
- If the Firewall Threat Defense device does not receive a response on the failover link, but it does receive a response on a data interface, then the unit does not failover. The failover link is marked as failed. You

should restore the failover link as soon as possible because the unit cannot fail over to the standby while the failover link is down.

- If the Firewall Threat Defense device does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed.

Note During a high-availability failover event, the Firewall Threat Defense device device may briefly appear as **Offline** in the device's health monitoring dashboard. This happens because health alerts are cleared during the process and are only updated after the process is complete. Wait for the failover operation to finish.

Heartbeat module redundancy

Heartbeat module redundancy is a high availability feature that

- sends heartbeat messages using the data plane transport infrastructure to supplement control plane heartbeat packets
- increments a counter when the peer receives heartbeat packets in the data plane
- prevents false failover or split-brain scenarios when the control plane is congested with traffic.

Heartbeat module redundancy behavior

Each unit in the HA periodically sends a broadcast keepalive heartbeat packet over the failover link. If the control plane is too busy handling traffic, sometimes the heartbeat packets do not reach the peers, or the peers do not process the heartbeat packets due to CPU overloading. When peers cannot communicate the keepalive status within the configurable timeout period, a false failover or split-brain scenario occurs.

The heartbeat module in the data plane helps to avoid the occurrence of false failover or split-brain due to traffic congestion in the control plane.

- The additional heartbeat module works similarly to the control plane module but sends and receives heartbeat messages using the data plane transport infrastructure.
- When the peer receives heartbeat packets in the data plane, a counter gets incremented.
- If the heartbeat transfer in the control plane fails, the node checks the heartbeat counter in the data plane. If the counter is incrementing, then the peer is alive, and the cluster does not perform a failover in this situation.

Note

- The additional heartbeat module is enabled by default whenever HA is enabled. You do not have to set a poll interval for the additional heartbeat module in the data plane. This module uses the same heartbeat interval that you set for the control plane.

Interface monitoring

Interface monitoring is a failover capability that

- tracks the health of up to 1025 interfaces to detect interface failures

- performs interface tests when hello messages are not received within 15 seconds, and
- triggers failover when the number of failed interfaces meets the defined threshold.

Interface monitoring operation

When a unit does not receive hello messages on a monitored interface for 15 seconds, it runs interface tests. If one of the interface tests fails for an interface, but this same interface on the other unit continues to successfully pass traffic, then the interface is considered to be failed, and the device stops running tests.

If the threshold you define for the number of failed interfaces is met (see **Devices** > **Device Management**, and then **High Availability** > **Failover Trigger Criteria**), and the active unit has more failed interfaces than the standby unit, then a failover occurs. If an interface fails on both units, then both interfaces go into the "Unknown" state and do not count towards the failover limit defined by failover interface policy.

An interface becomes operational again if it receives any traffic. A failed device returns to standby mode if the interface failure threshold is no longer met.

If an interface has IPv4 and IPv6 addresses configured on it, the device uses the IPv4 addresses to perform the health monitoring. If an interface has only IPv6 addresses configured on it, then the device uses IPv6 neighbor discovery instead of ARP to perform the health monitoring tests. For the broadcast ping test, the device uses the IPv6 all nodes address (FE02::1).

Interface tests

Interface tests are monitoring mechanisms that:

- evaluate interface operational status during failover scenarios
- run sequentially with approximately 1.5 second duration per test, and
- determine interface failure status on Firewall Threat Defense device units.

Interface test sequence

The Firewall Threat Defense device uses these interface tests in sequence:

1. Link Up/Down test—A test of the interface status. If the Link Up/Down test indicates that the interface is down, then the device considers it failed, and testing stops. If the status is Up, then the device performs the Network Activity test.
2. Network Activity test—A received network activity test. At the start of the test, each unit clears its received packet count for its interfaces. As soon as a unit receives any eligible packets during the test, then the interface is considered operational. If both units receive traffic, then testing stops. If one unit receives traffic and the other unit does not, then the interface on the unit that does not receive traffic is considered failed, and testing stops. If neither unit receives traffic, then the device starts the ARP test.
3. ARP test—A test for successful ARP replies. Each unit sends a single ARP request for the IP address in the most recent entry in its ARP table. If the unit receives an ARP reply or other network traffic during the test, then the interface is considered operational. If the unit does not receive an ARP reply, then the device sends a single ARP request for the IP address in the *next* entry in the ARP table. If the unit receives an ARP reply or other network traffic during the test, then the interface is considered operational. If both units receive traffic, then testing stops. If one unit receives traffic, and the other unit does not, then the interface on the unit that does not receive traffic is considered failed, and testing stops. If neither unit receives traffic, then the device starts the Broadcast Ping test.

4. Broadcast Ping test—A test for successful ping replies. Each unit sends a broadcast ping, and then counts all received packets. If the unit receives any packets during the test, then the interface is considered operational. If both units receive traffic, then testing stops. If one unit receives traffic, and the other unit does not, then the interface on the unit that does not receive traffic is considered failed, and testing stops. If neither unit receives traffic, then testing starts over again with the ARP test. If both units continue to receive no traffic from the ARP and Broadcast Ping tests, then these tests will continue running in perpetuity.

Interface status

Interface status is a monitoring indicator that

- shows the current operational state of monitored interfaces in a failover configuration
- tracks traffic reception and hello packet communication between peer units, and
- determines whether an interface is actively monitored by the failover process.

Interface status types

Monitored interfaces can have these status types:

- **Unknown**: Initial status. This status can also mean the status cannot be determined.
- **Normal**: The interface is receiving traffic.
- **Normal (Waiting)**: The interface is up, but has not yet received a hello packet from the corresponding interface on the peer unit.
- **Normal (Not-Monitored)**: The interface is up, but is not monitored by the failover process.
- **Testing**: Hello messages are not heard on the interface for five poll times.
- **Link Down**: The interface or VLAN is administratively down.
- **Link Down (Waiting)**: The interface or VLAN is administratively down and has not yet received a hello packet from the corresponding interface on the peer unit.
- **Link Down (Not-Monitored)**: The interface or VLAN is administratively down, but is not monitored by the failover process.
- **No Link**: The physical link for the interface is down.
- **No Link (Waiting)**: The physical link for the interface is down and has not yet received a hello packet from the corresponding interface on the peer unit.
- **No Link (Not-Monitored)**: The physical link for the interface is down, but is not monitored by the failover process.
- **Failed**: No traffic is received on the interface, yet traffic is heard on the peer interface.

Failover triggers and detection timing

Failover triggers and detection timing are high availability mechanisms that:

- initiate automatic switchover when specific failure conditions occur on the active unit,

- monitor system health through configurable detection thresholds and timing parameters, and
- ensure service continuity by transferring control to the standby unit when failures exceed defined limits.

Failover triggering events and timing parameters

These events trigger failover in a Firepower high availability pair:

- More than 50% of the Snort instances on the active unit are down.
- Disk space on the active unit is more than 90% full.
- The **no failover active** command is run on the active unit or the **failover active** command is run on the standby unit.
- The active unit has more failed interfaces than the standby unit.
- Interface failure on the active device exceeds the threshold configured.

  By default, failure of a single interface causes failover. You can change the default value by configuring a threshold for the number of interfaces or a percentage of monitored interfaces that must fail for the failover to occur. If the threshold is exceeded on the active device, failover occurs. If the threshold is exceeded on the standby device, the unit moves to **Fail** state.

  To change the default failover criteria, enter this command in global configuration mode:

Table 24: Interface policy command

Command	Purpose
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	Changes the default failover criteria. When specifying a specific number of interfaces, the *num* argument can be from 1 to 250. When specifying a percentage of interfaces, the *num* argument can be from 1 to 100.

This table shows the failover triggering events and associated failure detection timing. If failover occurs, you can view the reason for the failover in the Message Center, along with various operations pertaining to the high availability pair. You can configure these thresholds to a value within the specified minimum-maximum range.

Table 25: Firewall Threat Defense failover times

Failover triggering event	Minimum	Default	Maximum
Active unit loses power, hardware goes down, or the software reloads or crashes. When any of these occur, the monitored interfaces or failover link do not receives any hello message.	800 milliseconds	15 seconds	45 seconds
Active unit interface physical link down.	500 milliseconds	5 seconds	15 seconds
Active unit interface up, but connection problem causes interface testing.	5 seconds	25 seconds	75 seconds

Active/standby failover

Active/standby failover is a high availability configuration that

- lets you use a standby Firewall Threat Defense device to take over the functionality of a failed unit,
- enables the standby unit to become the active unit when the active unit fails, and
- allows the failed unit to come back online as the standby unit if the problem is temporary.

The failed unit must be replaced if the problem is not temporary. Set the standby unit to primary before replacing the failed unit to retain the configuration of the secondary unit.

For multiple context mode, the ASA can fail over the entire unit (including all contexts) but cannot fail over individual contexts separately.

Primary/secondary roles and active/standby status

Primary/secondary roles and active/standby status are failover configuration concepts that

- define unit hierarchy, with primary units taking precedence during simultaneous startup
- determine IP address and MAC address usage patterns during failover operations, and
- establish traffic flow responsibilities between paired units in Active/Standby failover configurations.

Primary and secondary unit differences

When setting up Active/Standby failover, you configure one unit to be primary and the other to be secondary. During configuration, the primary unit's policies are synchronized to the secondary unit. At this point, the two units act as a single device for device and policy configuration. However, for events, dashboards, reports and health monitoring, they continue to display as separate devices.

The main differences between the two units in a failover pair are related to which unit is active and which unit is standby, namely which IP addresses to use and which unit actively passes traffic.

However, a few differences exist between the units depending on which unit is primary (as specified in the configuration) and which unit is secondary:

- The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).
- The primary unit MAC addresses are always coupled with the active IP addresses. The exception to this rule occurs when the secondary unit becomes active and cannot obtain the primary unit MAC addresses over the failover link. In this case, the secondary unit MAC addresses are used.

Active unit determination at startup

Active unit determination at startup is a high availability process that

- sets a unit to standby if it boots and detects a peer already running as active,
- sets a unit to active if it boots and does not detect a peer, and
- sets the primary unit as active and secondary unit as standby if both units boot simultaneously.

Failover events

A failover event is a system condition that

- triggers an active unit to transfer control to a standby unit in Active/Standby failover configurations
- occurs on a unit basis, and
- follows specific failover policies that determine whether failover occurs and what actions each unit takes.

Failover event policies and actions

This table shows the failover action for each failure event. For each failure event, the table shows the failover policy (failover or no failover), the action taken by the active unit, the action taken by the standby unit, and any special notes about the failover condition and actions.

Table 26: Failover events

Failure Event	Policy	Active Unit Action	Standby Unit Action	Notes
Active unit failed (power or hardware)	Failover	n/a	Become active Mark active as failed	No hello messages are received on any monitored interface or the failover link.
Formerly active unit recovers	No failover	Become standby	No action	None.
Standby unit failed (power or hardware)	No failover	Mark standby as failed	n/a	When the standby unit is marked as failed, then the active unit does not attempt to fail over, even if the interface failure threshold is surpassed.
Failover link failed during operation	No failover	Mark failover link as failed	Mark failover link as failed	You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down.
Failover link failed at startup	No failover	Become active Mark failover link as failed	Become active Mark failover link as failed	If the failover link is down at startup, both units become active.
State link failed	No failover	No action	No action	State information becomes out of date, and sessions are terminated if a failover occurs.
Interface failure on active unit above threshold	Failover	Mark active as failed	Become active	None.
Interface failure on standby unit above threshold	No failover	No action	Mark standby as failed	When the standby unit is marked as failed, then the active unit does not attempt to fail over even if the interface failure threshold is surpassed.

Config-sync optimization

Config-sync optimization is a configuration synchronization enhancement that

- compares configuration hash values between active and joining devices to determine if full synchronization is necessary
- enables faster device rejoining by skipping full configuration synchronization when hash values match, and
- reduces maintenance window and upgrade time during high availability operations.

Guidelines and limitations of configuration sync optimization

When a device reboots or rejoins after a suspend or resume high availability, the joining device clears its running configuration. The active device then sends its entire configuration to the joining device for a full configuration synchronization. If the active device has a large configuration, this process can take several minutes.

The configuration sync optimization functionality enables comparing the configuration of the joining device and the active device by exchanging configuration hash values. If the hash computed on both active and joining devices match, the joining device skips full configuration synchronization and rejoin the high availability configuration. This functionality ensures faster peering and reduces maintenance window and upgrade time.

Guidelines and limitations:

- The configuration sync optimization functionality is enabled by default.
- Firewall Threat Defense multiple context mode supports configuration sync optimization by sharing the context order during full configuration synchronization, allowing comparison of context order during subsequent node-rejoin.
- If you configure passphrase and failover IPsec key, then configuration sync optimization is not effective as the hash value computed in the active and standby devices differs.
- If you configure the device with dynamic ACL or SNMPv3, configuration sync optimization is not effective.
- Active device synchronizes full configuration with flapping LAN links as default behavior. During failover flaps between active and standby devices, configuration sync optimization is not triggered and devices perform a full configuration synchronization.
- Configuration sync optimization gets triggered when the high availability configuration recovers from an interruption or loss of network communication between the active and standby devices.

Monitoring config-sync optimization:

- Syslog messages are generated displaying whether the hash values computed on the active and joining unit match, does not match, or if the operation timeout expires.
- The syslog message also displays the time elapsed, from the time of sending the hash request to the time of getting and comparing the hash response.

Note The Configuration State in **show failover state** command displays the config sync state status during HA joining. This state does not reflect the later config deployments or changes, and replication on device until a resync has been initiated.

Requirements and prerequisites for high availability

This reference provides the requirements and prerequisites needed to implement high availability functionality.

Model support

Secure Firewall Threat Defense

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for High availability

Model Support

- 1010:
  - You should not use the switch port functionality when using High availability. Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. High availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High availability network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot. Though Firewall Management Center allows you to configure switch ports / VLAN interfaces in HA, it may lead to misconfiguration due to network loops when connecting to external switches.
  - You can only use a firewall interface as the failover link.
- Firepower 9300—Intra-chassis High Availability is not supported.
- The Firewall Threat Defense Virtual on public cloud networks such as Microsoft Azure and Amazon Web Services are not supported with High availability because Layer 2 connectivity is required.

Additional Guidelines

- When a device that is part of a Threat Defense HA pair with site-to-site VPN configuration is reverted to a previous version, re-establishing the HA pair or deployment may fail. In this scenarion, you must follow these steps:

  1. After the revert, choose **Devices** > **VPN** > **Site to Site**.
  2. Select the VPN topology associated with the HA device.
  3. Re-select the correct VPN interface for the affected device.
  4. Save the VPN topology.
  5. Deploy configuration on the device.
  6. Re-establish the HA pair.

- When the active unit fails over to the standby unit, the connected switch port running Spanning Tree Protocol (STP) can go into a blocking state for 30 to 50 seconds when it senses the topology change. To avoid traffic loss while the port is in a blocking state, you can enable the STP PortFast feature on the switch:

  interface *interface_id* **spanning-tree portfast**

  This workaround applies to switches connected to both routed mode and bridge group interfaces. The PortFast feature immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

- Configuring port security on the switches connected to the Firewall Threat Defense device failover pair can cause communication problems when a failover event occurs. This problem occurs when a secure MAC address configured or learned on one secure port moves to another secure port, a violation is flagged by the switch port security feature.

- For Active/Standby High availability and a VPN IPsec tunnel, you cannot monitor both the active and standby units using SNMP over the VPN tunnel. The standby unit does not have an active VPN tunnel, and will drop traffic destined for the NMS. You can instead use SNMPv3 with encryption so the IPsec tunnel is not required.

- Both the peer devices go into unknown state and high-availability configuration fails if you run clish in any of the peer devices while creating a High Availability pair.

- Immediately after failover, the source address of syslog messages will be the failover interface address for a few seconds.

- For better convergence (during a failover), you must shut down the interfaces on a HA pair that are not associated with any configuration or instance.

- In high availability deployments with a shared failover and state interfaces, if the connectivity over failover interface fails while the standby unit is in sync config state, and eventually when the standby unit switches to active state, it results in a split brain. This is observed even when there is a monitored interface.

  The connectivity over failover interface can fail in the following situations:

  - After the standby unit reboots, the connectivity over failover interface fails while the standby unit is in sync config state.

- After enabling previously disabled failover on the standby unit, the connectivity over failover interface fails while the standby unit is in sync config state.

To avoid split brain, use failover and state interfaces. If the connectivity failures over the failover interfaces persist, isolate the new active (previously standby) unit from the network.

- If you configure failover encryption in evaluation mode, the systems use DES for the encryption. If you then register the devices using an export-compliant account, the devices will use AES after a reboot. Thus, if a system reboots for any reason, including after installing an upgrade, the peers will be unable to communicate and both units will become the active unit. We recommend that you do not configure encryption until after you register the devices. If you do configure this in evaluation mode, we recommend you remove the encryption before registering the devices.
- When using SNMPv3 with failover, if you replace a failover unit, then SNMPv3 users are not replicated to the new unit. You must remove the users, re-add them, and then redeploy your configuration to force the users to replicate to the new unit.
- The device does not share SNMP client engine data with its peer.
- If you have a very large number of access control and NAT rules, the size of the configuration can prevent efficient configuration replication, resulting in the standby unit taking an excessively long time to reach standby ready state. This can also impact your ability to connect to the standby unit during replication through the console or SSH session. To enhance configuration replication performance, enable transactional commit for both access rules and NAT, using the **asp rule-engine transactional-commit access-group** and **asp rule-engine transactional-commit nat** commands.
- A unit in a High availability pair transitioning to the standby role synchronizes its clock with the active unit.

  Example:

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- The units in High availability do not dynamically synchronize the clock. Here are some examples of events when synchronization takes place:
  - A new High availability pair is created.
  - High availability is broken and re-created.
  - Communication over the failover link was disrupted and reestablished.
  - Failover status was manually changed at the CLI using the **no failover/failover** or **configure high-availability suspend/resume** (Firewall Threat Defense) commands.
- Enabling High availability forces all routes to be deleted and are re-added after the High availability progression changes to the Active state. You could experience connection loss during this phase.

- If you replace the primary unit, then when you re-create high-availability, you should set the replacement unit as the *secondary* unit so that the configurations are replicated from the former secondary unit to the replacement unit. If you set the replacement unit as primary, you will accidentally overwrite the configuration that is present on the operational unit.
- Configure identical strong encryption on both Threat Defense devices before forming the High availability. If they are non-identical, the HA peers may enter a split-brain state.
- Deploying Firepower 1100 and 2100 devices in high availability with hundreds of interfaces configured on them can result in increased delay in the failover time (seconds).
- In the High availability configuration, short-lived connections, usually using port 53, are closed quickly and never transferred or synchronized from Active to Standby, so there might be a difference in the number of connections on both High availability devices. This is expected behavior for short-lived connections. You can try to compare the connections that are long-lived (for example, more than 30-60 seconds).
- In the High availability configuration, embryonic connections—connection requests that have not yet completed the three-way handshake process—are closed quickly and not synchronized between the active and standby devices. This design ensures HA system efficiency and security. For this reason, there might be a difference in the number of connections on both High availability devices, which is to be expected.
- If the failover LAN link is not connected back-to-back and instead connected through one or more switches, a failure within the intermediate path can cause the active unit to lose connectivity with the standby unit, resulting in inconsistent active/standby states. Although this does not impact High availability functionality, it is recommended to check and recover the failover-link path between the active and standby units.

  When the failover LAN link is down, it is not recommended to deploy any configuration, as it may not be replicated to the peer unit.
- See the Secure Firewall Threat Defense Virtual getting started guides and review your Firewall Threat Defense Virtual device configurations for high availability.
- In OSPF, after a failover, the OSPF connection with the peer device becomes invalid. Terminate the invalid connection, and then establish a new OSPF connection.
- In transparent mode, if you have problems with the active unit losing the MAC address of the hot-standby router (HSRP), create a static mapping for the MAC address.
- UCAPL or CC compliance mode cannot be changed if the threat defense device is in high availability. Modify the compliance mode before forming the high availability pair.

Add a high availability pair

Establish an Active/Standby high-availability pair to ensure network protection continuity in case of device failure.

When establishing an Active/Standby high-availability pair, you designate one of the devices as primary and the other as secondary. The Firewall Management Center deploys a merged configuration to the paired devices. If there is a conflict, the primary device setting is used. In a multidomain deployment, devices in a high-availability pair must belong to the same domain.

Note The failover link and the stateful failover link are in a private IP space and are only used for communication between peers in a high-availability pair. After high availability is established, selected interface links and encryption settings cannot be modified without breaking the high-availability pair and reconfiguring it.

Caution Creating or breaking a high-availability pair immediately restarts the Snort process on the primary and secondary devices, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129. The system warns you that continuing to create a high-availability pair restarts the Snort process on the primary and secondary devices and allows you to cancel.

Before you begin

Confirm that both devices:

- Are the same model.
- Have the same number and type of interfaces.
- Are in the same domain and group.
- Have normal health status and are running the same software.
- Are either in routed or transparent mode.

Note Only routed mode is supported for manager access on a data interface.

- Have the same NTP configuration. See Synchronize time on FTD devices, on page 908.
- Are fully deployed with no uncommitted changes.
- Do not have DHCP or PPPoE configured on any interfaces.
- For manager access on a data interface:
  - Use the same data interface on both devices for manager access.
  - Redundant manager access data interface is not supported.
  - You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and zero-touch provisioning.

Note If you use zero-touch provisioning to register the device, when you use the outside interface for manager access, it uses DHCP by default. Before you can enable high availability, you need to change the IP address to a static address. See Change the device IP address, on page 763. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

- Have different static IP addresses in the same subnet.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

Note The high availability formation is possible between the two Firewall Threat Defense devices when the certificate available on the primary device is not present on the secondary device. When high availability is formed, the certificate will be synched on the secondary device.

Procedure

Step 1 Add both devices to the Firewall Management Center according to Registration with the management center, on page 32.

Step 2 Choose **Devices** > **Device Management**.

Step 3 From the **Add** drop-down menu, choose **High Availability**.

Step 4 Enter a display **Name** for the high-availability pair.

Step 5 Under **Device Type**, choose **Firepower Threat Defense**.

Step 6 Choose the **Primary Peer** device for the high-availability pair.

Step 7 Choose the **Secondary Peer** device for the high-availability pair.

Step 8 Click **Continue**.

Step 9 Under **LAN Failover Link**, choose an **Interface** with enough bandwidth to reserve for failover communications.

Note Only interfaces that do not have a logical name and do not belong to a security zone, will be listed in the **Interface** drop-down in the **Add High Availability Pair** dialog.

Step 10 Type any identifying **Logical Name**.

Step 11 Type a **Primary IP** address for the failover link on the active unit.

This address should be on an unused subnet.

Note 169.254.1.0/24 and fd00:0:0:*::/64 are internally used subnets and cannot be used for the failover or state links.

Step 12 Optionally, choose **Use IPv6 Address**.

Step 13 Type a **Secondary IP** address for the failover link on the standby unit. This IP address must be in the same subnet as the primary IP address.

Step 14 If IPv4 addresses are used, type a **Subnet Mask** that applies to both the primary and secondary IP addresses.

Step 15 Optionally, under **Stateful Failover Link**, choose the same **Interface**, or choose a different interface and enter the high availability configuration information.

Note 169.254.1.0/24 and fd00:0:0:*::/64 are internally used subnets and cannot be used for the failover or state links.

Step 16 (Optional) Choose **Enabled** and choose the **Key Generation** method for IPsec Encryption between the failover links.

Step 17 Click **OK**. This process takes a few minutes as the process synchronizes system data.

After a successful configuration, the high availability pair is established with one device as active and the other as standby. .

Note We recommend to back up the devices. You can use the backup to quickly replace the devices when they fail and to restore the high availability service without being delinked from the Firewall Management Center. For more information, see *Cisco Secure Firewall Management Center Administration Guide*.

Configure optional high availability parameters

You can view the initial High Availability Configuration on the Firewall Management Center. You cannot edit these settings without breaking the high availability pair and then re-establishing it. To edit these settings, you must first break the high availability pair and re-establish it. You can modify the Failover Trigger Criteria to improve failover results. Interface Monitoring helps you determine which interfaces are best suited for failover.

Configure standby IP addresses and interface monitoring

Configure standby IP addresses for high availability interfaces to enable the active unit to perform network tests and check standby interface health beyond just tracking link state.

For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

By default, monitoring is enabled on all named physical interfaces and, for the 1010, all VLAN interfaces,. You might want to exclude interfaces attached to less critical networks from affecting your failover policy. Switch ports are not eligible for interface monitoring.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device high-availability pair you want to edit, click the **Edit** ( ).

Step 3 Click the **High Availability** tab.

Step 4 In the **Monitored Interfaces** area, click the **Edit** (✎) next to the interface you want to edit.

Step 5 Check the **Monitor this interface for failures** check box.

Step 6 On the **IPv4** tab, enter the **Standby IP Address**.

This address must be a free address on the same network as the active IP address.

Step 7 If you configured the IPv6 address manually, on the **IPv6** tab, click the **Edit** (✎) next to the active IP address, enter the **Standby IP Address**, and click **OK**.

This address must be a free address on the same network as the active IP address. For autogenerated and **Enforce EUI 64** addresses, the standby address is automatically generated.

Step 8 Click **OK**.

Edit high availability failover criteria

This task allows you to customize failover criteria for high availability device pairs to match your specific network deployment requirements.

You can customize failover criteria based on your network deployment.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device high-availability pair you want to edit, click the **Edit** (✎).

Step 3 Choose **High Availability**.

Step 4 Next to **Failover Trigger Criteria**, click the **Edit** (✎).

Step 5 Under **Interface Failure Threshold**, choose the number or percentage of interfaces that must fail before the device fails over.

Step 6 Under **Hello packet Intervals**, choose how often hello packets are sent over the failover link.

Note If you use remote access VPN on the Firepower 2100, use the default hello packet intervals. Otherwise, you might see high CPU usage that can cause a failover to occur.

Step 7 Click **OK**.

Configure virtual MAC addresses

Configure active and standby MAC addresses to minimize loss of traffic during failover and provide redundancy against IP address mapping for failover.

You can configure active and standby MAC addresses for failover using the following methods in the Secure Firewall Management Center:

- From the **Advanced tab** on the **Edit Interface** page during interface configuration; see Configure the MAC address, on page 718.
- From the **Add Interface MAC Address** dialog-box which is accessed from the **High Availability** page; see this procedure.

Note To configure the MAC address in both primary and secondary units (so that the MAC address is transferred to all sub-interfaces to both the high-availability units), the recommended approach is to use the **Interfaces** tab to replicate the MAC addresses on sub-interfaces over both active and standby high-availability units.

If you configure active and standby MAC addresses in both locations, the addresses defined during interface configuration take precedence for failover.

You can minimize loss of traffic during failover by designating active and standby MAC addresses to the physical interface. This feature offers redundancy against IP address mapping for failover.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device high-availability pair you want to edit, click **Edit** ( ).

Step 3 Click **High Availability**.

Step 4 Click the **Add** ( ) icon next to Interface MAC Addresses.

Step 5 Choose a **Physical Interface**.

Step 6 Enter the **Active Interface MAC Address**.

Step 7 Enter the **Standby Interface MAC Address**.

Step 8 Click **OK**.

Note For detailed information, see Task 2, steps from 10 to 14 in Configure FTD High Availability on Firepower Appliances.

Manage High availability

This section describes how to manage High availability units after you enable High availability, including how to change the High availability setup and how to force failover from one unit to another.

Switch the Active Peer in the Firewall Threat Defense High Availability Pair

This task allows you to manually switch the active and standby units in a high availability pair, effectively forcing failover for reasons such as persistent fault or health events on the current active unit.

After you establish the Firewall Threat Defense high availability pair, you can manually switch the active and standby units, effectively forcing failover for reasons such as persistent fault or health events on the current active unit. Both units should be fully deployed before you complete this procedure.

Before you begin

Refresh node status for a single Firewall Threat Defense high availability pair, on page 312. This ensures that the status on the Firewall Threat Defense high availability device pair is in sync with the status on the Firewall Management Center.

Follow these steps to switch the active peer in the high availability pair:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the high availability pair where you want to change the active peer, click the **Switch Active Peer**.

Step 3 Choose an option:

- Click **Yes** to immediately make the standby device the active device in the high availability pair.
- Click **No** to cancel and return to the Device Management page.

Refresh node status for a single Firewall Threat Defense high availability pair

Refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair when communication issues result in out of sync data.

Whenever active or standby devices in the Firewall Threat Defense high availability pair are rebooted, the Firewall Management Center may not display accurate high availability status for either device. This is because when the device reboots, the high availability status is immediately updated on the device and its corresponding event is sent to the Firewall Management Center. However, the status may not be updated on the Firewall Management Center because the communication between the device and the Firewall Management Center is yet to be established.

Communication failures or weak communication channels between the Firewall Management Center and devices may result in out of sync data. When you switch the active and standby devices in a high availability pair, the change may not be reflected in the Firewall Management Center even after a significant time duration.

In these scenarios, you can refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the high availability pair where you want to refresh the node status, click the **Refresh HA Node Status**.

Step 3 Click **Yes** to refresh the node status.

Suspend and resume high availability

You can suspend a unit in a high-availability pair, which is useful when:

- Both units are in an active-active situation, and fixing the communication on the failover link does not correct the problem.
- You want to troubleshoot an active or standby unit and do not want the units to fail over during that time.

When you suspend high availability, the currently active device remains active and continues handling all user connections. However, failover criteria are no longer monitored, and the system will never fail over to the now pseudo-standby device.

When using a data interface for manager access, the management connection will be broken until after you resume.

The primary difference between suspending high availability and breaking high availability is that on a suspended high-availability device, the high-availability configuration is retained. When you break high availability, the configuration is erased. Thus, you have the option to resume high availability on a suspended system, which enables the existing configuration and makes the two devices function as a failover pair again.

To suspend high availability, use the **configure high-availability suspend** command.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

If you suspend high availability from the active unit, the configuration is suspended on both the active and standby units. The standby unit interface configuration is also erased. If you suspend it from the standby unit, it is suspended on the standby unit only, but the active unit will not attempt to fail over to a suspended unit.

To resume failover, use the **configure high-availability resume** command.

```
> configure high-availability resume
Successfully resumed high-availablity.
```

You can resume a unit only if it is in Suspended state. The unit will negotiate active/standby status with the peer unit.

Note Suspending high availability is a temporary state. If you reload a unit, it resumes the high-availability configuration automatically and negotiates the active/standby state with the peer.

Replace a unit in Firewall Threat Defense high availability pair

This reference explains the process for replacing a failed unit in a Firewall Threat Defense high availability pair, including both backup restore and manual replacement procedures.

To replace a failed unit in the Firewall Threat Defense high availability pair using a backup file, see *Restoring Firewall Management Centers and Managed Devices* in the *Cisco Secure Firewall Management Center Administration Guide*.

If you do not have a backup of the failed device, you must break high availability. Then, register the replacement device to the Secure Firewall Management Center and reestablish high availability. The process varies depending on whether the device is primary or secondary:

- Replace a Primary Firewall Threat Defense HA Unit with no Backup, on page 314
- Replace a Secondary Firewall Threat Defense HA Unit with no Backup, on page 315

Replace a Primary Firewall Threat Defense HA Unit with no Backup

This task replaces a failed primary unit in a Firewall Threat Defense high availability pair to restore redundancy and maintain network protection.

Follow these steps below to replace a failed primary unit in the Firewall Threat Defense high availability pair. Failing to follow these steps can overwrite the existing high availability configuration.

Caution Creating or breaking the Firewall Threat Defense high availability pair immediately restarts the Snort process on the primary and secondary devices, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129. The system warns you that continuing to create a high availability pair restarts the Snort process on the primary and secondary devices and allows you to cancel.

Caution Never move a disk from sensor or Firewall Management Center to another device without reimaging the disk. This is an unsupported configuration and can cause breakage in functionality.

Procedure

Step 1 Choose **Force Break** to separate the high availability pair; see Break a high availability pair, on page 316.

Note The break operation removes all the configuration related to HA from Firewall Threat Defense and Firewall Management Center, and you need to recreate it manually later. To successfully configure the same HA pair, ensure that you save the IPs, MAC addresses, and monitoring configuration of all the interfaces/subinterfaces prior to executing the HA break operation.

Step 2 Unregister the failed primary Firewall Threat Defense device from the Firewall Management Center; see Delete (Unregister) a Device from the Firewall Management Center , on page 54.

Step 3 Register the replacement Firewall Threat Defense to the Firewall Management Center; see Registration with the management center, on page 32.

Step 4 Configure high availability, using the existing secondary/active unit as the primary device and the replacement device as the secondary/standby device during registration; see Add a high availability pair, on page 306.

Replace a Secondary Firewall Threat Defense HA Unit with no Backup

This task allows you to restore high availability functionality by replacing a failed secondary unit in an Firewall Threat Defense high availability pair.

When a secondary unit fails in a high availability configuration, you need to replace it and recreate the HA pair to maintain network redundancy and protection.

Caution Creating or breaking the Firewall Threat Defense high availability pair immediately restarts the Snort process on the primary and secondary devices, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129. The system warns you that continuing to create a high availability pair restarts the Snort process on the primary and secondary devices and allows you to cancel.

Procedure

Step 1 Choose **Force Break** to separate the high availability pair.

See Break a high availability pair, on page 316.

Note The break operation removes all the configuration related to HA from Firewall Threat Defense and Firewall Management Center, and you need to recreate it manually later. To successfully configure the same HA pair, ensure that you save the IPs, MAC addresses, and monitoring configuration of all the interfaces/subinterfaces prior to executing the HA break operation.

Step 2 Unregister the secondary Firewall Threat Defense device from the Firewall Management Center.

See Delete (Unregister) a Device from the Firewall Management Center , on page 54.

Step 3 Register the replacement Firewall Threat Defense to the Firewall Management Center.

See Registration with the management center, on page 32.

Step 4 Configure high availability, using the existing primary/active unit as the primary device and the replacement device as the secondary/standby device during registration.

See Add a high availability pair, on page 306.

Break a high availability pair

Break a high availability pair to remove the high-availability configuration from both units while maintaining traffic flow on the active unit.

When you break a high-availability pair, the high-availability configuration is removed from both units.

When using the Management interface for manager access: The active unit remains up and passing traffic. The standby unit interface configuration is erased.

When using a data interface for manager access: See the following details.

- The active unit remains up and passing traffic.
- The standby unit data interfaces are shut down except for the manager access interface, which remains up using the standby IP address so it can maintain the management connection.
- In a remote branch deployment setup, all standby unit data interfaces that are assigned with a logical name are shut down except for the manager access interface, which remains up to maintain the management connection.
- If the primary unit is in the standby state:
  - The IP addresses for manager access are swapped permanently in the Firewall Management Center configuration: the primary unit uses the standby IP address, and the secondary unit uses the active IP address.
  - If the Firewall Management Center initiated the management connection, and you specified a hostname for the device, then you need to update the DNS server so the swapped IP addresses are associated with the correct hostnames.
  - Breaking high availability causes a deployment to the standby unit. If the management connection is not yet reestablished because of the swapped IP addresses, the deployment may fail. In this case, you will need to manually trigger the deployment later (after the management connection is established). Be sure to complete the standby deployment before deploying changes to the active unit.

Policies that were not deployed to the active unit prior to the break operation continue to remain un-deployed after the break operation is complete. Deploy the policies on the standalone device after the break operation is complete.

Note

- When IPsec is enabled on high availability interfaces on the Firewall Threat Defense device, the device cannot prioritize the encrypted packets into the high-priority receive queue. As a result, during high-volume data traffic scenarios, attempts to break high availability may fail as the device cannot efficiently manage and prioritize the large number of encrypted connections. To view the device's resource usage and the maximum throughput, use the `show resource usage` command.
- If you cannot reach the high-availability pair using the Firewall Management Center, connect to the CLI on each device and enter **configure high-availability disable** to manually break high availability. See also Delete (Unregister) a High Availability Pair and Register to a New Firewall Management Center, on page 318.

Caution Breaking the Firewall Threat Defense high-availability pair immediately restarts the Snort process on the primary and secondary units, temporarily interrupting traffic inspection on both devices. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Before you begin

- Refresh node status for a single Firewall Threat Defense high availability pair, on page 312. This ensures that the status on the high-availability pair is in sync with the status on the Firewall Management Center.

Follow these steps to break a high availability pair:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the high-availability pair you want to break, click **More** (⋮) and choose **Break**.

Step 3 If the standby peer does not respond, check **Force Break**.

Step 4 Click **Yes**.

The Break operation removes the high-availability configuration from the active and standby units.

A FlexConfig policy deployed on the active unit may show a deployment failure after the break high-availability operation. You must alter and re-deploy the FlexConfig policy on the active unit.

What to do next

If you are using a FlexConfig policy on the active unit, alter and re-deploy the FlexConfig policy to eliminate deployment errors.

Note After you break high availability, the Firewall Threat Defense device that was operating as the active unit will still have the standby unit's IP address listed in its configuration. To resolve this, do an additional deployment on the formerly active Firewall Threat Defense device to remove the standby unit's IP address from its configuration.

Delete (Unregister) a High Availability Pair and Register to a New Firewall Management Center

This task allows you to unregister a High Availability pair from the Firewall Management Center, which keeps the High Availability pair intact. You might want to unregister the pair if you want to register it to a new Firewall Management Center or if the Firewall Management Center can no longer reach the pair.

Unregistering a High Availability pair:

- Severs all communication between the Firewall Management Center and the pair.
- Removes the pair from the **Device Management** page.
- Returns the pair to local time management if the pair's platform settings policy is configured to receive time from the Firewall Management Center using NTP.
- Leaves the configuration intact, so the pair continues to process traffic.

  Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.

Registering the pair again to the same or a different Firewall Management Center causes the configuration to be removed, so the pair will stop processing traffic at that point; the High Availability configuration remains intact so you can add the pair as a whole. You can choose an access control policy at registration, but you will have to re-apply other policies after registration and then deploy the configuration before it will process traffic again.

Before you begin

- This procedure requires CLI access to the primary unit.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the High Availability pair you want to unregister, click **More** (⋮) and choose **Delete**.

Step 3 Click **Yes**. The device High Availability pair is unregistered.

Step 4 You can register the pair to a new (or the same) Firewall Management Center by adding the primary unit as a new device.

a) Determine the primary unit by connecting to the CLI on one unit, and entering the **show failover** command.

The first line of the output shows whether this unit is Primary or Secondary.

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) At the primary unit's CLI, identify the new Firewall Management Center using the **configure manager add** command. See Modify Firewall Threat Defense management interface settings at the CLI , on page 763.

c) Choose **Devices** > **Device Management**, and then click **Add** > **Device**.

You only need to add the primary unit as a device, and the Firewall Management Center will discover the secondary unit.

Monitoring High availability

Monitoring High availability is a system capability that enables you to view the High availability status.

View failover history

View the failover history of both high availability devices in a single view to understand the chronological order of failover events and their reasons.

You can view the failover history of both high availability devices in a single view. The history displays in chronological order and includes the reason for any failover.

Before you begin

Follow these steps to view failover history:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device high-availability pair you want to edit, click **Edit** ( ).

Step 3 Choose **Summary**.

Step 4 Under General, click **View** ( ).

View stateful failover statistics

This task allows you to monitor the stateful failover link statistics to assess the performance and health of your high availability configuration.

You can view the stateful failover link statistics of both the primary and secondary devices in the high availability pair.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device high-availability pair you want to edit, click **Edit** ( ).

Step 3 Choose **High Availability**.

Step 4 Under Stateful Failover Link, click **View** ( ).

Step 5 Choose a device to view statistics.

Troubleshoot configuration sync failure

When forming a failover pair, the joining unit clears its running configuration and replicates the entire configuration from the active unit. Upon completing full configuration sync, the joining unit assumes the standby ready role and establishes the failover pair. After the unit joins the failover pair, any configuration change on the active unit are also replicated on the standby unit to keep both the units synchronized.

If the standby unit fails to replicate any configuration change commands, it reports configuration sync failure and exit the high availability by disabling failover. This section describes steps for identifying and troubleshooting configuration sync failure error reported by the standby unit.

To view the configuration sync errors or stats, you can use these CLI commands through an SSH session or the Threat Defense CLI:

- **show failover config-sync errors all** to display all configuration synchronization errors related to failover.
- **show failover config-sync stats all** to view statistics regarding failover configuration synchronization.

To re-enable high availability:

- Re-enable failover by executing the **failover reset** command on the active unit.
- If re-enabling the failover is not successful, delete or update the configuration change that the standby unit failed to replicate, and then re-enable the failover.

Note If the maximum interface limit is reached, the number of VPN tunnels on the active and standby units may be inconsistent. In this situation run the**write standby**command on the active unit to sync the configuration.

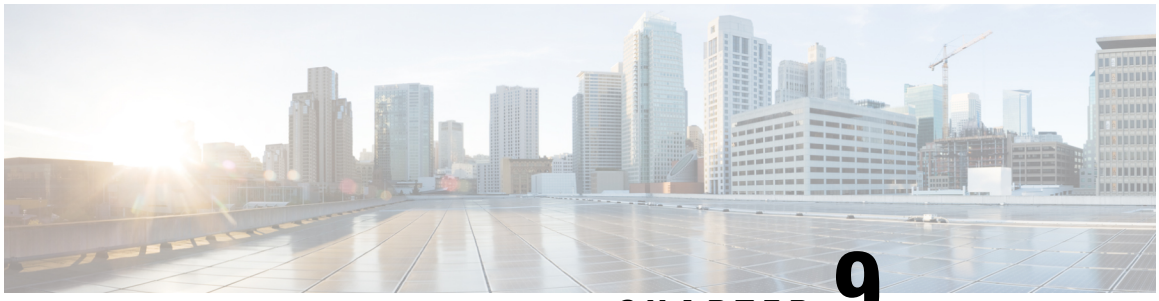
History for high availability

This reference provides a chronological history of high availability features, enhancements, and improvements implemented across various software versions. The information helps you track the evolution of high availability capabilities and understand when specific features were introduced.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
High availability support for the manager access data interface	7.4	7.4	You can now use a data interface for manager access with Firewall Threat Defense high availability.
Unregistering a high-availability pair now allows you to re-register without breaking the pair	7.3	Any	When you DELETE (unregister) a high-availability pair, you no longer have to manually break the pair at the CLI and re-register standalone devices. You can now add the primary unit to a new Firewall Management Center, and the standby unit will be discovered automatically. Re-registering the pair will still erase the configuration, and your policies will need to be re-applied.
Policy rollback support for high availability	7.2	Any	The **configure policy rollback** command is supported for high availability.
Config-Sync Optimization feature for faster HA peering	7.2	Any	The Config-Sync Optimization feature enables comparing the configuration of the joining unit and the active unit by exchanging config-hash values. If the hash computed on both active and joining units match, the joining unit skips full config-sync and rejoin the HA. This feature enables faster HA peering and reduces maintenance window and upgrade time.
Improvements to the upgrade workflow for clustered and high-availability devices	7.1	Any	We made improvements to the upgrade workflow for clustered and high-availability devices: • The upgrade wizard now correctly displays clustered and high-availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high-availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can GET the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.
Clearing routes in a high-availability group or cluster.	7.1	Any	In previous releases, the **clear route** command cleared the routing table on the unit only. Now, when operating in a high-availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details

FTD High Availability Hardening	6.2.3	Any	Version 6.2.3 introduces features for FTD devices in high availability:
			• Whenever active or standby FTD devices in a high-availability pair restart, the FMC may not display accurate high-availability status for either managed device. However, the status may not upgrade on the FMC because the communication between the device and the FMC is not established yet. The **Refresh Node Status** option on the **Devices** > **Device Management** page allows you to refresh the high-availability unit status to obtain accurate information about the active and standby device in a high-availability pair.
			• The **Devices** > **Device Management** page of the FMC UI has a new **Switch Active Peer** icon.
			• Version 6.2.3 includes a new REST API object, **Device High Availability Pair Services**, that contains four functions:
			  • **DELETE ftddevicehapairs**
			  • **PUT ftddevicehapairs**
			  • **POST ftddevicehapairs**
			  • **GET ftddevicehapairs**



CHAPTER 9

Clustering: Secure Firewall 3100/4200

Clustering lets you group multiple Firewall Threat Defense nodes together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

Note Some features are not supported when using clustering. See Unsupported features with clustering, on page 370.

- Clustering for the Secure Firewall 3100/4200, on page 323
- Licenses for clustering, on page 325
- Prerequisites for clustering, on page 325
- Guidelines for clustering, on page 326
- Clustering configuration, on page 331
- Cluster node management, on page 351
- Monitor the cluster, on page 361
- Troubleshoot the cluster, on page 365
- Clustering examples, on page 368
- Reference for Clustering, on page 370
- History for Clustering, on page 382

Clustering for the Secure Firewall 3100/4200

This section describes the clustering architecture and how it works.

How a cluster fits into your network

The cluster consists of multiple firewalls acting as a single unit. To act as a cluster, the firewalls need the following infrastructure:

- Isolated, high-speed backplane network for intra-cluster communication, known as the *cluster control link*.
- Management access to each firewall for configuration and monitoring.

Infrastructure requirements

When you place the cluster in your network, the upstream and downstream routers need to be able to load-balance the data coming to and from the cluster using Spanned EtherChannels. Interfaces on multiple members of the cluster are grouped into a single EtherChannel; the EtherChannel performs load balancing between units.

Control and data node roles

One member of the cluster is the control node. If multiple cluster nodes come online at the same time, the control node is determined by the priority setting; the priority is set between 1 and 100, where 1 is the highest priority. All other members are data nodes. When you first create the cluster, you specify which node you want to be the control node, and it will become the control node simply because it is the first node added to the cluster.

All nodes in the cluster share the same configuration. The node that you initially specify as the control node will overwrite the configuration on the data nodes when they join the cluster, so you only need to perform initial configuration on the control node before you form the cluster.

Some features do not scale in a cluster, and the control node handles all traffic for those features.

Cluster interfaces

You can configure data interfaces as Spanned EtherChannels. Refer Cluster interfaces, on page 331 for more information.

Interface type restrictions

- You can use regular firewall interfaces or IPS-only interfaces (inline sets or passive interfaces).
-

Note Individual interfaces are not supported, with the exception of a management interface.

Cluster control links

A cluster control link is a dedicated hardware interface that each unit must allocate for cluster communication. For more information, refer Cluster control link, on page 331.

Configuration replication

All nodes in the cluster share a single configuration. You can only make configuration changes on the control node (with the exception of the bootstrap configuration), and changes are automatically synced to all other nodes in the cluster.

Management network

You must manage each node using the Management interface; management from a data interface is not supported with clustering.

Licenses for clustering

Lists the licensing requirements for clustering.

Feature license assignment

You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

When you add the control node to the Firewall Management Center, you can specify the feature licenses you want to use for the cluster. Before you create the cluster, it doesn't matter which licenses are assigned to the data nodes; the license settings for the control node are replicated to each of the data nodes. You can modify licenses for the cluster by clicking **Edit Licenses** in **System** (⚙) > **Licenses** > **Smart Licenses** or choosing **Devices** > **Device Management**, clicking **Edit** (✎) for the cluster, and then in the **License** area, clicking **Edit** (✎).

APEX, PLUS, and VPN-Only licenses are not supported for clustering. Before you create a cluster, remove unsupported license assignments from the devices that will become cluster nodes.

Note If you add the cluster before the Firewall Management Center is licensed (and running in Evaluation mode), then when you license the Firewall Management Center, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

Prerequisites for clustering

Review these prerequisites before configuring clustering on Secure Firewall devices.

Model requirements

- Secure Firewall 3100—Maximum 8 nodes
- Secure Firewall 4200—Maximum 8 nodes

User roles

- Admin
- Access Admin
- Network Admin

Hardware and software requirements

- All units in a cluster must be the same model.
- All units must include the same number of interfaces and the same network modules, and must use the same network module slot assignments.
- The Firewall Management Center access must be from the Management interface; data interface management is not supported.
- All units must run the identical software except at the time of an image upgrade. Hitless upgrade is supported. For a cluster that uses centralized VPN, all units must run the same software version. After an upgrade or downgrade, complete the operation on all units and verify that every unit runs the target software version before you resume VPN traffic.
- All units must be in the same firewall mode, routed or transparent.
- All units must use the same compliance mode.
- If core allocation is supported, all units must use the same core allocation profile.
- All units must be in the same domain and the same group, with no deployment pending or in progress.
- The control node must not have any unsupported features configured (refer Unsupported features with clustering, on page 370), and data nodes must not have any VPN configured. The control node can have site-to-site VPN configured.



Note

- Clustering is not supported for Threat Defense instances, such as instances in container mode.
- All units must use the same compliance mode.
- If core allocation is supported, all units must use the same core allocation profile.

Switch requirements

Be sure to complete the switch configuration before you configure clustering. Make sure the ports connected to the cluster control link have the correct (higher) MTU configured. By default, the cluster control link MTU is set to 100 bytes higher than the data interfaces. If the switches have an MTU mismatch, the cluster formation will fail.

Guidelines for clustering

Configuration requirements

Ensure that firewall mode configuration matches on all units in the cluster.

- High Availability is not supported with clustering.
- The cluster control link is only supported using IPv4.

Switch and EtherChannel configuration

Disable the LACP Graceful Convergence feature on all cluster-facing EtherChannel interfaces for Cisco Nexus switches.

Topology change management

When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the Threat Defense device or the switch, adding an additional switch to form a VSS or vPC) you should disable the health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the interface health check feature.

Operational considerations

Expect temporary, limited packet, or connection drop when adding a unit to an existing cluster or when reloading a unit.

- In some cases, the dropped packets can hang your connection; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel, when the syslog server port is down and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the ASA cluster. These messages can result in some units of the ASA cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

Default clustering settings

Review the default clustering configuration settings before deployment.

- The cLACP system ID is auto-generated, and the system priority is 1 by default.
- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Firewall Mode

The firewall mode must match on all units.

High Availability

High Availability is not supported with clustering.

IPv6

The cluster control link is only supported using IPv4.

Switches

- Make sure connected switches match the MTU for both cluster data interfaces and the cluster control link interface. You should configure the cluster control link interface MTU to be at least 100 bytes higher than the data interface MTU, so make sure to configure the cluster control link connecting switch appropriately. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead. In addition, we do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.
- For Cisco IOS XR systems, if you want to set a non-default MTU, set the IOS XR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the **mtu-ignore** option is used. Note that the cluster device MTU should match the IOS XR IPv4 MTU. This adjustment is not required for Cisco Catalyst and Cisco Nexus switches.
- On the switch, we recommend that you use one of these EtherChannel load-balancing algorithms: **source-dest-ip** or **src-dst-mixed-ip-port** (see the Cisco Nexus OS and Cisco IOS-XE **port-channel load-balance** command).

  Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
- If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.
- On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

  router(config)# **port-channel** *id* **hash-distribution fixed**

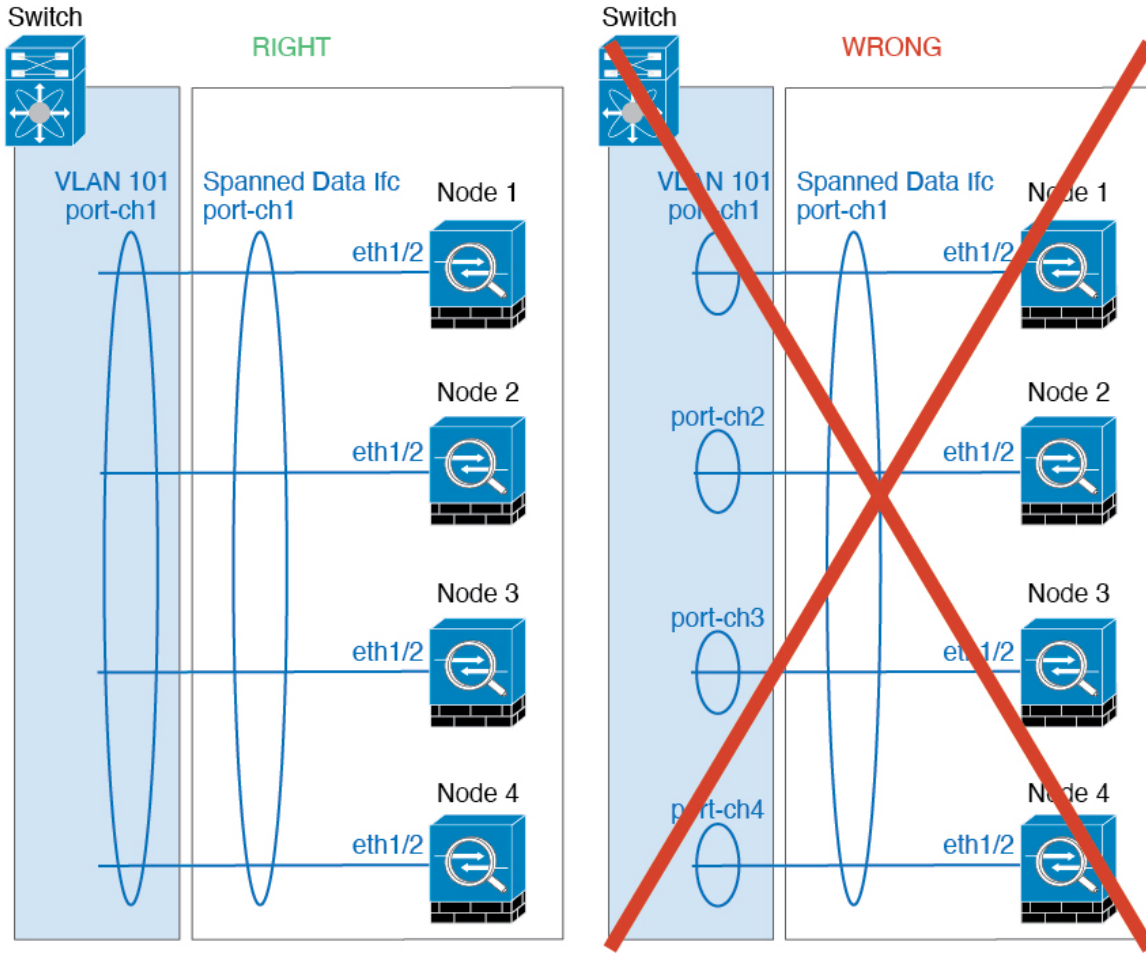
  Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
- Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
- Port-channel bundling downtime should not exceed the configured keepalive interval.
- You should disable the LACP Graceful Convergence feature on all cluster-facing EtherChannel interfaces for Cisco Nexus switches.

EtherChannels

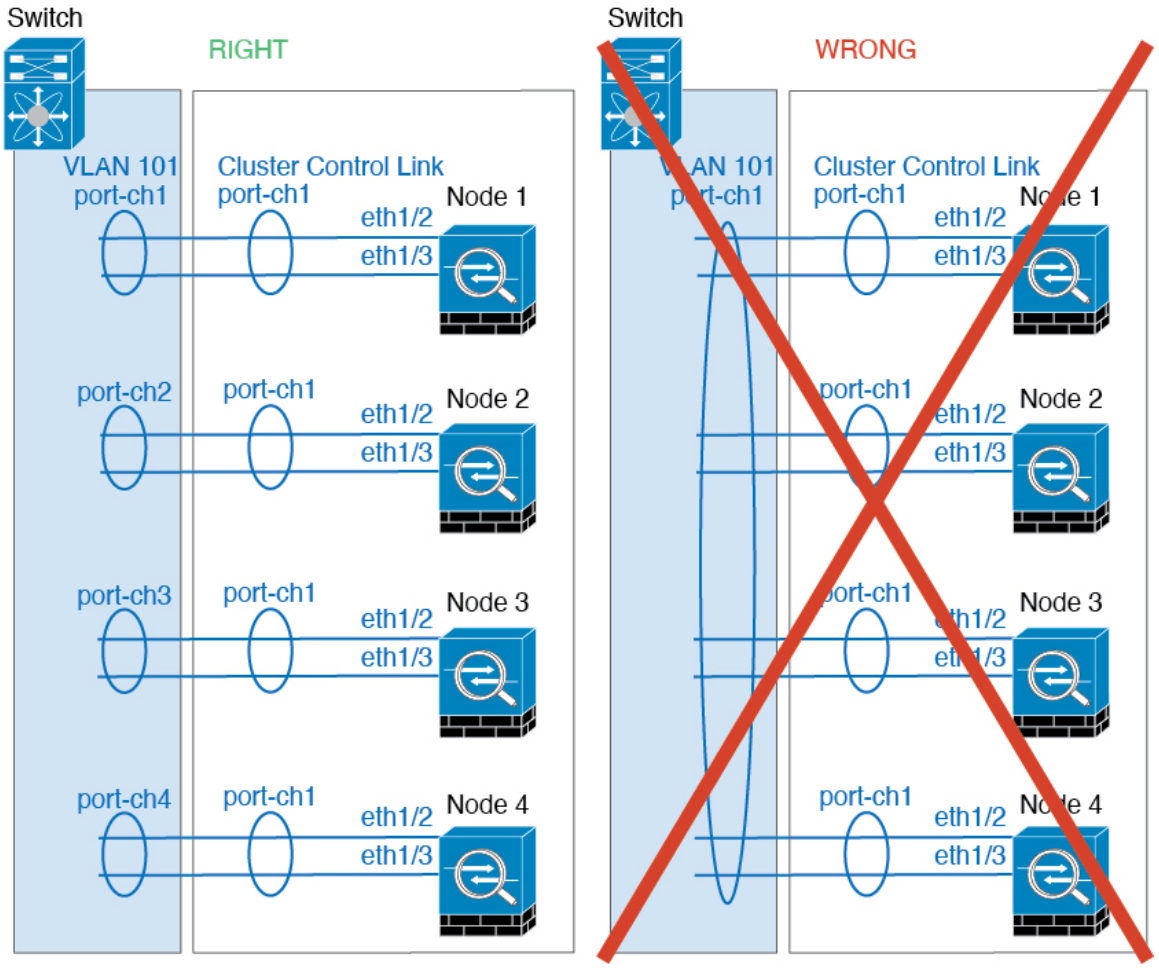
- In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the control unit switch is powered down, then the EtherChannel connected

to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  - Spanned EtherChannels—For cluster unit Spanned EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.



  - Device-local EtherChannels—For cluster unit Device-local EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels on the switch; do not combine multiple cluster unit EtherChannels into one EtherChannel on the switch.



Additional guidelines

- When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the Threat Defense or the switch, adding an additional switch to form a VSS or vPC) you should disable the health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the interface health check feature.
- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang your connection; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel, when the syslog server port is down and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the ASA cluster. These messages can result in some units of the ASA cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a

new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

Defaults for clustering

- The cLACP system ID is auto-generated, and the system priority is 1 by default.
- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Clustering configuration

To add a cluster to the Firewall Management Center, add each node to the Firewall Management Center as a standalone unit, configure interfaces on the unit you want to make the control node, and then form the cluster.

Cluster interfaces

You can configure data interfaces as Spanned EtherChannels.

You can use regular firewall interfaces or IPS-only interfaces (inline sets or passive interfaces).

Each unit must also dedicate at least one hardware interface as the cluster control link.

Cluster control link

A cluster control link is a dedicated hardware interface that enables communication between cluster units and supports cluster operation coordination.

Each unit must dedicate at least one hardware interface as the cluster control link. We recommend using an EtherChannel for the cluster control link if available.

Cluster control link traffic

Cluster control link traffic includes both control and data traffic.

Control traffic includes:

- Control node election.
- Configuration replication.
- Health monitoring.

Data traffic includes:

- State replication.
- Connection ownership queries and data packet forwarding.

Cluster control link interfaces and network

You can use any physical interface or EtherChannel for the cluster control link. You cannot use a VLAN subinterface as the cluster control link. You also cannot use the Management interface.

Each cluster control link has an IP address on the same subnet. This subnet should be isolated from all other traffic, and should include only the cluster control link interfaces.



Note For a 2-member cluster, do not directly connect the cluster control link from one node to the other node. If you directly connect the interfaces, then when one unit fails, the cluster control link fails, and thus the remaining healthy unit fails. If you connect the cluster control link through a switch, then the cluster control link remains up for the healthy unit.

If you need to directly connect the units (for testing purposes, for example), configure and enable the cluster control link interface on both nodes before forming the cluster.

Size the cluster control link

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features.

For example:

- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.



Note If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Cluster control link MTU ping testing

Use Cluster control link MTU ping testing to

- verify MTU compatibility between cluster nodes during the join process
- use ping-based fragmentation tests to confirm the network path supports proper packet handling, and
- allow nodes to join even if tests fail while providing diagnostic messages for troubleshooting MTU mismatches.

When a node joins the cluster, the control node send a ping with a payload size of twice the MTU. This process tests the network's ability to handle packet fragmentation because the underlying IP layer will fragment packets that exceed the MTU limit.

A successful ping confirms that the network path supports proper fragmentation and that the cluster control link can reliably process traffic at the configured MTU size.

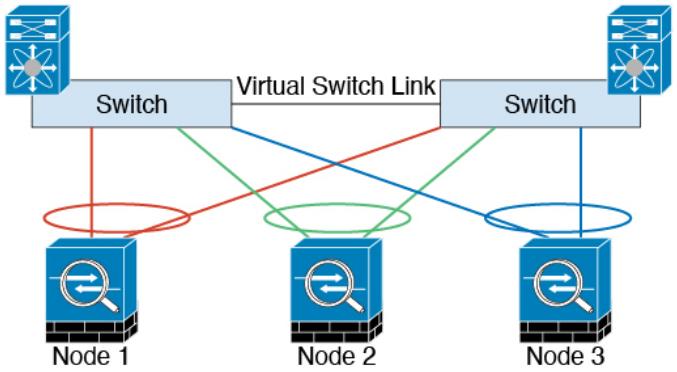
If the ping fails, view these messages:

- **show cluster history**—`Event: CCL MTU test to unit name failed`
- Console WARNING—`WARNING: Unit name is not reachable in CCL jumbo frame ICMP test, please check cluster interface and switch MTU configuration`

Even if the ping fails, the node is allowed to join the cluster. In this case, you need to resolve the MTU mismatch as soon as possible.

Cluster control link redundancy

The diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS), Virtual Port Channel (vPC), StackWise, or StackWise Virtual environment. All links in the EtherChannel are active. When the switch is part of a redundant system, then you can connect firewall interfaces within the same EtherChannel to separate switches in the redundant system. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.



Cluster control link reliability for inter-chassis clustering

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

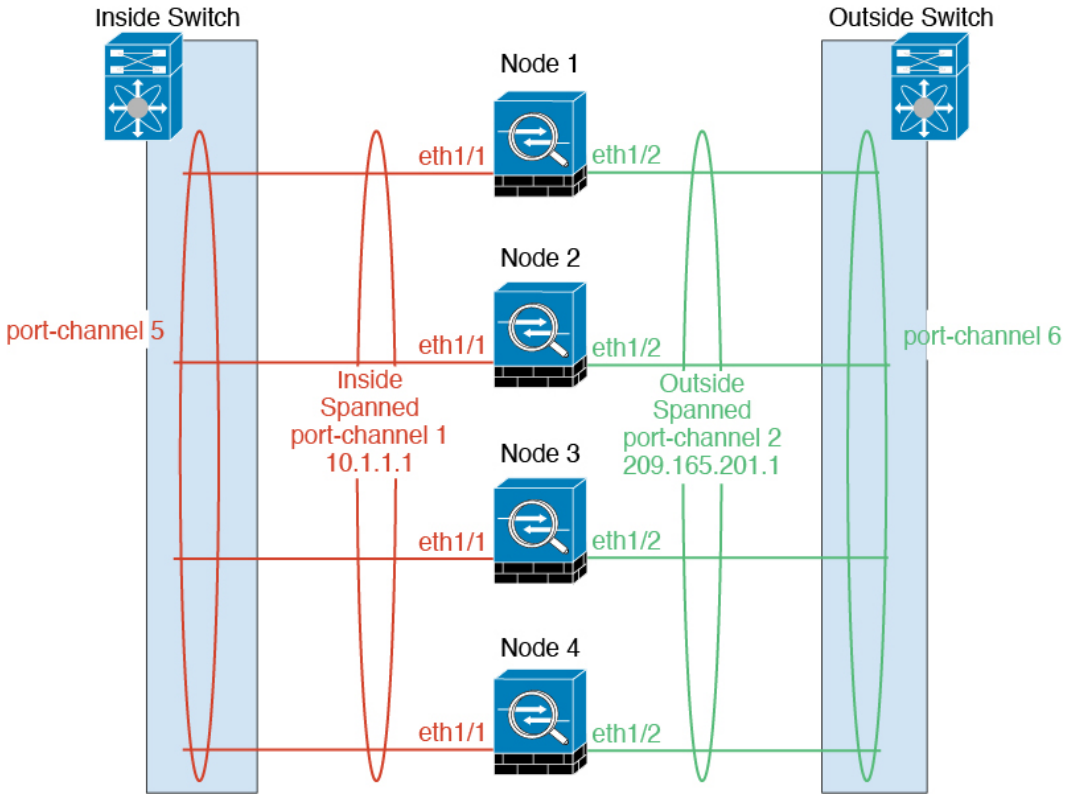
The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Spanned EtherChannels

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel.

For regular firewall interfaces:A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the BVI, not to the bridge group member interface.

The EtherChannel inherently provides load balancing as part of basic operation.



Guidelines for maximum throughput

To achieve maximum throughput, follow these guidelines:

- Use a symmetric load-balancing hash algorithm, meaning that packets from both directions will have the same hash and will be sent to the same Firewall Threat Defense in the Spanned EtherChannel. We recommend using the source and destination IP address (the default) or the source and destination port as the hashing algorithm.
- Use the same type of line cards when connecting the Firewall Threat Defenses to the switch so that hashing algorithms applied to all packets are the same.

Load balancing

The EtherChannel link is selected using a proprietary hash algorithm, based on source or destination IP addresses and TCP and UDP port numbers.

Note On the switch, we recommend that you use one of the following algorithms: **source-dest-IP** or **source-dest-IP-port** (see the Cisco Nexus OS or Cisco IOS **port-channel load-balance** command). Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the nodes in a cluster.

The number of links in the EtherChannel affects load balancing.

Symmetric load balancing is not always possible. If you configure NAT, then forward and return packets will have different IP addresses and/or ports. Return traffic will be sent to a different unit based on the hash, and the cluster will have to redirect most returning traffic to the correct unit.

EtherChannel redundancy

The EtherChannel has built-in redundancy. It monitors the line protocol status of all links. If one link fails, traffic is re-balanced between remaining links. If all links in the EtherChannel fail on a particular unit, but other units are still active, then the unit is removed from the cluster.

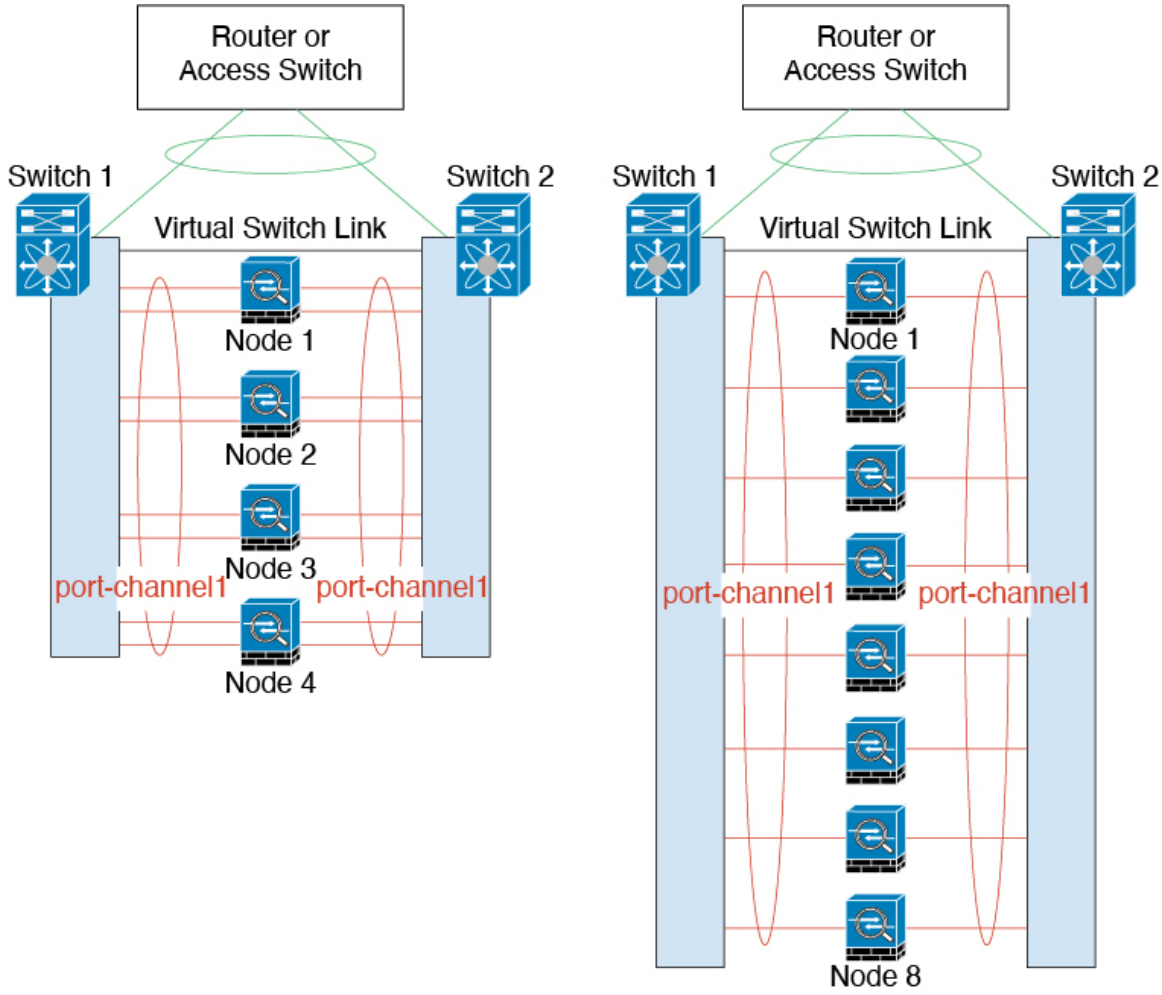
Connecting to a redundant switch system

You can include multiple interfaces per Firewall Threat Defense in the Spanned EtherChannel. Multiple interfaces per Firewall Threat Defense are especially useful for connecting to both switches in a VSS, vPC, StackWise, or StackWise Virtual system.

Depending on your switches, you can configure up to 32 active links in the spanned EtherChannel. This feature requires both switches in the vPC to support EtherChannels with 16 active links each (for example the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module).

For switches that support 8 active links in the EtherChannel, you can configure up to 16 active links in the spanned EtherChannel when connecting to two switches in a redundant system.

This figure shows a 16-active-link spanned EtherChannel in a 4-node cluster and an 8-node cluster.



Cable and add devices to the Firewall Management Center

Before configuring clustering, you need to prepare your devices. In particular, the cluster will not come up unless all nodes can communicate over the cluster control link. Therefore, before you form the cluster, the cluster control link must be ready to go.

Procedure

Step 1 Cable the cluster control link network, management network, and data networks.

Step 2 Configure the upstream and downstream equipment.

a) For the cluster control link network, set the MTU to be at least 100 bytes higher than the data interface MTU.

By default, the data interface MTU is 1500 bytes, so the cluster control link MTU on the cluster node will be set to 1600 bytes. If you use higher MTUs on your data interfaces, increase the cluster control link MTU on connecting switches accordingly.

b) Configure cluster control link interfaces on upstream and downstream equipment, including for an optional EtherChannel.

For more information, refer to Cluster control link interfaces and network, on page 332 for cluster control link requirements.

c) Configure data interfaces on upstream and downstream equipment, including Spanned EtherChannels.

For more information, refer to Cluster interfaces, on page 331 for information about how to cable Spanned EtherChannels.

Step 3 Add each node to the Firewall Management Center as a standalone device in the same domain and group.

For more information, refer to Add a Device Using a Registration Key , on page 32.You can create a cluster with a single device, and then add more nodes later. The initial settings (licensing, access control policy) that you set when you add a device will be inherited by all cluster nodes from the control node. You will choose the control node when forming the cluster.

Step 4 Enable the cluster control link on the device you want to be the control node.

When you add the other nodes, they will inherit the cluster control link configuration.

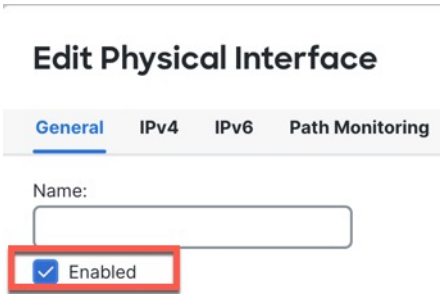
Note Do *not* configure the name or IP addressing for the cluster control link. The MTU of the cluster control link interface is automatically set to 100 bytes more than the highest data interface MTU when you form the cluster, so you do not need to set it now. However, we do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation. If the MTU is set in this range when you add the cluster, we recommend returning to the **Interfaces** page and manually increasing it above 8362. When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, a notification is generated so you can fix the MTU mismatch on connecting switches and try again.

a) On the device you want to be the control node, choose **Devices** > **Device Management**, and click **Edit** ( ).

b) Click **Interfaces**.

c) Enable the interface. If you are going to use an EtherChannel for the cluster control link, enable all members.For more information, refer to Enable the physical interface and configure Ethernet settings, on page 611.

Figure 120: Enable the cluster control link interface



d) (Optional) Add an EtherChannel.For more information, refer to Configure an EtherChannel, on page 619.

We recommend using the On mode for cluster control link member interfaces to reduce unnecessary traffic on the cluster control link (Active mode is the default). The cluster control link does not need the overhead of LACP traffic because it is an isolated, stable network. **Note:** We recommend setting *data* EtherChannels to Active mode.

e) Click **Save** and then **Deploy** to deploy the interface changes to the control node.

Create a Cluster

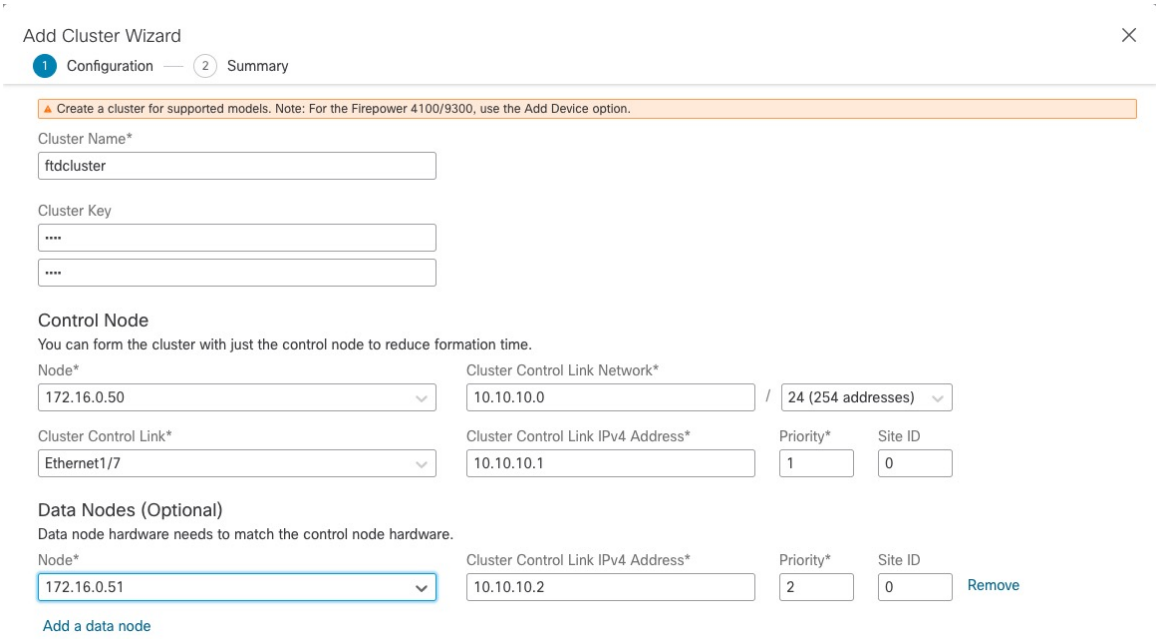
Form a cluster from one or more devices in the Firewall Management Center.

Procedure

Step 1 Choose **Devices** > **Device Management**, and then choose **Add** > **Cluster**.

The **Add Cluster Wizard** appears.

Figure 121: Add Cluster Wizard



Step 2 Specify a **Cluster Name** and an authentication **Cluster Key** for control traffic.

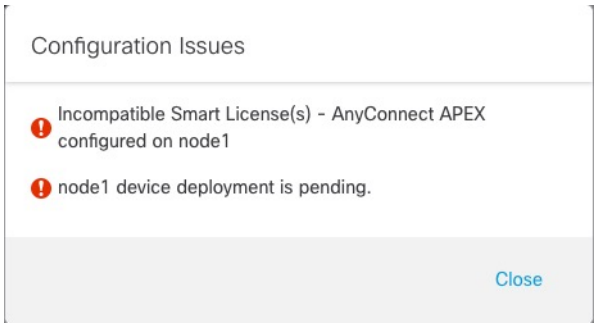
- **Cluster Name**—An ASCII string of 1 to 38 characters. The cluster name can contain only letters, digits, underscores (_), and hyphens (-).
- **Cluster Key**—An ASCII string of 1 to 63 characters. The cluster key cannot be a single digit and must not contain spaces. The **Cluster Key** value is used to generate the encryption key. This encryption does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in clear text.

Step 3 For the **Control Node**, configure these parameters:

- **Node**—Choose the device that you want to be the control node initially. When the Firewall Management Center forms the cluster, it will add this node to the cluster first so it will be the control node.

Note If you see an **Error** ( ) icon next to the node name, click the icon to view configuration issues. You must cancel cluster formation, resolve the issues, and then return to cluster formation. For example:

Figure 122: Configuration Issues



To resolve the above issues, remove the unsupported VPN license and deploy pending configuration changes to the device.

- **Cluster Control Link Network**—Specify an IPv4 subnet; IPv6 is not supported for this interface. Specify a **24**, **25**, **26**, or **27** subnet.
- **Cluster Control Link**—Choose the physical interface or EtherChannel you want to use for the cluster control link.

Note The MTU of the cluster control link interface is automatically set to 100 bytes more than the highest data interface MTU; by default, the MTU is 1600 bytes. We do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation. If the MTU is set in this range when you add the cluster, we recommend increasing the MTU above 8362. Choose **Devices** > **Device Management** and then click **Interfaces**.

Make sure you configure switches connected to the cluster control link to the correct (higher) MTU; otherwise, cluster formation can fail.

- **Cluster Control Link IPv4 Address**—This field will be auto-populated with the first address on the cluster control link network. You can edit the host address if desired.
- **Priority**—Set the priority of this node for control node elections. The priority is between 1 and 100, where 1 is the highest priority. Even if you set the priority to be lower than other nodes, this node will still be the control node when the cluster is first formed.

- **Site ID**—(FlexConfig feature) Enter the site ID for this node between 1 and 8. A value of 0 disables inter-site clustering. Additional inter-site cluster customizations to enhance redundancy and stability, such as director localization, site redundancy, and cluster flow mobility, are only configurable using the FlexConfig feature.

Step 4 For **Data Nodes (Optional)**, click **Add a data node** to add a node to the cluster.

You can form the cluster with only the control node for faster cluster formation, or you can add all nodes now. Set the following for each data node:

- **Node**—Choose the device that you want to add.

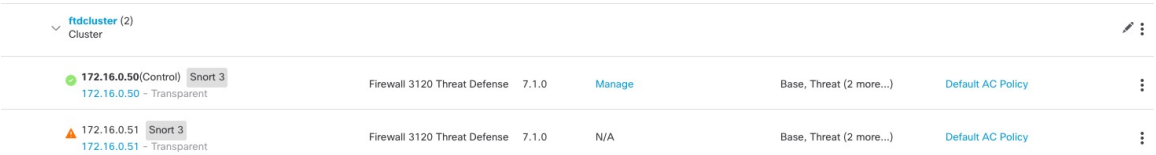
Note If you see an **Error** ( ) icon next to the node name, click the icon to view configuration issues. You must cancel cluster formation, resolve the issues, and then return to cluster formation.

- **Cluster Control Link IPv4 Address**—This field will be auto-populated with the next address on the cluster control link network. You can edit the host address if desired.
- **Priority**—Set the priority of this node for control node elections. The priority is between 1 and 100, where 1 is the highest priority.
- **Site ID**—(FlexConfig feature) Enter the site ID for this node between 1 and 8. A value of 0 disables inter-site clustering. Additional inter-site cluster customizations to enhance redundancy and stability, such as director localization, site redundancy, and cluster flow mobility, are only configurable using the FlexConfig feature.

Step 5 Click **Continue**. Review the **Summary**, and then click **Save**.

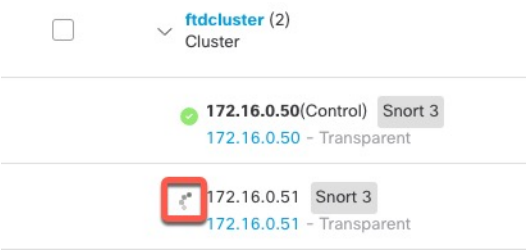
The cluster name shows on the **Devices** > **Device Management** page; expand the cluster to see the cluster nodes.

Figure 123: Cluster Management

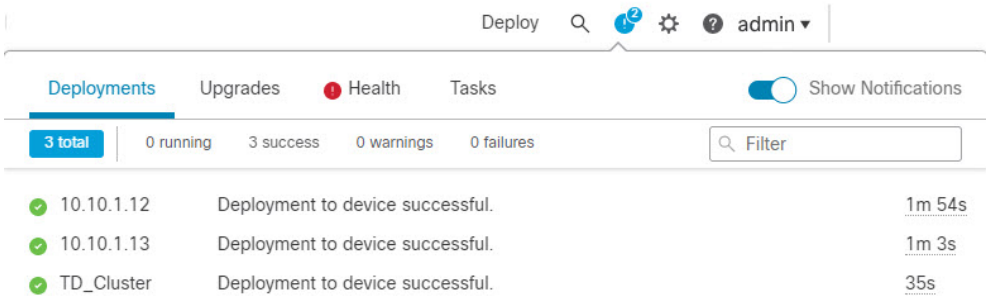


A node that is currently registering shows the loading icon.

Figure 124: Node Registration



You can monitor cluster node registration by clicking the **Notifications** icon and choosing **Tasks**. The Firewall Management Center updates the Cluster Registration task as each node registers.

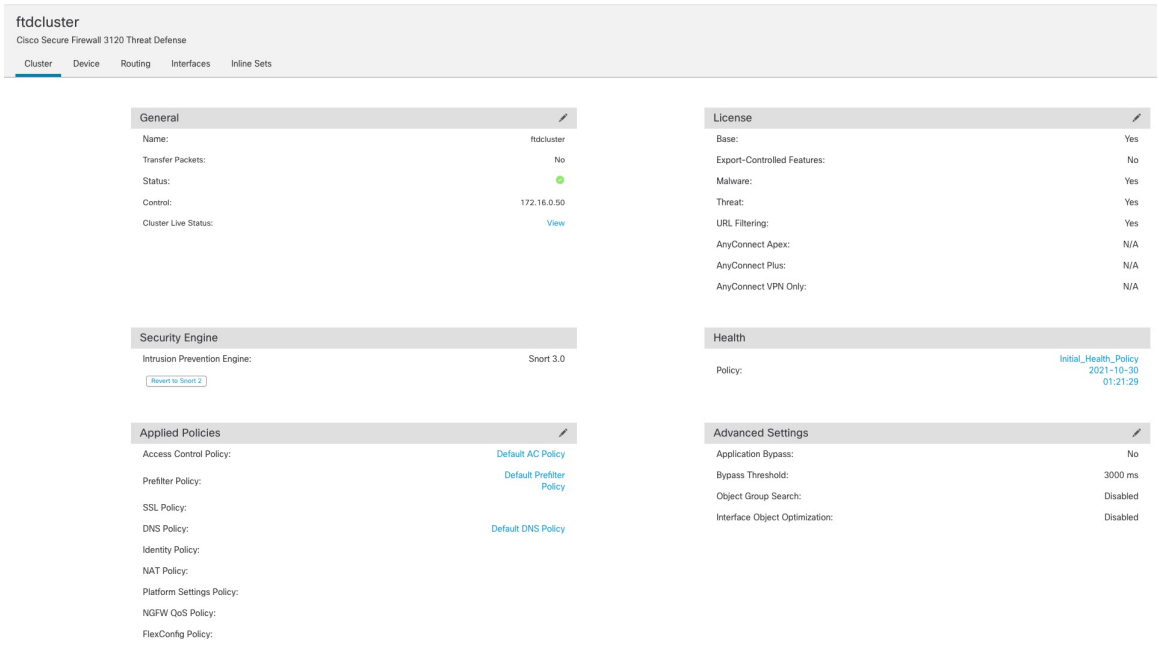


Step 6 Configure device-specific settings by clicking the **Edit** (✎) for the cluster.

Most configuration can be applied to the cluster as a whole, and not nodes in the cluster. For example, you can change the display name per node, but you can only configure interfaces for the whole cluster.

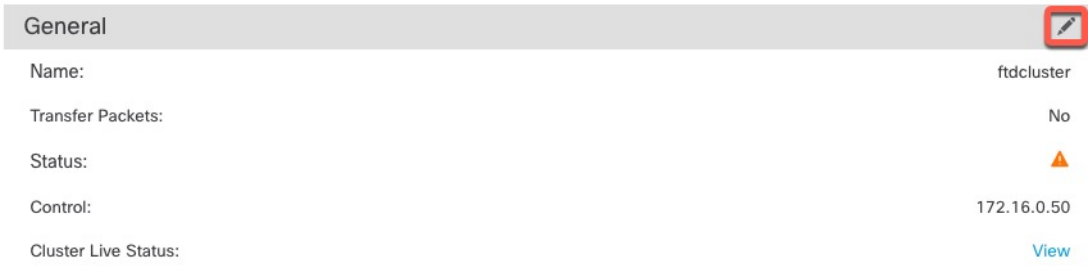
Step 7 On the **Devices** > **Device Management** and then choose **Add**, **Cluster** screen, you see **General** and other settings for the cluster.

Figure 125: Cluster Settings

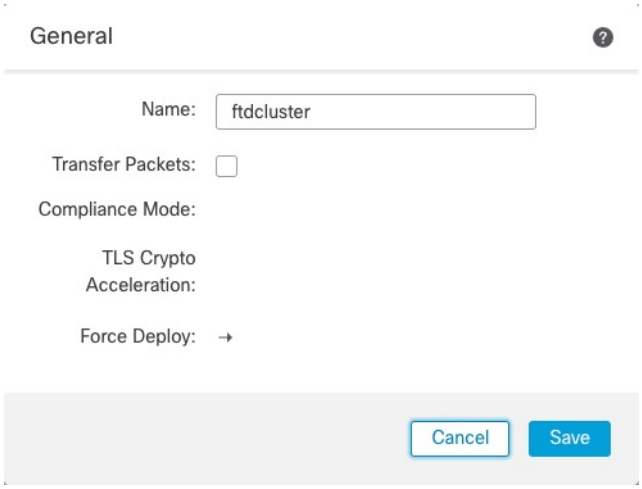


See these cluster-specific items in the **General** area:

- **General** > **Name**—Change the cluster display name by clicking the **Edit** (✎).



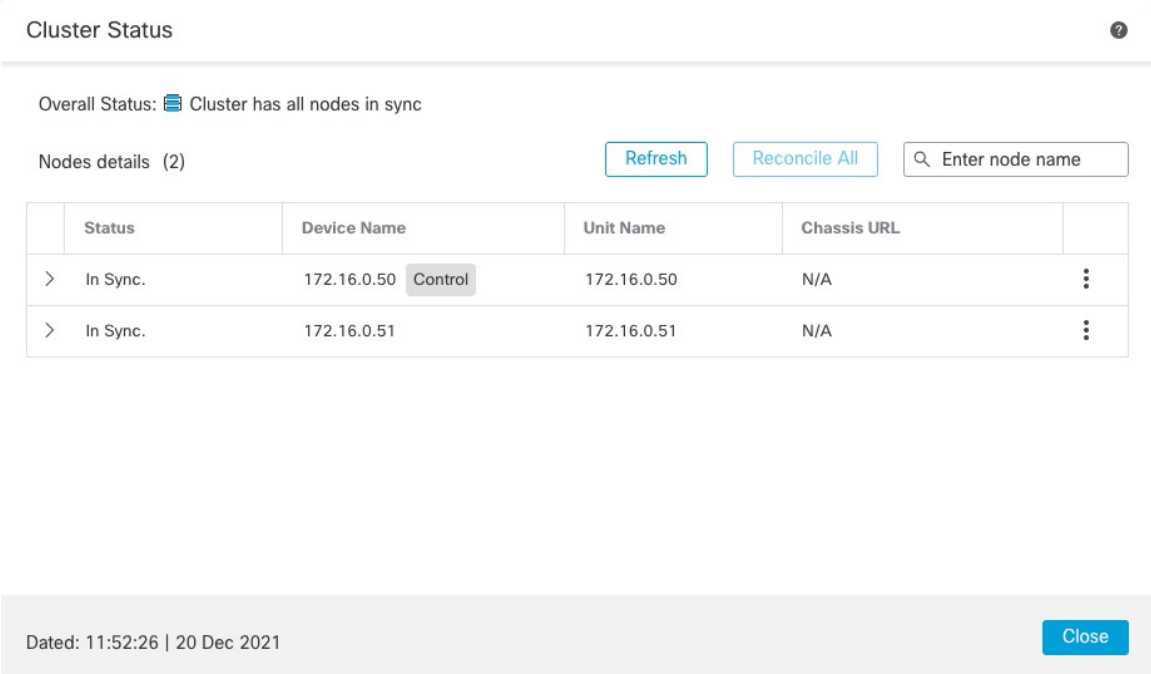
Then set the **Name** field.



- **General > Cluster Live Status**—Click the **View** link to open the **Cluster Status** dialog box.

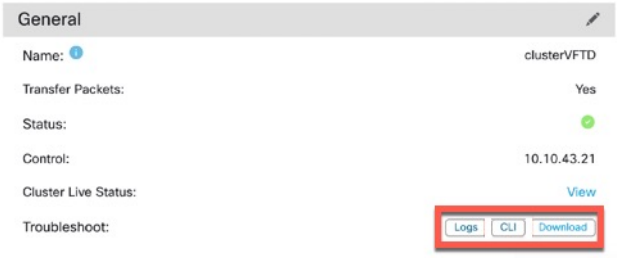


The **Cluster Status** dialog box also lets you retry data unit registration by clicking **Reconcile All**. You can also ping the cluster control link from a node. Refer Perform a ping on the cluster control link, on page 367.



- **General > Troubleshoot**—You can generate and download troubleshooting logs, and you can view cluster CLIs. Refer Troubleshoot the cluster, on page 365 .

Figure 126: Troubleshoot



Step 8 On the **Devices** > **Device Management** and then choose **Add**, **Device**, you can choose each member in the cluster from the top right drop-down menu and configure these settings.

Figure 127: Device Settings

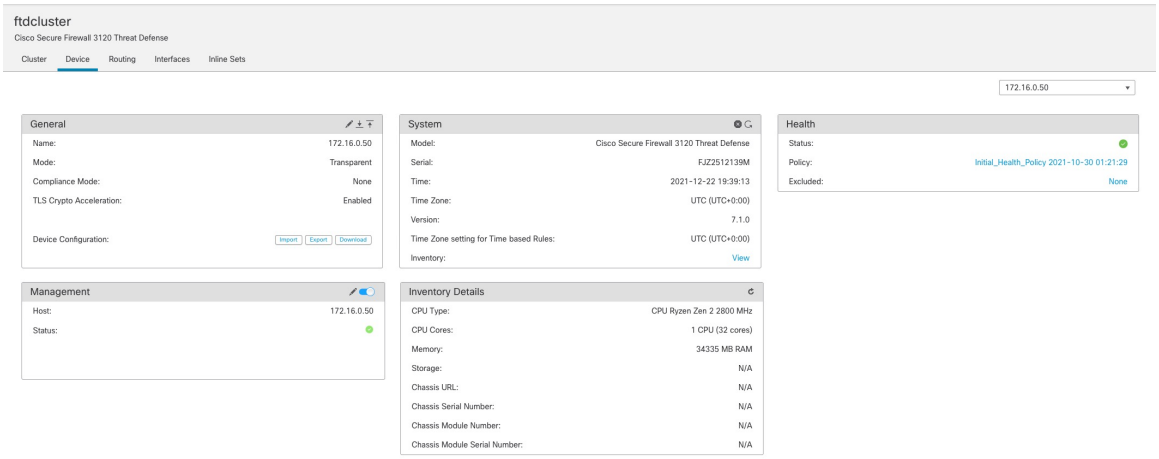
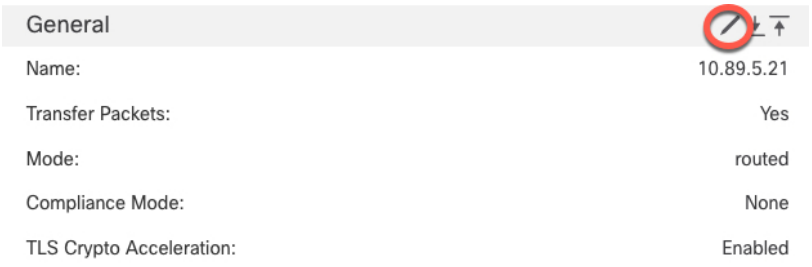


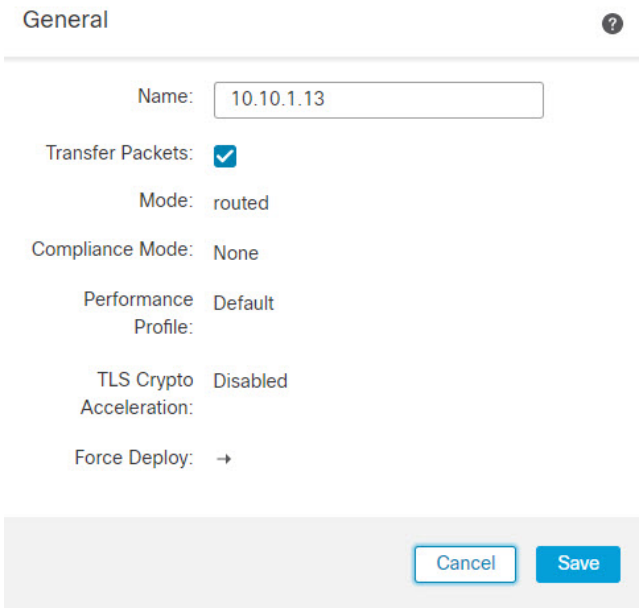
Figure 128: Choose Node



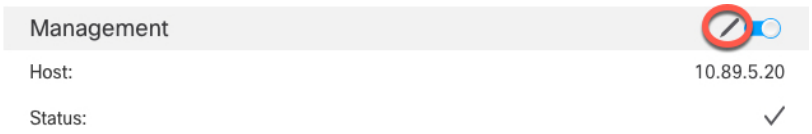
- **General > Name**—Change the cluster member display name by clicking the **Edit** ( ) .



Then set the **Name** field.



- **Management > Host** —If you change the management IP address in the device configuration, you must match the new address in the Firewall Management Center so that it can reach the device on the network. First disable the connection, edit the **Host** address in the **Management** area, then re-enable the connection.



Configure interfaces

Configure interfaces to enable proper cluster communication and operation.

Configure data interfaces as Spanned EtherChannels.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** ( ) next to the cluster.

Step 2 Click **Interfaces**.

Step 3 Configure Spanned EtherChannel data interfaces.

a) Configure one or more EtherChannels. See Configure an EtherChannel, on page 619.

You can include one or more member interfaces in the EtherChannel. Because this EtherChannel is spanned across all of the nodes, you only need one member interface per node; however, for greater throughput and redundancy, multiple members are recommended.

b) (Optional) For regular firewall interfaces, configure VLAN subinterfaces on the EtherChannel. The rest of this procedure applies to the subinterfaces. See Add a subinterface, on page 669.

c) Click **Edit** ( ) for the EtherChannel interface.

d) Configure the name and other parameters. For regular firewall interfaces, see Configure routed mode interfaces, on page 690 or, for transparent mode, Bridge group interfaces, on page 695. For IPS-only interfaces, see Inline Sets and Passive Interfaces, on page 727.

- If the cluster control link interface MTU is not at least 100 bytes higher than the data interface MTU, you will see an error that you must reduce the MTU of the data interface. By default, the cluster control link MTU is 1600 bytes. If you want to increase the MTU of data interfaces, first increase the cluster control link MTU. Note that we do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.
- For routed mode, DHCP, PPPoE, IPv6 autoconfig and manual link-local addresses are not supported. For point-to-point connections, you can specify a 31-bit subnet mask (255.255.255.254). In this case, no IP addresses are reserved for the network or broadcast addresses.

e) Set a unique, manual global MAC address for the EtherChannel. Click **Advanced**, and in the **Active MAC Address** field, enter a MAC address in H.H.H format, where H is a 16-bit hexadecimal digit.

For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.

Do not set the **Standby MAC Address**; it is ignored.

You must configure a unique MAC address not currently in use on your network for a Spanned EtherChannel to avoid potential network connectivity problems. With a manually-configured MAC address, the MAC address stays with the current control unit. If you do not configure a MAC address, then if the control unit changes, the new control unit uses a new MAC address for the interface, which can cause a temporary network outage.

f) Click **OK**. Repeat the above steps for other data interfaces.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure cluster health monitor settings

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings described in the table below.

Figure 129: Cluster Health Monitor Settings

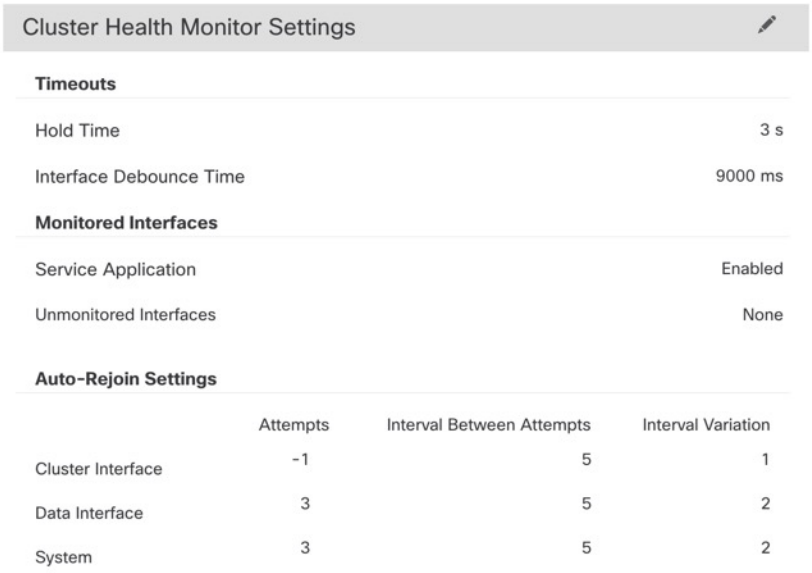


Table 27: Cluster Health Monitor Settings Section Table Fields

Field	Description
Timeouts	
Hold Time	Between .3 and 45 seconds; The default is 3 seconds. To determine node system health, the cluster nodes send heartbeat messages on the cluster control link to other nodes. If a node does not receive any heartbeat messages from a peer node within the hold time period, the peer node is considered unresponsive or dead.
Interface Debounce Time	Between 300 and 9000 ms. The default is 500 ms. The interface debounce time is the amount of time before the node considers an interface to be failed, and the node is removed from the cluster.
Monitored Interfaces	The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The amount of time before the node removes a member from the cluster depends on the type of interface and whether the node is an established node or is joining the cluster.
Service Application	Shows whether the Snort and disk-full processes are monitored.
Unmonitored Interfaces	Shows unmonitored interfaces.
Auto-Rejoin Settings	
Cluster Interface	Shows the auto-rejoin settings after a cluster control link failure.

Field	Description
Attempts	Between -1 and 65535. The default is -1 (unlimited). Sets the number of rejoin attempts.
Interval Between Attempts	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
Interval Variation	Between 1 and 3. The default is 1x the interval duration. Defines if the interval duration increases at each attempt.
Data Interfaces	Shows the auto-rejoin settings after a data interface failure.
Attempts	Between -1 and 65535. The default is 3. Sets the number of rejoin attempts.
Interval Between Attempts	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
Interval Variation	Between 1 and 3. The default is 2x the interval duration. Defines if the interval duration increases at each attempt.
System	Shows the auto-rejoin settings after internal errors. Internal failures include: application sync timeout; inconsistent application statuses; and so on.
Attempts	Between -1 and 65535. The default is 3. Sets the number of rejoin attempts.
Interval Between Attempts	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
Interval Variation	Between 1 and 3. The default is 2x the interval duration. Defines if the interval duration increases at each attempt.

Note If you disable the system health check, fields that do not apply when the system health check is disabled will not show.

You can change these settings from this section.

You can monitor any port-channel ID, single physical interface ID, as well as the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored.

Procedure

Step 1 Choose **Devices** > **Device Management**.

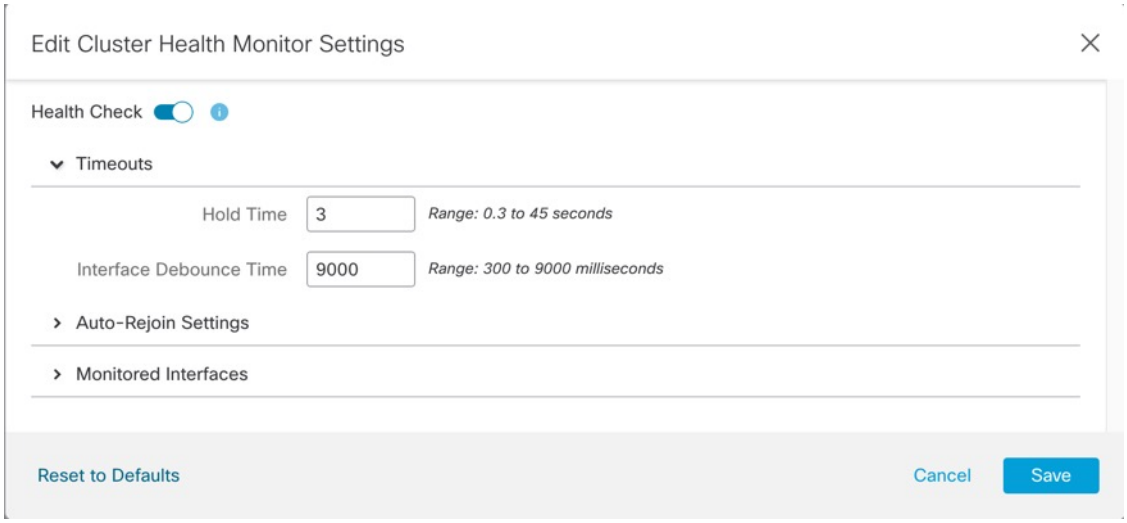
Step 2 Next to the cluster you want to modify, click **Edit** ( ).

Step 3 Click **Cluster**.

Step 4 In the **Cluster Health Monitor Settings** section, click **Edit** ( ).

Step 5 Disable the system health check by clicking the **Health Check** slider .

Figure 130: Disable the System Health Check



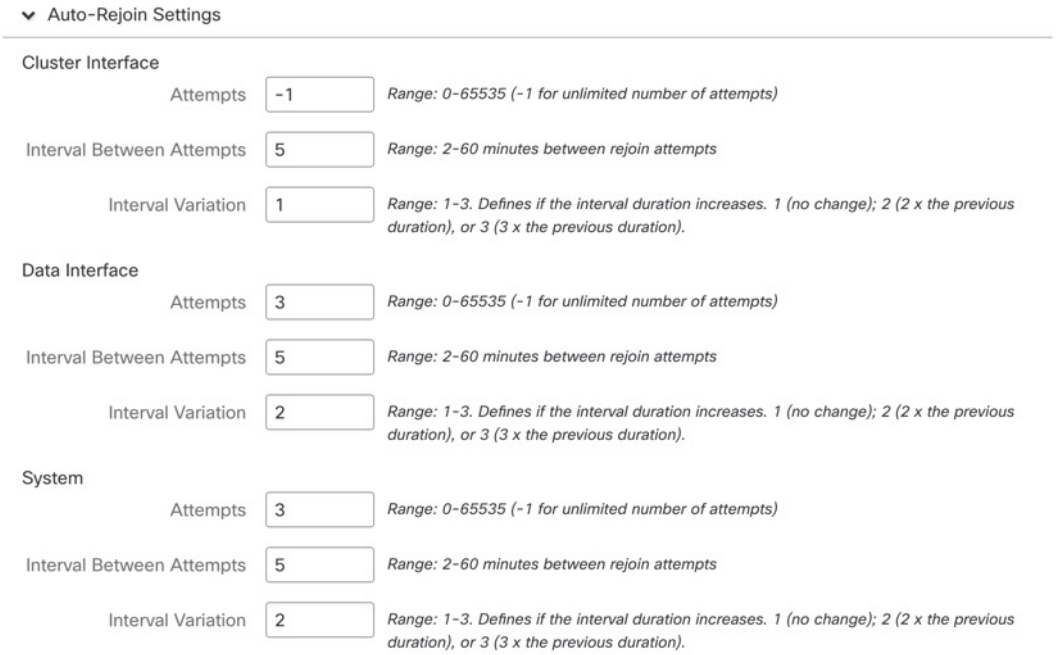
When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between .3 and 45 seconds; The default is 3 seconds.
- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the number of milliseconds specified before marking the interface as failed, and the node is removed from the cluster. In the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster node just because another cluster node was faster at bundling the ports.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 131: Configure Auto-Rejoin Settings

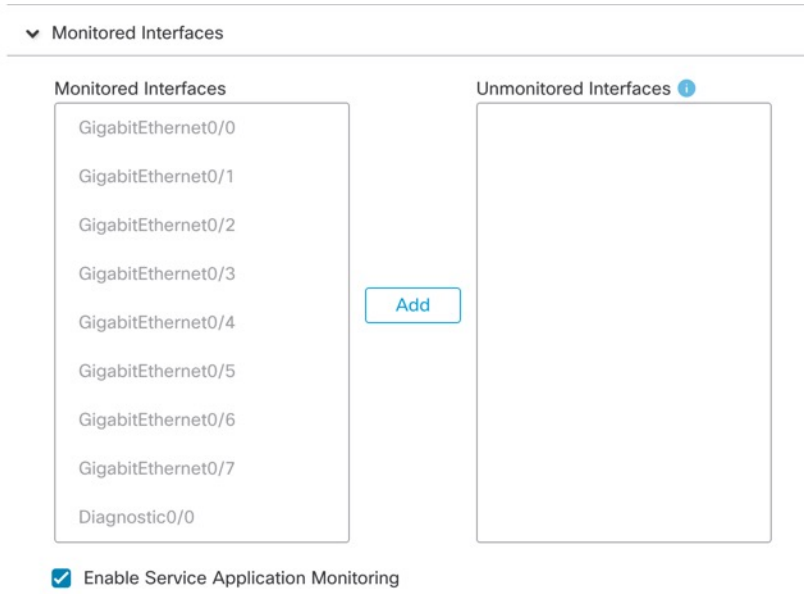


Set the following values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8 Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 132: Configure Monitored Interfaces



The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The amount of time before the node removes a member from the cluster depends on the type of interface and whether the node is an established node or is joining the cluster. Health check is enabled by default for all interfaces and for the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save** and deploy the configuration changes.

Cluster node management

After you deploy the cluster, you can change the configuration and manage cluster nodes.

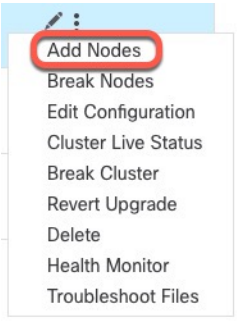
Add a new cluster node

You can add one or more new cluster nodes to an existing cluster.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster, and choose **Add Nodes**.

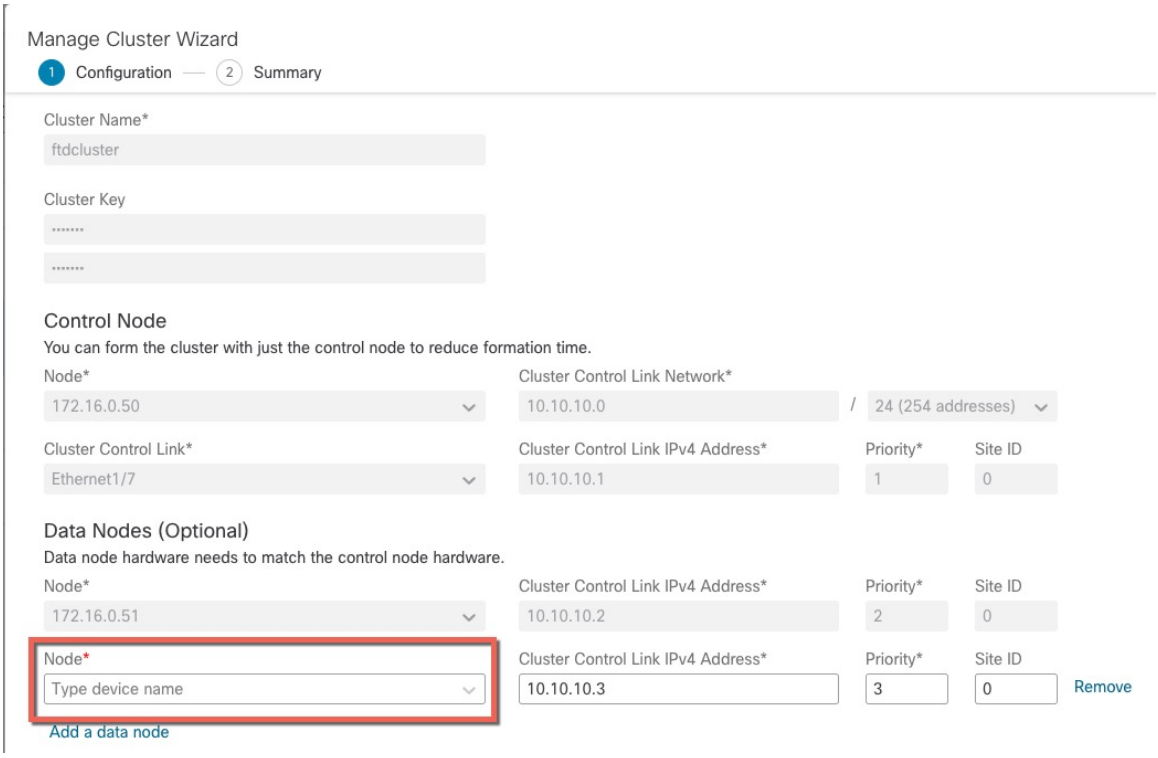
Figure 133: Add nodes



The **Manage Cluster Wizard** appears.

Step 2 From the **Node** menu, choose a device, adjust the IP address, priority, and Site ID if desired.

Figure 134: Manage cluster wizard

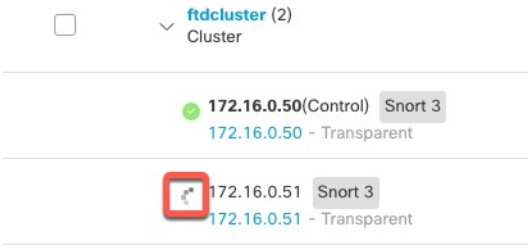


Step 3 To add additional nodes, click **Add a data node**.

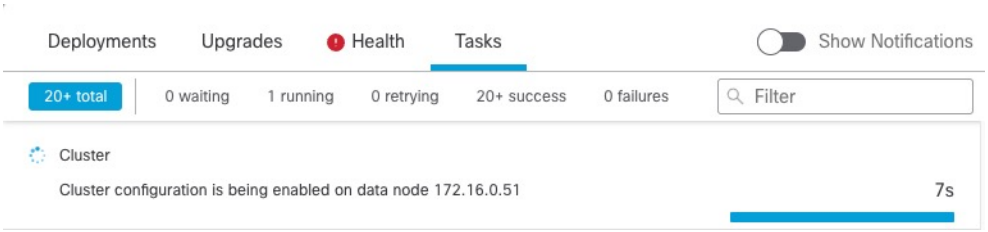
Step 4 Click **Continue**. Review the **Summary**, and then click **Save**

The node that is currently registering shows the loading icon.

Figure 135: Node registration



You can monitor cluster node registration by clicking the **Notifications** icon and choosing **Tasks**.



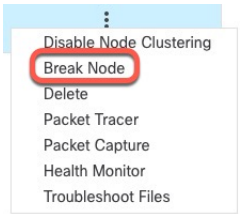
Break a node

You can remove a node from the cluster so that it becomes a standalone device. You cannot break the control node unless you break the entire cluster. The data node has its configuration erased.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the node you want to break, and choose **Break Node**.

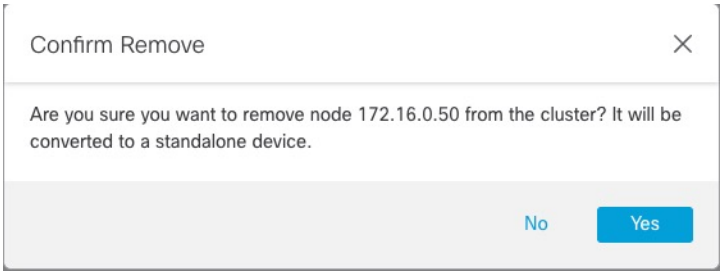
Figure 136: Break a node



You can optionally break one or more nodes from the cluster More menu by choosing **Break Nodes**.

Step 2 You are prompted to confirm the break; click **Yes**.

Figure 137: Confirm break



You can monitor the cluster node break by clicking the **Notifications** icon and choosing **Tasks**.

Break the cluster

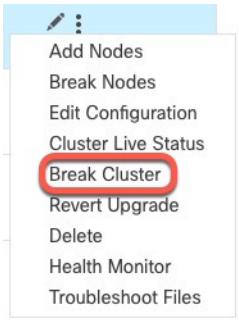
You can break the cluster and convert all nodes to standalone devices. The control node retains the interface and security policy configuration, while data nodes have their configuration erased.

Procedure

Step 1 Make sure all cluster nodes are being managed by the Firewall Management Center by reconciling nodes. For more information, refer to Reconcile cluster nodes, on page 358.

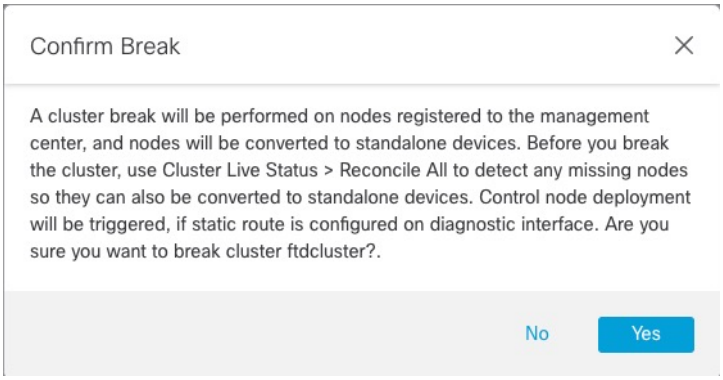
Step 2 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster, and choose **Break Cluster**.

Figure 138: Break cluster



Step 3 You are prompted to break the cluster; click **Yes**.

Figure 139: Confirm break



You can monitor the cluster break by clicking the **Notifications** icon and choosing **Tasks**.

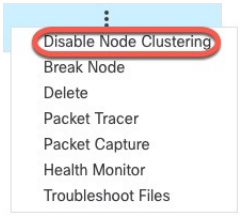
Disable clustering

You may want to deactivate a node in preparation for deleting the node, or temporarily for maintenance. This procedure is meant to temporarily deactivate a node; the node will still appear in the Firewall Management Center device list. When a node becomes inactive, all data interfaces are shut down.

Procedure

Step 1 For the unit you want to disable, choose **Devices** > **Device Management**, click **More** (⋮), and choose **Disable Node Clustering**.

Figure 140: Disable clustering



If you disable clustering on the control node, one of the data nodes will become the new control node. Note that for centralized features, if you force a control node change, then all connections are dropped, and you have to re-establish the connections on the new control node. You cannot disable clustering on the control node if it is the only node in the cluster.

Step 2 Confirm that you want to disable clustering on the node.

The node will show **(Disabled)** next to its name in the **Devices** > **Device Management** list.

Step 3 To reenable clustering, refer Rejoin the cluster, on page 356.

Rejoin the cluster

If a node was removed from the cluster, for example for a failed interface or if you manually disabled clustering, you must manually rejoin the cluster. Make sure the failure is resolved before you try to rejoin the cluster. Refer Rejoin the cluster, on page 378 for more information about why a node can be removed from a cluster.

Procedure

Step 1 For the unit you want to reactivate, choose **Devices** > **Device Management**, click **More** (⋮), and choose **Enable Node Clustering**.

Step 2 Confirm that you want to enable clustering on the unit.

Change the control node

Use this procedure when you need to specify the exact unit you want to become the control node. For centralized features, forcing a control node change will drop all connections, requiring you to re-establish the connections on the new control node.



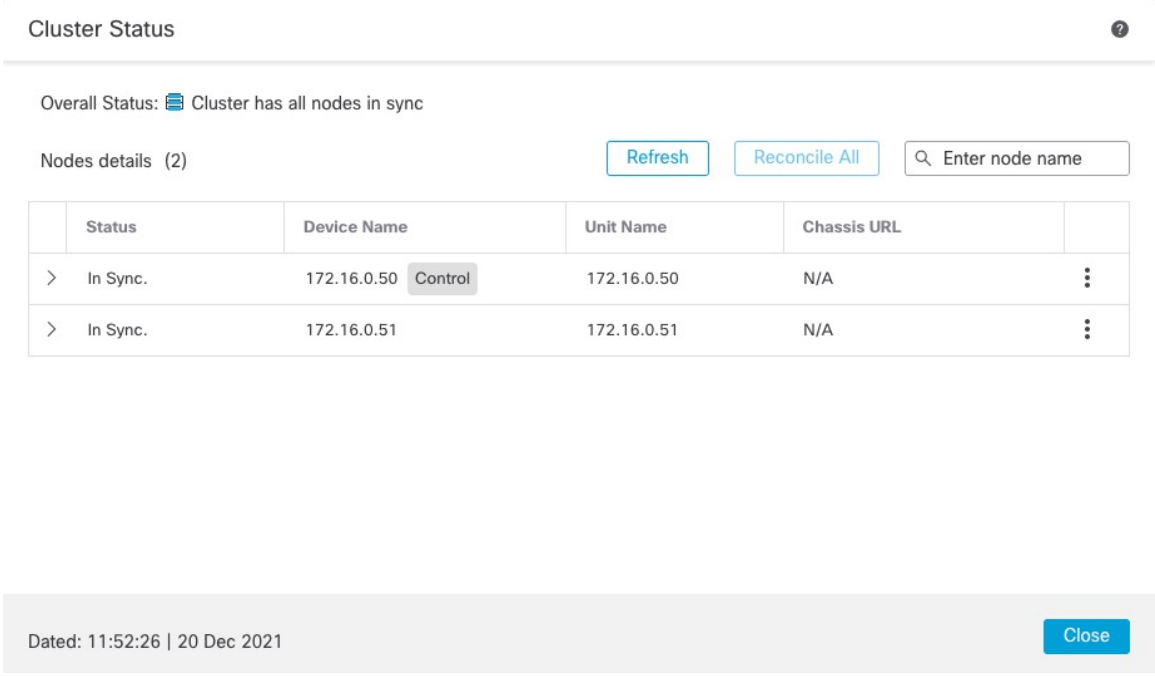
Caution The best method to change the control node is to disable clustering on the control node, wait for a new control election, and then re-enable clustering. If you must specify the *exact* unit you want to become the control node, use the procedure in this section. Note that for centralized features, if you force a control node change using either method, then all connections are dropped, and you have to re-establish the connections on the new control node.

Follow these steps to change the control node:

Procedure

Step 1 Open the **Cluster Status** dialog box by choosing **Devices** > **Device Management More** (⋮) **Cluster Live Status**.

Figure 141: Cluster status



Step 2 For the unit you want to become the control unit, choose **More** (⋮) **Change Role to Control**.

Step 3 You are prompted to confirm the role change. Check the check box, and click **OK**.

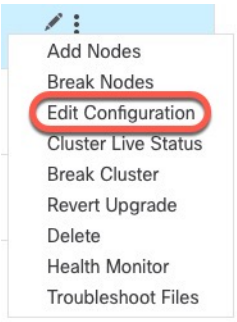
Edit the cluster configuration

You can edit the cluster configuration. If you change the cluster key, cluster control link interface, or cluster control link network, the cluster will be broken and reformed automatically. Until the cluster is reformed, you may experience traffic disruption. If you change the cluster control link IP address for a node, node priority, or site ID, only the affected nodes are broken and readded to the cluster.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster, and choose **Edit Configuration**.

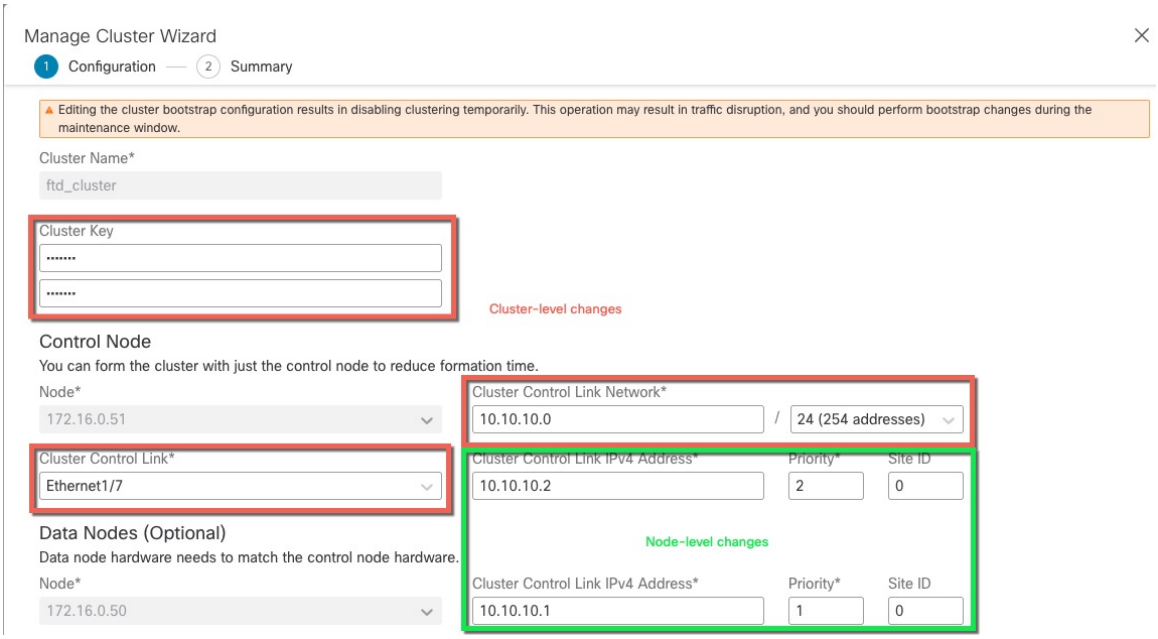
Figure 142: Edit configuration



The **Manage Cluster Wizard** appears.

Step 2 Update the cluster configuration.

Figure 143: Manage cluster wizard



If the cluster control link is an EtherChannel, you can edit the interface membership and LACP configuration by clicking **Edit** (✎) next to the interface drop-down menu.

Step 3 Click **Continue**. Review the **Summary**, and then click **Save**

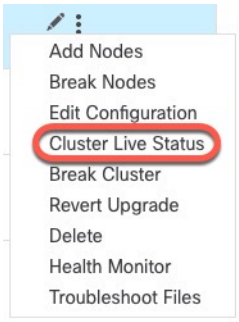
Reconcile cluster nodes

If a cluster node fails to register, you can reconcile the cluster membership from the device to the Firewall Management Center. For example, a data node might fail to register if the Firewall Management Center is occupied with certain processes, or if there is a network issue.

Procedure

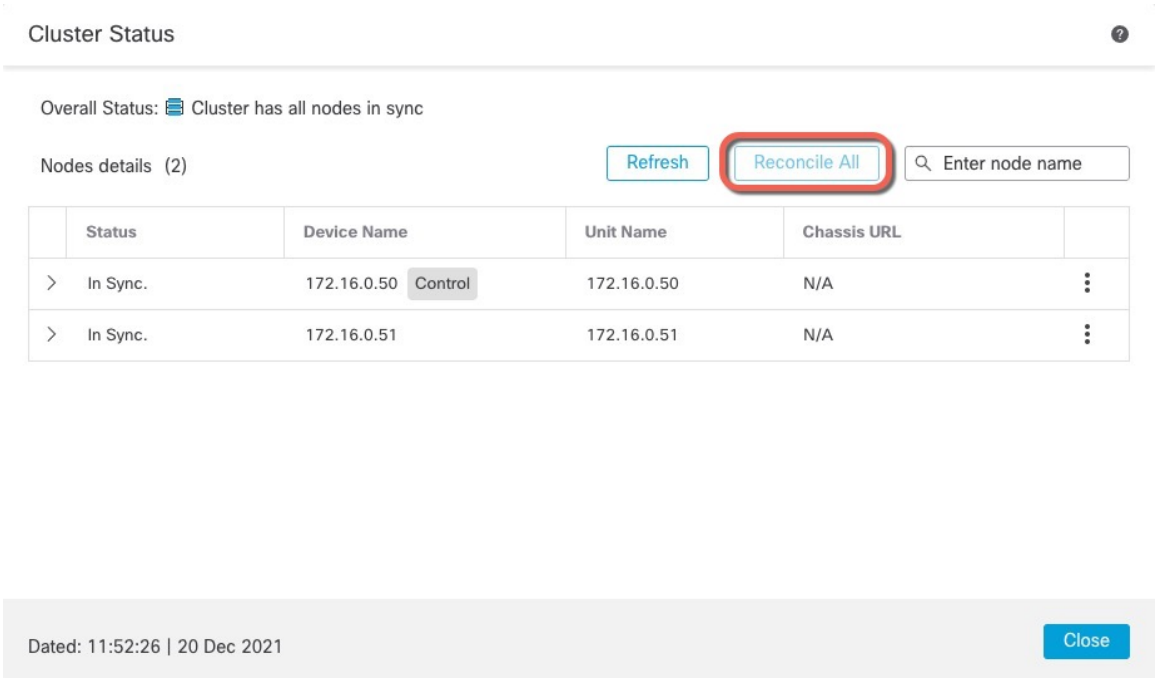
Step 1 Choose **Devices** > **Device Management More** (⋮) for the cluster, and then choose **Cluster Live Status** to open the **Cluster Status** dialog box.

Figure 144: Cluster live status



Step 2 Click **Reconcile All**.

Figure 145: Reconcile all



For more information about the cluster status, refer to Monitor the cluster, on page 361.

Delete (Unregister) the Cluster or Nodes and Register to a New Firewall Management Center

You can unregister the cluster from the Firewall Management Center, which keeps the cluster intact. You might want to unregister the cluster if you want to add the cluster to a new Firewall Management Center.

You can also unregister a node from the Firewall Management Center without breaking the node from the cluster. Although the node is not visible in the Firewall Management Center, it is still part of the cluster, and it will continue to pass traffic and could even become the control node. You cannot unregister the current control node. You might want to unregister the node if it is no longer reachable from the Firewall Management Center, but you still want to keep it as part of the cluster while you troubleshoot management connectivity.

Unregistering a cluster:

- Severs all communication between the Firewall Management Center and the cluster.
- Removes the cluster from the **Device Management** page.
- Returns the cluster to local time management if the cluster's platform settings policy is configured to receive time from the Firewall Management Center using NTP.
- Leaves the configuration intact, so the cluster continues to process traffic.

  Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.

Registering the cluster again to the same or a different Firewall Management Center causes the configuration to be removed, so the cluster will stop processing traffic at that point; the cluster configuration remains intact so you can add the cluster as a whole. You can choose an access control policy at registration, but you will have to re-apply other policies after registration and then deploy the configuration before it will process traffic again.

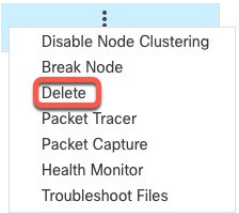
Before you begin

This procedure requires CLI access to one of the nodes.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster or node, and choose **Delete**.

Figure 146: Delete cluster or node



Step 2 You are prompted to delete the cluster or node; click **Yes**.

Step 3 You can register the cluster to a new (or the same) Firewall Management Center by adding one of the cluster members as a new device.

You only need to add one of the cluster nodes as a device, and the rest of the cluster nodes will be discovered.

a) Connect to one cluster node's CLI, and identify the new Firewall Management Center using the **configure manager add** command. See Modify Firewall Threat Defense management interface settings at the CLI , on page 763.
b) Choose **Devices** > **Device Management**, and then click **Add** > **Device**.

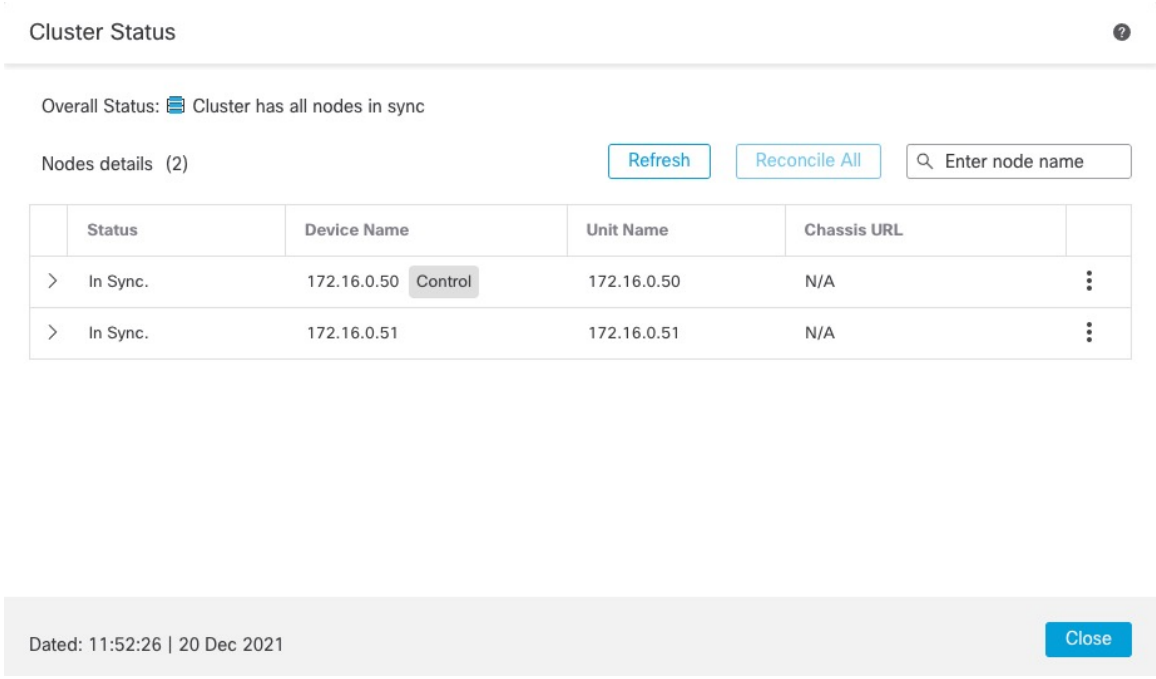
Step 4 To re-add an unregistered node, refer to Reconcile cluster nodes, on page 358.

Monitor the cluster

You can monitor the cluster in the Firewall Management Center and at the Firewall Threat Defense CLI.

- **Cluster Status** dialog box, which is available from the **Devices** > **Device Management More** (⋮) icon or from the **Devices** > **Device Management** > **Cluster** page **General** area **Cluster Live Status** link.

Figure 147: Cluster status



The Control node has a graphic indicator identifying its role.

Cluster member **Status** includes these states:

- **In Sync**—The node is registered with the Firewall Management Center.
- **Pending Registration**—The node is part of the cluster, but has not yet registered with the Firewall Management Center. If a node fails to register, you can retry registration by clicking **Reconcile All**.
- **Clustering is disabled**—The node is registered with the Firewall Management Center, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the node from the cluster.

- **Joining cluster**—The node is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the Firewall Management Center.

For each node, you can view the **Summary** or the **History**.

Figure 148: Node summary

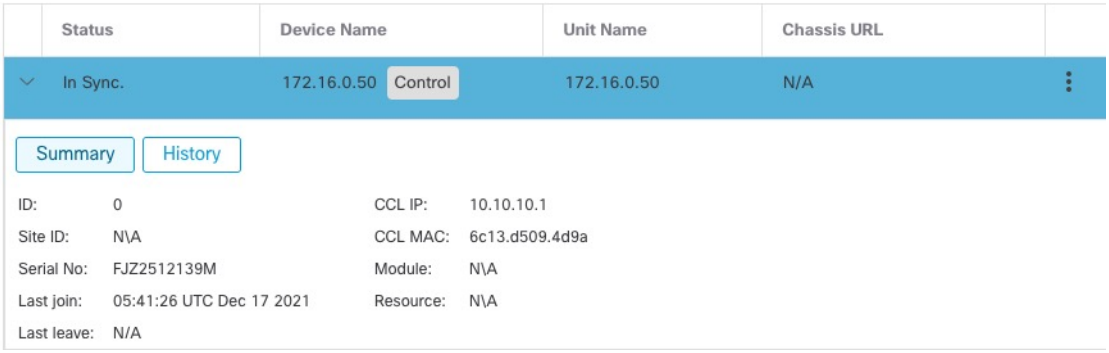
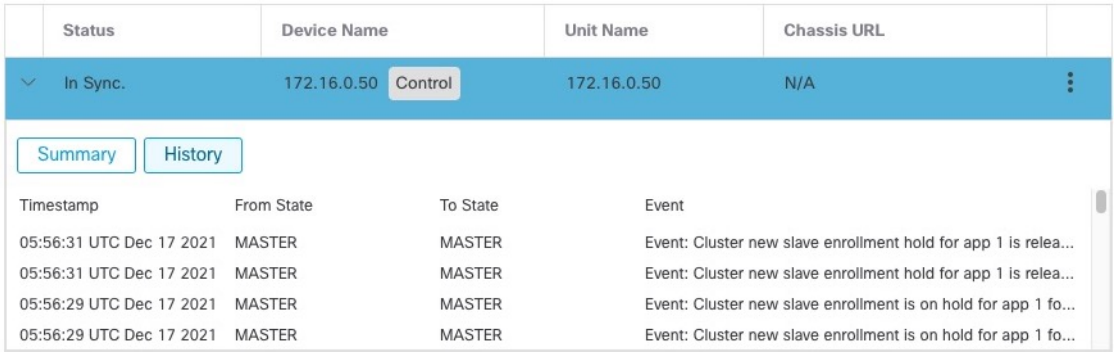


Figure 149: Node history



- **System** (⚙) > **Tasks** page.

  The **Tasks** page shows updates of the Cluster Registration task as each node registers.

- **Devices** > **Device Management***cluster_name*.

  When you expand the cluster on the devices listing page, you can see all member nodes, including the control node shown with its role next to the IP address. For nodes that are still registering, you can see the loading icon.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  To view aggregated data for the entire cluster or other information, use the **show cluster** command.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  To view cluster information, use the **show cluster info** command.

Cluster health monitor dashboard

The cluster health monitor dashboard provides visibility into cluster status, metrics, and statistics.

View cluster health

The cluster health monitor provides a detailed view of the health status of a cluster and its nodes. This cluster health monitor provides health status and trends of the cluster in an array of dashboards.

Before you begin

- You must be an Admin, Maintenance, or Security Analyst user to perform this procedure.
- Ensure you have created a cluster from one or more devices in the Firewall Management Center.

Procedure

	Command or Action	Purpose
Step 1	Choose **System** (⚙) > **Health** > **Monitor**.	Use the Monitoring navigation pane to access node-specific health monitors.
Step 2	In the device list, click **Expand**(>) and **Collapse** (⌄) to expand and collapse the list of managed cluster devices.	
Step 3	To view the cluster health statistics, click on the cluster name. The cluster monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:	• Overview— Highlights key metrics from the other predefined dashboards, including its nodes, CPU, memory, input and output rates, connection statistics, and NAT translation information. • Load Distribution— Traffic and packet distribution across the cluster nodes. • Member Performance— Node-level statistics on CPU usage, memory usage, input throughput, output throughput, active connection, and NAT translation. • CCL— Interface status and aggregate traffic statistics. You can navigate through the various metrics dashboards by clicking on the labels. For a comprehensive list of the supported cluster metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.
Step 4	You can configure the time range from the drop-down in the upper-right corner. The time range can reflect a period as short as the last hour (the default) or as long as two weeks.	Click the refresh icon to set auto refresh to 5 minutes or to toggle off auto refresh.

	Command or Action	Purpose
	Select **Custom** from the drop-down to configure a custom start and end date.	
Step 5	Click on deployment icon for a deployment overlay on the trend graph, with respect to the selected time range.	The deployment icon indicates the number of deployments during the selected time-range. A vertical band indicates the deployment start and end time. For multiple deployments, multiple bands/lines appear. Click on the icon on top of the dotted line to view the deployment details.
Step 6	(For node-specific health monitor) View the **Health Alerts** for the node in the alert notification at the top of page, directly to the right of the device name.	Hover your pointer over the **Health Alerts** to view the health summary of the node. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.
Step 7	(For node-specific health monitor) The device monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:	• Overview — Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information. • CPU — CPU utilization, including the CPU usage by process and by physical cores. • Memory — Device memory utilization, including data plane and Snort memory usage. • Interfaces — Interface status and aggregate traffic statistics. • Connections — Connection statistics (such as elephant flows, active connections, peak connections, and so on) and NAT translation counts. • Snort — Statistics that are related to the Snort process. • ASP drops — Statistics related to the dropped packets against various reasons. You can navigate through the various metrics dashboards by clicking on the labels. For more information, refer to Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

	Command or Action	Purpose
Step 8	Click the plus sign **Add New Dashboard**(+) in the upper right corner of the health monitor to create a custom dashboard by building your own variable set from the available metric groups.	For cluster-wide dashboard, choose Cluster metric group, and then choose the metric.

Cluster metrics

The cluster health monitor tracks statistics that are related to a cluster and its nodes, and aggregate of load distribution, performance, and CCL traffic statistics.

Table 28: Cluster metrics

Metric	Description	Format
CPU	Average of CPU metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Memory	Average of memory metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Data Throughput	Incoming and outgoing data traffic statistics for a cluster.	bytes
CCL Throughput	Incoming and outgoing CCL traffic statistics for a cluster.	bytes
Connections	Count of active connections in a cluster.	number
NAT Translations	Count of NAT translations for a cluster.	number
Distribution	Connection distribution count in the cluster for every second.	number
Packets	Packet distribution count in the cluster for every second.	number

Troubleshoot the cluster

Use these methods to troubleshoot the devices and clusters:

- Use **Logs** to generates troubleshooting files for all nodes in the cluster. Use this option when you need one cluster-level collection instead of generating troubleshooting files from each node separately.
- Use **CLI** to run a predefined set of cluster diagnostic commands and displays the output. Use this option to check cluster configuration, member state, cluster health, control-plane transport statistics, packet drops, interface status, CPU usage, memory buffers, ARP entries, and reachability. The **CLI** option displays command output; it does not open an interactive CLI session.

Commands
show running-config cluster: Review the cluster group configuration, local unit, cluster interface, priority, health-check, auto-rejoin, and cLACP settings.
show cluster info: Confirm that clustering is enabled and identify the control node, member state, software version, serial number, CCL IP address, CCL MAC address, and last join or leave state.
show cluster info health: Check unit, interface, service, and overall cluster health.
show cluster info transport cp: Review control-plane transport counters, including reliable and unreliable message counters, errors, retransmits, drops, and buffer conditions.
show version: Capture platform, software, build, UUID, LSP, VDB, uptime, resource, and license context.
show asp drop: Identify accelerated security path packet or flow drop reasons and counters.
show counters: Review protocol, feature, and cluster CCL counters.
show arp: Verify ARP entries for interfaces that participate in cluster communication.
show int ip brief: Check interface IP addresses and administrative and line protocol status.
show blocks: Check buffer availability and failed allocations.
show cpu detailed: Check data path, control point, and total CPU usage.
show interface *ccl_interface*: Review interface state, MTU, MAC address, IP address, traffic counters, errors, and drops for the cluster-related interface.
ping *ccl_ip* **size** *ccl_mtu* **repeat 2**: Test reachability to a cluster peer by using the packet size selected by the tool.

- Use the **CCL Ping** when you need to test cluster control link connectivity between joined cluster nodes.
- Troubleshooting files—If a node fails to join the cluster, a troubleshooting file is automatically generated. You can also generate and download troubleshooting files from the **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area. For more information, refer to Generate troubleshooting files, on page 745.

  You can also generate files from the **Device Management** page. Click **More** (⋮) and choose **Troubleshoot Files**.
- CLI output—Choose **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area, you can view a set of pre-defined CLI outputs that can help you troubleshoot the cluster. These commands are automatically run for the cluster:

  You can also enter any **show** command in the **Command** field.

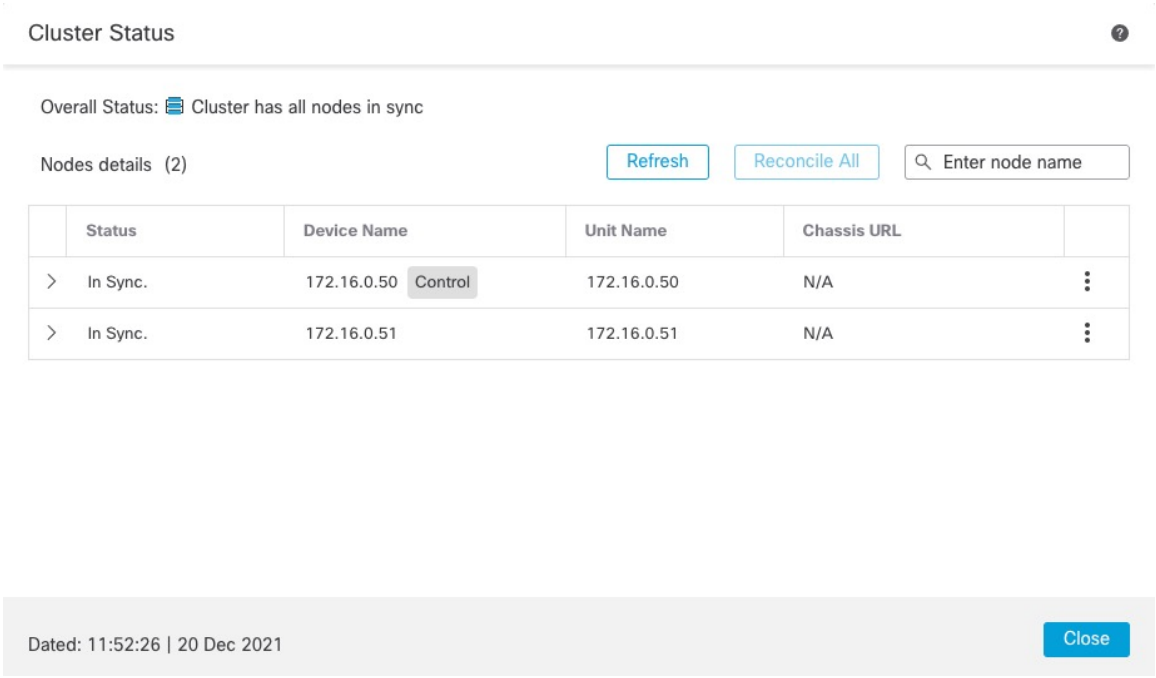
Perform a ping on the cluster control link

You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs.

Procedure

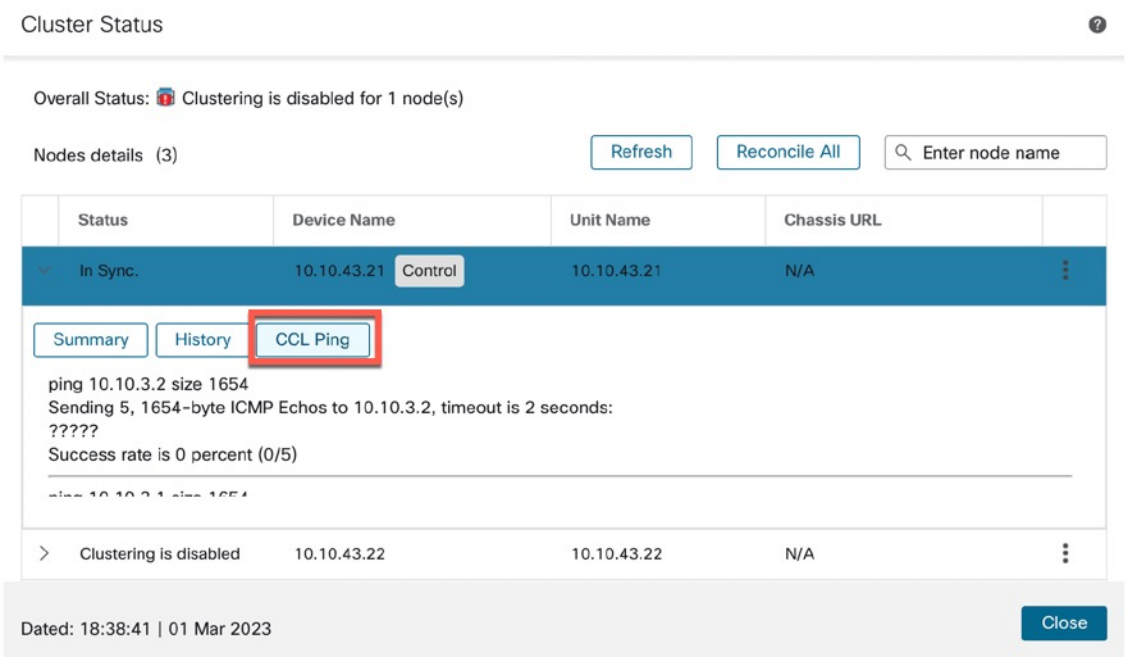
Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) icon next to the cluster, and choose **Cluster Live Status**.

Figure 150: Cluster status



Step 2 Expand one of the nodes, and click **CCL Ping**.

Figure 151: CCL ping



The node sends a ping on the cluster control link to every other node using a packet size that matches the maximum MTU.

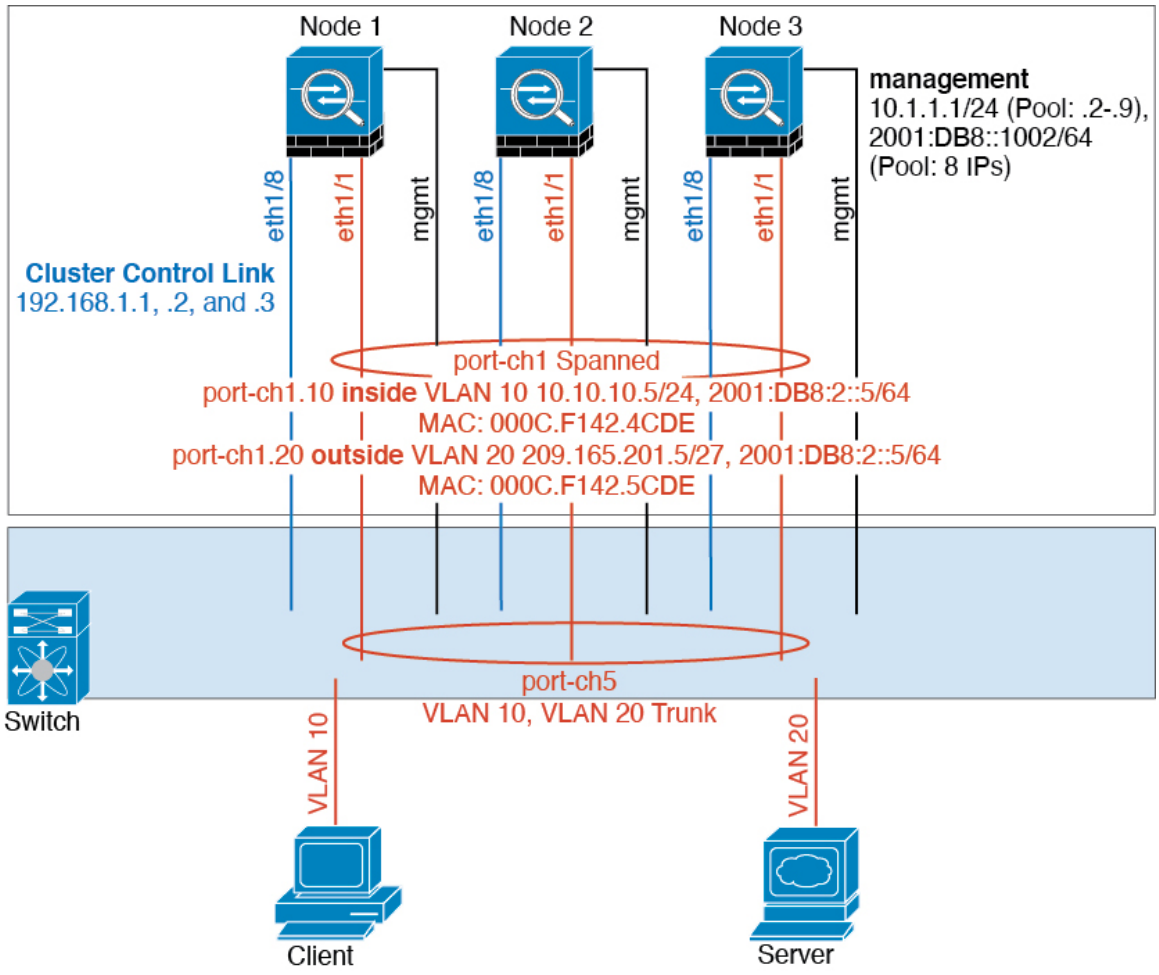
Clustering examples

These examples include examples for typical deployments.

Firewall on a stick

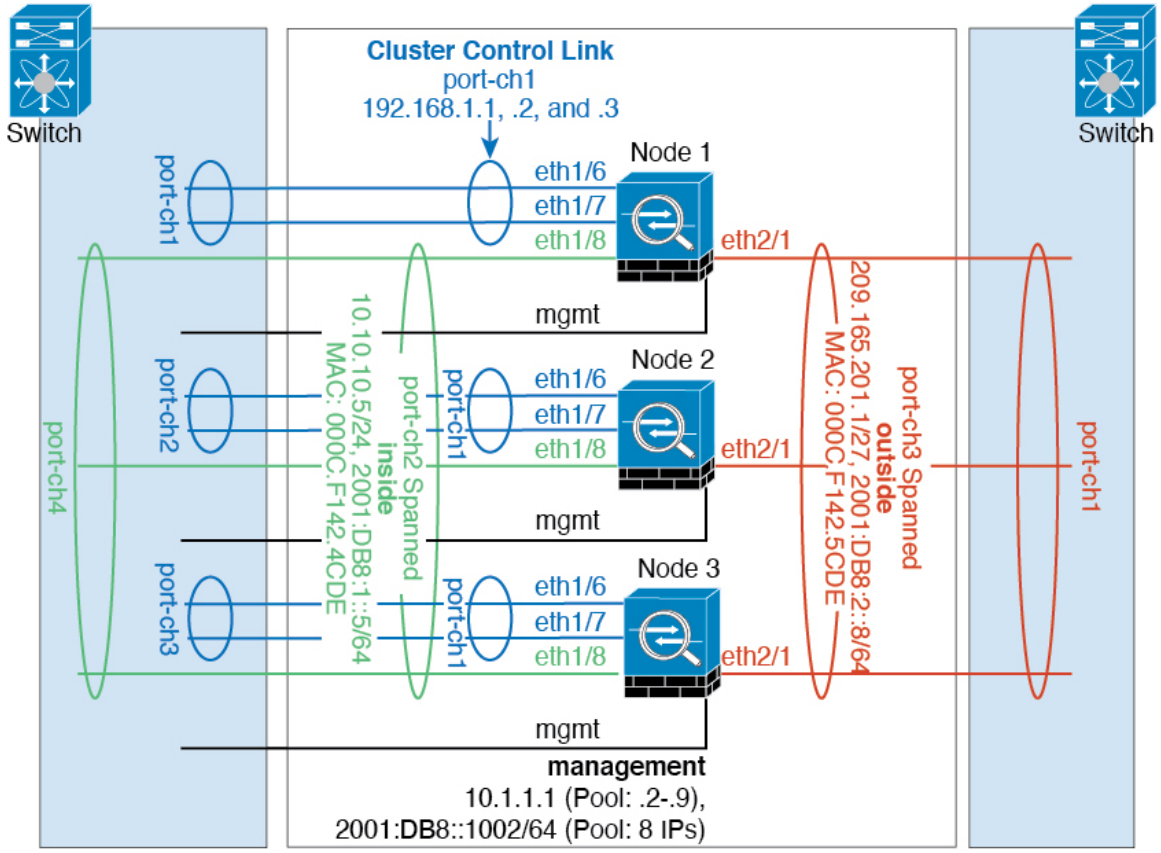
Data traffic from different security domains are associated with different VLANs. For example, VLAN 10 for the inside network and VLAN 20 for the outside network. Each Threat Defense has a single physical port connected to the external switch or router. Trunking is enabled so that all packets on the physical link are 802.1q encapsulated. The Threat Defense is the firewall between VLAN 10 and VLAN 20.

When using Spanned EtherChannels, all data links are grouped into one EtherChannel on the switch side. If the Threat Defense becomes unavailable, the switch will rebalance traffic between the remaining units.



Traffic segregation

You may prefer physical separation of traffic between the inside and outside network.



As shown in the diagram above, there is one Spanned EtherChannel on the left side that connects to the inside switch, and the other on the right side to outside switch. You can also create VLAN subinterfaces on each EtherChannel if desired.

Reference for Clustering

This section includes more information about how clustering operates.

Firewall Threat Defense features and clustering

Some Firewall Threat Defense features are not supported with clustering, and some are only supported on the control unit. Other features might have caveats for proper usage.

Unsupported features with clustering

These features cannot be configured with clustering enabled, and the commands will be rejected.

Note To view FlexConfig features that are also not supported with clustering, for example WCCP inspection, refer to the ASA general operations configuration guide. FlexConfig lets you configure many ASA features that are not present in the Firewall Management Center GUI. For more information, refer to FlexConfig policies, on page 921.

- Remote access VPN (SSL VPN and IPsec VPN)
- DHCP client, server, and proxy. DHCP relay is supported.
- Virtual Tunnel Interfaces (VTIs)
- High Availability
- Integrated Routing and Bridging
- Firewall Management Center UCAPL/CC mode
- DHCP client, server, and proxy. DHCP relay is supported.

Centralized features for clustering

These features are only supported on the control node, and are not scaled for the cluster.

Note Traffic for centralized features is forwarded from member nodes to the control node over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-control nodes before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the control node.

For centralized features, if the control node fails, all connections are dropped, and you have to re-establish the connections on the new control node.

Note To view FlexConfig features that are also centralized with clustering, for example RADIUS inspection, refer to the ASA general operations configuration guide. FlexConfig lets you configure many ASA features that are not present in the Firewall Management Center GUI. For more information, refer to FlexConfig policies, on page 921.

- These application inspections are supported:
  - DCERPC and ESMTP
  - NetBIOS and PPTP
  - RSH
  - SQLNET and SUNRPC
  - TFTP

- XDMCP

- Static route monitoring
- Site-to-site VPN
- IGMP multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- PIM multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- Dynamic routing

Connection settings and clustering

Connection limits are enforced cluster-wide. Each node has an estimate of the cluster-wide counter values based on broadcast messages. Due to efficiency considerations, the configured connection limit across the cluster might not be enforced exactly at the limit number. Each node may overestimate or underestimate the cluster-wide counter value at any given time. However, the information will get updated over time in a load-balanced cluster.

FTP and Clustering

- If FTP data channel and control channel flows are owned by different cluster members, then the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

NAT and clustering

NAT can impact the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different devices in the cluster because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When a packet arrives at the device that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link.

Note that the receiving node does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

Guidelines for NAT and clustering

General guidelines for NAT and clustering

- NAT pool address distribution for dynamic PAT—When you configure a PAT pool, the cluster divides each IP address in the pool into port blocks. By default, each block is 512 ports, but if you configure port block allocation rules, your block setting is used instead. These blocks are distributed evenly among the nodes in the cluster, so that each node has one or more blocks for each IP address in the PAT pool. Thus, you could have as few as one IP address in a PAT pool for a cluster, if that is sufficient for the number of PAT'ed connections you expect. Port blocks cover the 1024-65535 port range, unless you configure the option to include the reserved ports, 1-1023, on the PAT pool NAT rule.
- Reusing a PAT pool in multiple rules—To use the same PAT pool in multiple rules, you must be careful about the interface selection in the rules. You must either use specific interfaces in all rules, or "any" in all rules. You cannot mix specific interfaces and "any" across the rules, or the system might not be able

to match return traffic to the right node in the cluster. Using unique PAT pools per rule is the most reliable option.

- Dynamic NAT xlates managed by the control node—The control node maintains and replicates the xlate table to data nodes. When a data node receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the control node. The data node owns the connection.
- Stale xlates—The xlate idle time on the connection owner does not get updated. Thus, the idle time might exceed the idle timeout. An idle timer value higher than the configured timeout with a refcnt of 0 is an indication of a stale xlate.
- If you have an extremely large number of NAT rules, over ten thousand, you should enable the transactional commit model using the **asp rule-engine transactional-commit nat** command in the device CLI. Otherwise, the node might not be able to join the cluster.

PAT with port block allocation guidelines

- Maximum-per-host limit is not a cluster-wide limit, and is enforced on each node individually. Thus, in a 3-node cluster with the maximum-per-host limit configured as 1, if the traffic from a host is load-balanced across all 3 nodes, then it can get allocated 3 blocks with 1 in each node.
- Port blocks created on the backup node from the backup pools are not accounted for when enforcing the maximum-per-host limit.
- On-the-fly PAT rule modifications, where the PAT pool is modified with a completely new range of IP addresses, will result in xlate backup creation failures for the xlate backup requests that were still in transit while the new pool became effective. This behavior is not specific to the port block allocation feature, and is a transient PAT pool issue seen only in cluster deployments where the pool is distributed and traffic is load-balanced across the cluster nodes.
- When operating in a cluster, you cannot simply change the block allocation size. The new size is effective only after you reload each device in the cluster. To avoid having to reload each device, we recommend that you delete all block allocation rules and clear all xlates related to those rules. You can then change the block size and recreate the block allocation rules.

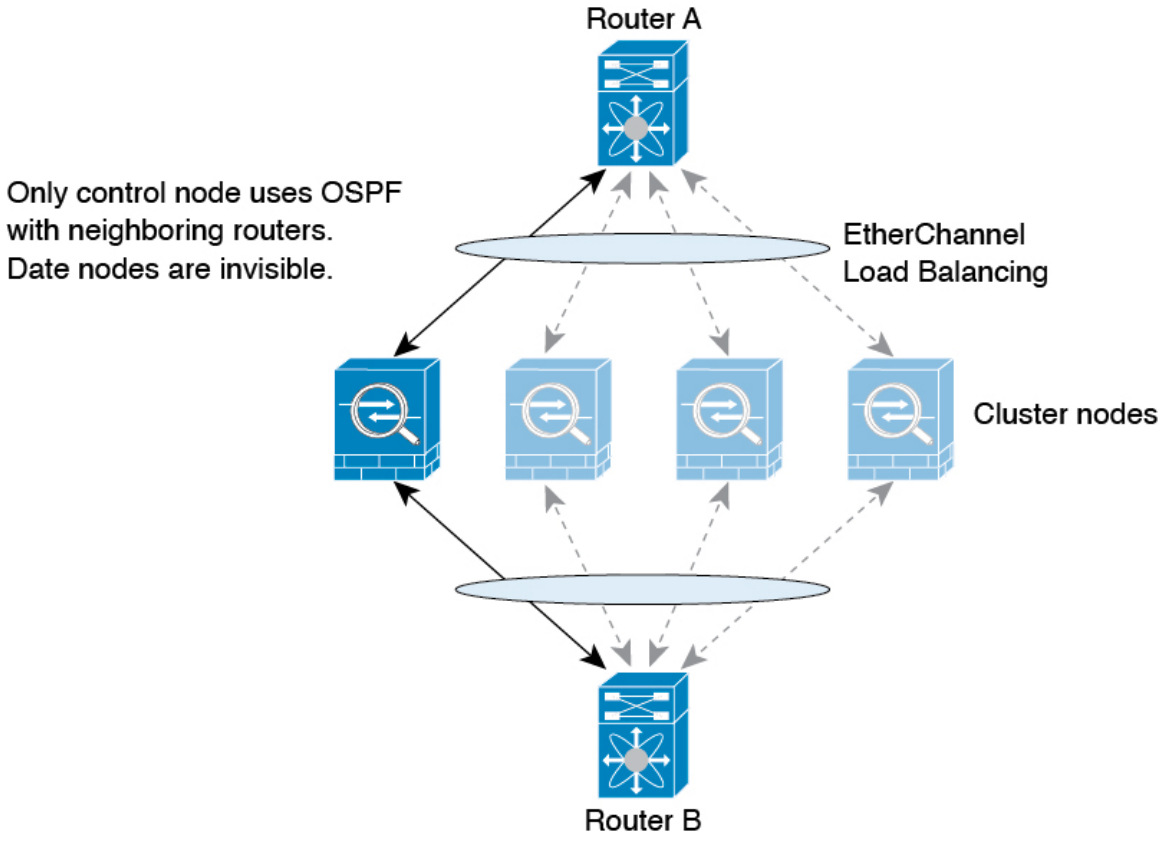
Limitations for NAT and Clustering

- No static PAT for these inspections:
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- No round-robin—Round-robin for a PAT pool is not supported with clustering.
- No extended PAT—Extended PAT is not supported with clustering.

Dynamic routing

The routing process only runs on the control node, and routes are learned through the control node and replicated to data nodes. If a routing packet arrives at a data node, it is redirected to the control node.

Figure 152: Dynamic routing in spanned EtherChannel mode



After the data node learn the routes from the control node, each node makes forwarding decisions independently.

The OSPF LSA database is not synchronized from the control node to data nodes. If there is a control node switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.

SIP inspection and clustering

A control flow can be created on any node (due to load balancing); its child data flows must reside on the same node.

SNMP and clustering

You should always use the local address, and not the main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new control node is elected, the poll to the new control node will fail.

When using SNMPv3 with clustering, if you add a new cluster node after the initial cluster formation, then SNMPv3 users are not replicated to the new node. You must remove the users, and re-add them, and then redeploy your configuration to force the users to replicate to the new node.

Syslog and clustering

Syslog and clustering is a network management configuration that enables logging functionality within clustered network environments.

- Each node in the cluster generates its own syslog messages. You can configure logging so that each node uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all nodes in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all nodes look as if they come from a single node. If you configure logging to use the local-node name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different nodes.

Cisco TrustSec and clustering

Only the control node learns security group tag (SGT) information. The control node then populates the SGT to data nodes, and data nodes can make a match decision for SGT based on the security policy.

VPN and clustering

Site-to-site VPN is a centralized feature; only the control node supports VPN connections.



Note Remote access VPN is not supported with clustering.

VPN functionality is limited to the control node and does not take advantage of the cluster high availability capabilities. If the control node fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control node is elected, you must reestablish the VPN connections.

When you connect a VPN tunnel to a Spanned EtherChannel address, connections are automatically forwarded to the control node.

VPN-related keys and certificates are replicated to all nodes.

Performance scaling factor

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately 80% of the maximum combined throughput.

Throughput calculation

For example, if your model can handle approximately 10 Gbps of traffic when running alone, then for a cluster of 8 units, the maximum combined throughput will be approximately 80% of 80 Gbps (8 units x 10 Gbps): 64 Gbps.

Control node election

Summary

The key components involved in the control node election process are:

- Cluster nodes: Communicate over the cluster control link and participate in the election process
- Election requests: Broadcast every 3 seconds by nodes when clustering is enabled
- Priority values: Set between 1 and 100 where 1 is the highest priority
- Control node: The elected node that coordinates cluster operations

Workflow

These stages describe how cluster nodes elect a control node:

1. When clustering is enabled for a node (or when it first starts up with clustering already enabled), the node broadcasts an election request every 3 seconds.
2. Any other nodes with a higher priority respond to the election request. The priority is set between 1 and 100, where 1 is the highest priority.
3. If after 45 seconds, a node does not receive a response from another node with a higher priority, then it becomes the control node.

Note If multiple nodes tie for the highest priority, the cluster node name and then the serial number is used to determine the control node.

4. If a node later joins the cluster with a higher priority, it does not automatically become the control node. The existing control node always remains as the control node unless it stops responding, at which point a new control node is elected.
5. In a "split brain" scenario when there are temporarily multiple control nodes, the node with highest priority retains the role while the other nodes return to data node roles.

Note You can manually force a node to become the control node. For centralized features, if you force a control node change, then all connections are dropped, and you have to re-establish the connections on the new control node.

High availability within clusters

Clustering provides high availability by monitoring node and interface health and by replicating connection states between nodes.

Node health monitoring

Each node periodically sends a broadcast heartbeat packet over the cluster control link. If the control node does not receive any heartbeat packets or other packets from a data node within the configurable timeout period, then the control node removes the data node from the cluster. If the data nodes do not receive packets from the control node, then a new control node is elected from the remaining nodes.

Split brain scenario

If nodes cannot reach each other over the cluster control link because of a network failure and not because a node has actually failed, then the cluster may go into a "split brain" scenario where isolated data nodes will elect their own control nodes. For example, if a router fails between two cluster locations, then the original control node at location 1 will remove the location 2 data nodes from the cluster. Meanwhile, the nodes at location 2 will elect their own control node and form their own cluster. Note that asymmetric traffic may fail in this scenario. After the cluster control link is restored, then the control node that has the higher priority will keep the control node's role.

Interface monitoring

Each node monitors the link status of all named hardware interfaces in use, and reports status changes to the control node.

- **Spanned EtherChannel**—Uses cluster Link Aggregation Control Protocol (cLACP). Each node monitors the link status and the cLACP protocol messages to determine if the port is still active in the EtherChannel. The status is reported to the control node.

When you enable health monitoring, all physical interfaces (including the main EtherChannel) are monitored by default; you can optionally disable monitoring per interface. Only named interfaces can be monitored. For example, the named EtherChannel must fail to be considered failed, which means all member ports of an EtherChannel must fail to trigger cluster removal.

A node is removed from the cluster if its monitored interfaces fail. The amount of time before the Firewall Threat Defense removes a member from the cluster depends on whether the node is an established member or is joining the cluster. If the interface is down on an established member, then the Firewall Threat Defense removes the member after 9 seconds. The Firewall Threat Defense does not monitor interfaces for the first 90 seconds that a node joins the cluster. Interface status changes during this time will not cause the Firewall Threat Defense to be removed from the cluster. For non-EtherChannels, the node is removed after 500 ms, regardless of the member state.

Status after failure

When a node in the cluster fails, the connections hosted by that node are seamlessly transferred to other nodes; state information for traffic flows is shared over the control node's cluster control link.

If the control node fails, then another member of the cluster with the highest priority (lowest number) becomes the control node.

The device automatically tries to rejoin the cluster, depending on the failure event.



Note When the device becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management interface can send and receive traffic.

Rejoin the cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

- Failed cluster control link when initially joining—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering.
- Failed cluster control link after joining the cluster—The Firewall Threat Defense automatically tries to rejoin every 5 minutes, indefinitely.
- Failed data interface—The Firewall Threat Defense automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the Firewall Threat Defense application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.
- Failed node—If the node was removed from the cluster because of a node health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the node will rejoin the cluster when it starts up again as long as the cluster control link is up. The Firewall Threat Defense application attempts to rejoin the cluster every 5 seconds.
- Internal error—Internal failures include: application sync timeout; inconsistent application statuses; and so on.
- Failed configuration deployment—If you deploy a new configuration from Firewall Management Center, and the deployment fails on some cluster members but succeeds on others, then the nodes that failed are removed from the cluster. You must manually rejoin the cluster by re-enabling clustering. If the deployment fails on the control node, then the deployment is rolled back, and no members are removed. If the deployment fails on all data nodes, then the deployment is rolled back, and no members are removed.

Data path connection state replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

Table 29: Features replicated across the cluster

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	—
MAC address table	Yes	—
User Identity	Yes	—
IPv6 Neighbor database	Yes	—
Dynamic routing	Yes	—

Traffic	State Support	Notes
SNMP Engine ID	No	—

How the cluster manages connections

Connections can be load-balanced to multiple nodes of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

Connection roles

These roles are defined for each connection:

- **Owner**—Usually, the node that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new nodes receive packets from the connection, the director chooses a new owner from those nodes.
- **Backup owner**—The node that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then the first node to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

  As long as the director (see below) is not the same node as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

  For clustering on the Firepower 9300, which can include up to 3 cluster nodes in one chassis, if the backup owner is on the same chassis as the owner, then an additional backup owner will be chosen from another chassis to protect flows from a chassis failure.
- **Director**—The node that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and ports (see below for ICMP hash details), and sends a message to the director to register the new connection. If packets arrive at any node other than the owner, the node queries the director about which node is the owner so it can forward the packets. A connection has only one director. If a director fails, the owner chooses a new director.

  As long as the director is not the same node as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.

  ICMP/ICMPv6 hash details:

  - For Echo packets, the source port is the ICMP identifier, and the destination port is 0.
  - For Reply packets, the source port is 0, and the destination port is the ICMP identifier.
  - For other packets, both source and destination ports are 0.
- **Forwarder**—A node that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner.

A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.



Note We do not recommend disabling TCP sequence randomization when using clustering. There is a small chance that some TCP sessions won't be established, because the SYN/ACK packet might be dropped.

- **Fragment Owner**—For fragmented packets, cluster nodes that receive a fragment determine a fragment owner using a hash of the fragment source IP address, destination IP address, and the packet ID. All fragments are then forwarded to the fragment owner over the cluster control link. Fragments may be load-balanced to different cluster nodes, because only the first fragment includes the 5-tuple used in the switch load balance hash. Other fragments do not contain the source and destination ports and may be load-balanced to other cluster nodes. The fragment owner temporarily reassembles the packet so it can determine the director based on a hash of the source/destination IP address and ports. If it is a new connection, the fragment owner will register to be the connection owner. If it is an existing connection, the fragment owner forwards all fragments to the provided connection owner over the cluster control link. The connection owner will then reassemble all fragments.

New connection ownership

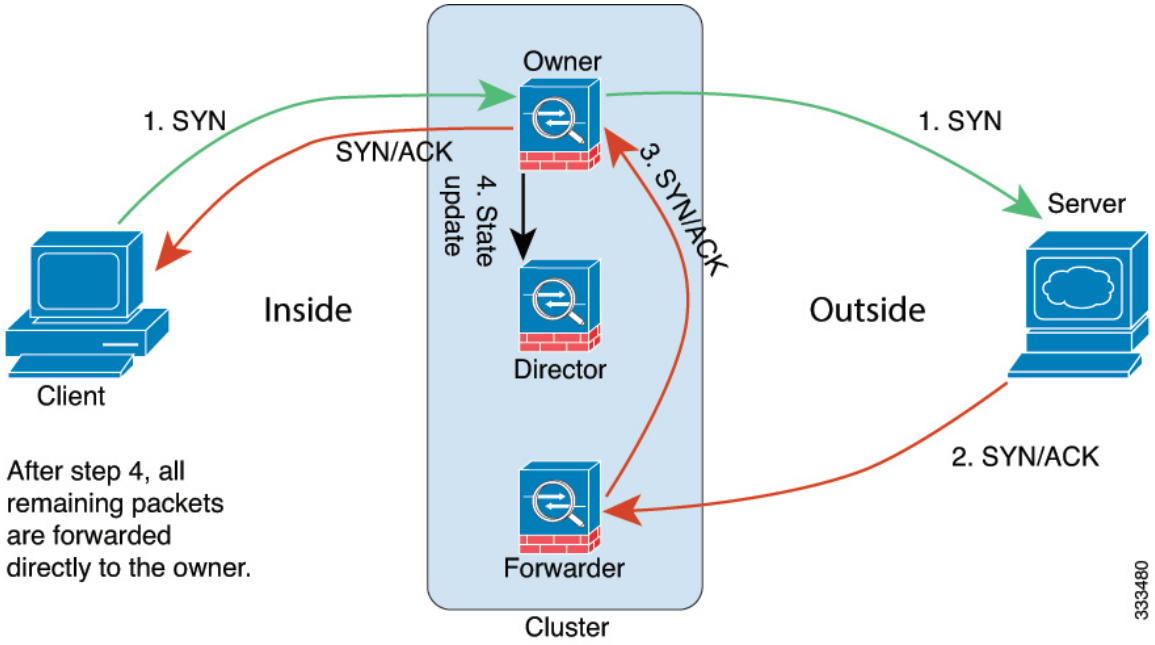
Traffic redirection is not supported in this release. When a new connection is directed to a node of the cluster via load balancing, that node owns both directions of the connection. All the subsequent packets for the same connection should arrive the same node. If any connection packets arrive at a different node, they will be dropped. If a reverse flow arrives at a different node, it will be dropped as well. For centralized features, if the connections do not arrive on the control node, they will be dropped.

Sample data flow for TCP

Summary

This example shows the establishment of a new connection.

Workflow



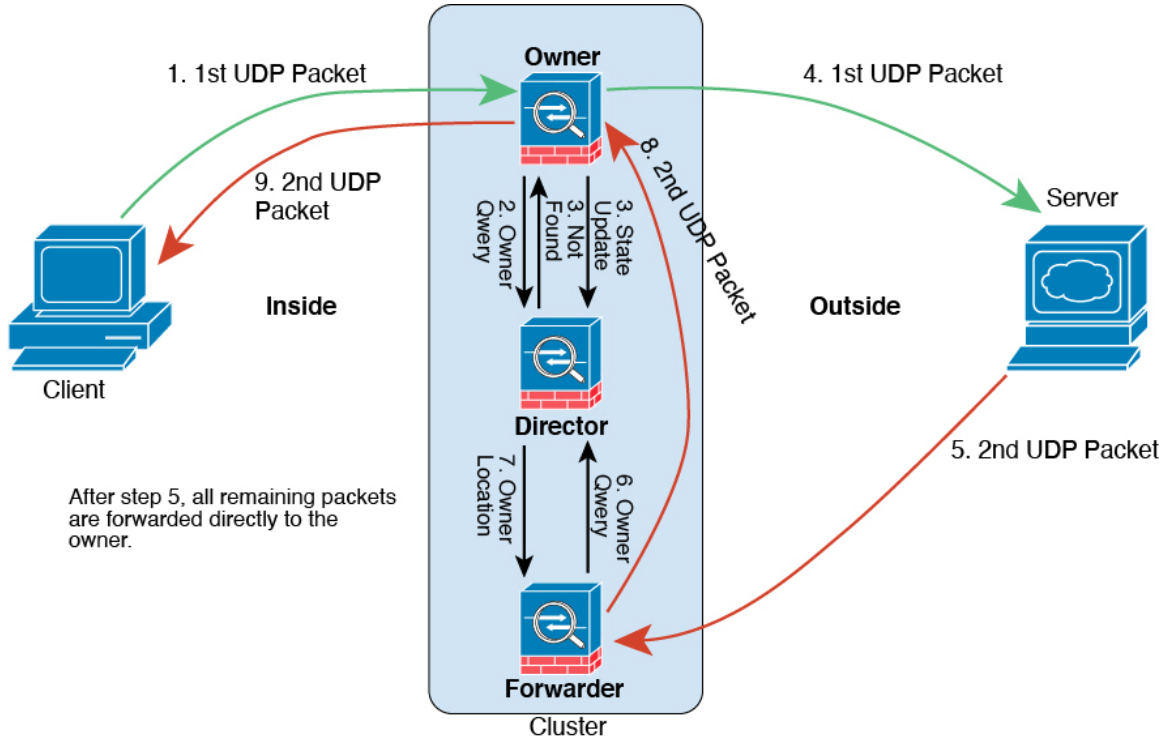
1. The SYN packet originates from the client and is delivered to one device (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.
2. The SYN-ACK packet originates from the server and is delivered to a different device (based on the load balancing method). This device is the forwarder.
3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.
4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.
5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.
6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.
7. If packets are delivered to any additional nodes, it will query the director for the owner and establish a flow.
8. Any state change for the flow results in a state update from the owner to the director.

Sample data flows for ICMP and UDP

Summary

This example shows the establishment of a new connection.

Workflow



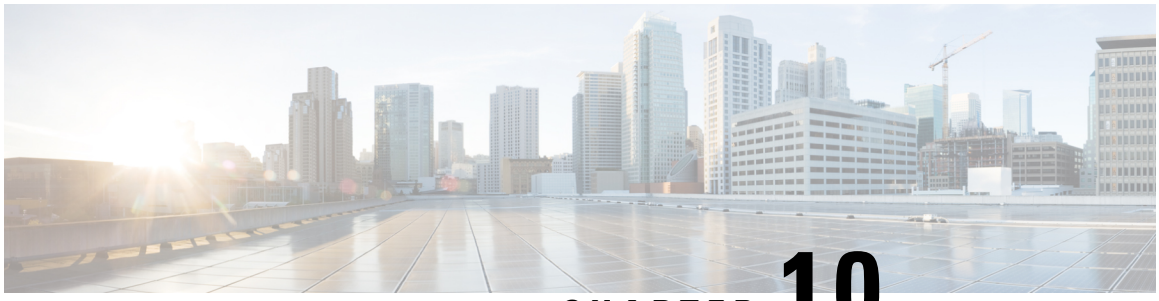
1. The first UDP packet originates from the client and is delivered to one device (based on the load balancing method).
2. The node that received the first packet queries the director node that is chosen based on a hash of the source/destination IP address and ports.
3. The director finds no existing flow, creates a director flow and forwards the packet back to the previous node. In other words, the director has elected an owner for this flow.
4. The owner creates the flow, sends a state update to the director, and forwards the packet to the server.
5. The second UDP packet originates from the server and is delivered to the forwarder.
6. The forwarder queries the director for ownership information. For short-lived flows such as DNS, instead of querying, the forwarder immediately sends the packet to the director, which then sends it to the owner.
7. The director replies to the forwarder with ownership information.
8. The forwarder creates a forwarding flow to record owner information and forwards the packet to the owner.
9. The owner forwards the packet to the client.

History for Clustering

Lists the clustering features introduced in each release.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cluster control link ping tool.	7.2.6 7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** > **Cluster Live Status.**
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**
Automatic generation of a troubleshooting file on a node when it fails to join the cluster.	7.4.1	7.4.1	If a node fails to join the cluster, a troubleshooting file is automatically generated for the node. You can download the file from **Tasks** or from the **Cluster** page.
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**
Clustering for the Secure Firewall 4200	7.4.0	7.4.0	The Secure Firewall 4200 supports Spanned EtherChannel clustering for up to 8 nodes.
Cluster health monitor settings	7.3.0	Any	You can now edit cluster health monitor settings. New/modified screens: **Devices** > **Device Management** > **Cluster** > **Cluster Health Monitor Settings** **Note** If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.
Cluster health monitor dashboard	7.3.0	Any	You can now view cluster health on the cluster health monitor dashboard. New/modified screens: **System** > **Health** > **Monitor**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Automatic configuration of the cluster control link MTU	7.2.0	7.2.0	The MTU of the cluster control link interface is now automatically set to 100 bytes more than the highest data interface MTU; by default, the MTU is 1600 bytes.
Clustering for the Secure Firewall 3100	7.1.0	7.1.0	The Secure Firewall 3100 supports Spanned EtherChannel clustering for up to 8 nodes. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** Supported platforms: Secure Firewall 3100



CHAPTER 10

Clustering: Private Cloud

Clustering lets you group multiple Firewall Threat Defense Virtuals together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. You can deploy Firewall Threat Defense Virtual clusters in a private cloud using VMware and KVM. Only routed firewall mode is supported.

Note Some features are not supported when using clustering. See Unsupported features and clustering, on page 422.

- About clustering: private cloud, on page 385
- Licenses for clustering: Private cloud, on page 389
- Prerequisites for clustering: Private cloud, on page 390
- Guidelines for clustering: Private cloud, on page 391
- Configure clustering: private cloud, on page 392
- Manage cluster nodes, on page 404
- Monitor cluster status, on page 414
- Troubleshoot the cluster, on page 419
- Reference for clustering, on page 422
- History for clustering: private cloud, on page 434

About clustering: private cloud

This section describes the clustering architecture and how it works.

How the cluster fits into your network

The cluster consists of multiple firewalls acting as a single device. To act as a cluster, the firewalls need the following infrastructure:

- Isolated network for intra-cluster communication, known as the cluster control link, using VXLAN interfaces. VXLANs, which act as Layer 2 virtual networks over Layer 3 physical networks, let the Firewall Threat Defense Virtual send broadcast/multicast messages over the cluster control link.
- Management access to each firewall for configuration and monitoring. The Firewall Threat Defense Virtual deployment includes a Management 0/0 interface that you will use to manage the cluster nodes.

When you place the cluster in your network, the upstream and downstream routers need to be able to load-balance the data coming to and from the cluster using Layer 3 Individual interfaces and one of the following methods:

- Policy-Based Routing—The upstream and downstream routers perform load balancing between nodes using route maps and ACLs.
- Equal-Cost Multi-Path Routing—The upstream and downstream routers perform load balancing between nodes using equal cost static or dynamic routes.

Layer 2 Spanned EtherChannels are not supported.

Control and data node roles

When you add a cluster in the Firewall Management Center , you choose one firewall to be the control node, and all additional firewalls to be data nodes. When you first create the cluster, the control node you specify will become the control node simply because it is the first node added to the cluster. Later, if multiple cluster nodes come online at the same time, the control node is determined by the priority setting; the priority is set between 1 and 100, where 1 is the highest priority.

When you create the cluster and deploy the cluster configuration, the Firewall Management Center deploys a special bootstrap configuration to each node that includes fundamental settings such as the cluster control link configuration. The bootstrap configuration lets each node join the cluster. Most bootstrap settings are defined in the cluster wizard; however, you define the cluster control link interface hardware configuration (for example, creating an EtherChannel or setting the Ethernet speed) on the control node before you create the cluster. The cluster control link settings are copied to the bootstrap configuration for each node.

All nodes in the cluster share the same policy configuration. The node that you initially specify as the control node will overwrite the configuration on the data nodes when they join the cluster, so you only need to perform initial configuration on the control node before you form the cluster. After you create the cluster, all configuration changes are made at the cluster level and are shared by all nodes.

Some features do not scale in a cluster, and the control node handles all traffic for those features.

Individual interfaces

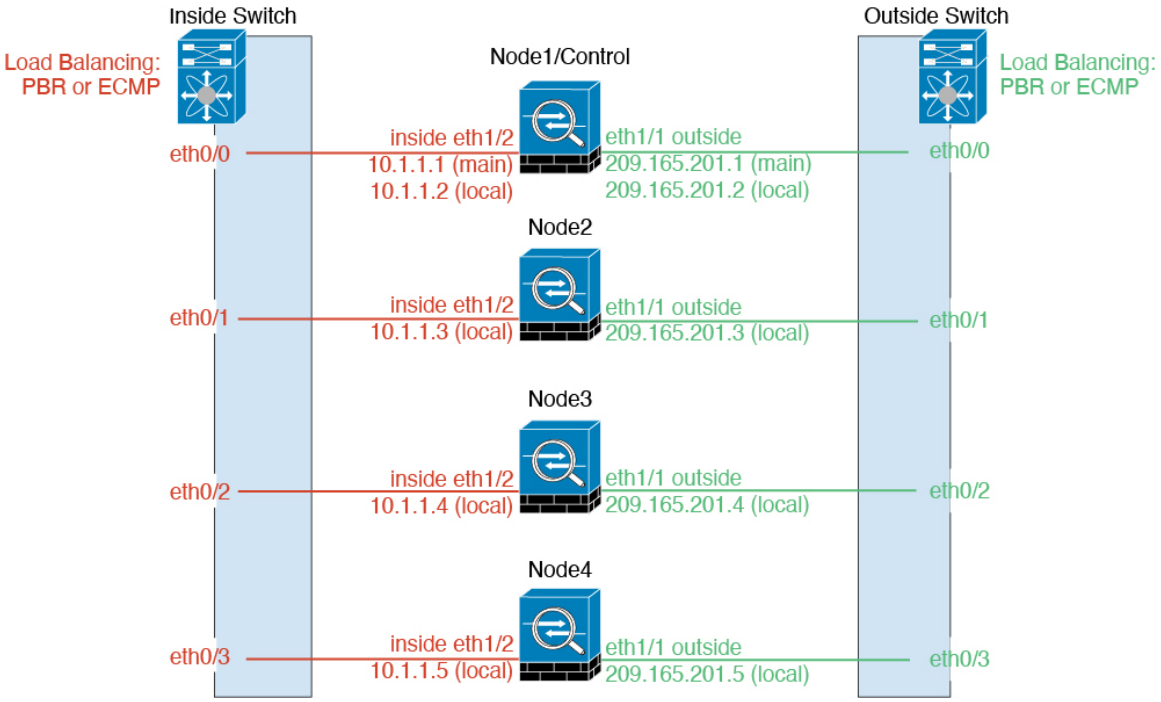
You can configure cluster interfaces as individual interfaces.

Individual interfaces are normal routed interfaces, each with their own *local IP address* used for routing. The *main cluster IP address* for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly.

IPS-only interfaces (inline sets and passive interfaces) are not supported as Individual interfaces.

Because interface configuration must be done only on the control node, configure a pool of IP addresses for a given interface on the cluster nodes, including one for the control node.

Load balancing must be configured separately on the upstream switch.



Layer 2 Spanned EtherChannels are not supported.

Policy-based routing

When using individual interfaces, each Firewall Threat Defense interface maintains its own IP address and MAC address. One method of load balancing is Policy-Based Routing (PBR).

We recommend this method if you are already using PBR, and want to take advantage of your existing infrastructure.

PBR makes routing decisions based on a route map and ACL. You must manually divide traffic between all Firewall Threat Defenses in a cluster. Because PBR is static, it may not achieve the optimum load balancing result at all times. To achieve the best performance, we recommend that you configure the PBR policy so that forward and return packets of a connection are directed to the same Firewall Threat Defense.

For example, if you have a Cisco router, redundancy can be achieved by using Cisco IOS PBR with Object Tracking. Cisco IOS Object Tracking monitors each Firewall Threat Defense using ICMP ping. PBR can then enable or disable route maps based on reachability of a particular Firewall Threat Defense.

Equal-cost multi-path routing

When using Individual interfaces, each Firewall Threat Defense interface maintains its own IP address and MAC address. One method of load balancing is Equal-Cost Multi-Path (ECMP) routing.

We recommend this method if you are already using ECMP, and want to take advantage of your existing infrastructure.

ECMP routing considerations

ECMP routing can forward packets over multiple best paths that tie for top place in the routing metric. Like EtherChannel, a hash of source and destination IP addresses and/or source and destination ports can be used to send a packet to one of the next hops.

If you use static routes for ECMP routing, then the Firewall Threat Defense failure can cause problems; the route continues to be used, and traffic to the failed Firewall Threat Defense will be lost.

If you use static routes, be sure to use a static route monitoring feature such as Object Tracking. We recommend using dynamic routing protocols to add and remove routes, in which case, you must configure each Firewall Threat Defense to participate in dynamic routing.

Cluster Control Link

Each node must dedicate one interface as a VXLAN (VTEP) interface for the cluster control link. For more information about VXLAN, see Configure VXLAN interfaces, on page 680 .

VXLAN Tunnel Endpoint

VXLAN tunnel endpoint (VTEP) devices perform VXLAN encapsulation and decapsulation. Each VTEP has two interface types: one or more virtual interfaces called VXLAN Network Identifier (VNI) interfaces, and a regular interface called the VTEP source interface that tunnels the VNI interfaces between VTEPs. The VTEP source interface is attached to the transport IP network for VTEP-to-VTEP communication.

VTEP Source Interface

The VTEP source interface is a regular Firewall Threat Defense Virtual interface with which you plan to associate the VNI interface. You can configure one VTEP source interface to act as the cluster control link. The source interface is reserved for cluster control link use only. Each VTEP source interface has an IP address on the same subnet. This subnet should be isolated from all other traffic, and should include only the cluster control link interfaces.

VNI Interface

A VNI interface is similar to a VLAN interface. It is a virtual interface that keeps network traffic separated on a given physical interface by using tagging. You can only configure one VNI interface. Each VNI interface has an IP address on the same subnet.

Peer VTEPs

Unlike regular VXLAN for data interfaces, which allows a single VTEP peer, Firewall Threat Defense Virtual clustering allows you to configure multiple peers.

Cluster control link traffic overview

Cluster control link traffic includes both control and data traffic.

Control traffic includes:

- Control node election.
- Configuration replication.
- Health monitoring.

Data traffic includes:

- State replication.
- Connection ownership queries and data packet forwarding.

Configuration replication

All nodes in the cluster share a single configuration. You can only make configuration changes on the control node (with the exception of the bootstrap configuration), and changes are automatically synced to all other nodes in the cluster.

Management network

You must manage each node using the Management interface. Management from a data interface is not supported with clustering.

Licenses for clustering: Private cloud

Performance tier license requirements

Each Firewall Threat Defense Virtual cluster node requires the same performance tier license. We recommend using the same number of CPUs and memory for all members, or else performance will be limited on all nodes to match the least capable member. The throughput level will be replicated from the control node to each data node so they match.

Feature license assignment

You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

When you add the control node to the Firewall Management Center, you can specify the feature licenses you want to use for the cluster. Before you create the cluster, it doesn't matter which licenses are assigned to the data nodes; the license settings for the control node are replicated to each of the data nodes. You can modify licenses for the cluster by clicking **Edit Licenses** in **System** (⚙) > **Licenses** > **Smart Licenses** or choosing **Devices** > **Device Management**, clicking **Edit** (✎) for the cluster, and then in the **License** area, clicking **Edit** (✎).

Note If you add the cluster before the Firewall Management Center is licensed (and running in Evaluation mode), then when you license the Firewall Management Center, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

Note APEX, PLUS, and VPN-Only licenses are not supported for clustering. Before you create a cluster, remove unsupported license assignments from the devices that will become cluster nodes.

Prerequisites for clustering: Private cloud

This reference provides the complete set of requirements that must be met before configuring clustering for threat defense virtual devices in private cloud deployments.

Model requirements

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100
- VMware or KVM
- A maximum of 16 nodes in a cluster in a 4x4 configuration is supported. You can set up a maximum of four hosts with a maximum of four threat defense virtual instances in each host.

User roles

- Admin
- Access Admin
- Network Admin

Hardware and software requirements

All units in a cluster:

- Must have jumbo frame reservation enabled for the cluster control link. Do this in the Day 0 configuration when you deploy the Firewall Threat Defense Virtual by setting `"DeploymentType": "Cluster"`. Otherwise, you must restart each node to enable jumbo frames after the cluster has formed and is healthy.
- (KVM only) Must use CPU hard partitioning (CPU pinning) for all VMs on the KVM host.
- Must be the same performance tier. We recommend using the same number of CPUs and memory for all nodes, or performance will be limited on all nodes to match the least capable node.
- Must use the management interface for Firewall Management Center communications. Data interface management is not supported.
- Must run the same version, except during upgrade. Hitless upgrade is supported.
- Must be in the same domain and group.
- Must not have any deployment pending or in progress.
- Must not have any unsupported features configured on the control node: Unsupported features and clustering, on page 422.
- Must not have VPN configured on the data nodes. The control node can have site-to-site VPN configured.

Firewall Management Center Requirements

Make sure the Firewall Management Center NTP server is set to a reliable server that is reachable by all cluster nodes to ensure proper clock sync. By default, the device uses the same NTP server as the Firewall Management Center. If the time is not set to be the same on all cluster nodes, they can be removed automatically from the cluster.

Switch requirements

Be sure to complete the switch configuration before you configure clustering. Make sure the ports connected to the cluster control link have the correct (higher) MTU configured. By default, the cluster control link MTU is set to 154 bytes higher than the data interfaces. If the switches have an MTU mismatch, the cluster formation will fail.

Guidelines for clustering: Private cloud

High availability

High Availability is not supported with clustering.

IPv6

The cluster control link is only supported using IPv4.

Additional clustering guidelines

Consider these additional guidelines when configuring clustering:

- When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the Firewall Threat Defense Virtual, adding an additional switch to form a VSS or vPC, configuring IP addresses or interface flap on the cluster) you should disable the health check feature and also disable interface monitoring for the interfaces that are affected by the topology changes. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the interface health check feature.
- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang your connection; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.
- We do not support VXLAN for data interfaces; only the cluster control link supports VXLAN.

Default cluster configurations

Consider these default configurations when setting up clustering:

- The cLACP system ID is auto-generated, and the system priority is 1 by default.
- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.

- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Upgrade guidelines

Configure clustering: private cloud

To configure clustering after you deploy your Firewall Threat Defense Virtuals, perform the following tasks.

Add nodes to the Management Center

This task allows you to prepare cluster nodes for clustering configuration by adding them to the management center as individual devices.

Before configuring clustering, deploy each cluster node, then add the devices as standalone units on the Firewall Management Center.

Procedure

Step 1 Deploy each cluster node by following the procedures given in the Secure Firewall Threat Defense Virtual getting started guides.

All units in a cluster:

- Must have jumbo frame reservation enabled for the cluster control link. Do this in the Day 0 configuration when you deploy the Firewall Threat Defense Virtual by setting `"DeploymentType": "Cluster"`. Otherwise, you must restart each node to enable jumbo frames after the cluster has formed and is healthy.
- (KVM only) Must use CPU hard partitioning (CPU pinning) for all VMs on the KVM host.

Step 2 Add each node to the Firewall Management Center as a standalone device in the same domain and group.

See Add a Device Using a Registration Key , on page 32. You can create a cluster with a single device, and then add more nodes later. The initial settings (licensing, access control policy) that you set when you add a device will be inherited by all cluster nodes from the control node. You will choose the control node when forming the cluster.

Create a cluster

Creating a cluster allows multiple devices to work together as a single logical unit, providing high availability and increased throughput capacity.

Form a cluster from one or more devices in the Firewall Management Center.

Before you begin

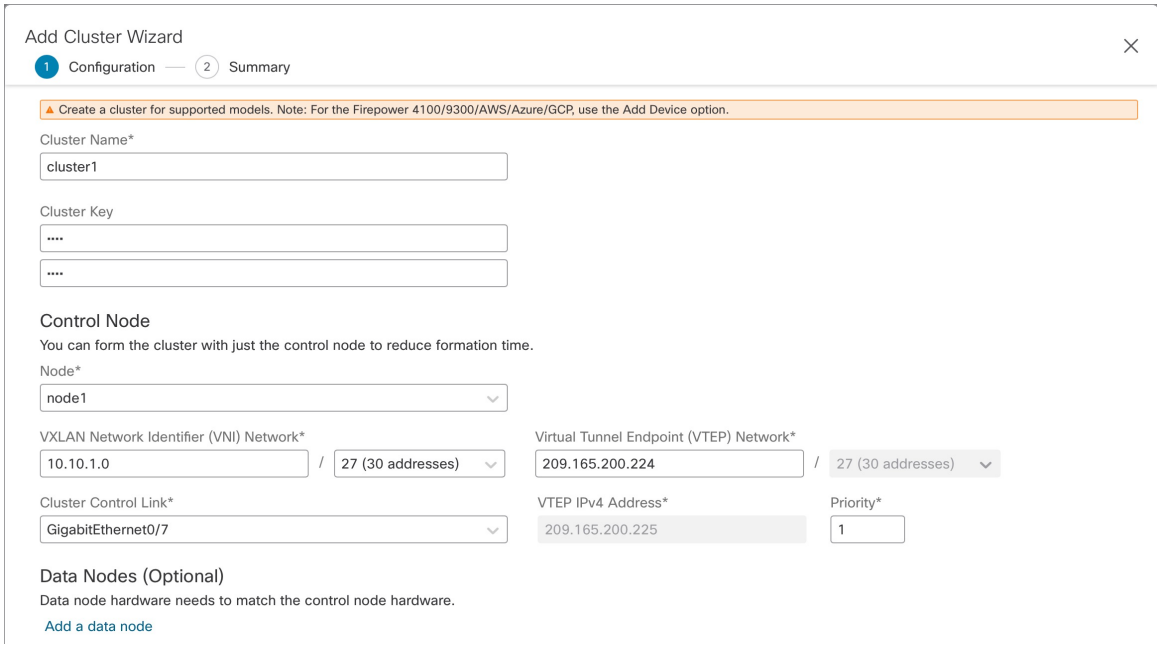
Some features are not compatible with clustering. Wait to configure until clustering is enabled. Some features will block cluster creation if they are already configured. For example, do not configure any IP addresses on interfaces, or unsupported interface types such as BVIs.

Procedure

Step 1 Choose **Devices** > **Device Management**, and then choose **Add** > **Cluster**.

The **Add Cluster Wizard** appears.

Figure 153: Add Cluster Wizard



Step 2 Specify a **Cluster Name** and an authentication **Cluster Key** for control traffic.

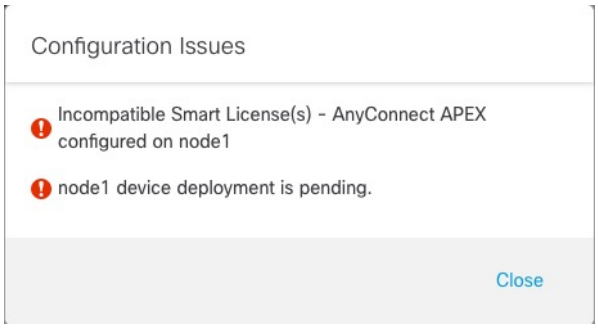
- **Cluster Name**—An ASCII string of 1 to 38 characters. The cluster name can contain only letters, digits, underscores (_), and hyphens (-).
- **Cluster Key**—An ASCII string of 1 to 63 characters. The cluster key cannot be a single digit and must not contain spaces. The **Cluster Key** value is used to generate the encryption key. This encryption does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in clear text.

Step 3 For the **Control Node**, set the following:

- **Node**—Choose the device that you want to be the control node initially. When the Firewall Management Center forms the cluster, it will add this node to the cluster first so it will be the control node.

Note If you see an **Error** ( ) icon next to the node name, click the icon to view configuration issues. You must cancel cluster formation, resolve the issues, and then return to cluster formation. For example:

Figure 154: Configuration Issues



To resolve the above issues, remove the unsupported VPN license and deploy pending configuration changes to the device.

- **VXLAN Network Identifier (VNI) Network**—Specify an IPv4 subnet for the VNI network; IPv6 is not supported for this network. Specify a **24**, **25**, **26**, or **27** subnet. An IP address will be auto-assigned to each node on this network. The VNI network is the encrypted virtual network that runs on top of the physical VTEP network.
- **Cluster Control Link**—Choose the physical interface you want to use for the cluster control link.
- **Virtual Tunnel Endpoint (VTEP) Network**—Specify an IPv4 subnet for the physical interface network; IPv6 is not supported for this network. The VTEP network is a different network than the VNI network, and it is used for the physical cluster control link.
- **VTEP IPv4 Address**—This field will be auto-populated with the first address on the VTEP network.
- **Priority**—Set the priority of this node for control node elections. The priority is between 1 and 100, where 1 is the highest priority. Even if you set the priority to be lower than other nodes, this node will still be the control node when the cluster is first formed.

Step 4 For **Data Nodes (Optional)**, click **Add a data node** to add a node to the cluster.

You can form the cluster with only the control node for faster cluster formation, or you can add all nodes now. Set the following for each data node:

- **Node**—Choose the device that you want to add.

Note If you see an **Error** ( ) icon next to the node name, click the icon to view configuration issues. You must cancel cluster formation, resolve the issues, and then return to cluster formation.

- **VTEP IPv4 Address**—This field will be auto-populated with the next address on the VTEP network.

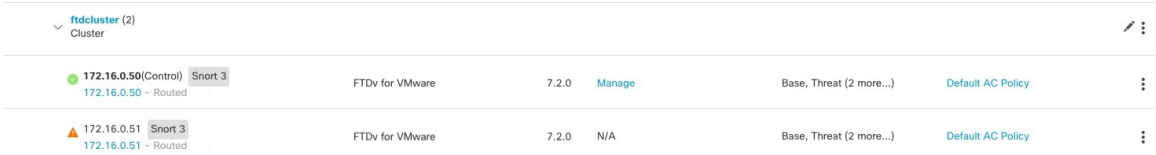
- **Priority**—Set the priority of this node for control node elections. The priority is between 1 and 100, where 1 is the highest priority.

Step 5 Click **Continue**. Review the **Summary**, and then click **Save**.

The cluster bootstrap configuration is saved to the cluster nodes. The bootstrap configuration includes the VXLAN interface used for the cluster control link.

The cluster name shows on the **Devices** > **Device Management** page; expand the cluster to see the cluster nodes.

Figure 155: Cluster Management

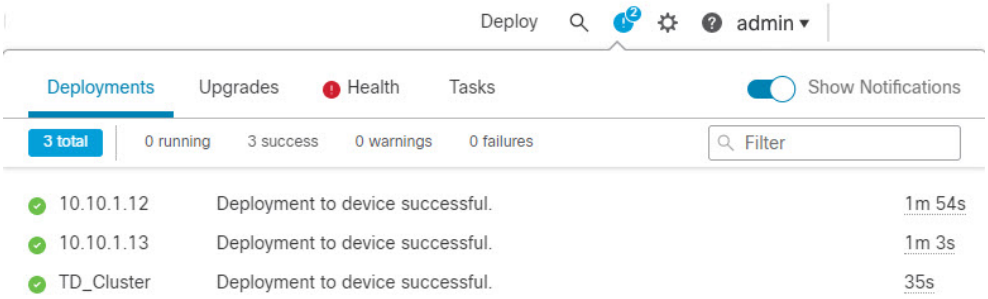


A node that is currently registering shows the loading icon.

Figure 156: Node Registration



You can monitor cluster node registration by clicking the **Notifications** icon and choosing **Tasks**. The Firewall Management Center updates the Cluster Registration task as each node registers.

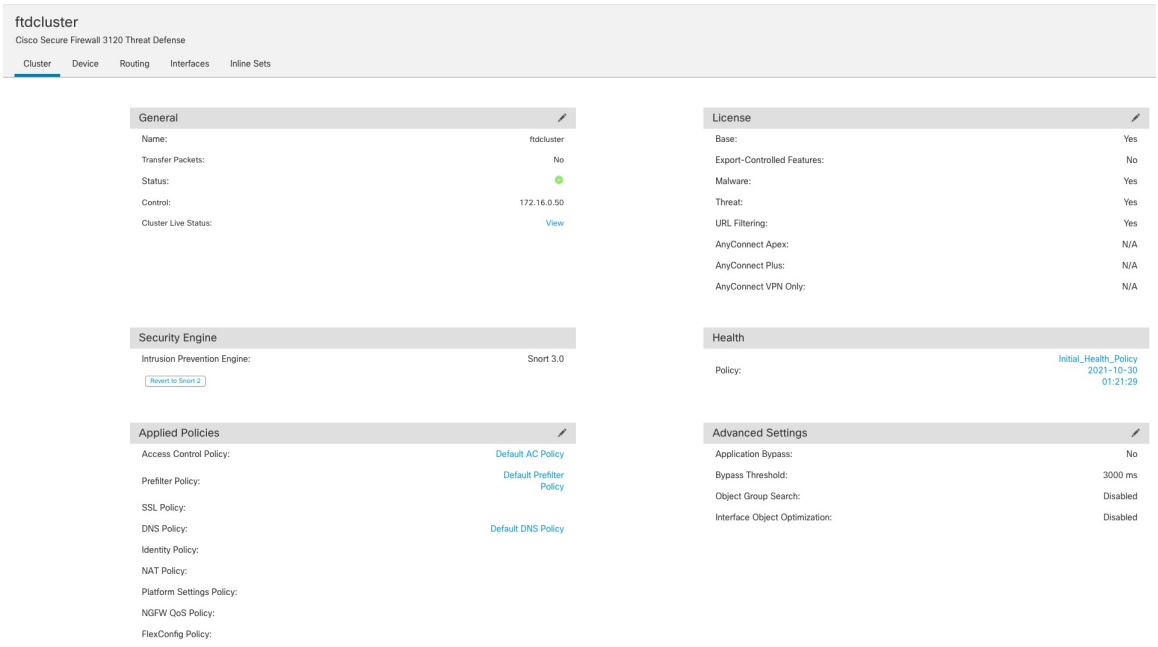


Step 6 Configure device-specific settings by clicking the **Edit** (✎) for the cluster.

Most configuration can be applied to the cluster as a whole, and not nodes in the cluster. For example, you can change the display name per node, but you can only configure interfaces for the whole cluster.

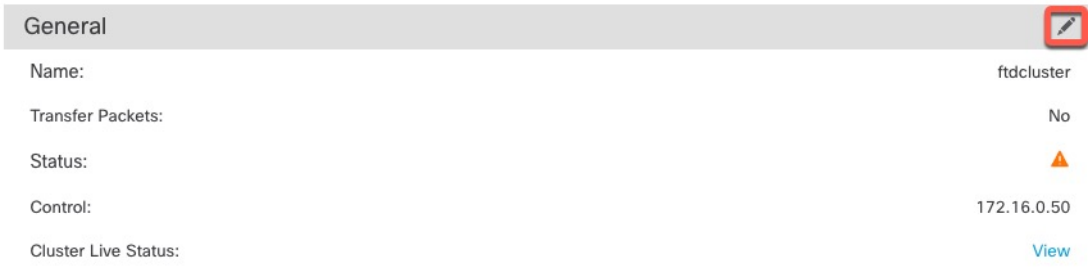
Step 7 On the **Devices** > **Device Management**, **Cluster** screen, you see **General** and other settings for the cluster.

Figure 157: Cluster Settings

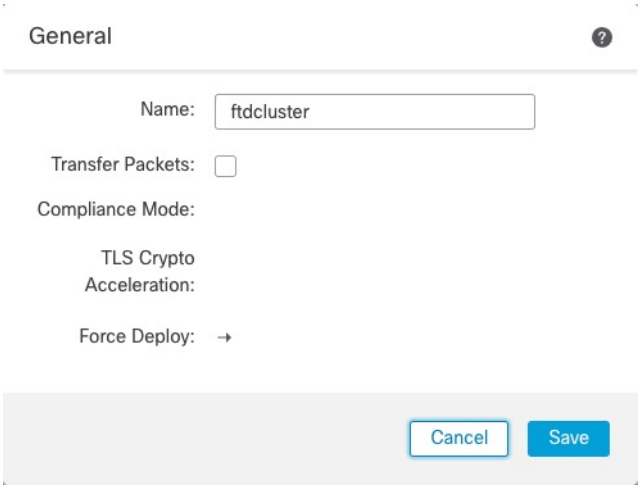


See the following cluster-specific items in the **General** area:

- **General > Name**—Change the cluster display name by clicking the **Edit** (✎).



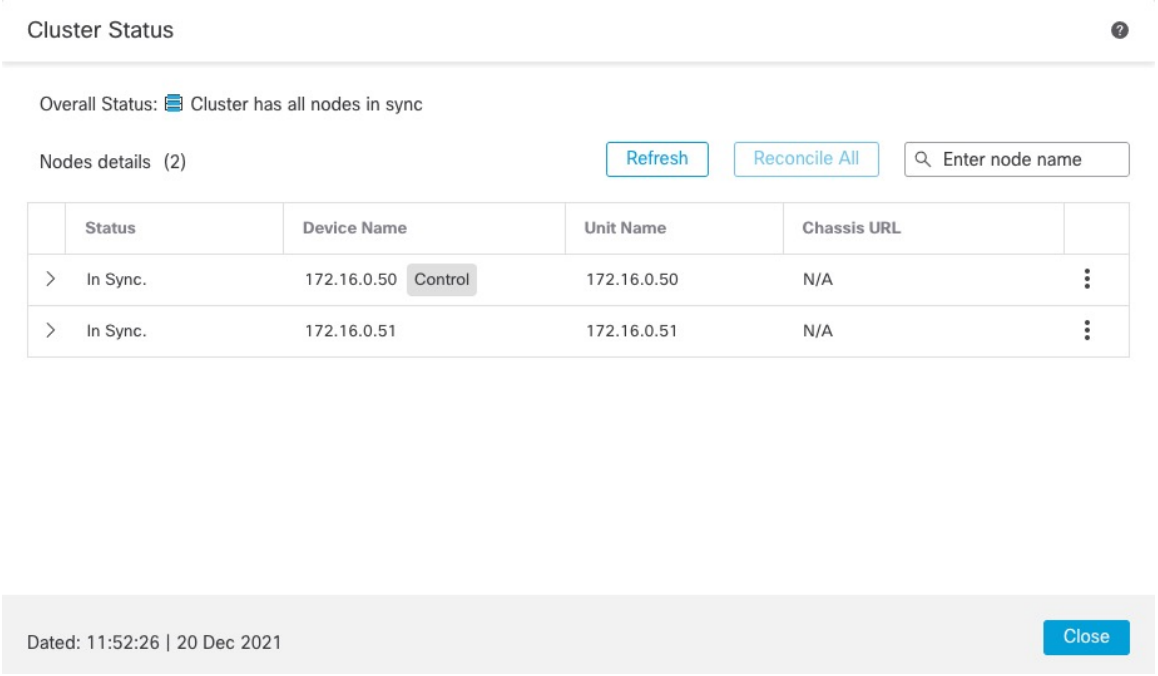
Then set the **Name** field.



- **General > View**—Click the **View** link to open the **Cluster Status** dialog box.



The **Cluster Status** dialog box also lets you retry data unit registration by clicking **Reconcile All**.You can also ping the cluster control link from a node. See Perform a ping on the cluster control link, on page 367.



- **General > Troubleshoot**— Use **Logs** to generate troubleshooting files for all nodes in the cluster, **CLI** to view output from predefined cluster diagnostic commands, and **Download** to download the generated cluster troubleshooting archive

  For more information, refer to Troubleshoot the cluster, on page 365.

Figure 158: Troubleshoot



Step 8 On the **Devices** > **Device Management** and then click **Add** > **Device**, you can choose each member in the cluster from the top right drop-down menu and configure the following settings.

Figure 159: Device Settings

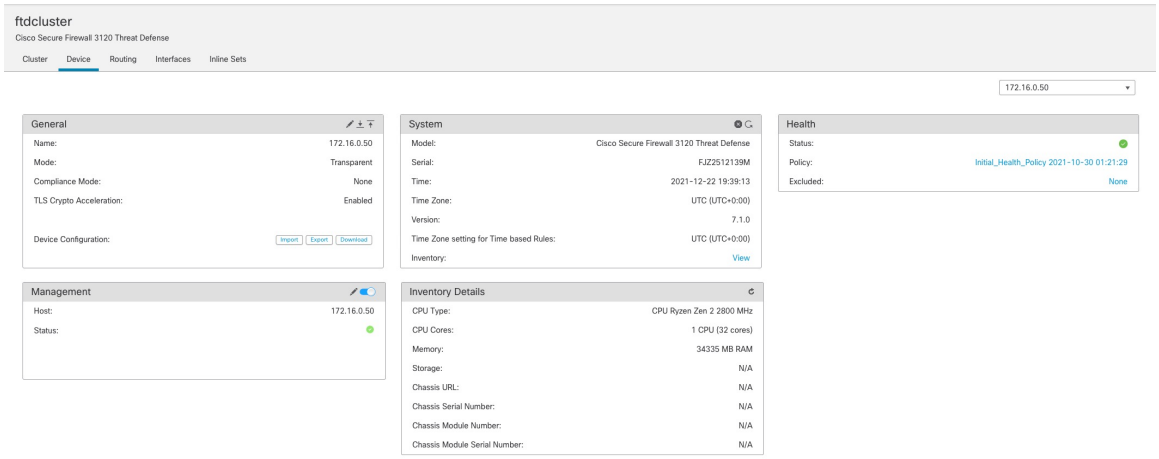
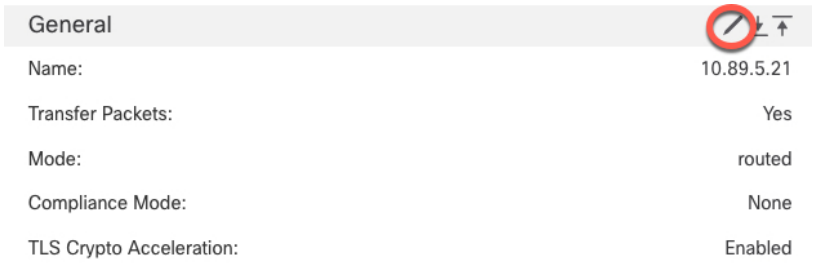


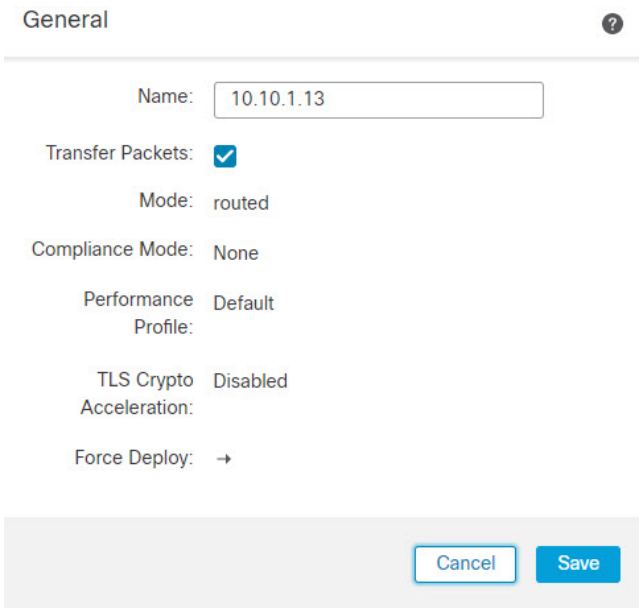
Figure 160: Choose Node



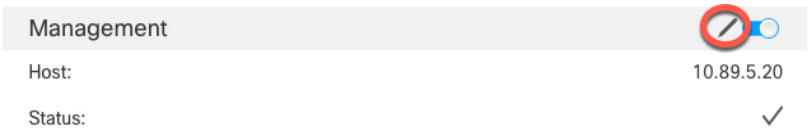
- **General > Name**—Change the cluster member display name by clicking the **Edit** ( ).



Then set the **Name** field.



- **Management > Host**—If you change the management IP address in the device configuration, you must match the new address in the Firewall Management Center so that it can reach the device on the network. First disable the connection, edit the **Host** address in the **Management** area, then re-enable the connection.



Step 9 If you deployed your cluster nodes without enabling jumbo-frame reservation, then restart all cluster nodes to enable jumbo frames, which are required for the cluster control link. See Shut down or restart the device, on page 55.

If you previously enabled jumbo-frame reservation, you can skip this step.

Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead (100 bytes) and VXLAN overhead (54 bytes). When you create the cluster, the MTU is set to 154 bytes higher than the highest data interface MTU (1654 by default). If you later increase the data interface MTU, be sure to also increase the cluster control link MTU. For example, because the maximum MTU is 9198 bytes, then the highest data interface MTU can be 9044, while the cluster control link can be set to 9198. See Configure the MTU, on page 717.

Make sure you configure switches connected to the cluster control link to the correct (higher) MTU; otherwise, cluster formation might fail.

Configure interfaces

Configure interfaces to be compatible with clustering by setting up individual interfaces that are normal routed interfaces, each with their own IP address taken from a pool of IP addresses.

Individual interfaces are normal routed interfaces, each with their own IP address taken from a pool of IP addresses. The Main cluster IP address is a fixed address for the cluster that always belongs to the current control node. All data interfaces must be Individual interfaces.

Note You cannot use subinterfaces.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Address Pools** to add an IPv4 address pool, an IPv6 address pool, or both. See Configure address pools, on page 2356.

Include at least as many addresses as there are units in the cluster. The Virtual IP address is not a part of this pool, but needs to be on the same network. You cannot determine the exact Local address assigned to each unit in advance.

Step 2 Choose **Devices** > **Device Management**, and click **Edit** ( ) next to the cluster.

Step 3 Click **Interfaces**, and then click **Edit** ( ) for a data interface.

Step 4 On the **IPv4**, enter the **IP Address** and mask. This IP address is a fixed address for the cluster, and always belongs to the current control unit.

Step 5 From the **IPv4 Address Pool** drop-down list, choose the address pool you created.

Note If you want to manually assign a MAC address to this interface, you need to create a **MAC-address pool** using FlexConfig.

Step 6 On **IPv6** > **Basic**, from the **IPv6 Address Pool** drop-down list, choose the address pool you created.

Step 7 Configure other interface settings as normal.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure Cluster Health Monitor Settings

This task allows you to modify cluster health monitor settings to control how cluster nodes monitor system health and automatically rejoin the cluster after failures.

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings for monitoring cluster node health. You can monitor any port-channel ID, any single physical interface ID, and the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link. It is always monitored.

When a topology change occurs (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature. Also, disable interface monitoring for any interfaces that are disabled. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management**.

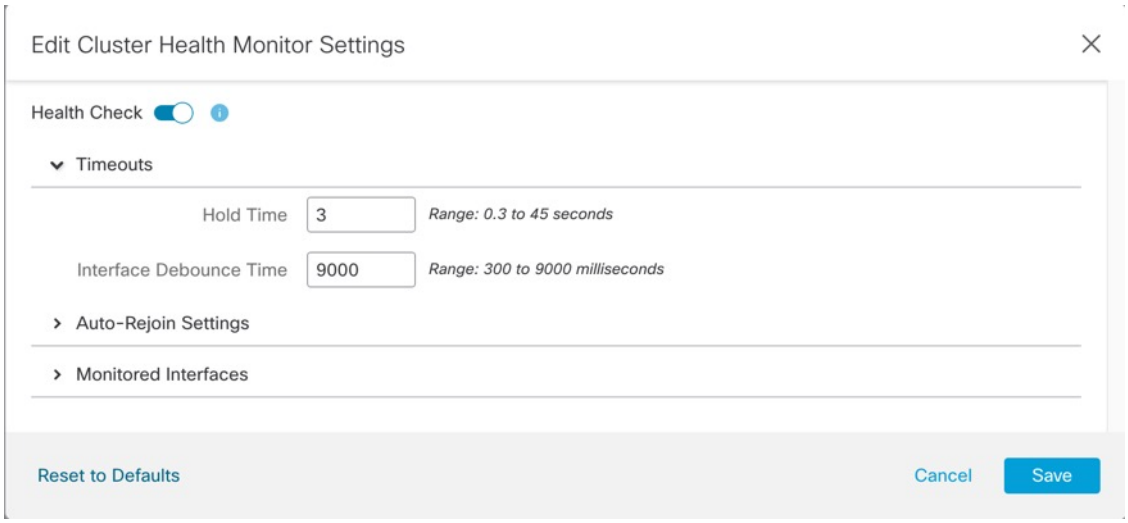
Step 2 Next to the cluster you want to modify, click **Edit** ( ).

Step 3 Click **Cluster**.

Step 4 In the **Cluster Health Monitor Settings** section, click **Edit** ( ).

Step 5 Disable the system health check by clicking the **Health Check** slider.

Figure 161: Disable the system health check



When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

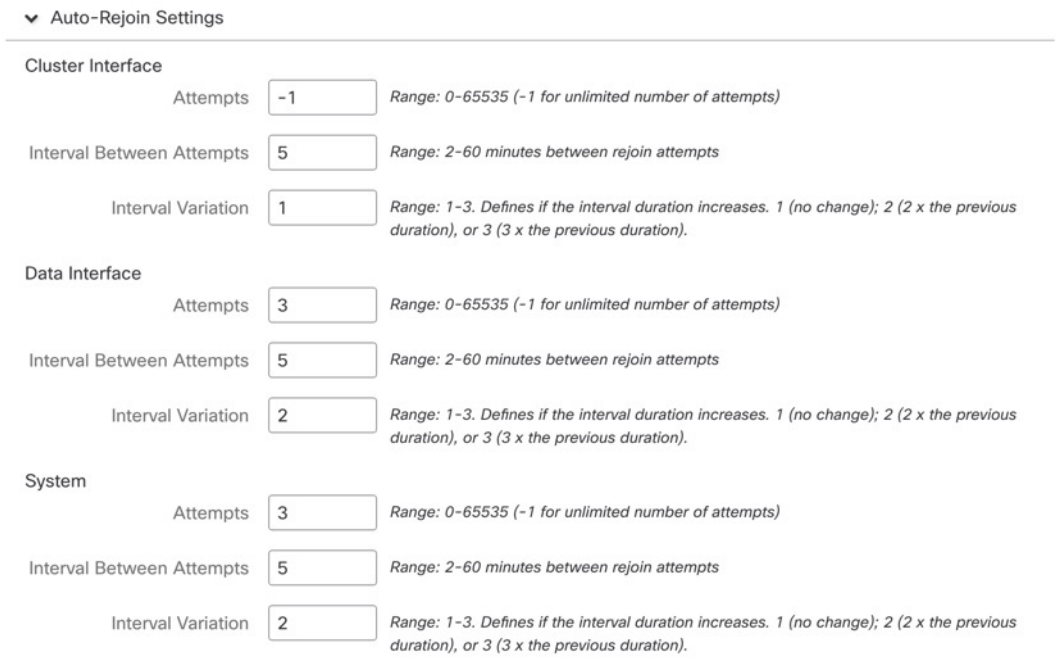
Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between 0.3 and 45 seconds. The default is 3 seconds.
- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the specified number of milliseconds before marking the interface as failed and removing the node from the cluster. If an EtherChannel transitions from a down state to an up state, such as after the switch reloads

or enables an EtherChannel, a longer debounce time can prevent the interface from appearing failed on a cluster node if another cluster node bundles the ports more quickly.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 162: Configure Auto-Rejoin settings

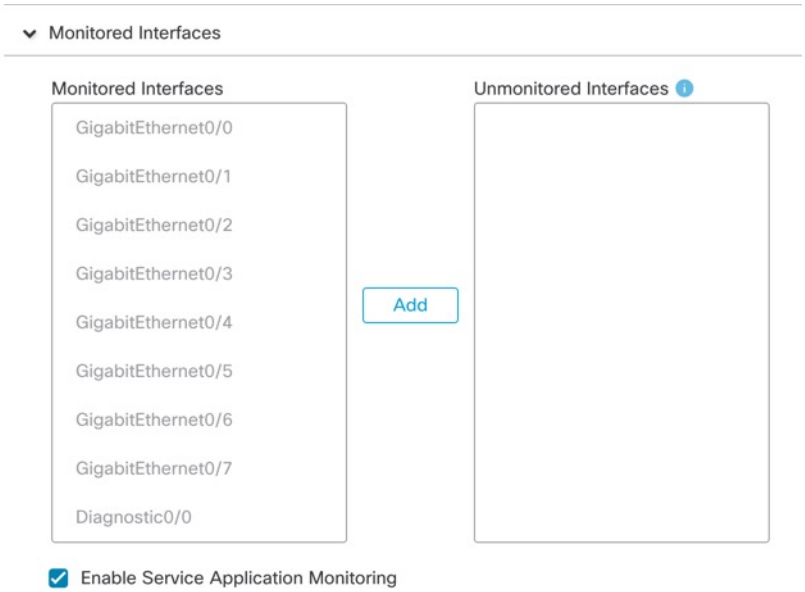


Set values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8 Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 163: Configure monitored interfaces



The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The time required to remove a member from the cluster depends on the type of interface and whether the node is established or is joining the cluster. By default, health check is enabled for all interfaces and the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save**.

Deploy configuration changes; see Deploy configuration changes, on page 135.

Manage cluster nodes

Describes how to manage cluster nodes to maintain high availability and optimal performance across your Cisco Secure Firewall cluster deployment.

Add a new cluster node

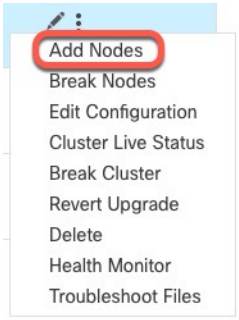
Adding new cluster nodes expands cluster capacity and provides additional redundancy for your security infrastructure.

You can add one or more new cluster nodes to an existing cluster.

Procedure

Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) for the cluster, and choose **Add Nodes**.

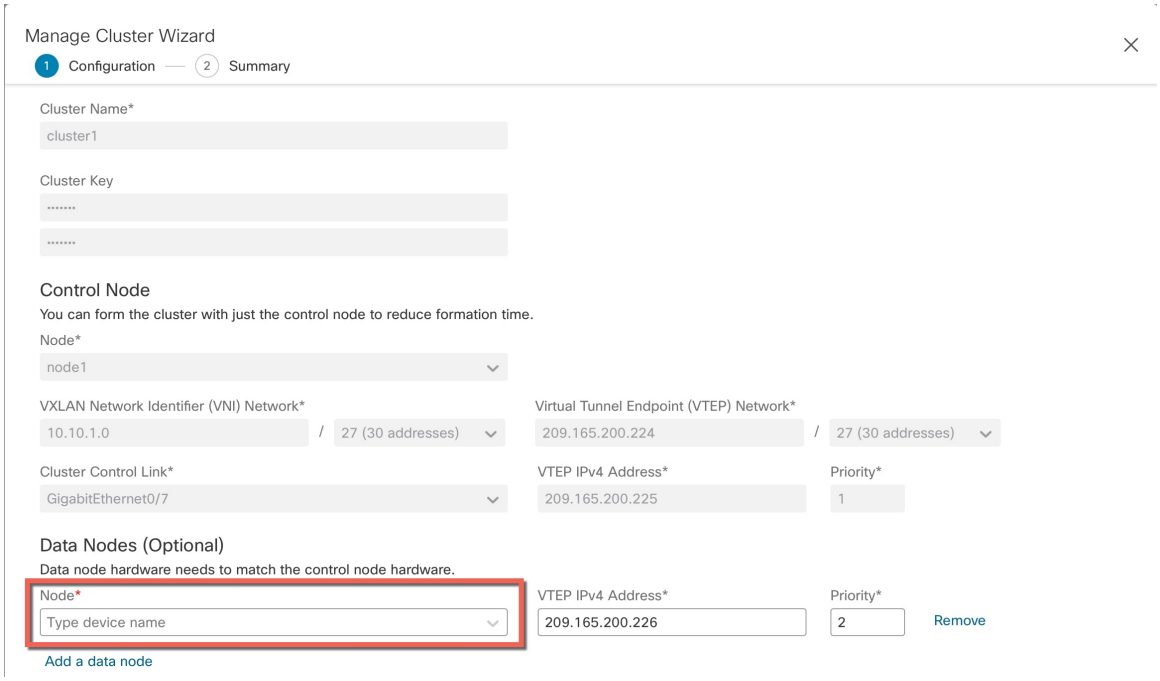
Figure 164: Add nodes



The **Manage Cluster Wizard** appears.

Step 2 From the **Node** menu, choose a device, and adjust the IP address and priority if desired.

Figure 165: Manage cluster wizard

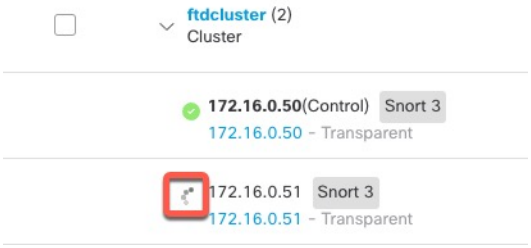


Step 3 To add additional nodes, click **Add a data node**.

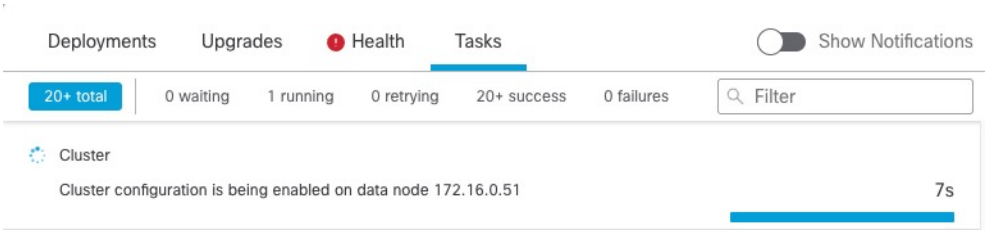
Step 4 Click **Continue**. Review the **Summary**, and then click **Save**

The node that is currently registering shows the loading icon.

Figure 166: Node registration



You can monitor cluster node registration by clicking the **Notifications** icon and choosing **Tasks**.



Break a node

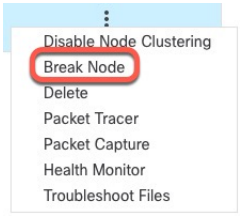
Breaking a node removes it from the cluster configuration, converting it to a standalone device.

You can remove a node from the cluster so that it becomes a standalone device. You cannot break the control node unless you break the entire cluster. The data node has its configuration erased.

Procedure

Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) for the node you want to break, and choose **Break Node**.

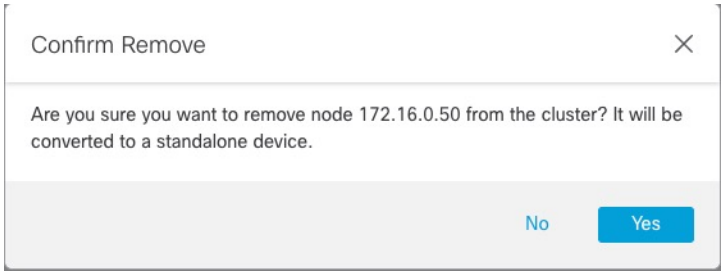
Figure 167: Break a node



You can optionally break one or more nodes from the cluster More menu by choosing **Break Nodes**.

Step 2 You are prompted to confirm the break. Click **Yes**.

Figure 168: Confirm break



You can monitor the cluster node break by clicking the **Notifications** icon and choosing **Tasks**.

Break the cluster

Break the cluster to convert all nodes to standalone devices when clustering is no longer needed.

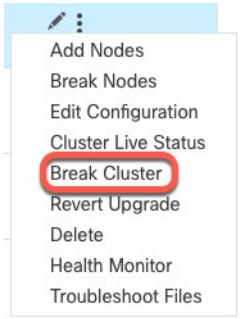
You can break the cluster and convert all nodes to standalone devices. The control node retains the interface and security policy configuration, while data nodes have their configuration erased.

Procedure

Step 1 Make sure all cluster nodes are being managed by the Firewall Management Center by reconciling nodes. Refer to Reconcile cluster nodes, on page 411.

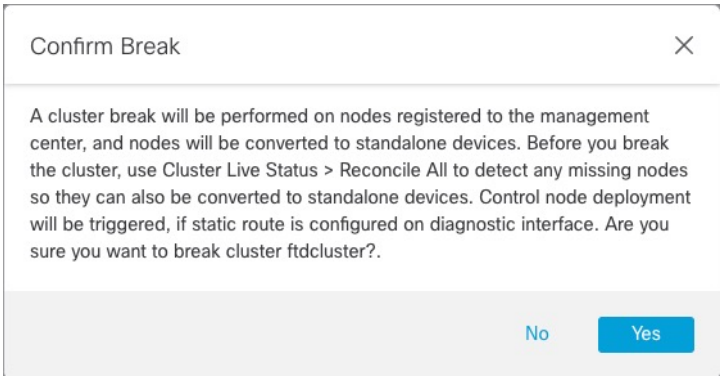
Step 2 Choose **Devices** > **Device Management**, click the **More** (⋮) for the cluster, and choose **Break Cluster**.

Figure 169: Break cluster



Step 3 You are prompted to break the cluster. Click **Yes**.

Figure 170: Confirm break



You can monitor the cluster break by clicking the **Notifications** icon and choosing **Tasks**.

Disable clustering

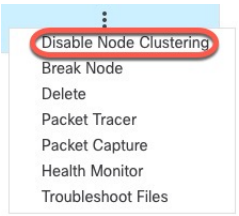
Temporarily deactivate a node in a cluster while keeping it visible in the device list.

You may want to deactivate a node in preparation for deleting the node, or temporarily for maintenance. This procedure is meant to temporarily deactivate a node; the node will still appear in the Firewall Management Center device list. When a node becomes inactive, all data interfaces are shut down.

Procedure

Step 1 For the unit you want to disable, choose **Devices** > **Device Management**, click **More** (⋮), and choose **Disable Node Clustering**.

Figure 171: Disable clustering



If you disable clustering on the control node, one of the data nodes will become the new control node. For centralized features, if you force a control node change, then all connections are dropped, and you have to reestablish the connections on the new control node. You cannot disable clustering on the control node if it is the only node in the cluster.

Step 2 Confirm that you want to disable clustering on the node.

The node will show **(Disabled)** next to its name in the **Devices** > **Device Management** list.

Step 3 To reenable clustering, refer to Rejoin the cluster, on page 409.

Rejoin the cluster

Rejoin a node to the cluster after it was removed because of failure or when clustering was manually disabled.

If a node was removed from the cluster, for example, due to a failed interface or if you manually disabled clustering, you must manually rejoin the cluster. Make sure the failure is resolved before you try to rejoin the cluster. Refer to Rejoining the cluster, on page 429 for more information about why a node can be removed from a cluster.

Procedure

Step 1 For the unit you want to reactivate, choose **Devices** > **Device Management**, click **More** (⋮), and choose **Enable Node Clustering**.

Step 2 Confirm that you want to enable clustering on the node.

Change the control node

This task changes the control node in a cluster when you need to specify the exact unit you want to become the control node.

The best method to change the control node is to disable clustering on the control node, wait for a new control election, and then re-enable clustering. Use this procedure when you must specify the exact unit you want to become the control node.

Caution If you must specify the *exact* unit you want to become the control node, use the procedure in this section. Note that for centralized features, if you force a control node change using either method, then all connections are dropped, and you have to re-establish the connections on the new control node.

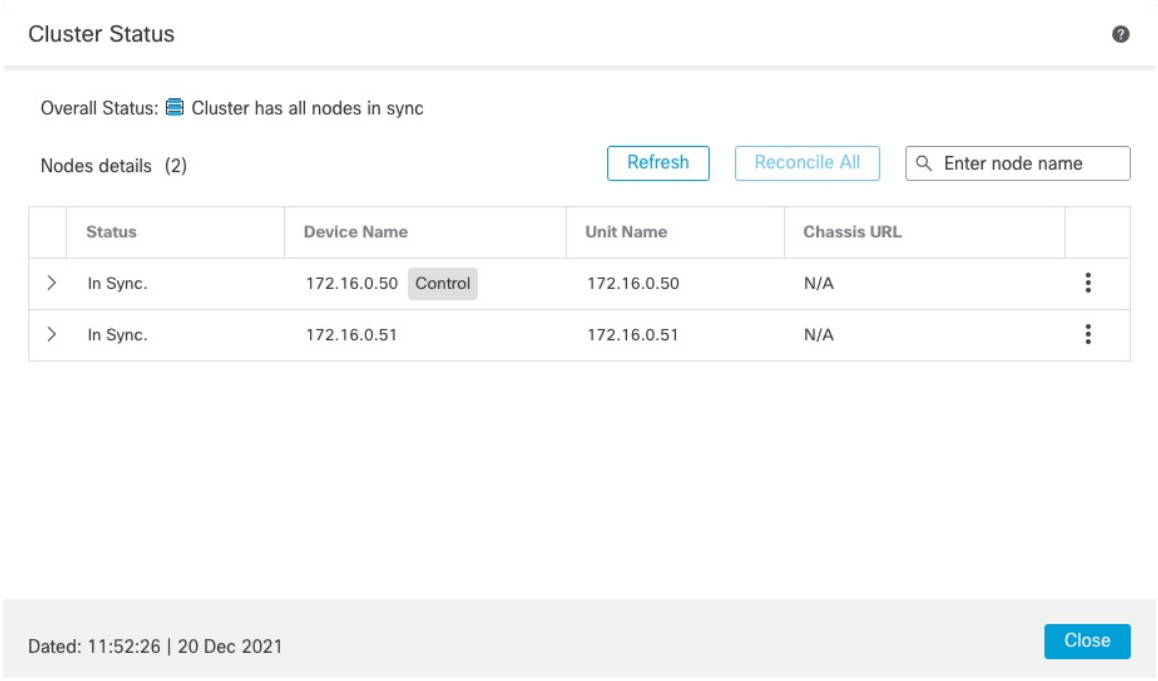
Before you begin

Follow these steps to change the control node:

Procedure

Step 1 Open the **Cluster Status** dialog box by choosing **Devices** > **Device Management**, **More** (⋮) > **Cluster Live Status**.

Figure 172: Cluster status



Step 2 For the unit you want to become the control unit, choose **More** > **Change Role to Control**.

Step 3 You are prompted to confirm the role change. Select the checkbox and click **OK**.

Edit the cluster configuration

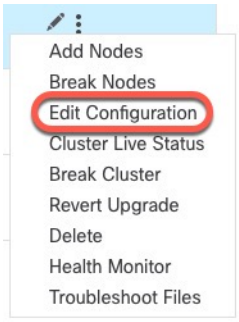
Edit the cluster configuration to modify cluster settings and parameters as needed for your network environment.

You can edit the cluster configuration. If you change any values other than the VTEP IP address for a node or node priority, the cluster will be broken and reformed automatically. Until the cluster is reformed, you may experience traffic disruption. If you change the VTEP IP address for a node or node priority, only the affected nodes are broken and readded to the cluster.

Procedure

Step 1 Choose **Devices** > **Device Management**, click the **More** for the cluster, and choose **Edit Configuration**.

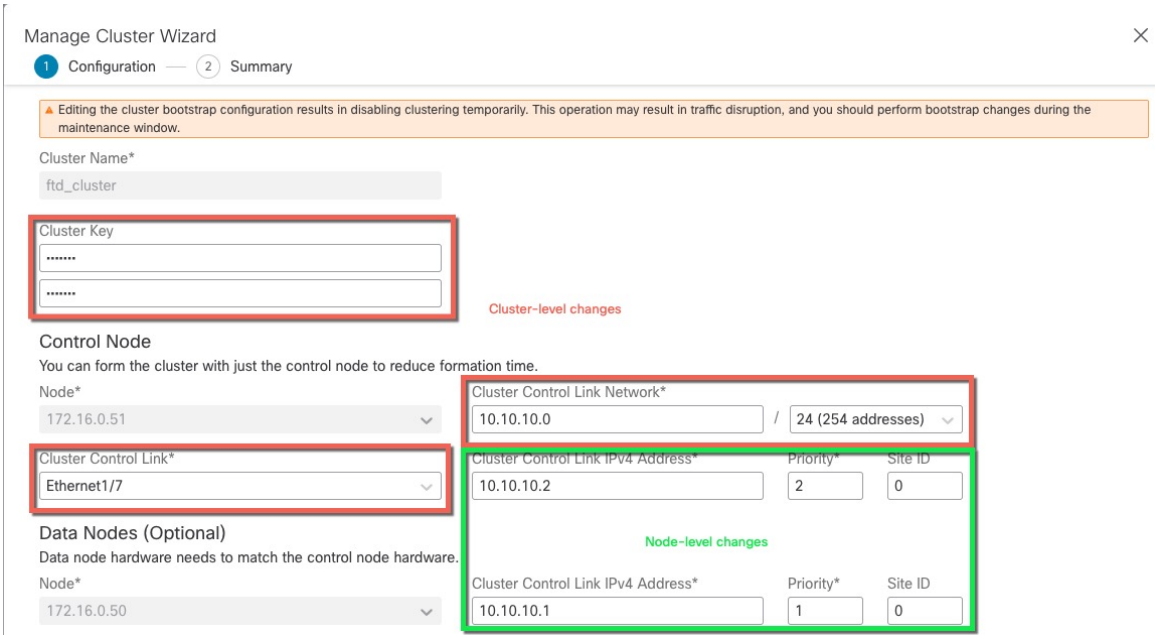
Figure 173: Edit configuration



The **Manage Cluster Wizard** appears.

Step 2 Update the cluster configuration.

Figure 174: Manage cluster wizard



Step 3 Click **Continue**. Review the **Summary**, and then click **Save**.

Reconcile cluster nodes

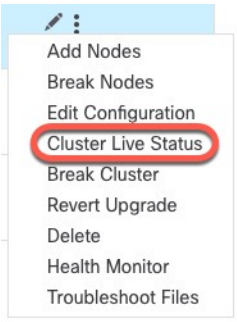
Use this procedure to reconcile cluster membership when a cluster node fails to register with the Firewall Management Center.

If a cluster node fails to register, you can reconcile the cluster membership from the device to the Firewall Management Center. For example, a data node might fail to register if the Firewall Management Center is occupied with certain processes, or if there is a network issue.

Procedure

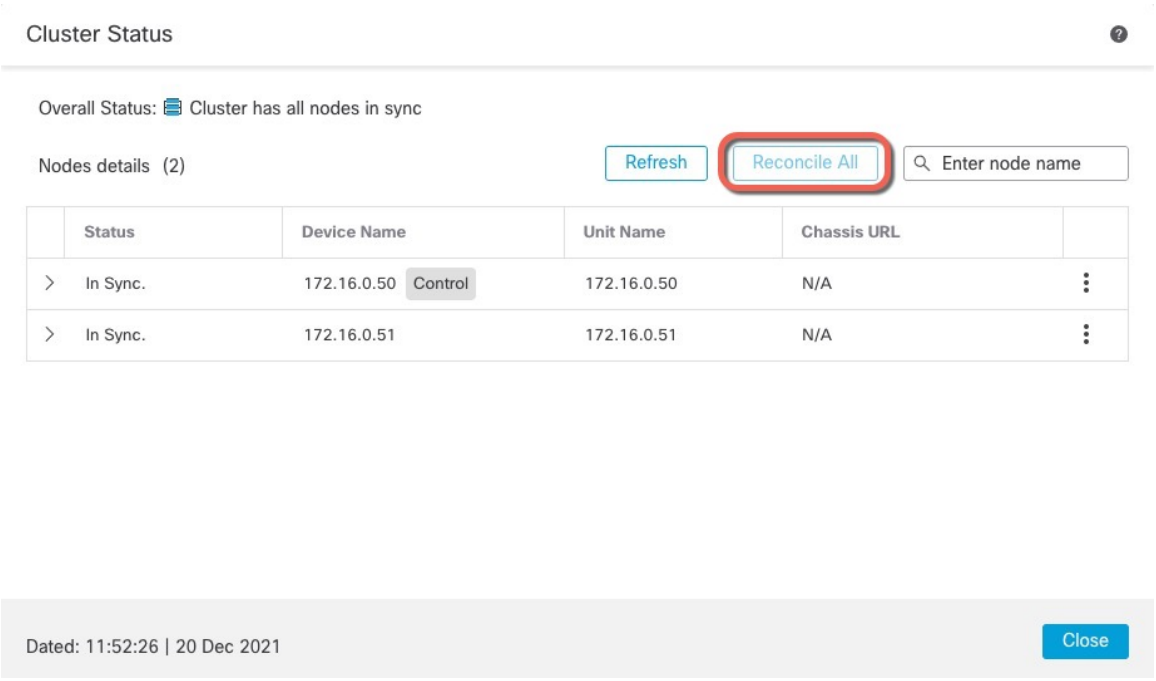
Step 1 Choose **Devices** > **Device Management**, **More** (⋮) for the cluster, and then choose **Cluster Live Status** to open the **Cluster Status** dialog box.

Figure 175: Cluster live status



Step 2 Click **Reconcile All**.

Figure 176: Reconcile all



Delete (Unregister) the cluster or nodes and register to a New Firewall Management Center

This task allows you to unregister cluster nodes from the current management center and register them to a different Management Center system.

Use this procedure when you need to move cluster nodes between Management Centers or when reconfiguring your management infrastructure.

You can unregister the cluster from the Firewall Management Center, which keeps the cluster intact. You might want to unregister the cluster if you want to add the cluster to a new Firewall Management Center.

You can also unregister a node from the Firewall Management Center without breaking the node from the cluster. Although the node is not visible in the Firewall Management Center, it is still part of the cluster, and it will continue to pass traffic and could even become the control node. You cannot unregister the current control node. You might want to unregister the node if it is no longer reachable from the Firewall Management Center, but you still want to keep it as part of the cluster while you troubleshoot management connectivity.

Unregistering a cluster:

- Severs all communication between the Firewall Management Center and the cluster.
- Removes the cluster from the **Device Management** page.
- Returns the cluster to local time management if the cluster's platform settings policy is configured to receive time from the Firewall Management Center using NTP.
- Leaves the configuration intact, so the cluster continues to process traffic.

  Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.

Registering the cluster again to the same or a different Firewall Management Center causes the configuration to be removed, so the cluster will stop processing traffic at that point; the cluster configuration remains intact so you can add the cluster as a whole. You can choose an access control policy at registration, but you will have to re-apply other policies after registration and then deploy the configuration before it will process traffic again.

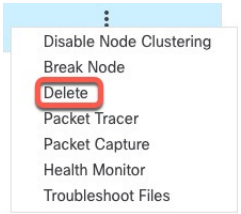
Before you begin

This procedure requires CLI access to one of the nodes.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster or node, and choose **Delete**.

Figure 177: Delete cluster or node



Step 2 You are prompted to delete the cluster or node; click **Yes**.

Step 3 You can register the cluster to a new or the same Firewall Management Center by adding one of the cluster nodes as a new device.

a) Connect to the CLI of one cluster node, and identify the new Firewall Management Center using the **configure manager add** command. See Modify Threat Defense Management Interfaces at the CLI.

b) Choose **Devices** > **Device Management**, and then click **Add Device**.

Add one of the cluster nodes as a device. The system will discover the remaining cluster nodes.

Step 4 To re-add a deleted node, refer to Reconcile cluster nodes, on page 411.

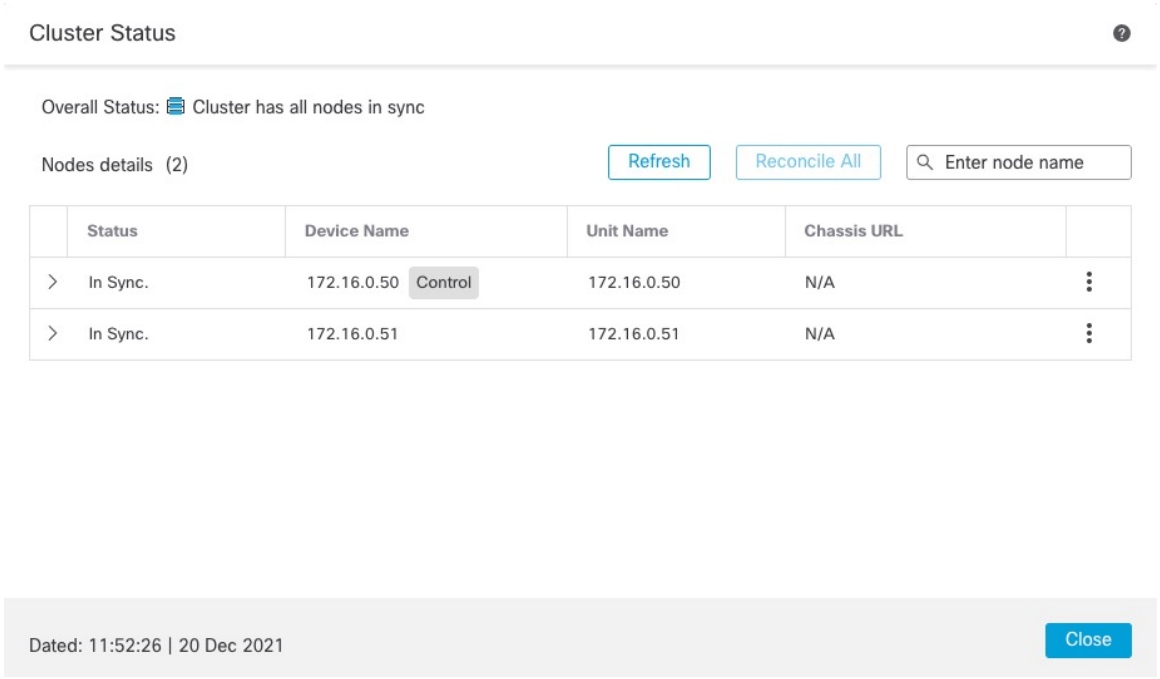
Monitor cluster status

You can monitor the cluster in the Firewall Management Center and at the Firewall Threat Defense CLI.

Monitor cluster status through these methods:

- **Cluster Status** dialog box, which is available from the **Devices** > **Device Management**, **More** (⋮) icon or from the **Devices** > **Device Management**, click **Add**, choose the **Cluster** page **General** area **Cluster Live Status** link.

Figure 178: Cluster status



The Control node has a graphic indicator identifying its role.

Cluster member **Status** includes these states:

- In Sync—The node is registered with the Firewall Management Center.

- Pending Registration—The node is part of the cluster, but has not yet registered with the Firewall Management Center. If a node fails to register, you can retry registration by clicking **Reconcile All**.
- Clustering is disabled—The node is registered with the Firewall Management Center, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the node from the cluster.
- Joining cluster...—The node is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the Firewall Management Center.

For each node, you can view the **Summary** or the **History**.

Figure 179: Node summary

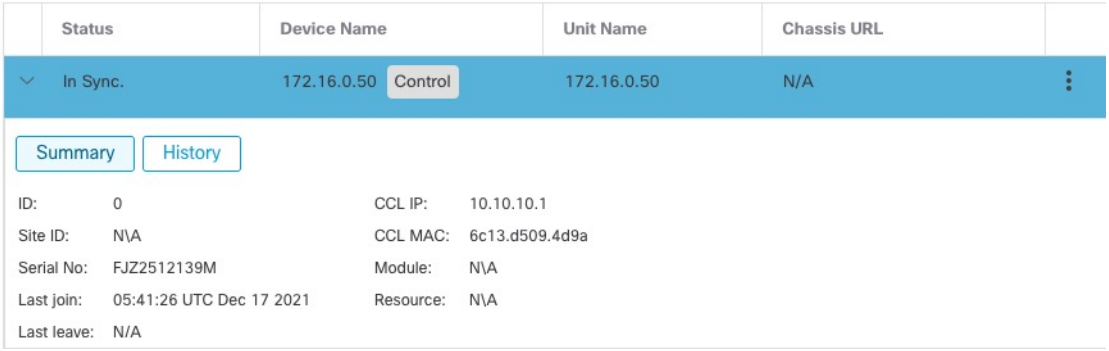
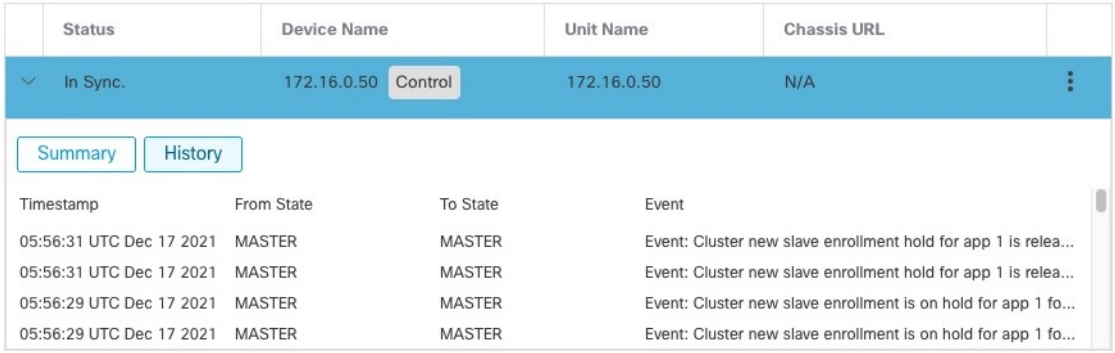


Figure 180: Node history



- **System** (⚙) > **Tasks** page.

  The **Tasks** page shows updates of the Cluster Registration task as each node registers.

- **Devices** > **Device Management** and then click **Add** > **Device** *cluster_name*.

  When you expand the cluster on the devices listing page, you can see all member nodes, including the control node shown with its role next to the IP address. For nodes that are still registering, you can see the loading icon.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  To view aggregated data for the entire cluster or other information, use the **show cluster** command.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  To view cluster information, use the **show cluster info** command.

Cluster health monitor

When a Firewall Threat Defense is the control node of a cluster, the Firewall Management Center collects various metrics periodically from the device metric data collector.

The cluster health monitor is comprised of these components:

- Overview dashboard: Displays information about the cluster topology, cluster statistics, and metric charts:
  - The topology section displays a cluster's live status, the health of individual threat defense, threat defense node type (control node or data node), and the status of the device. The status of the device could be *Disabled* (when the device leaves the cluster), *Added out of box* (in a public cloud cluster, the additional nodes that do not belong to the Firewall Management Center), or *Normal* (ideal state of the node).
  - The cluster statistics section displays current metrics of the cluster with respect to the CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.

Note The CPU and memory metrics display the individual average of the data plane and snort usage.

  - The metric charts, namely, CPU Usage, Memory Usage, Throughput, and Connections, diagrammatically display the statistics of the cluster over the specified time period.

- Load Distribution dashboard: Displays load distribution across the cluster nodes in two widgets:
  - The Distribution widget displays the average packet and connection distribution over the time range across the cluster nodes. This data depicts how the load is being distributed by the nodes. Using this widget, you can easily identify any abnormalities in the load distribution and rectify it.
  - The Node Statistics widget displays the node level metrics in table format. It displays metric data on CPU usage, memory usage, input rate, output rate, active connections, and NAT translations across the cluster nodes. This table view enables you to correlate data and easily identify any discrepancies.

- Member Performance dashboard: Displays current metrics of the cluster nodes. You can use the selector to filter the nodes and view the details of a specific node. The metric data include CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.
- CCL dashboard: Displays, graphically, the cluster control link data namely, the input, and output rate.
- Troubleshooting and Links: Provides convenient links to frequently used troubleshooting topics and procedures.
- Time range: An adjustable time window to constrain the information that appears in the various cluster metrics dashboards and widgets.

- Custom Dashboard: Displays data on both cluster-wide metrics and node-level metrics. However, node selection only applies for the threat defense metrics and not for the entire cluster to which the node belongs.

View the cluster health monitor

The cluster health monitor provides a detailed view of the health status of a cluster and its nodes. This cluster health monitor provides health status and trends of the cluster in an array of dashboards.

Before you begin

Ensure you have created a cluster from one or more devices in the Firewall Management Center.

Follow these steps to view the cluster health monitor:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**.

Use the Monitoring navigation pane to access node-specific health monitors.

Step 2 In the device list, click **Expand**(>) and **Collapse** (⌄) to expand and collapse the list of managed cluster devices.

Step 3 Click on the cluster name to view the cluster health statistics.

The cluster monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including its nodes, CPU, memory, input and output rates, connection statistics, and NAT translation information.
- Load Distribution: Traffic and packet distribution across the cluster nodes.
- Member Performance: Node-level statistics on CPU usage, memory usage, input throughput, output throughput, active connection, and NAT translation.
- CCL: Interface status and aggregate traffic statistics.

You can navigate through the various metrics dashboards by clicking on the labels. For a comprehensive list of the supported cluster metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

Step 4 Configure the time range from the drop-down in the upper-right corner.

The time range can reflect a period as short as the last hour (the default) or as long as two weeks. Select **Custom** from the drop-down to configure a custom start and end date.

Click the refresh icon to set auto refresh to 5 minutes or to toggle off auto refresh.

Step 5 Click on deployment icon for a deployment overlay on the trend graph, with respect to the selected time range.

The deployment icon indicates the number of deployments during the selected time-range. A vertical band indicates the deployment start and end time. For multiple deployments, multiple bands/lines appear. Click on the icon on top of the dotted line to view the deployment details.

Step 6 View the **Health Alerts** for the node in the alert notification at the top of page, directly to the right of the device name.

Hover your pointer over the **Health Alerts** to view the health summary of the node. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.

Step 7 View device monitor health and performance metrics in several predefined dashboards.

The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information.
- CPU: CPU utilization, including the CPU usage by process and by physical cores.
- Memory: Device memory utilization, including data plane and Snort memory usage.
- Interfaces: Interface status and aggregate traffic statistics.
- Connections: Connection statistics (such as elephant flows, active connections, peak connections, and so on) and NAT translation counts.
- Snort: Statistics that are related to the Snort process.
- ASP drops: Statistics related to the dropped packets against various reasons.

You can navigate through the various metrics dashboards by clicking on the labels. Refer to Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Step 8 Click the plus sign **Add New Dashboard**(+) in the upper right corner of the health monitor to create a custom dashboard by building your own variable set from the available metric groups.

For cluster-wide dashboard, choose Cluster metric group, and then choose the metric.

Cluster metrics

The cluster health monitor tracks statistics that are related to a cluster and its nodes, and aggregate of load distribution, performance, and CCL traffic statistics.

Table 30: Cluster Metrics

Metric	Description	Format
CPU	Average of CPU metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Memory	Average of memory metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Data Throughput	Incoming and outgoing data traffic statistics for a cluster.	bytes
CCL Throughput	Incoming and outgoing CCL traffic statistics for a cluster.	bytes

Metric	Description	Format
Connections	Count of active connections in a cluster.	number
NAT Translations	Count of NAT translations for a cluster.	number
Distribution	Connection distribution count in the cluster for every second.	number
Packets	Packet distribution count in the cluster for every second.	number

Troubleshoot the cluster

Use these methods to troubleshoot the devices and clusters:

- Use **Logs** to generates troubleshooting files for all nodes in the cluster. Use this option when you need one cluster-level collection instead of generating troubleshooting files from each node separately.
- Use **CLI** to run a predefined set of cluster diagnostic commands and displays the output. Use this option to check cluster configuration, member state, cluster health, control-plane transport statistics, packet drops, interface status, CPU usage, memory buffers, ARP entries, and reachability. The **CLI** option displays command output; it does not open an interactive CLI session.

Commands
show running-config cluster: Review the cluster group configuration, local unit, cluster interface, priority, health-check, auto-rejoin, and cLACP settings.
show cluster info: Confirm that clustering is enabled and identify the control node, member state, software version, serial number, CCL IP address, CCL MAC address, and last join or leave state.
show cluster info health: Check unit, interface, service, and overall cluster health.
show cluster info transport cp: Review control-plane transport counters, including reliable and unreliable message counters, errors, retransmits, drops, and buffer conditions.
show version: Capture platform, software, build, UUID, LSP, VDB, uptime, resource, and license context.
show asp drop: Identify accelerated security path packet or flow drop reasons and counters.
show counters: Review protocol, feature, and cluster CCL counters.
show arp: Verify ARP entries for interfaces that participate in cluster communication.
show int ip brief: Check interface IP addresses and administrative and line protocol status.
show blocks: Check buffer availability and failed allocations.
show cpu detailed: Check data path, control point, and total CPU usage.

Commands
show interface *ccl_interface*: Review interface state, MTU, MAC address, IP address, traffic counters, errors, and drops for the cluster-related interface.
ping *ccl_ip* **size** *ccl_mtu* **repeat 2**: Test reachability to a cluster peer by using the packet size selected by the tool.

- Use the **CCL Ping** when you need to test cluster control link connectivity between joined cluster nodes.
- Troubleshooting files—If a node fails to join the cluster, a troubleshooting file is automatically generated. You can also generate and download troubleshooting files from the **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area. For more information, refer to Generate troubleshooting files, on page 745.

  You can also generate files from the **Device Management** page. Click **More** (⋮) and choose **Troubleshoot Files**.
- CLI output—Choose **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area, you can view a set of pre-defined CLI outputs that can help you troubleshoot the cluster. These commands are automatically run for the cluster:

  You can also enter any **show** command in the **Command** field.

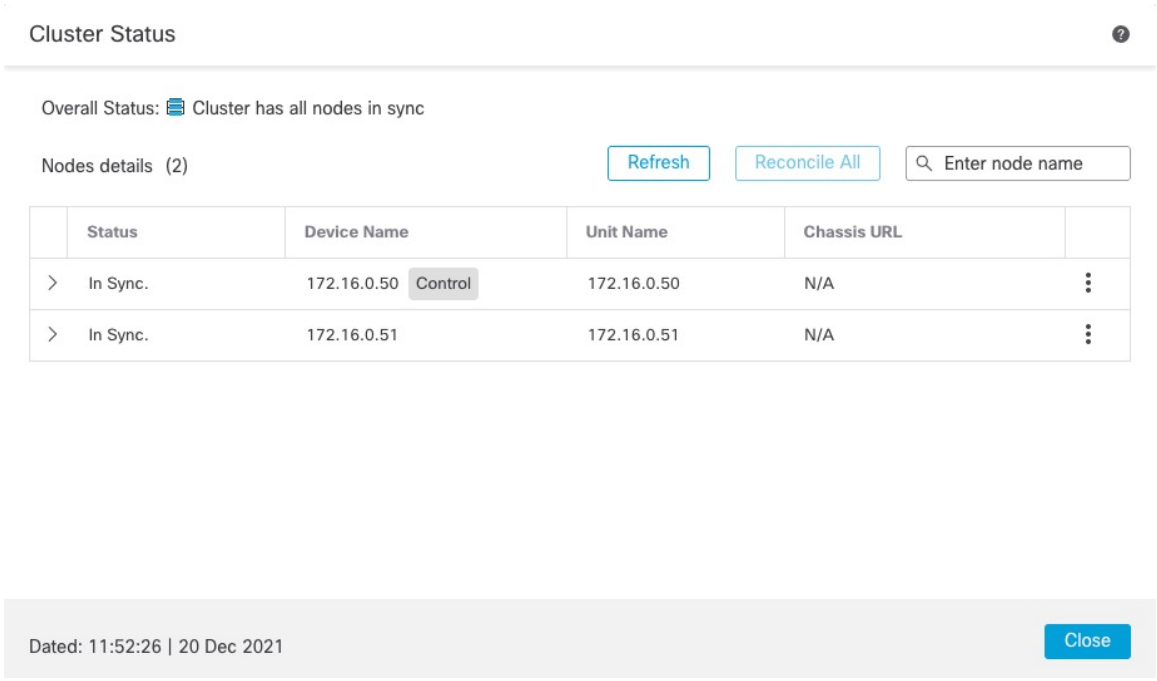
Perform a ping on the cluster control link

You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs.

Procedure

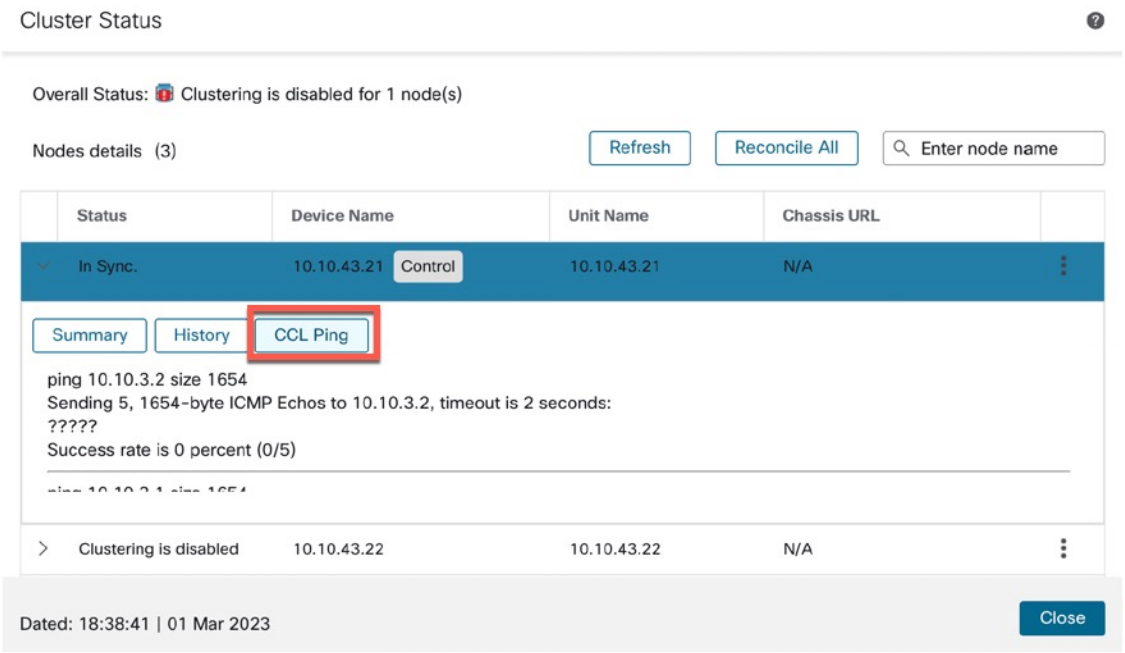
Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) icon next to the cluster, and choose **Cluster Live Status**.

Figure 181: Cluster status



Step 2 Expand one of the nodes, and click **CCL Ping**.

Figure 182: CCL ping



The node sends a ping on the cluster control link to every other node using a packet size that matches the maximum MTU.

Reference for clustering

This section includes more information about how clustering operates.

Threat Defense features and clustering

Some Firewall Threat Defense features are not supported with clustering, and some are only supported on the control unit. Other features might have caveats for proper usage.

Unsupported features and clustering

Centralized features for clustering

These features are only supported on the control node, and are not scaled for the cluster.

Note Traffic for centralized features is forwarded from member nodes to the control node over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-control nodes before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the control node.

For centralized features, if the control node fails, all connections are dropped, and you have to re-establish the connections on the new control node.

Note To view FlexConfig features that are also centralized with clustering, for example RADIUS inspection, refer to the ASA general operations configuration guide. FlexConfig lets you configure many ASA features that are not present in the Firewall Management Center GUI. For more information, refer to FlexConfig policies, on page 921.

- These application inspections are supported:
  - DCERPC and ESMTP
  - NetBIOS and PPTP
  - RSH
  - SQLNET and SUNRPC
  - TFTP
  - XDMCP

- Static route monitoring
- Site-to-site VPN
- IGMP multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- PIM multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- Dynamic routing

Connection settings and clustering

Connection limits are enforced cluster-wide. Each node has an estimate of the cluster-wide counter values based on broadcast messages. Due to efficiency considerations, the configured connection limit across the cluster might not be enforced exactly at the limit number. Each node may overestimate or underestimate the cluster-wide counter value at any given time. However, the information will get updated over time in a load-balanced cluster.

Dynamic routing and clustering

Dynamic routing and clustering are network configuration approaches that

- enable each node to run the routing protocol as a standalone router in Individual interface mode,
- allow routes to be learned by each node independently, and
- require separate router IDs for each node when communicating with external routers.

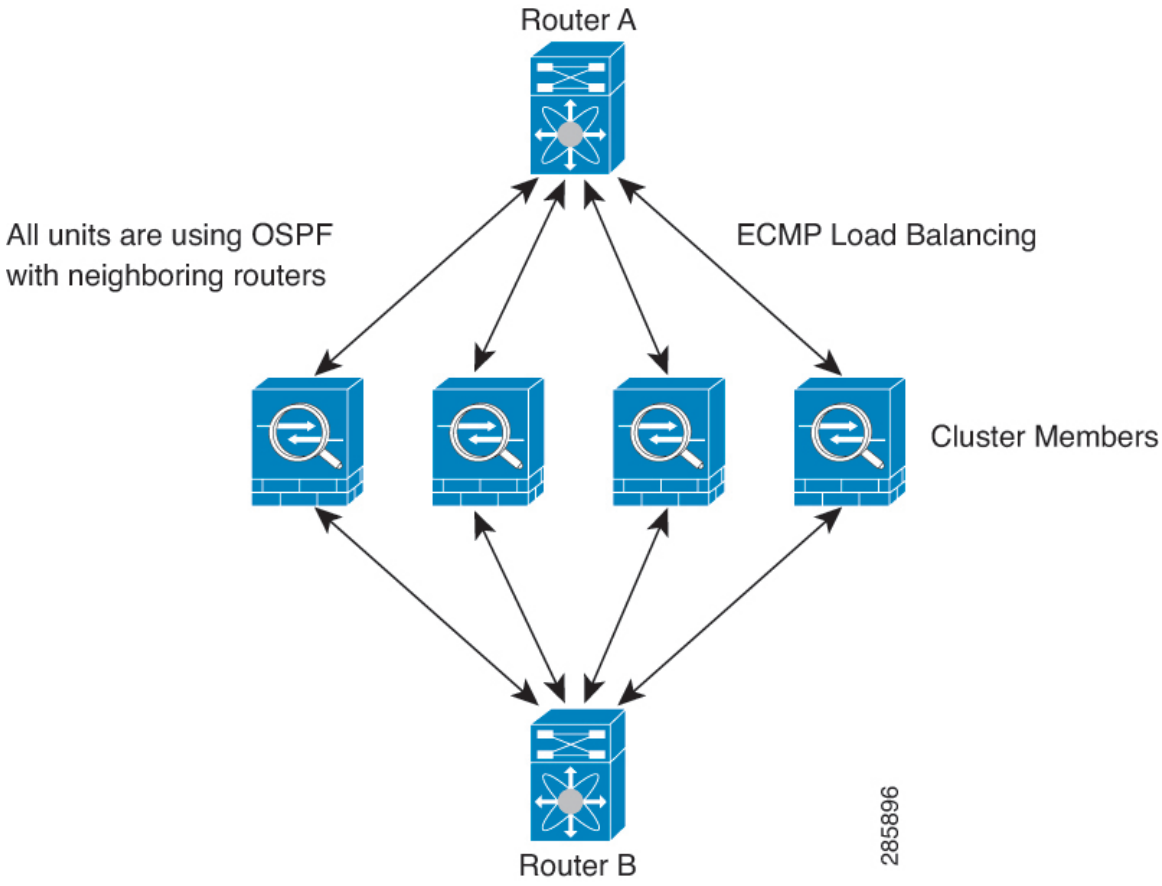
Routing behavior and load balancing

In Individual interface mode, ECMP is used to load balance traffic between multiple equal-cost paths. External routers can discover multiple paths to destinations through different cluster nodes.

Router A learns that there are 4 equal-cost paths to Router B, each through a node. ECMP is used to load balance traffic between the 4 paths. Each node picks a different router ID when communicating with external routers.

You must configure a cluster pool for the router ID so that each node has a separate router ID.

Figure 183: Dynamic routing in individual interface mode



FTP and clustering

- If FTP data channel and control channel flows are owned by different cluster members, then the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

NAT and clustering

Provides information about NAT behavior and limitations in clustering deployments.

NAT can affect the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different Firewall Threat Defenses in the cluster, because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When a packet arrives at the Firewall Threat Defense that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link. Note that the receiving node does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

If you still want to use NAT in clustering, then consider the following guidelines:

- No Proxy ARP—For individual interfaces, a proxy ARP reply is never sent for mapped addresses. This prevents the adjacent router from maintaining a peer relationship with an ASA that may no longer be in the cluster. The upstream router requires a static route or policy-based routing (PBR) with Object Tracking for the mapped addresses, which must point to the main cluster IP address.
- No interface PAT on an individual interface—Interface PAT is not supported for Individual interfaces.
- PAT with Port Block Allocation—See the following guidelines for this feature:
  - Maximum-per-host limit is not a cluster-wide limit, and is enforced on each node individually. Thus, in a 3-node cluster with the maximum-per-host limit configured as 1, if the traffic from a host is load-balanced across all 3 nodes, then it can get allocated 3 blocks with 1 in each node.
  - Port blocks created on the backup node from the backup pools are not accounted for when enforcing the maximum-per-host limit.
  - On-the-fly PAT rule modifications, where the PAT pool is modified with a completely new range of IP addresses, will result in xlate backup creation failures for the xlate backup requests that were still in transit while the new pool became effective. This behavior is not specific to the port block allocation feature, and is a transient PAT pool issue seen only in cluster deployments where the pool is distributed and traffic is load-balanced across the cluster nodes.
  - When operating in a cluster, you cannot simply change the block allocation size. The new size is effective only after you reload each device in the cluster. To avoid having to reload each device, we recommend that you delete all block allocation rules and clear all xlates related to those rules. You can then change the block size and recreate the block allocation rules.
- NAT pool address distribution for dynamic PAT—When you configure a PAT pool, the cluster divides each IP address in the pool into port blocks. By default, each block is 512 ports, but if you configure port block allocation rules, your block setting is used instead. These blocks are distributed evenly among the nodes in the cluster, so that each node has one or more blocks for each IP address in the PAT pool. Thus, you could have as few as one IP address in a PAT pool for a cluster, if that is sufficient for the number of PAT'ed connections you expect. Port blocks cover the 1024-65535 port range, unless you configure the option to include the reserved ports, 1-1023, on the PAT pool NAT rule.
- Reusing a PAT pool in multiple rules—To use the same PAT pool in multiple rules, you must be careful about the interface selection in the rules. You must either use specific interfaces in all rules, or "any" in all rules. You cannot mix specific interfaces and "any" across the rules, or the system might not be able to match return traffic to the right node in the cluster. Using unique PAT pools per rule is the most reliable option.
- No round-robin—Round-robin for a PAT pool is not supported with clustering.
- No extended PAT—Extended PAT is not supported with clustering.
- Dynamic NAT xlates managed by the control node—The control node maintains and replicates the xlate table to data nodes. When a data node receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the control node. The data node owns the connection.
- Stale xlates—The xlate idle time on the connection owner does not get updated. Thus, the idle time might exceed the idle timeout. An idle timer value higher than the configured timeout with a refcnt of 0 is an indication of a stale xlate.
- No static PAT for the following inspections—
  - FTP

- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- If you have an extremely large number of NAT rules, over ten thousand, you should enable the transactional commit model using the **asp rule-engine transactional-commit nat** command in the device CLI. Otherwise, the node might not be able to join the cluster.

SIP inspection and clustering

A control flow can be created on any node (due to load balancing); its child data flows must reside on the same node.

SNMP and clustering

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new control node is elected, the poll to the new control node will fail.

When using SNMPv3 with clustering, if you add a new cluster node after the initial cluster formation, then SNMPv3 users are not replicated to the new node. You must remove the users, and re-add them, and then redeploy your configuration to force the users to replicate to the new node.

Syslog and clustering

- Each node in the cluster generates its own syslog messages. You can configure logging so that each node uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all nodes in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all nodes look as if they come from a single node. If you configure logging to use the local-node name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different nodes.

Cisco trustsec and clustering

Only the control node learns security group tag (SGT) information. The control node then populates the SGT to data nodes, and data nodes can make a match decision for SGT based on the security policy.

VPN and clustering

VPN functionality is limited to the control node and does not take advantage of the cluster high availability capabilities. If the control node fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control node is elected, you must reestablish the VPN connections.

For connections to an individual interface when using Policy-Based Routing (PBR) or Equal-Cost Multi-Path (ECMP), you must always connect to the Main cluster IP address, not a Local address.

VPN-related keys and certificates are replicated to all nodes.

Note Remote access VPN is not supported with clustering.

Performance scaling factor

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately 80% of the maximum combined throughput.

Throughput calculation

For example, if your model can handle approximately 10 Gbps of traffic when running alone, then for a cluster of 8 units, the maximum combined throughput will be approximately 80% of 80 Gbps (8 units x 10 Gbps): 64 Gbps.

Control node election

The key components involved in the control node election process are:

- Cluster nodes: Communicate over the cluster control link and participate in the election process
- Election requests: Broadcast every three seconds by nodes when clustering is enabled
- Priority values: Set between 1 and 100 where 1 is the highest priority
- Control node: The elected node that coordinates cluster operations

These stages describe how cluster nodes elect a control node:

1. When clustering is enabled for a node (or when it first starts up with clustering already enabled), the node broadcasts an election request every three seconds.
2. Any other nodes with a higher priority respond to the election request. The priority is set between 1 and 100, where 1 is the highest priority.
3. If after 45 seconds, a node does not receive a response from another node with a higher priority, then it becomes the control node.

Note If multiple nodes tie for the highest priority, the cluster node name and then the serial number is used to determine the control node.

4. If a node later joins the cluster with a higher priority, it does not automatically become the control node. The existing control node always remains as the control node unless it stops responding, at which point a new control node is elected.
5. In a "split-brain" scenario where multiple control nodes exist temporarily, the node with the highest priority retains the role, while the other nodes return to data node roles.

Note You can manually force a node to become the control node. For centralized features, if you force a control node change, then all connections are dropped, and you have to re-establish the connections on the new control node.

High availability within the cluster

Clustering provides high availability by monitoring node and interface health and by replicating connection states between nodes.

Node health monitoring

Each node periodically sends a broadcast heartbeat packet over the cluster control link. If the control node does not receive any heartbeat packets or other packets from a data node within the configurable timeout period, then the control node removes the data node from the cluster. If the data nodes do not receive packets from the control node, then a new control node is elected from the remaining nodes.

Split brain scenario

If nodes cannot reach each other over the cluster control link because of a network failure and not because a node has actually failed, then the cluster may go into a "split brain" scenario where isolated data nodes will elect their own control nodes. For example, if a router fails between two cluster locations, then the original control node at location 1 will remove the location 2 data nodes from the cluster. Meanwhile, the nodes at location 2 will elect their own control node and form their own cluster. Note that asymmetric traffic may fail in this scenario. After the cluster control link is restored, then the control node that has the higher priority will keep the control node's role.

Interface monitoring

Each node monitors the link status of all named hardware interfaces in use, and reports status changes to the control node.

All physical interfaces are monitored; only named interfaces can be monitored. You can optionally disable monitoring per interface.

A node is removed from the cluster if its monitored interfaces fail. The node is removed after 500 milliseconds.

Status after failure

When a node in the cluster fails, the connections hosted by that node are seamlessly transferred to other nodes; state information for traffic flows is shared over the control node's cluster control link.

If the control node fails, then another member of the cluster with the highest priority (lowest number) becomes the control node.

The Firewall Threat Defense automatically tries to rejoin the cluster, depending on the failure event.

Note When the Firewall Threat Defense becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management interface can send and receive traffic.

Rejoining the cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

- Failed cluster control link when initially joining—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering.
- Failed cluster control link after joining the cluster—The Firewall Threat Defense automatically tries to rejoin every 5 minutes, indefinitely.
- Failed data interface—The Firewall Threat Defense automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the Firewall Threat Defense application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.
- Failed node—If the node was removed from the cluster because of a node health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the node will rejoin the cluster when it starts up again as long as the cluster control link is up. The Firewall Threat Defense application attempts to rejoin the cluster every 5 seconds.
- Internal error—Internal failures include: application sync timeout; inconsistent application statuses; and so on.
- Failed configuration deployment—If you deploy a new configuration from Firewall Management Center, and the deployment fails on some cluster members but succeeds on others, then the nodes that failed are removed from the cluster. You must manually rejoin the cluster by re-enabling clustering. If the deployment fails on the control node, then the deployment is rolled back, and no members are removed. If the deployment fails on all data nodes, then the deployment is rolled back, and no members are removed.

Data path connection state replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

Table 31: Features Replicated Across the Cluster

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	—
MAC address table	Yes	—
User Identity	Yes	—
IPv6 Neighbor database	Yes	—
Dynamic routing	Yes	—

Traffic	State Support	Notes
SNMP Engine ID	**No**	—

How the cluster manages connections

Connections can be load-balanced to multiple nodes of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

Connection roles

See the following roles defined for each connection:

- Owner—Usually, the node that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new nodes receive packets from the connection, the director chooses a new owner from those nodes.
- Backup owner—The node that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then the first node to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

  As long as the director (see below) is not the same node as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

  For clustering on the Firepower 9300, which can include up to 3 cluster nodes in one chassis, if the backup owner is on the same chassis as the owner, then an additional backup owner will be chosen from another chassis to protect flows from a chassis failure.
- Director—The node that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and ports (see below for ICMP hash details), and sends a message to the director to register the new connection. If packets arrive at any node other than the owner, the node queries the director about which node is the owner so it can forward the packets. A connection has only one director. If a director fails, the owner chooses a new director.

  As long as the director is not the same node as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.

  ICMP/ICMPv6 hash details:

  - For Echo packets, the source port is the ICMP identifier, and the destination port is 0.
  - For Reply packets, the source port is 0, and the destination port is the ICMP identifier.
  - For other packets, both source and destination ports are 0.
- Forwarder—A node that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner.

A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.



Note We do not recommend disabling TCP sequence randomization when using clustering. There is a small chance that some TCP sessions won't be established, because the SYN/ACK packet might be dropped.

- Fragment Owner—For fragmented packets, cluster nodes that receive a fragment determine a fragment owner using a hash of the fragment source IP address, destination IP address, and the packet ID. All fragments are then forwarded to the fragment owner over the cluster control link. Fragments may be load-balanced to different cluster nodes, because only the first fragment includes the 5-tuple used in the switch load balance hash. Other fragments do not contain the source and destination ports and may be load-balanced to other cluster nodes. The fragment owner temporarily reassembles the packet so it can determine the director based on a hash of the source/destination IP address and ports. If it is a new connection, the fragment owner will register to be the connection owner. If it is an existing connection, the fragment owner forwards all fragments to the provided connection owner over the cluster control link. The connection owner will then reassemble all fragments.

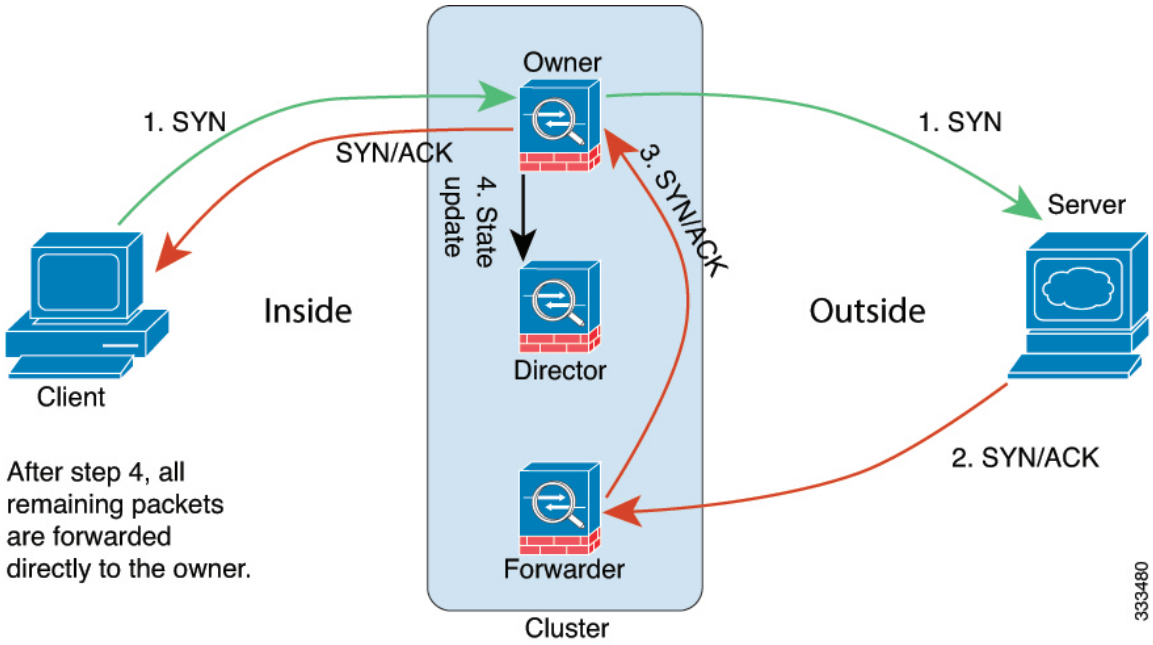
Port Address Translation Connections

New connection ownership

Traffic redirection is not supported in this release. When a new connection is directed to a node of the cluster via load balancing, that node owns both directions of the connection. All the subsequent packets for the same connection should arrive the same node. If any connection packets arrive at a different node, they will be dropped. If a reverse flow arrives at a different node, it will be dropped as well. For centralized features, if the connections do not arrive on the control node, they will be dropped.

Sample data flow for TCP

The following example shows the establishment of a new connection.

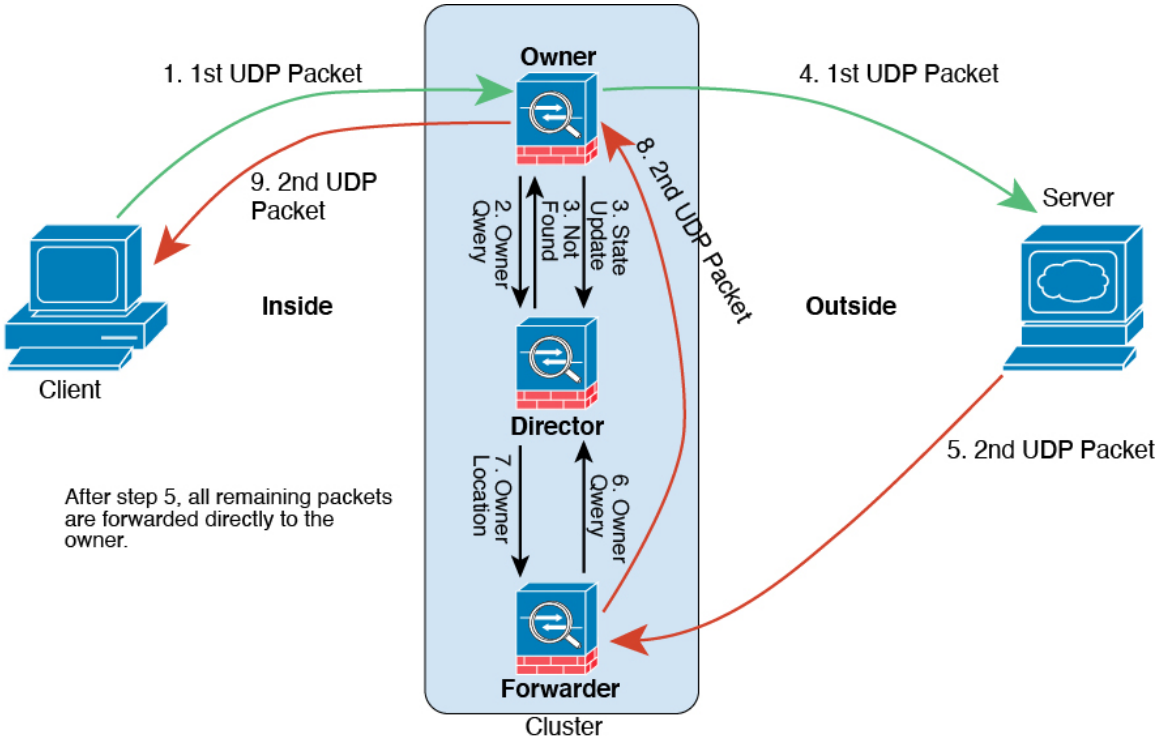


1. The SYN packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.
2. The SYN-ACK packet originates from the server and is delivered to a different Firewall Threat Defense (based on the load balancing method). This Firewall Threat Defense is the forwarder.
3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.
4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.
5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.
6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.
7. If packets are delivered to any additional nodes, it will query the director for the owner and establish a flow.
8. Any state change for the flow results in a state update from the owner to the director.

Sample data flow for ICMP and UDP

The following example shows the establishment of a new connection.

1. *Figure 184: ICMP and UDP Data Flow*



The first UDP packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method).

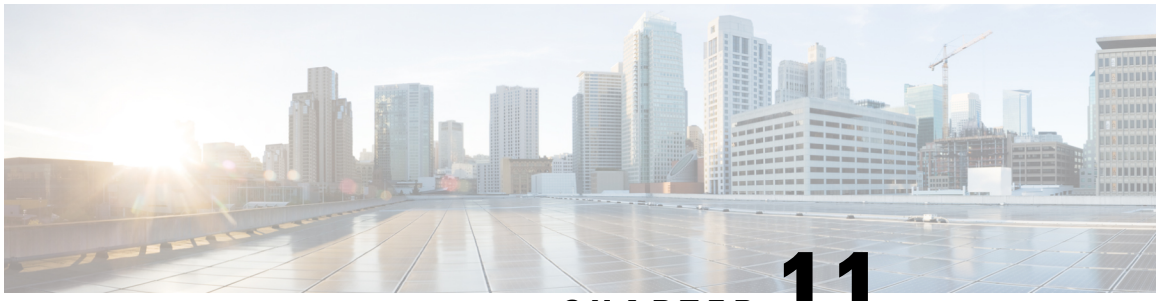
2. The node that received the first packet queries the director node that is chosen based on a hash of the source/destination IP address and ports.
3. The director finds no existing flow, creates a director flow and forwards the packet back to the previous node. In other words, the director has elected an owner for this flow.
4. The owner creates the flow, sends a state update to the director, and forwards the packet to the server.
5. The second UDP packet originates from the server and is delivered to the forwarder.
6. The forwarder queries the director for ownership information. For short-lived flows such as DNS, instead of querying, the forwarder immediately sends the packet to the director, which then sends it to the owner.
7. The director replies to the forwarder with ownership information.
8. The forwarder creates a forwarding flow to record owner information and forwards the packet to the owner.
9. The owner forwards the packet to the client.

History for clustering: private cloud

This reference provides the feature history for clustering functionality in private cloud environments, including version information, platform compatibility, and detailed descriptions of enhancements and new capabilities.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Clustering for the Firewall Threat Defense Virtual on VMware and KVM	7.4.1	7.4.1	The Firewall Threat Defense Virtual now supports individual interface clustering for up to 16 nodes on VMware and KVM.
Cluster control link ping tool.	7.2.6/7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** > **Cluster Live Status.**
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**
Automatic generation of a troubleshooting file on a node when it fails to join the cluster.	7.4.1	7.4.1	If a node fails to join the cluster, a troubleshooting file is automatically generated for the node. You can download the file from **Tasks** or from the **Cluster** page.
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cluster health monitor settings	7.3.0	Any	You can now edit cluster health monitor settings. New/Modified screens: **Devices** > **Device Management** > **Cluster** > **Cluster Health Monitor Settings** **Note** If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.
Cluster health monitor dashboard	7.3.0	Any	You can now view cluster health on the cluster health monitor dashboard. New/Modified screens: **System** > **Health** > **Monitor**
Clustering for the Firewall Threat Defense Virtual on VMware and KVM	7.2.0	7.2.0	The Firewall Threat Defense Virtual supports Individual interface clustering for up to 4 nodes on VMware and KVM. New/Modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** Supported platforms: Firewall Threat Defense Virtual on VMware and KVM



CHAPTER 11

Clustering: Public Cloud

Clustering lets you group multiple Firewall Threat Defense Virtuals together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. You can deploy Firewall Threat Defense Virtual clusters in a public cloud using the following public cloud platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Currently, only routed firewall mode is supported.

Note Some features are not supported when using clustering. See Unsupported Features and Clustering.

- About Threat Defense Virtual clustering in the public cloud, on page 437
- Licenses for Threat Defense Virtual clustering, on page 440
- Requirements and prerequisites for Threat Defense Virtual clustering, on page 441
- Guidelines for Threat Defense Virtual clustering, on page 443
- Deploy the cluster in AWS, on page 444
- Deploy the cluster in Azure, on page 466
- Deploy the cluster in GCP, on page 485
- Add the cluster to the Management Center (manual deployment), on page 493
- Edit cluster health monitor settings, on page 500
- Manage cluster nodes, on page 503
- Monitor cluster status, on page 506
- Troubleshoot the cluster, on page 512
- Upgrade the cluster, on page 514
- Reference for clustering, on page 515
- History for Threat Defense Virtual clustering in the public cloud, on page 527

About Threat Defense Virtual clustering in the public cloud

This section describes the clustering architecture and how it works.

How the cluster fits into your network

The cluster consists of multiple firewalls acting as a single device. To act as a cluster, the firewalls need the following infrastructure:

- Isolated network for intra-cluster communication, known as the cluster control link, using VXLAN interfaces. VXLANs, which act as Layer 2 virtual networks over Layer 3 physical networks, let the Firewall Threat Defense Virtual send broadcast or multicast messages over the cluster control link.
- Load Balancer(s)—For external load balancing, you have the following options depending on your public cloud:
  - AWS Gateway Load Balancer

    The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The Firewall Threat Defense Virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint) using a Geneve interface single-arm proxy.
  - Azure Gateway Load Balancer

    In an Azure service chain, Firewall Threat Defense Virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The Firewall Threat Defense Virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.
  - Native GCP load balancers, internal and external
  - Equal-Cost Multi-Path Routing (ECMP) using inside and outside routers such as Cisco Cloud Services Router

    ECMP routing can forward packets over multiple “best paths” that tie for top place in the routing metric. Like EtherChannel, a hash of source and destination IP addresses or source and destination ports, or both, can be used to send a packet to one of the next hops. If you use static routes for ECMP routing, then the Firewall Threat Defense failure can cause problems; the route continues to be used, and traffic to the failed Firewall Threat Defense will be lost. If you use static routes, be sure to use a static route monitoring feature such as Object Tracking. We recommend using dynamic routing protocols to add and remove routes, in which case, you must configure each Firewall Threat Defense to participate in dynamic routing.

Note Layer 2 Spanned EtherChannels are not supported for load balancing.

Individual interfaces

You can configure cluster interfaces as individual interfaces.

Individual interfaces are normal routed interfaces, each with their own local IP address. The IP address for the interface will be configured automatically via DHCP. Static IP configuration is not supported.

Control and data node roles

When you add a cluster in the Firewall Management Center , you choose one firewall to be the control node, and all additional firewalls to be data nodes. When you first create the cluster, the control node you specify will become the control node simply because it is the first node added to the cluster. Later, if multiple cluster nodes come online at the same time, the control node is determined by the priority setting; the priority is set between 1 and 100, where 1 is the highest priority.

When you create the cluster and deploy the cluster configuration, the Firewall Management Center deploys a special bootstrap configuration to each node that includes fundamental settings such as the cluster control link configuration. The bootstrap configuration lets each node join the cluster. Most bootstrap settings are defined in the cluster wizard; however, you define the cluster control link interface hardware configuration (for example, creating an EtherChannel or setting the Ethernet speed) on the control node before you create the cluster. The cluster control link settings are copied to the bootstrap configuration for each node.

All nodes in the cluster share the same policy configuration. The node that you initially specify as the control node will overwrite the configuration on the data nodes when they join the cluster, so you only need to perform initial configuration on the control node before you form the cluster. After you create the cluster, all configuration changes are made at the cluster level and are shared by all nodes.

Some features do not scale in a cluster, and the control node handles all traffic for those features.

Cluster Control Link

Each node must dedicate one interface as a VXLAN (VTEP) interface for the cluster control link. For more information about VXLAN, see Configure VXLAN interfaces, on page 680 .

VXLAN Tunnel Endpoint

VXLAN tunnel endpoint (VTEP) devices perform VXLAN encapsulation and decapsulation. Each VTEP has two interface types: one or more virtual interfaces called VXLAN Network Identifier (VNI) interfaces, and a regular interface called the VTEP source interface that tunnels the VNI interfaces between VTEPs. The VTEP source interface is attached to the transport IP network for VTEP-to-VTEP communication.

VTEP Source Interface

The VTEP source interface is a regular Firewall Threat Defense Virtual interface with which you plan to associate the VNI interface. You can configure one VTEP source interface to act as the cluster control link. The source interface is reserved for cluster control link use only. Each VTEP source interface has an IP address on the same subnet. This subnet should be isolated from all other traffic, and should include only the cluster control link interfaces.

VNI Interface

A VNI interface is similar to a VLAN interface. It is a virtual interface that keeps network traffic separated on a given physical interface by using tagging. You can only configure one VNI interface. Each VNI interface has an IP address on the same subnet.

Peer VTEPs

Unlike regular VXLAN for data interfaces, which allows a single VTEP peer, Firewall Threat Defense Virtual clustering allows you to configure multiple peers.

Cluster control link traffic overview

Cluster control link traffic includes both control and data traffic.

Control traffic includes:

- Control node election.
- Configuration replication.
- Health monitoring.

Data traffic includes:

- State replication.
- Connection ownership queries and data packet forwarding.

Configuration replication

All nodes in the cluster share a single configuration. You can only make configuration changes on the control node (with the exception of the bootstrap configuration), and changes are automatically synced to all other nodes in the cluster.

Management network

You must manage each node using the management interface. Management from a data interface is not supported with clustering.

Licenses for Threat Defense Virtual clustering

You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

Note APEX, PLUS, and VPN-Only licenses are not supported for clustering. Before you create a cluster, remove unsupported license assignments from the devices that will become cluster nodes.

Performance tier license requirements

Each Firewall Threat Defense Virtual cluster node requires the same performance tier license. We recommend using the same number of CPUs and memory for all members, or else performance will be limited on all nodes to match the least capable member. The throughput level will be replicated from the control node to each data node so they match.

When you add the control node to the Firewall Management Center, you can specify the feature licenses you want to use for the cluster. You can modify licenses for the cluster in the **Devices** > **Device Management**, **Cluster** > **License** area.

Note If you add the cluster before the Firewall Management Center is licensed (and running in Evaluation mode), then when you license the Firewall Management Center, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

Requirements and prerequisites for Threat Defense Virtual clustering

This reference provides the requirements and prerequisites for Threat Defense Virtual clustering, including model specifications, user roles, hardware and software requirements, and MTU configuration.

Model requirements

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100

Note FTDv5 and FTDv10 do not support Amazon Web Services (AWS) Gateway Load Balancer (GWLB) and Azure GWLB.

- Supported public cloud services:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)
- Maximum of 16 nodes

See also the general requirements for the Firewall Threat Defense Virtual in the Secure Firewall Threat Defense Virtual getting started guides.

User roles

- Admin
- Access Admin
- Network Admin

Hardware and software requirements

All units in a cluster:

- Must be in the same performance tier. We recommend using the same number of CPUs and memory for all nodes, or else performance will be limited on all nodes to match the least capable node.

- Must run the identical software except at the time of an image upgrade. Hitless upgrade is supported.
- The Firewall Management Center access must be from the Management interface. Data interface management is not supported.
- Multiple Availability Zone deployment is supported from Firewall Threat Defense Virtual version 7.6.0 and later. The earlier versions supports only single Availability Zone deployment.
- Cluster requires a minimum of *four* interfaces: Management, Diagnostics, Data (Geneve), and CCL (Cluster Control Link).
- Cluster control link interfaces of all units must be in the same subnet.

MTU

Make sure the ports connected to the cluster control link have the correct (higher) MTU configured. If there is an MTU mismatch, the cluster formation will fail.

The cluster control link MTU should be 154 bytes higher than the data interfaces. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead (100 bytes) plus VXLAN overhead (54 bytes).

For AWS with GWLB, the data interface uses Geneve encapsulation. In this case, the entire Ethernet datagram is being encapsulated, so the new packet is larger and requires a larger MTU. You should set the source interface MTU to be the network MTU + 326 bytes. So for the standard 1500 MTU network path, the source interface MTU should be 1826, and the cluster control link MTU should be +154, 1980.

For Azure with GWLB, the data interface uses VXLAN encapsulation. In this case, the entire Ethernet datagram is being encapsulated, so the new packet is larger and requires a larger MTU. You should set the cluster control link MTU to be the source interface MTU + 80 bytes.

The table shows the default values for the cluster control link MTU and the data interface MTU.

Note

- We do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.
- For Threat Defense Virtual clusters on Azure, modifying the cluster control link (CCL) MTU via FlexConfig in Management Center is not recommended, as it may cause cluster stability issues.

Table 32: Default MTU

Public Cloud	Cluster Control Link MTU	Data Interface MTU
AWS with GWLB	1980	1826
AWS	1654	1500
Azure with GWLB	1454	1374
Azure	1454	1300
GCP	1554	1400

Guidelines for Threat Defense Virtual clustering

High availability

High Availability is not supported with clustering.

IPv6

The cluster control link is only supported using IPv4.

Multi-zone clustering

Multi-zone clustering is supported for up to three zones.

Additional guidelines

- When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the Firewall Threat Defense or the switch, adding an additional switch to form a VSS or vPC or VNet) you should disable the health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the interface health check feature.
- When adding a node to an existing cluster, or when reloading a node, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang your connection; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- Do not power off a node without first disabling clustering on the node.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a new node. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.
- Dynamic scaling is supported from Secure Firewall version 7.3.
- If you are using Secure Firewall versions 7.2 or 7.3, Stateful Target Failover is not supported when you deploy the cluster on AWS.
- Perform a global deployment after the completion of each maintenance window.
- Ensure that you do not remove more than one device at a time from the auto scale group (AWS) / instance group (GCP) / scale set (Azure). We also recommend that you run the **cluster disable** command on the device before removing the device from the auto scale group (AWS) / instance group (GCP) / scale set (Azure).
- If you want to disable data nodes and the control node in a cluster, we recommend that you disable the data nodes before disabling the control node. If a control node is disabled while there are other data nodes in the cluster, one of the data nodes has to be promoted to be the control node. Note that the role change could disturb the cluster.
- In the customized day 0 configuration scripts given in this guide, you can change the IP addresses as per your requirement, provide custom interface names, and change the sequence of the CCL-Link interface.

- If you experience CCL instability issues, such as intermittent ping failures, after deploying a Threat Defense Virtual cluster on a cloud platform, we recommend that you address the reasons that are causing CCL instability. Also, you can increase the hold time as a temporary workaround to mitigate CCL instability issues to a certain extent. For more information on how to change the hold time, see Edit Cluster Health Monitor Settings.
- When you are configuring your security firewall rule or security group for the Management Center virtual, you must include both Private and Public IP addresses of the Firewall Threat Defense Virtual in the Source IP address range. Also, ensure to specify the Private and Public IP addresses of the Firewall Management Center Virtual in the security firewall rule or security group of the Firewall Threat Defense Virtual. This is important to ensure proper registration of nodes during clustering deployment.

Defaults for clustering

- The cLACP system ID is auto-generated, and the system priority is 1 by default.
- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

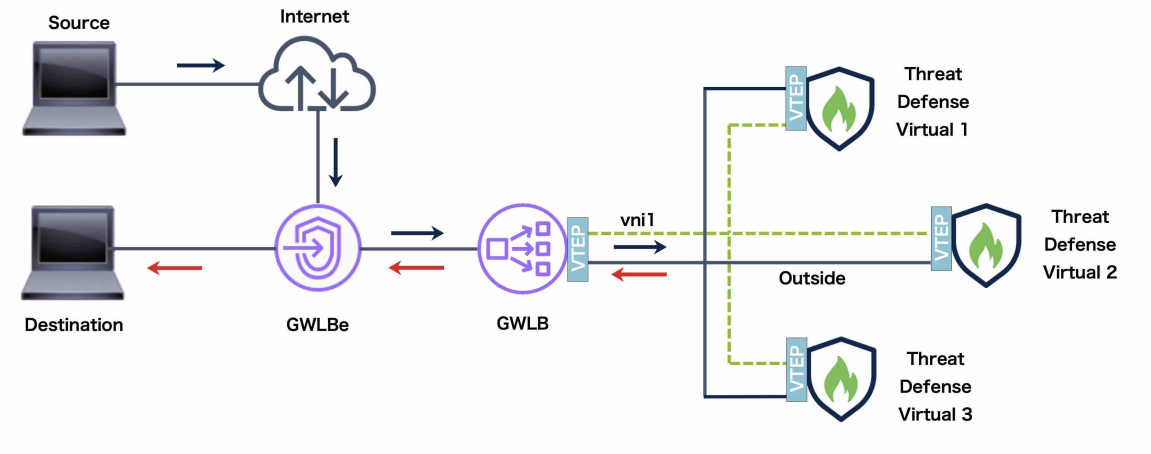
Deploy the cluster in AWS

You can deploy a cluster in AWS manually or by using CloudFormation templates to deploy a stack. You can use the cluster with AWS Gateway Load Balancer, or with a non-native load balancer such as the Cisco Cloud Services Router.

AWS gateway load balancer and Geneve single-arm proxy

This use case is the only currently supported use case for Geneve interfaces. The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The Threat Defense Virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint). The following figure shows traffic forwarded to the Gateway Load Balancer from the Gateway Load Balancer endpoint. The Gateway Load Balancer balances traffic among multiple Threat Defense Virtuals, which inspect the traffic before either dropping it or sending it back to the Gateway Load Balancer (U-turn traffic). The Gateway Load Balancer then sends the traffic back to the Gateway Load Balancer endpoint and to the destination.

Figure 185: Geneve Single-Arm Proxy



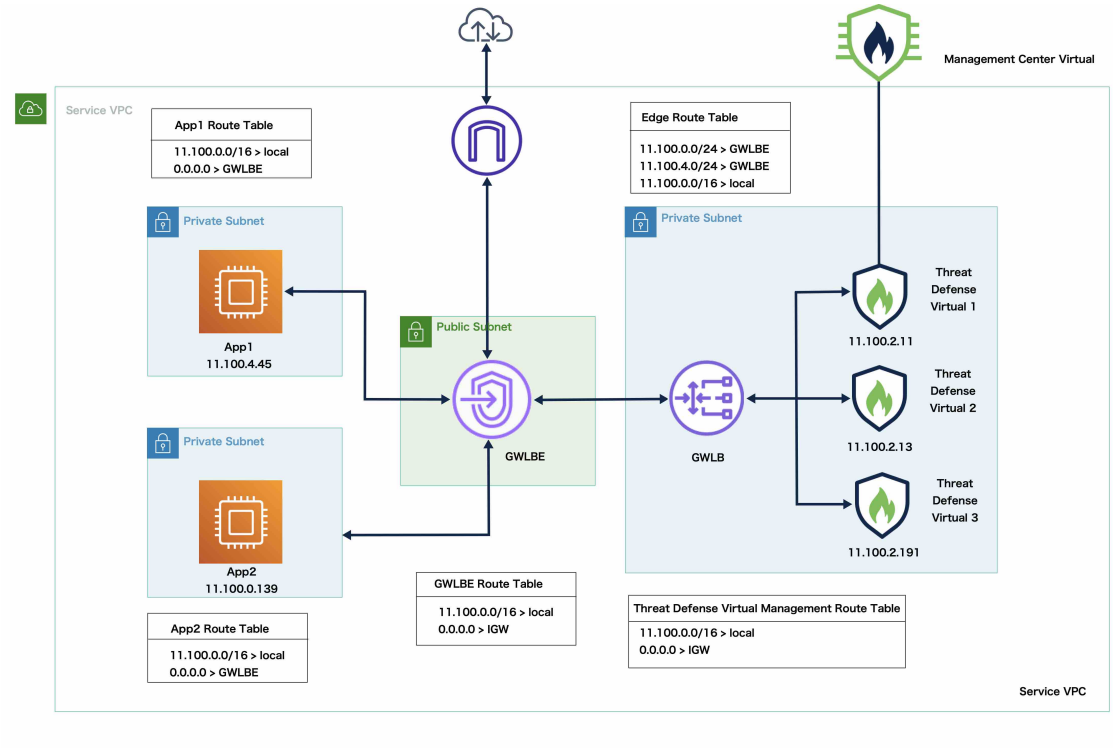
Note Transport Layer Security (TLS) Server Identity Discovery is not supported with Geneve single-arm setup on AWS.

Sample topology

The sample topology provided below

- depicts both inbound and outbound traffic flow through security appliances,
- includes three Threat Defense Virtual instances in a cluster connected to a GWLB, and
- uses a Management Center Virtual instance to manage the cluster.

Traffic flow



Inbound traffic from the internet goes to the GWLB endpoint which then transmits the traffic to the GWLB. Traffic is then forwarded to the Threat Defense Virtual cluster. After the traffic has been inspected by a Threat Defense Virtual instance in the cluster, it is forwarded to the application VM, App1 /App2.

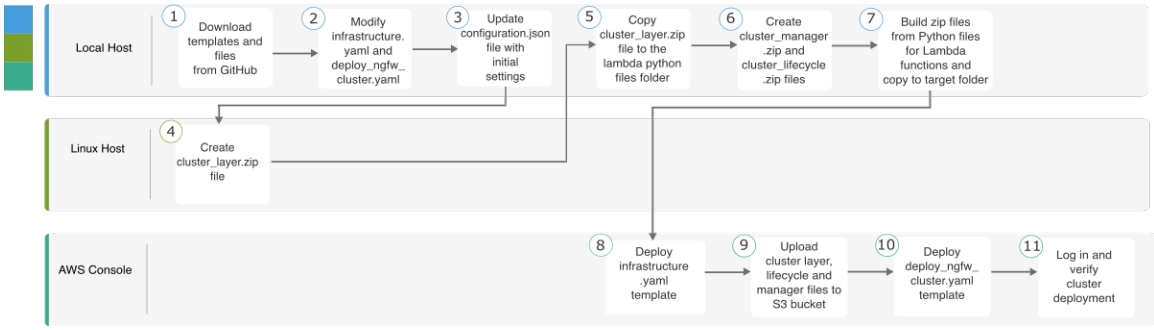
Outbound traffic from App1/App2 is transmitted to the GWLB endpoint which then sends it out to the internet.

End-to-end process for deploying Threat Defense Virtual cluster on AWS

Provides a workflow to help users successfully deploy and verify a Threat Defense Virtual cluster on AWS using either template-based or manual deployment processes.

Template-based Deployment

The following flowchart illustrates the workflow for template-based deployment of the Threat Defense Virtual cluster on AWS.



	Workspace	Steps
1	Local Host	Clone the repository from GitHub
2	Local Host	Modify *infrastructure.yaml* and *deploy_ngfw_cluster.yaml* templates.
3	Local Host	Update the *Configuration.json* file with FMC object names.
4	Linux Host	Create *cluster_layer.zip* file.
5	Local Host	Copy *cluster_layer.zip* file to the Lambda python files folder.
6	Local Host	Create *cluster_manager.zip*, *custom_metrics_publisher.zip*, and *cluster_lifecycle.zip* files.
7	Local Host	Build zip files from Python files for Lambda functions and copy to target folder.
8	AWS Console	Deploy *infrastructure.yaml* template.
9	AWS Console	Upload *cluster_layer.zip*, *cluster_lifecycle.zip*, *custom_metrics_publisher.zip*, and *cluster_manager.zip* to the S3 bucket.
10	AWS Console	Deploy *deploy_ngfw_cluster.yaml* template.
11	AWS Console	Log in and verify cluster deployment.

Manual Deployment

The following flowchart illustrates the workflow for manual deployment of the Threat Defense Virtual cluster on AWS.



	Workspace	Steps
1	Local Host	Create day 0 configuration script.
2	AWS Console	Deploy Threat Defense Virtual instance.
3	AWS Console	Attach interfaces to instance.
4	AWS Console	Verify if nodes have joined cluster.
5	AWS Console	Create target group and GWLB; attach target group to the GWLB.
6	AWS Console	Register instances with the target group using data interface IP.
7	Management Center	Register control node.

Templates

The templates are available in GitHub. The parameter values are self-explanatory with the parameter names, default values, allowed values, and description, given in the template.

- infrastructure.yaml – Template for infrastructure deployment.
- deploy_ngfw_cluster.yaml – Template for cluster deployment.

Note Ensure that you check the list of supported AWS instance types before deploying cluster nodes. This list is found in the *deploy_ngfw_cluster.yaml* template, under allowed values for the parameter InstanceType.

Deploy the Stack in AWS Using a CloudFormation template

Deploy the stack in AWS using the customized CloudFormation template.

Before you begin

- You need an Amazon Linux virtual machine with Python 3.
- To allow the cluster to auto-register with the Firewall Management Center , you need to create two users with administrative privileges on the Firewall Management Center that can use the REST API. See the *Cisco Secure Firewall Management Center Administration Guide* .
- Add an access policy in the Firewall Management Center that matches the name of the policy that you specified in `Configuration.json` .

Procedure

Step 1 Prepare the template.

a) Clone the GitHub repository to your local folder. See https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws .

b) Modify **infrastructure.yaml** and **deploy_ngfw_cluster.yaml** with the required parameters.

c) Modify **cluster/aws/lambda-python-files/Configuration.json** with initial settings.

For example:

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- Keep the fmcIpforDeviceReg setting as DONTRESOLVE.
- The fmcAccessPolicyName needs to match an access policy on the Firewall Management Center .

Note FTDv5 and FTDv10 tiers are not supported.

d) Create a file named **cluster_layer.zip** to provide essential Python libraries to Lambda functions.

We recommend using Amazon Linux with Python 3.9 installed to create the cluster_layer.zip file.

Note If you need an Amazon Linux environment, you can create an EC2 instance using Amazon Linux 2023 AMI or use AWS Cloudshell, which runs the latest version of Amazon Linux.

For creating the cluster-layer.zip file, you need to first create requirements.txt file that consists of the python library package details and then run the shell script.

1. Create the requirements.txt file by specifying the python package details.

   The following is the sample package details that you provide in the requirements.txt file:

```
$ cat requirements.txt
pycryptodome
paramiko
requests
scp
jsonschema
cffi
zipp
importlib-metadata
```

2. Run the following shell script to create cluster_layer.zip file.

```
$ pip3 install --platform manylinux2014_x86_64
--target=./python/lib/python3.9/site-packages
--implementation cp --python-version 3.9 --only-binary=:all:
--upgrade -r requirements.txt
$ zip -r cluster_layer.zip ./python
```



Note If you encounter a dependency conflict error during installation, such as urllib3 or cryptography, it is recommended that you include the conflicting packages along with their recommended versions in the requirements.txt file. After that, you can run the installation again to resolve the conflict.

e) Copy the resulting **cluster_layer.zip** file to the lambda python files folder - `cluster/aws/lambda-python-files` .

f) Create the **cluster_layer.zip** , **custom_metrics_publisher.zip** , **cluster_manger.zip** and **lifecycle_ftdv.zip** files.

A make.py file can be found in the cloned repository (`cluster/aws/make.py`). This will zip the python files into a Zip file and copy to a target folder.

python3 make.py build



Note If you are using a private IP address for the Management Center Virtual registration, then make sure that you set USE_PUBLIC_IP_FOR_FMC_CONN to False in the `cisco-ftdv/cluster/aws/lambda-python-files/constant.py` file.

Step 2 Deploy **infrastructure.yaml** and note the output values for cluster deployment. Before deploying the infrastructure stack, it is important to identify the AWS region and the availability zones that will be used. Each AWS region has a different set of availability zones and VPC infrastructure. Therefore, it is essential to select the correct region and availability zones for your deployment.

a) On the AWS Console, go to **CloudFormation** and click **Create stack** ; select **With new resources(standard)** .

b) Select **Upload a template file** , click **Choose file** , and select **infrastructure.yaml** from the target folder.

c) Click **Next** and provide the required information.

e

Parameter	Allowed Values/Type	Description
ClusterName	String	Enter unique Cluster name.
ClusterNumber	Number	Enter unique Cluster number.
VpcCidr	String	Enter the CIDR block for a new VPC
NoOfAZs	Number	Select 2 or 3 Availability Zones (AZs) for releases 7.6.0 and above; for lower releases, Select 1AZ.

Parameter	Allowed Values/Type	Description
		Management, Inside, Outside and CCL subnets will be distributed across the chosen AZs accordingly.
ListOfAZs	List	Select Availability Zones (Count should match with Number of Availability Zones)
MgmtSubnetNames	CommaDelimitedList	Management subnets name (With Internet GW as Route)
MgmtSubnetCidrs	CommaDelimitedList	Management subnets Cidr list
InsideSubnetNames	CommaDelimitedList	Inside subnets name (With Private Route)
InsideSubnetCidrs	CommaDelimitedList	Inside subnets Cidr list
CCLSubnetNames	CommaDelimitedList	Enter CCL subnet name
CCLSubnetCidrs	CommaDelimitedList	Enter CCL subnet CIDR
LambdaAZs	List	Select 2 Availability Zones for Lambda
LambdaSubnetNames	CommaDelimitedList	Enter Lambda Subnets name (With NAT GW as Route), for Lambda Functions
LambdaSubnetCidrs	CommaDelimitedList	Enter Lambda Subnet CIDRs

d) Enter a unique **Cluster Name** and **Cluster Number** for the cluster.
e) Select the availability zone from the **Availability Zone** list. This field lists only availability zones based on the AWS region that you select for deploying the infrastructure stack using the ClusterFormation template.
f) Click **Next** , then **Create stack** .
g) After the deployment is complete, go to **Outputs** and note the S3 **BucketName** .

Figure 186: Output of infrastructure.yaml

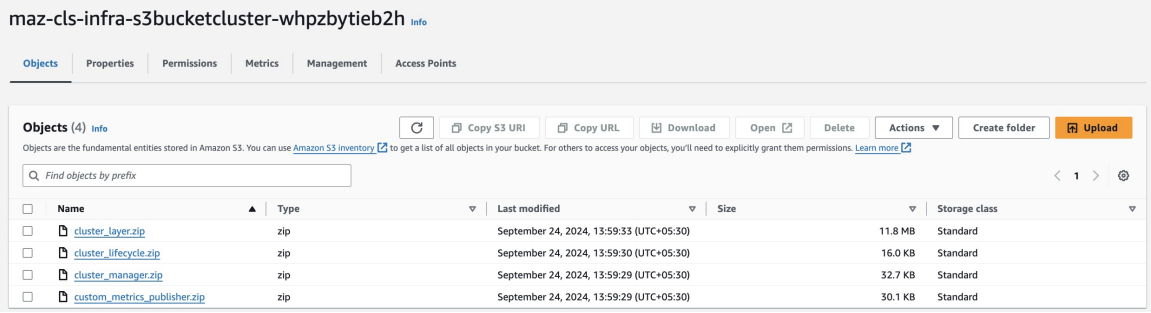
Outputs (13)

Search outputs

Key	Value	Description	Export name
BucketName	maz-cls-infra-s3bucketcluster-whpzbytieb2h	Name of the Amazon S3 bucket	-
BucketUrl	http://maz-cls-infra-s3bucketcluster-whpzbytieb2h.s3-website-us-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetIds	subnet-0bc04e2cc9e53e5c0,subnet-0d7d046a0fca25615,subnet-03ef42bf527551569	List of CCL subnet IDs (comma seperated)	-
EIPforNATgw	3.218.44.132	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-076880aa64df2db5c	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-06ed933d6624fe51b	Security Group ID for Inside Interfaces	-
InsideSubnetIds	subnet-03d12cab8ee0eafff,subnet-0be9158b0970aebab,subnet-0b53c96fceb7c1f4d	List of Inside subnet IDs (comma seperated)	-
InstanceSGId	sg-0680b74be473186aa	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-057da2a9954e0d204	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-03439803d989e6bdf,subnet-087488a9d6ffc95cd	List of lambda subnet IDs (comma seperated)	-
ListOfAZs	us-east-1a,us-east-1b,us-east-1c	Availability zones for NGFWv instances	-
MgmtSubnetIds	subnet-06f0bbbd3f207a504,subnet-0c339dc43688cddc9,subnet-0a67629632a655de7	List of Mangement subnet IDs (comma seperated)	-
VpcName	vpc-09c2b0ad995e2fb24	Name of the VPC created	-

Step 3 Upload **cluster_layer.zip** , **cluster_manager.zip** , **custom_metrics_publisher.zip** , and **cluster_lifecycle.zip** to the S3 bucket created by **infrastructure.yaml** .

Figure 187: S3 Bucket



Note Make sure that the Elastic IP address of the Lambda NAT Gateway is added to the security group associated with the Management Center Virtual.

Step 4 Deploy **deploy_ngfw_cluster.yaml** .

a) Go to **CloudFormation** and click on **Create stack** ; select **With new resources(standard)** .

b) Select **Upload a template file** , click **Choose file** , and select **deploy_ngfw_cluster.yaml** from the target folder.

c) Click **Next** and provide the required information.

d) Provide the following cluster and infrastructure configuration information.

Parameter	Allowed Values/Type	Description
Cluster Configuration		
ClusterGrpNamePrefix	String	This is the cluster name Prefix. The cluster number will be added as a suffix.
ClusterNumber	String	This is the cluster number. This will be suffixed to the cluster name (msa-ftdv-infra). For example, if this value is 1 , the group name will be msa-ftdv-infra-1. It should be at least 1 digit, but not more than 3 digits. Default: 1.
ClusterSize	Numbers	This is the total number of Firewall Threat Defense Virtual nodes in a cluster. Minimum: 1 Maximum:16
Infrastructure Details		
NoOfAZs	String	This is the total number of availability zones into which Firewall Threat Defense Virtual is deployed. (The number of availability zones varies from a Minimum 1 to Maximum 3 depending on a region).

Parameter	Allowed Values/Type	Description
		The subnet will be created in these availability zones. The availability zones available in this list is based on the region selected for deploying the cluster. **Note** Management, Inside, and Cluster Control Link (CCL) subnets are created across three availability zones based on this parameters.
AZ	String	The availability zone list is based on the region you plan to deploy. In Availability Zone list, select the valid availability zone (1 availability zone or 2 availability zones or 3 availability zones). Count should match with the value of Number of Availability Zones parameter.
NotifyEmailID	String	Email address to which cluster events email will be sent. You must accept a subscription email request to receive this email notification. For example, admin@company.com.
VpcId	String	The VPC ID for the cluster group. Type: AWS::EC2::VPC::Id
S3BktName	String	The S3 Bucket that contains the uploaded Lambda zip files. You must specify correct bucket name.
MgmtSubnetIds	List	Enter only one subnet per availability zone. If you select multiple subnets from a same availability zone, then selecting an incorrect subnet may cause issues while deploying the Firewall Threat Defense Virtual instances. Type: List<AWS::EC2::Subnet::Id>
InsideSubnetIds	List	Enter at least one subnet per availability zone. If multiple subnets from the same Availability Zone are selected, then selecting an incorrect subnet may cause issues while deploying the Firewall Threat Defense Virtual instances. Type: List<AWS::EC2::Subnet::Id>
LambdaSubnets	List	Enter at least two subnets for the Lambda functions. The two subnets you enter must have a NAT gateway to enable the Lambda functions to communicate with AWS services, which are public DNS.

Parameter	Allowed Values/Type	Description
		Type: List<AWS::EC2::Subnet::Id>
CCLSubnetIds	String	Enter at least one subnet per availability zone. If multiple subnets from the same Availability Zone are selected, then selecting an incorrect subnet may cause issues while deploying the Firewall Threat Defense Virtual instances. Type: List<AWS::EC2::Subnet::Id>
CCLSubnetRanges	String	Enter IP addresses range of CCL subnets for different availability zones. Exclude first 4 reserved IP addresses. IP address pool for Cluster Control Link (CCL). IP address is allocated to the CCL interfaces of the Firewall Threat Defense Virtual instance from CCL IP address pool.
MgmtInterfaceSG	List	Select security group ID for the Firewall Threat Defense Virtual instances. Type: List<AWS::EC2::SecurityGroup::Id>
InsideInterfaceSG	List	Select security group ID for the inside interface of Firewall Threat Defense Virtual instances. Type: List<AWS::EC2::SecurityGroup::Id>
LambdaSG	List	Select a security group for the Lambda functions. Ensure outbound connections are set to ANYWHERE . Type: List<AWS::EC2::SecurityGroup::Id>
CCLInterfaceSG	List	Select a security group ID for CCL interface of the Firewall Threat Defense Virtual instances.
GWLB Configuration		
DeployGWLBE	String	Click Yes to deploy the GWLB endpoint. By default, the value is set to No .
VpcIdLBE	String	Enter VPC to deploy Gateway Load Balancer Endpoint. **Note** Do not enter any value in this field if you are not deploying the GWLB endpoint.
GWLBESubnetId	String	Enter only one subnet ID. **Note**

Parameter	Allowed Values/Type	Description
		Do not enter any value in this field if you are not deploying the GWLB endpoint. Ensure that the subnet belongs to the correct VPC, and the availability zones that you have specified.
TargetFailover	String	Enable Target Failover support when a target fails or deregisters. (By default, the value of this parameter is set to rebalance). • no_rebalance : Directs existing flows to failed targets and new flows to healthy targets, ensuring backward compatibility. • rebalance : Redistributes existing flows while ensuring that new flows go to healthy targets. rebalance is supported from Firewall Threat Defense Virtual Version 7.4.1 and later.
TgHealthPort	String	Enter Health Check Port for GWLB. **Note** By default, this port must not be used for traffic. Ensure the value you provide is a valid TCP port. Default: 8080
Cisco NGFWv Instance Configuration		
InstanceType	String	Cisco Firewall Threat Defense Virtual EC2 instance type. Ensure that the AWS Region supports Instance Type you select. By default, **c5.xlarge** is selected.
LicenseType	String	Choose Cisco Firewall Threat Defense Virtual EC2 instance license type. Ensure that the AMI ID that you enter in **AMI-ID** parameter is of the same licensing type. By default, **BYOL** is selected.
AssignPublicIP	String	Set the value as **true** to assign a public IP address for Firewall Threat Defense Virtual from the AWS IP address pool.
AmiID	String	Choose the correct AMI ID as per the region, version, and license type (BYOL or PAYG). Firewall Threat Defense Virtual 7.2 and later support clustering, and Firewall Threat Defense Virtual Version

Parameter	Allowed Values/Type	Description
		7.6 and later support the autoscaling and multiple availability zone enhancements. Type: AWS::EC2::Image::Id
ngfwPassword	String	Firewall Threat Defense Virtual instance password. All Firewall Threat Defense Virtual instances come up with a default password, which is in the Userdata field of the Launch Template (Cluster Group). The password is activated after Firewall Threat Defense Virtual is accessible. Minimum length must be 8 characters. The password can either be a plain text password or a KMS encrypted password.
KmsArn	String	Enter ARN of an existing KMS (AWS KMS key to encrypt at rest). If you specify a value in this field, then the Firewall Threat Defense Virtual instance's admin password must be an encrypted password. Example of generating an encrypted password: " aws kms encrypt --key-id <KMS ARN> --plaintext <password> " The password encryption must be done using only the specified ARN.
FMC Automation Configuration		
fmcDeviceGrpName	String	Enter a unique name for the cluster group in management center.
fmcPublishMetrics	String	Select **`true`** to create a Lambda Function to poll management center and publish specific device group metrics to AWS CloudWatch. Allowed values: • true • false By default, the value is set to true .
fmcMetricsUsername	String	Enter a unique internal user name for polling memory metrics from management center. The user must have privileges of Network Admin and Maintenance User or more .

Parameter	Allowed Values/Type	Description
fmcMetricsPassword	String	Enter the password. If you have mentioned KMS Master Key ARN parameter, ensure to provide an encrypted password. Ensure to enter the correct password because entering incorrect password may result in failure of metrics collection.
fmcServer	String	The IP address can be an external IP address or the IP address reachable in Firewall Threat Defense Virtual management subnet in the VPC. Minimum length: 7 Maximum length:15
fmcOperationsUsername	String	Provide a unique internal user name for Firewall Management Center Virtual for CloudWatch. The user must have Administrator privileges.
fmcOperationsPassword	String	Enter the password. If you have mentioned KMS Master Key ARN parameter, ensure to provide an encrypted password.
Scaling Configuration		
CpuThresholds	CommaDelimitedList	(Optional) Specifying non-zero lower and upper thresholds will create scale policies. If (0,0) is selected, no CPU scaling alarm or policies will be created. Evaluation points and data points are at default or recommended values. By default, autoscaling is enabled in this template. Autoscale can be disabled after deployment.
MemoryThresholds	CommaDelimitedList	Specifying non-zero lower and upper threshold will create scale policies. If (0,0) is selected, no memory scaling alarm or policies will be created. Evaluation points and data points are at default or recommended values.

e) Click **Next** , then **Create stack** .

The Lambda functions manage the rest of the process, and the Firewall Threat Defense Virtual s will automatically register with the Firewall Management Center .

Figure 188: Deployed Resources

The status changes from CREATE_IN_PROGRESS to CREATE COMPLETE, indicating successful deployment.

Step 5 Verify the cluster deployment by logging into any one of the nodes and using the **show cluster info** command.

Figure 189: Cluster Nodes

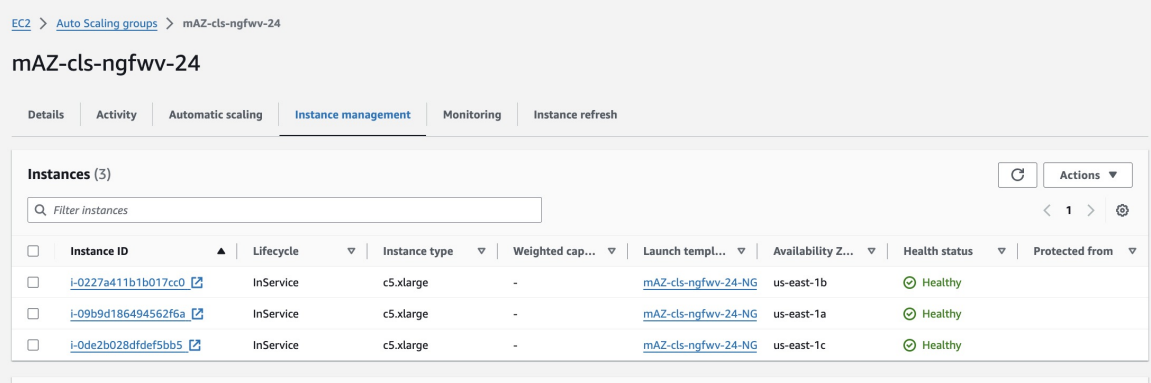
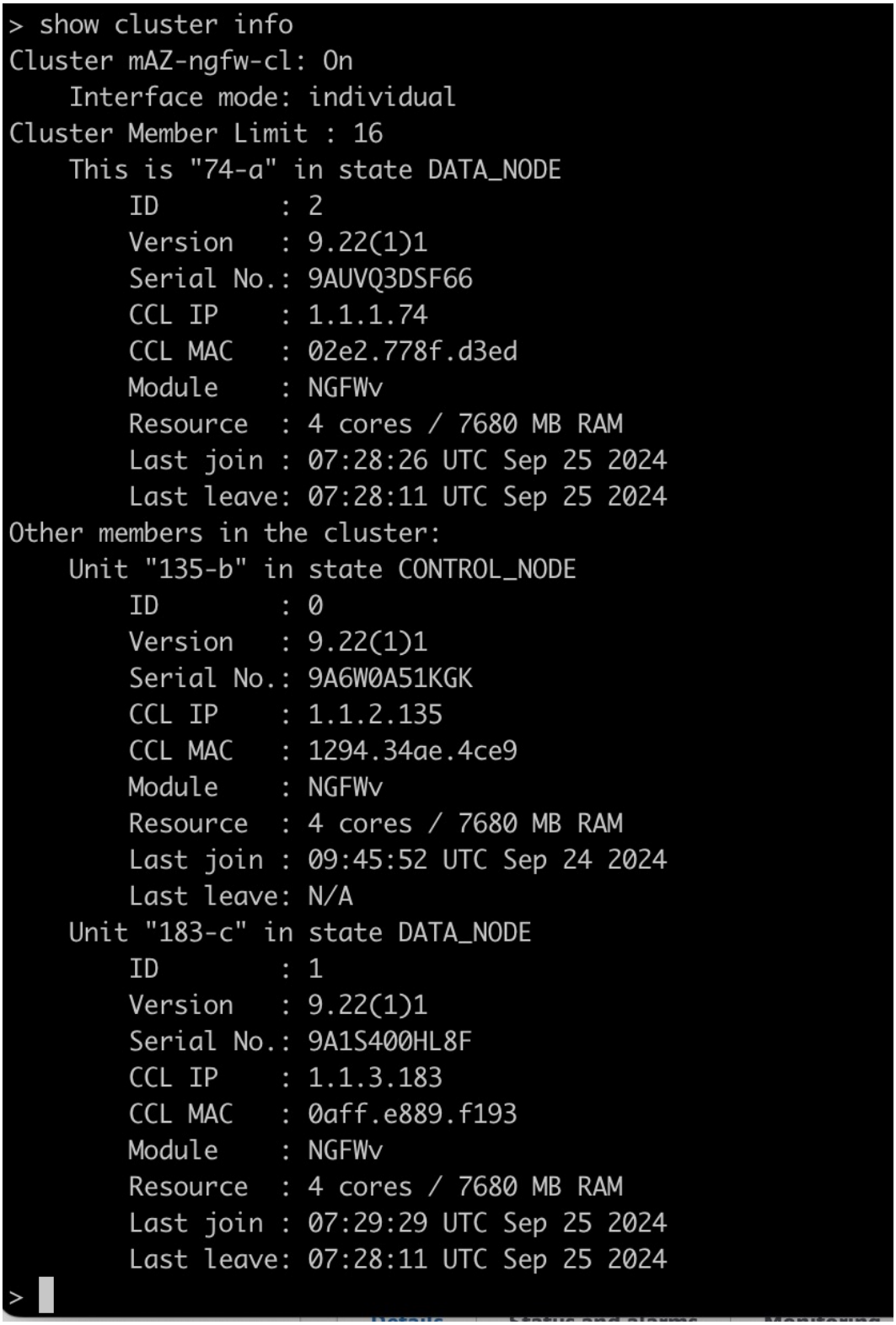


Figure 190: show cluster info



Manual cluster deployment in AWS

To deploy the cluster manually, prepare the day 0 configuration, deploy each node, and then add the control node to the Firewall Management Center.

On version 7.6.4-69 and from 10.0.0, each cluster node requires a unique AWS instance tag "cluster-node-id" with a value ranging from 1 to 16 for internal cluster configuration. Please ensure that the tag is added before the device boots up.

For example: key "cluster-node-id" -> value "1"

Additionally, make sure that "Allow tags in instance metadata" is set to "Enabled."

Create the Day0 configuration for AWS

You can use either a fixed configuration or a customized configuration. We recommend using the fixed configuration.

Create the Day0 configuration with a fixed configuration for AWS

The fixed configuration will auto-generate the cluster bootstrap configuration.

Single availability zone - Day0 configuration with a fixed configuration for AWS

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

For example:

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
              "CclSubnetRange": "10.5.90.4 10.5.90.30",
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

Configure the cluster infrastructure subnet range

Use a cluster infrastructure subnet range to allocate IP addresses within a /27 CIDR block. This range provides the usable IP addresses for your cluster infrastructure.

Before you begin

- Review the table to determine valid start and end IP addresses for the /27 CIDR blocks you plan to use.
- The first four IP addresses in each subnet (including the network address) are reserved by AWS. Configure the **CclSubnetRange** to begin with the fifth IP address in the subnet.

The table shows the valid start and end IP addresses for each /27 CIDR allocation.

Table 33: CclSubnetRange mapping

CIDR	Start IP Address	End IP Address
x.y.z.0/27	x.y.z.4	x.y.z.30
x.y.z.32/27	x.y.z.36	x.y.z.62
x.y.z.64/27	x.y.z.68	x.y.z.94
x.y.z.96/27	x.y.z.100	x.y.z.126
x.y.z.128/27	x.y.z.132	x.y.z.158
x.y.z.160/27	x.y.z.164	x.y.z.190
x.y.z.192/27	x.y.z.196	x.y.z.222
x.y.z.224/27	x.y.z.228	x.y.z.254

Complete these steps to configure the cluster infrastructure subnet range.

Procedure

Step 1 Identify the /27 CIDR block assigned to your cluster infrastructure subnet.

Step 2 Find the matching CIDR in the mapping table.

Step 3 Replace "x.y.z" with the first three octets of your subnet. For example, 172.20.10 or 10.100.5.

Step 4 Configure the range by entering the start and end IP addresses from the mapping table for your subnet.

- Example 1:
  - CIDR: 172.20.10.64/27
  - Subnet range: 172.20.10.68 to 172.20.10.94
- Example 2:
  - CIDR: 10.100.5.128/27

- Subnet range: 10.100.5.132 to 10.100.5.158

Deploy cluster nodes

Deploy cluster nodes to form a functional cluster that can handle traffic distribution and provide high availability for network security services.

Deploy the cluster nodes so they form a cluster.

Procedure

Step 1 Deploy the Threat Defense Virtual instance by using the cluster day 0 configuration with the required number of interfaces - four interfaces if you are using Gateway Load Balancer (GWLB), or five interfaces if you are using non-native load balancer. To do this, in the **Configure Instance Details** > **Advanced Details** section, paste the cluster day 0 configuration.

Note Ensure that you attach interfaces to the instances in the order given below.

- AWS Gateway Load Balancer - four interfaces - management, diagnostic, inside, and cluster control link.
- Non-native load balancers - five interfaces - management, diagnostic, inside, outside, and cluster control link.

For more information on deploying Threat Defense Virtual on AWS, refer to Deploy the Threat Defense Virtual on AWS.

Step 2 Repeat Step 1 to deploy the required number of additional nodes.

Step 3 Use the **show cluster info** command on the Threat Defense Virtual console to verify if all nodes have successfully joined the cluster.

Step 4 Configure the AWS Gateway Load Balancer.

a) Create a target group and GWLB.

b) Attach the target group to the GWLB.

Note Ensure that you configure the GWLB to use the correct security group, listener configuration, and health check settings.

c) Register the data interface (inside interface) with the Target Group using IP addresses.

For more information, refer to Create a Gateway Load Balancer.

Step 5 Add the control node to the Management Center. Refer to Add the cluster to the Management Center (manual deployment), on page 493.

Target failover for Secure Firewall Threat Defense Virtual clustering with GWLB in AWS

Threat Defense Virtual clustering in AWS utilizes the Gateway Load Balancer (GWLB) to balance and forward network packets for inspection to a designated Threat Defense Virtual node. The GWLB is designed to continue sending network packets to the target node in the event of a failover or deregistration of that node.

The Target Failover feature in AWS enables GWLB to redirect network packets to a healthy target node in the event of node deregistration during planned maintenance or a target node failure. It takes advantage of the cluster's stateful failover.

Configuration methods

In AWS, you can configure Target Failover through the AWS Elastic Load Balancing (ELB) API or AWS console.

Note If a target node fails while the GWLB routes traffic using certain protocols such as SSH, SCP, CURL, and so on, then there may be a delay in redirecting traffic to a healthy target. This delay is due to rebalancing and rerouting of traffic flow.

- AWS API — In the AWS ELB API *modify-target-group-attributes*, you can define the flow handling behavior by modifying the parameters.
  - target_failover.on_unhealthy - It defines how the GWLB handles the network flow when the target becomes unhealthy.
  - target_failover.on_deregistration - It defines how the GWLB handles the network flow when the target is deregistered.

  This command shows the sample API parameter configuration of defining these two parameters.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:…/my-targets/73e2d6bc24d8a067 \
--attributes \
Key=target_failover.on_unhealthy, Value=rebalance[no_rebalance] \
Key=target_failover.on_deregistration, Value=rebalance[no_rebalance]
```

  For more information, refer to TargetGroupAttribute in the AWS documentation.
- AWS Console — In the EC2 console, you can enable the Target Failover option on the Target Group page by configuring these options.
  - Edit Target Groups Attributes
  - Enable Target Failover
  - Verify Rebalance Flows

  For more information about how to enable Target Failover, refer to Enable target failover for Secure Firewall Threat Defense Virtual clustering in AWS, on page 465.

Enable target failover for Secure Firewall Threat Defense Virtual clustering in AWS

This task enables target failover configuration in AWS to ensure network flow continuity when Firewall Threat Defense Virtual cluster targets fail or become deregistered.

The data interface of Firewall Threat Defense Virtual is registered to a target group of GWLB in AWS. In the Firewall Threat Defense Virtual clustering, each instance is associated with a Target Group. The GWLB load balances and sends the traffic to this healthy instance identified or registered as a target node in the target group.

Before you begin

You must have deployed the cluster in AWS either by manual method or using CloudFormation templates.

If you are deploying a cluster using a CloudFormation template, you can also enable the **Target Failover** parameter by assigning the **rebalance** attribute that is available under **GWLB Configuration** section of the cluster deployment file, `deploy_ftdv_clustering.yaml`. In the template, by default, the value is set to **rebalance** for this parameter. However, the default value for this parameter is set to **no_rebalance** on the AWS console.

Where,

- **no_rebalance** - GWLB continues to send the network flow to the failed or deregistered target.
- **rebalance** - GWLB sends the network flow to another healthy target when the existing target is failed or deregistered.

For information on deploying stack in AWS, refer to:

- Deploy the Cluster in AWS Manually
- Deploy the Stack in AWS Using a CloudFormation Template

Procedure

Step 1 On the AWS Console, go to **Services > EC2**

Step 2 Click **Target Groups** to view the target groups page.

Step 3 Select the target group to which the Firewall Threat Defense Virtual data interface IPs are registered. The target group details page is displayed, where you can enable the Target failover attributes.

Step 4 Go to the **Attributes** menu.

Step 5 Click **Edit** to edit the attributes.

Step 6 Toggle the **Rebalance flows** slider button to the right to enable target failover to configure GWLB to rebalance and forward the existing network packets to a healthy target node in the event of target failover or deregistration.

Deploy the cluster in Azure

You can use the cluster with the Azure Gateway Load Balancer (GWLB), or with a non-native load balancer. To deploy a cluster in Azure, use Azure Resource Manager (ARM) templates to deploy a Virtual Machine Scale Set.

Sample topology for GWLB-based cluster deployment

Sample topologies for deploying Gateway Load Balancer (GWLB) clusters are given below.

Figure 191: Inbound traffic use case and topology with GWLB

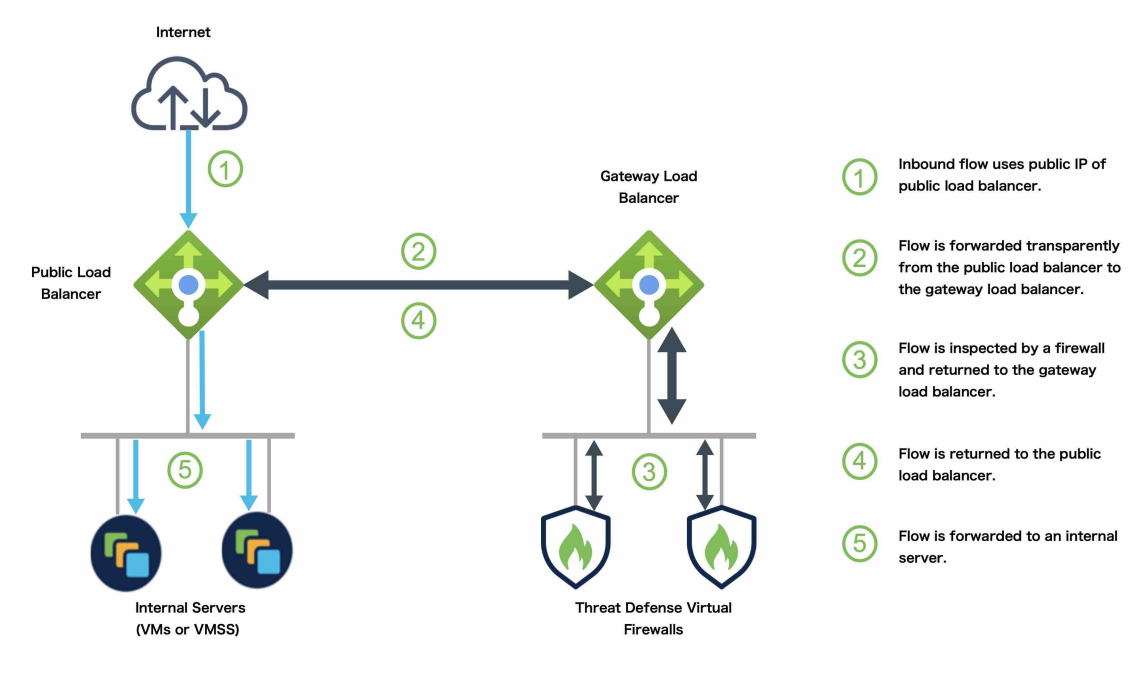
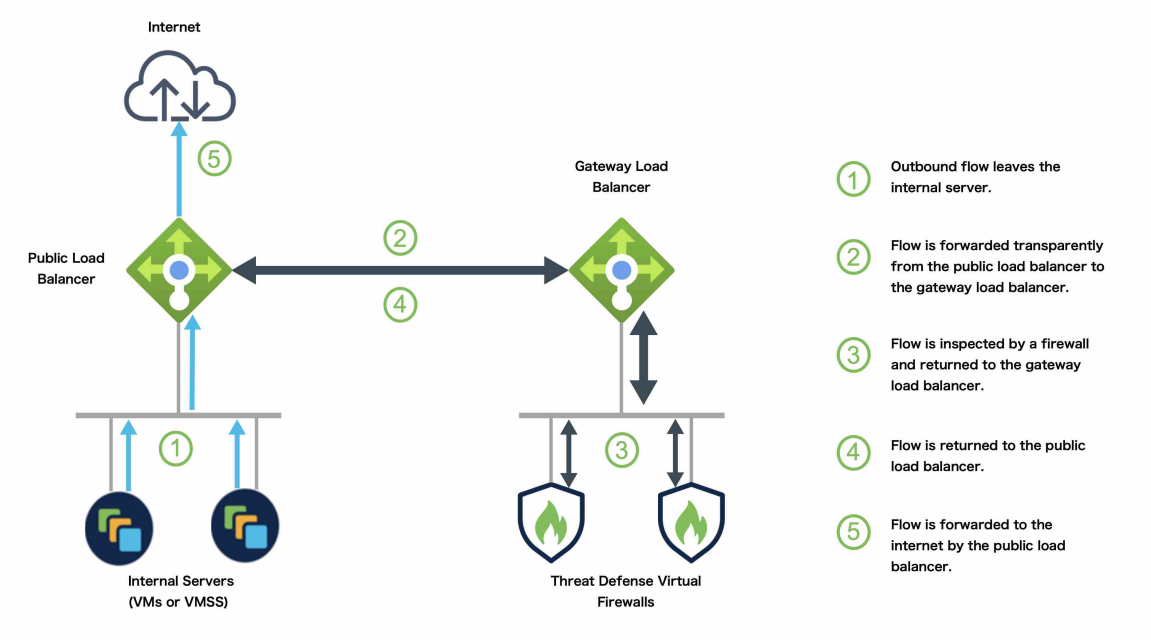


Figure 192: Outbound traffic use case and topology with GWLB

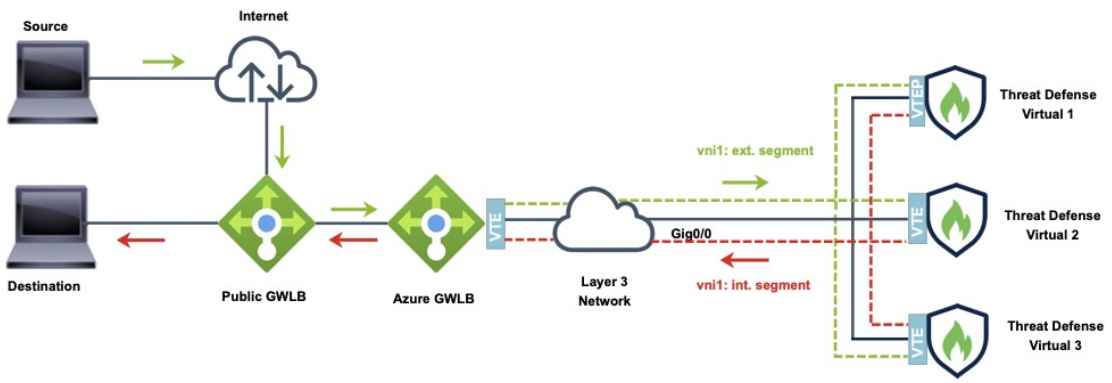


Azure gateway load balancer and paired proxy

In an Azure service chain, Threat Defense Virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The Threat Defense Virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

The figure shows traffic forwarded to the Azure Gateway Load Balancer from the Public Gateway Load Balancer on the external VXLAN segment. The Gateway Load Balancer balances traffic among multiple Threat Defense Virtuals, which inspect the traffic before either dropping it or sending it back to the Gateway Load Balancer on the internal VXLAN segment. The Azure Gateway Load Balancer then sends the traffic back to the Public Gateway Load Balancer and to the destination.

Figure 193: Azure gateway load balancer with paired proxy



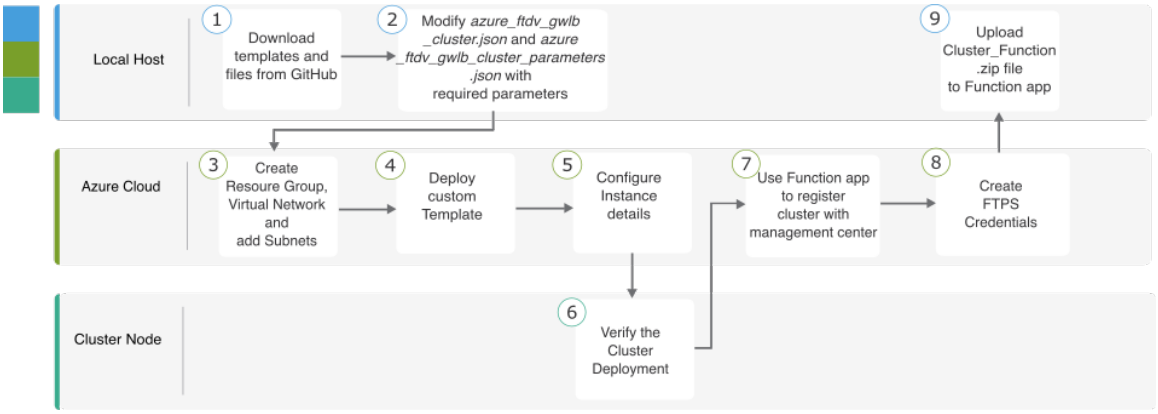
Traffic flow between GWLBe to GWLB (Geneve Single-Arm Proxy) in Azure

End-to-end process for deploying Threat Defense Virtual cluster in Azure with GWLB

Provides a workflow to help users successfully deploy and verify a Threat Defense Virtual cluster on Azure with GWLB using either template-based or manual deployment processes.

Template-based Deployment

The following flowchart illustrates the workflow for template-based deployment of the Threat Defense Virtual cluster in Azure with GWLB.

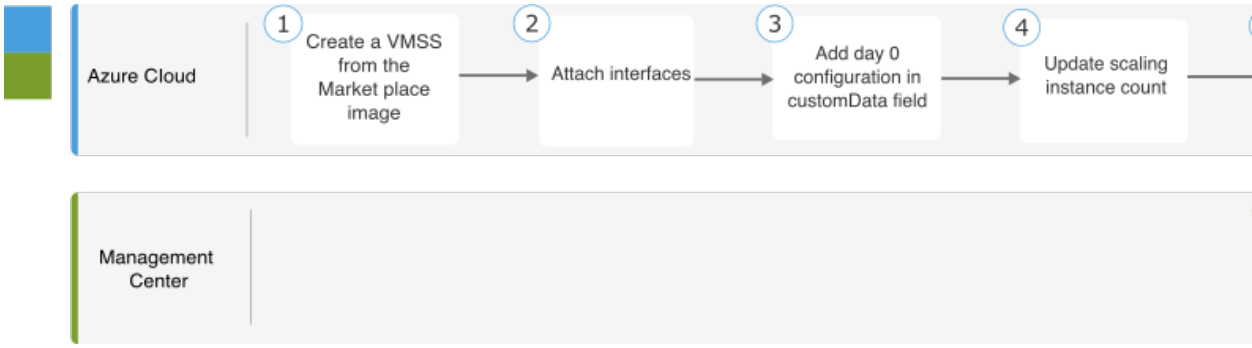


	Workspace	Steps
1	Local Host	Download templates and files from GitHub.
2	Local Host	Modify *azure_ftdv_gwlb_cluster.json* and *azure_ftdv_gwlb_cluster_parameters.json* with the required parameters.

	Workspace	Steps
3	Azure Cloud	Create the resource group, virtual network, and subnets.
4	Azure Cloud	Deploy custom template.
5	Azure Cloud	Configure instance details.
6	Cluster Node	Verify cluster deployment.
7	Azure Cloud	Use the Function app to register the cluster with the Management Center.
8	Azure Cloud	Create FTPS credentials.
9	Local Host	Upload *Cluster_Function.zip* file to the Function app.

Manual Deployment

The following flowchart illustrates the workflow of manual deployment of Threat Defense Virtual cluster in Azure with GWLB.



	Workspace	Steps
1	Local Host	Create a VMSS from the Marketplace image.
2	Local Host	Attach interfaces.
3	Local Host	Add day 0 configuration in the customData field.
4	Local Host	Update scaling instance count.
5	Local Host	Configure GWLB.

	Workspace	Steps
6	Management Center	Add control node.

Templates

The templates are available in GitHub. The parameter values are self-explanatory with the parameter names and values given in the template.

- azure_ftdv_gwlb_cluster_parameters.json – Template to enter parameters for the Firewall Threat Defense Virtual cluster.
- azure_ftdv_gwlb_cluster.json – Template to deploy Firewall Threat Defense Virtual cluster.

Prerequisites for Azure GWLB cluster deployment

Complete these prerequisite tasks before deploying the Azure GWLB cluster.

- To allow the cluster to auto-register to the management center, create a user with Network Admin & Maintenance User privileges on the management center. Users with these privileges can use REST API. Refer to the Cisco Secure Firewall Management Center Administration Guide.
- Add an access policy in the management center that matches the name of the policy that you will specify during template deployment.
- Ensure that the Management Center Virtual is licensed appropriately.
- Perform these steps after the cluster is added to the Management Center Virtual:
  1. Configure platform settings with the health check port number in the Management Center. For more information on configuring this, see Platform Settings.
  2. Create a static route for data traffic. For more information on creating a static route, see Add a Static Route.

     Sample static route configuration:

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```

Note *vxlan_tunnel_gw* is the data subnet's gateway IP address.

Deploy cluster on Azure with GWLB using an Azure resource manager template

This task creates a clustered deployment of Firewall Threat Defense Virtual instances on Azure using Gateway Load Balancer (GWLB) through Azure Resource Manager templates.

Deploy the Virtual Machine Scale Set for Azure GWLB using the customized Azure Resource Manager (ARM) template. The templates mentioned in the steps below are available on GitHub.

Procedure

Step 1 Prepare the template.

a) Clone the GitHub repository to your local folder. See https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure.

b) Modify azure_ftdv_gwlb_cluster.json and azure_ftdv_gwlb_cluster_parameters.json with the required parameters.

Step 2 Log in to the Azure Portal: https://portal.azure.com.

Step 3 Create a Resource Group.

a) In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.

b) Choose the required **Region**.

Step 4 Create a virtual network with three subnets: Management, Data, and Cluster Control Link (CCL).

a) Create the virtual network.

1. In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.
2. Choose the required **Region**. Click **Next: IP addresses**.

In the **IP Addresses** tab, click **Add subnet** and add the following subnets – Management, Data, and Cluster Control Link.

b) Add the subnets.

Step 5 Deploy the custom template.

a) Click **Create** > **Template deployment (deploy using custom templates)**.

b) Click **Build your own template in the editor**.

c) Click **Load File**, and upload **azure_ftdv_gwlb_cluster.json**.

d) Click **Save**.

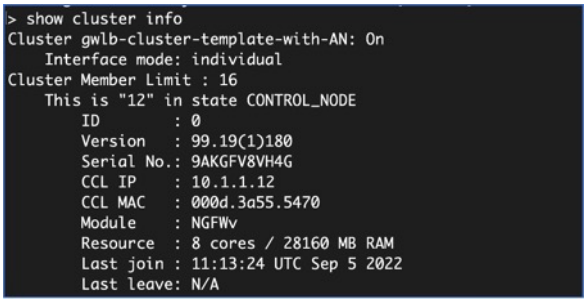
Step 6 Configure the Instance details.

a) Enter the required values and then click **Review + create**.

b) Click **Create** after the validation is passed.

c) After the instance is running, verify the cluster deployment by logging into any one of the nodes and entering the **show cluster info** command.

Figure 194: Show cluster info



Step 7 In the Azure Portal, click the Function app to register the cluster with the Firewall Management Center.

Note If you do not want to use the Function app, you can alternatively register the control node to the Firewall Management Center directly by using **Add** > **Device** (not **Add** > **Cluster**). The rest of the cluster nodes will register automatically.

Step 8 Create FTPS Credentials by clicking **Deployment Center** > **FTPS credentials** > **User scope** > **Configure Username and Password**, and then click **Save**.

Step 9 Upload the Cluster_Function.zip file to the Function app by executing the following **curl** command in the local terminal.

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

Note The **curl** command might take few minutes (~2 to 3 minutes) to complete command execution.

The function will be uploaded to the Function app. The function will start, and you can see the logs in the storage account's outqueue. The device registration with the Management Center will be initiated.

Figure 195: Functions

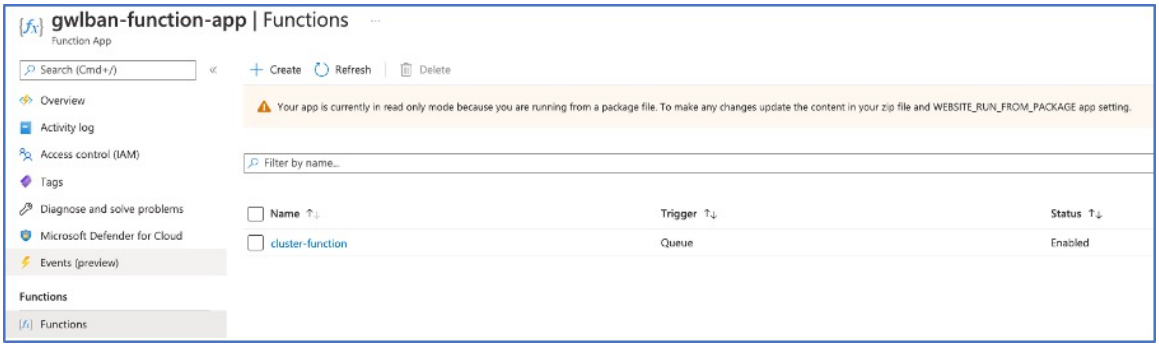


Figure 196: Queues

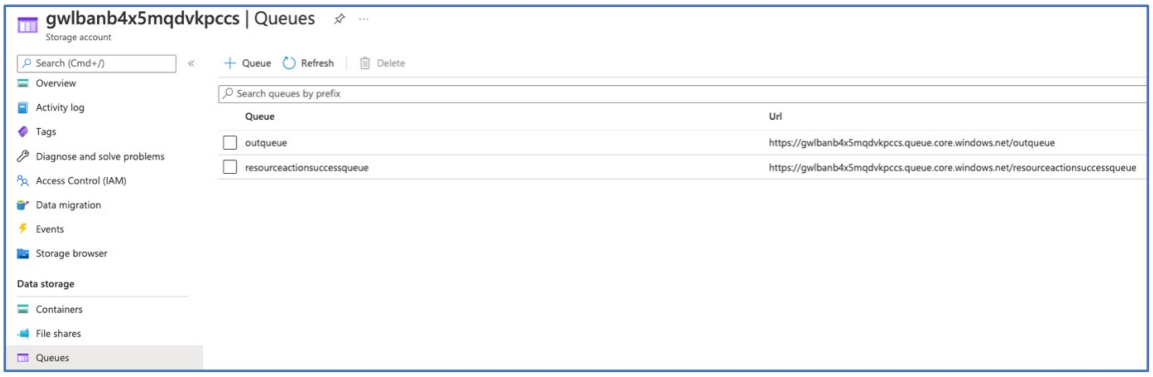
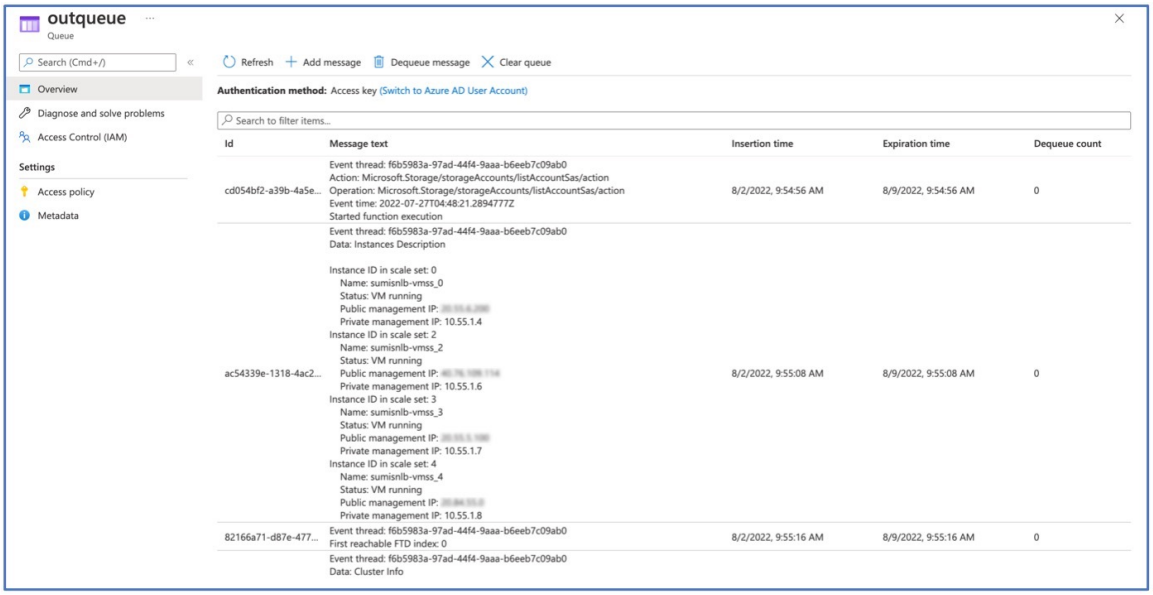


Figure 197: Outqueue



Sample topology for NLB-based cluster deployment

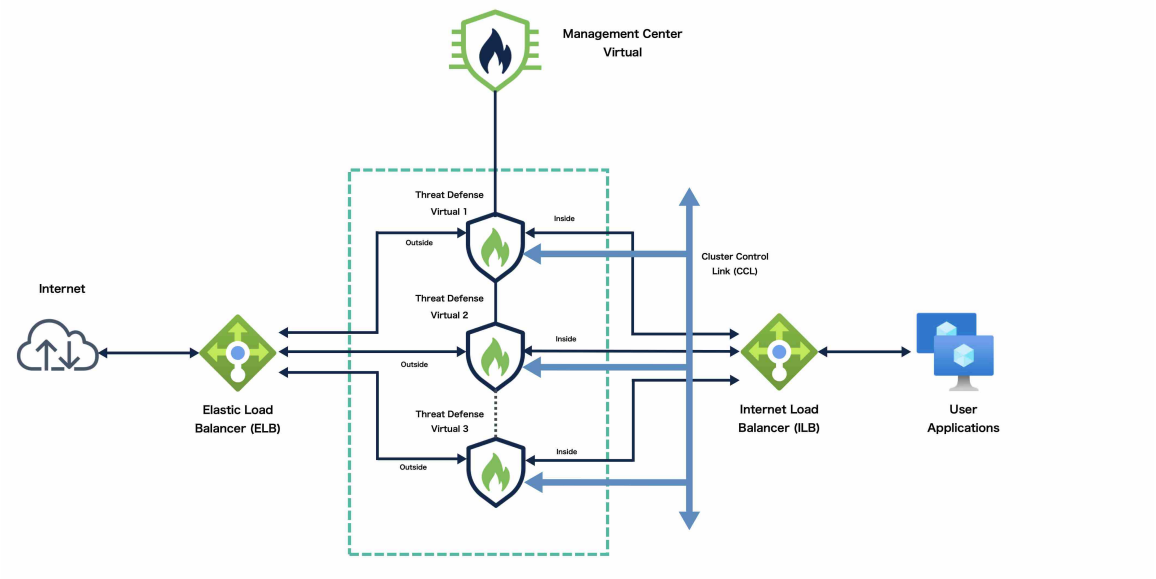
The sample topology provided here

- places the Threat Defense Virtual cluster between internal and external load balancers,
- uses a Management Center Virtual instance to manage the cluster, and
- depicts both inbound and outbound traffic flow patterns.

Traffic flow patterns

This topology shows how traffic moves through the network components:

- **Inbound traffic**: Traffic from the internet goes to the external load balancer, which transmits the traffic to the Threat Defense Virtual cluster. After the traffic has been inspected by a Threat Defense Virtual instance in the cluster, it is forwarded to the application virtual machine (VM).
- **Outbound traffic**: Traffic from the application VM is transmitted to the internal load balancer. Traffic is then forwarded to the Threat Defense Virtual cluster and then sent out to the internet.

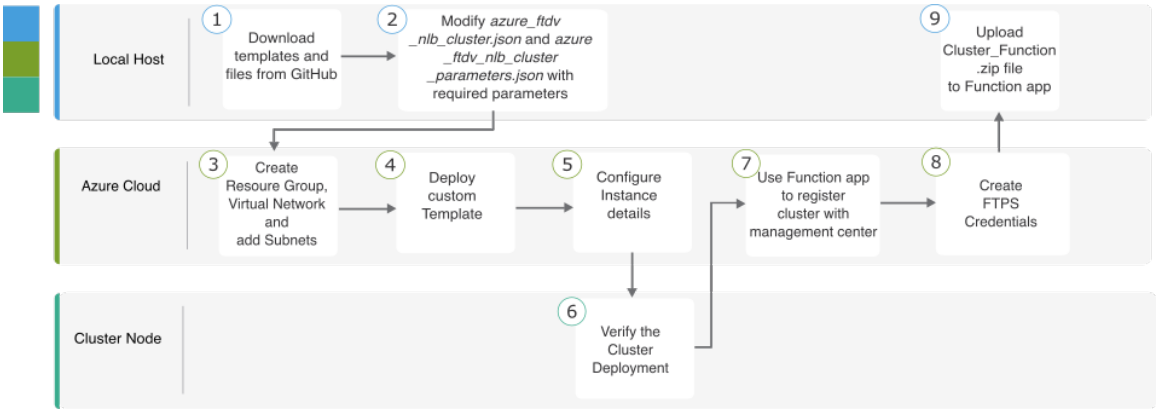


End-to-end process for deploying Threat Defense Virtual cluster in Azure with NLB

Provides a workflow to help users successfully deploy and verify a Threat Defense Virtual cluster on Azure with NLB using either template-based or manual deployment processes.

Template-based Deployment

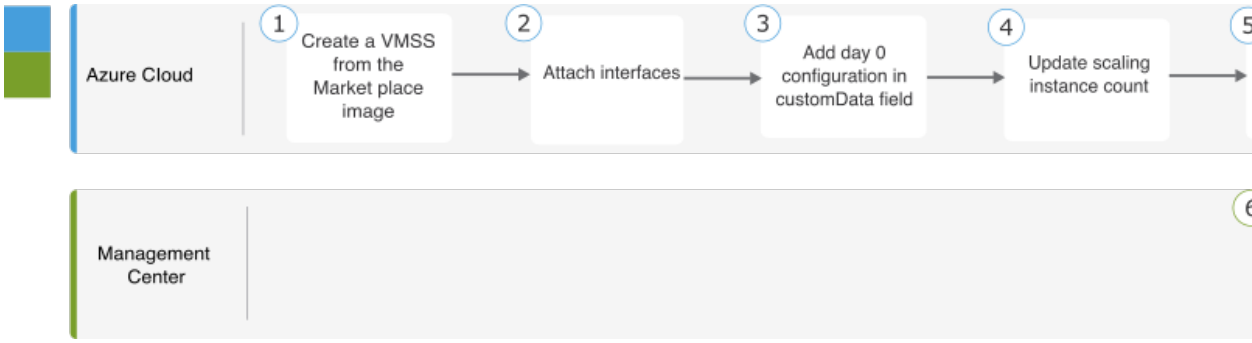
The following flowchart illustrates the workflow of template-based deployment of Threat Defense Virtual cluster in Azure with NLB.



	Workspace	Steps
1	Local Host	Download templates and files from GitHub.
2	Local Host	Modify *azure_ftdv_nlb_cluster.json* and *azure_ftdv_nlb_cluster_parameters.json* with the required parameters.
3	Azure Cloud	Create the resource group, virtual network, and subnets.
4	Azure Cloud	Deploy custom template.
5	Azure Cloud	Configure instance details.
6	Cluster Node	Verify cluster deployment.
7	Azure Cloud	Use the Function app to register the cluster with the Management Center.
8	Azure Cloud	Create FTPS credentials.
9	Local Host	Upload *Cluster_Function.zip* file to the Function app.

Manual Deployment

The following flowchart illustrates the workflow of manual deployment of Threat Defense Virtual cluster in Azure with NLB.



	Workspace	Steps
1	Local Host	Create a VMSS from the Marketplace image.
2	Local Host	Attach interfaces.
3	Local Host	Add day 0 configuration in the customData field.

	Workspace	Steps
4	Local Host	Update scaling instance count.
5	Local Host	Configure NLB.
6	Management Center	Add control node.

Templates

The templates are available in GitHub. The parameter values are self-explanatory with the parameter names and values given in the template.

These templates provide the necessary components for cluster deployment:

- azure_ftdv_nlb_cluster_parameters.json – Template to enter parameters for the Firewall Threat Defense Virtual cluster.
- azure_ftdv_nlb_cluster.json – Template to deploy Firewall Threat Defense Virtual cluster.

Prerequisites for Azure NLB cluster deployment

Before deploying an Azure Network Load Balancer cluster, ensure that you complete these prerequisite tasks.

- To allow the cluster to auto-register with the Management Center, create a user with Network Admin & Maintenance User privileges on the Management Center. Users with these privileges can use REST API. Refer to the Cisco Secure Firewall Management Center Administration Guide.
- Add an access policy in the Management Center that matches the name of the policy that you will specify during template deployment.
- Ensure that the Management Center Virtual is licensed appropriately.
- After the cluster is added to the Management Center Virtual, complete these configuration steps:
  1. Configure platform settings with the health check port number in the Management Center. For more information on configuring this, refer to Platform Settings.
  2. Create static routes for traffic from outside and inside interfaces. For more information on creating a static route, refer to Add a Static Route.

Important Configure static routes for both interface gateway paths when Azure Load Balancer health probes are enabled on both inside and outside interfaces of FTDv cluster nodes. Do not rely on a single default route. Azure health probes may arrive on either interface, so FTDv must respond using the correct interface path. Missing routing configuration can cause probe drops and load balancer health check failures. If SSH on port 22 is used as the health probe and SSH is enabled on both interfaces through Platform Settings, verify return path routing for both interfaces. Similarly, if HTTP is used as the health probe and HTTP or HTTPS is enabled on both interfaces through Platform Settings, verify return path routing for both interfaces.

Note Ensure that you do not configure your virtual network using the Microsoft-owned IP address range that includes 168.63.129.16. This configuration causes a conflict with the health probe's IP address. For more information, refer to Microsoft Azure design guidance.

Sample static route configuration for the outside interface:

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```

Note *ftdv-cluster-outside* is the outside subnet's gateway IP address.

Sample static route configuration for the inside interface:

```
Network: any-ipv4
Interface: inside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```

Note *ftdv-cluster-inside-gw* is the inside subnet's gateway IP address.

3. Configure NAT rule for data traffic. For more information on configuring NAT rules, refer to Network Address Translation.

Deploy cluster on Azure with NLB using an Azure resource manager template

This task enables you to deploy a cluster for Azure NLB using the customized Azure Resource Manager (ARM) template for scalable network security.

Deploy the cluster for Azure NLB using the customized Azure Resource Manager (ARM) template. Note that the templates mentioned in the steps below are available on GitHub.

Procedure

Step 1 Prepare the template.

a) Clone the GitHub repository to your local folder. See https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure.

b) Modify azure_ftdv_nlb_cluster.json and azure_ftdv_nlb_cluster_parameters.json with the required parameters.

Step 2 Log in to the Azure Portal: https://portal.azure.com.

Step 3 Create a Resource Group.

a) In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.

b) Choose the required **Region**.

Step 4 Create a virtual network with 5 subnets: Management, Diagnostic, Inside, Outside, and Cluster Control Link.

a) Create the virtual network.

1. In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.
2. Choose the required **Region**. Click **Next: IP addresses**.

b) Add the subnets.

In the **IP Addresses** tab, click **Add subnet** and add the following subnets – Management, Diagnostic, Inside, Outside, and Cluster Control Link.

Step 5 Deploy the custom template.

a) Click **Create** > **Template deployment (deploy using custom templates)**.

b) Click **Build your own template in the editor**.

c) Click **Load File**, and upload **azure_ftdv_nlb_cluster.json**.

d) Click **Save**.

Step 6 Configure the instance details.

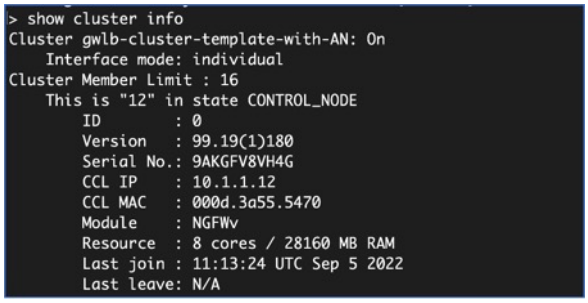
a) Enter the required values and then click **Review + create**.

Note For the cluster control link starting and ending addresses, specify only as many addresses as you need (up to 16). A larger range can affect performance.

b) Click **Create** after the validation is passed.

c) After the instance is running, verify the cluster deployment by logging into any one of the nodes and using the **show cluster info** command.

Figure 198: Show cluster info



Step 7 In the Azure Portal, click the Function app to register the cluster to the Firewall Management Center.

Note If you do not want to use the Function app, you can alternatively register the control node with the Management Center directly by using **Add** > **Device** (not **Add** > **Cluster**). The rest of the cluster nodes will register automatically.

Step 8 Create FTPS Credentials by clicking **Deployment Center** > **FTPS credentials** > **User scope** > **Configure Username and Password**, and then click **Save**.

Step 9 Upload the Cluster_Function.zip file to the Function app by executing the **curl** command in the local terminal.

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

Note The **curl** command might take a few minutes (~2 to 3 minutes) to complete command execution.

The function will be uploaded to the Function app. The function will start, and you can see the logs in the storage account's outqueue. The device registration with the Management Center will be initiated.

Manual cluster deployment in Azure

To deploy the cluster manually, prepare the day0 configuration, deploy each node, and then add the control node to the Firewall Management Center .

Create the Day0 configuration for Azure

You can use either a fixed configuration or a customized configuration.

Create the Day0 configuration with a fixed configuration for Azure

The fixed configuration will auto-generate the cluster bootstrap configuration.

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
```

```
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

Example

A sample day 0 configuration is given below.

```
"Cluster": {
"CclSubnetRange": "10.45.3.4 10.45.3.30",     //mandatory user input
"ClusterGroupName": "ngfwv-cluster",          //mandatory user input
"HealthProbePort": "7777",                    //mandatory user input
"GatewayLoadBalancerIP": "10.45.2.4",         //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "2000",
"ExternalPort": "2001",
"InternalSegId": "800",
"ExternalSegId": "801"
}
```

Note If you are copying and pasting the configuration given above, ensure that you remove **//mandatory user input** from the configuration

For the Azure health check settings, be sure to specify the **HealthProbePort** you set here.

For the **CclSubnetRange** variable, specify a range of IP addresses starting from x.x.x.4. Ensure that you have at least 16 available IP addresses for clustering. Some examples of start and end IP addresses are given below.

Note All cluster infrastructure subnets must use /27 CIDR

Table 34: Examples of start and end IP addresses

CIDR	Start IP Address	End IP Address
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222

CIDR	Start IP Address	End IP Address
10.1.1.224/27	10.1.1.228	10.1.1.254

Create the Day0 configuration with a customized configuration for azure

You can enter the entire cluster bootstrap configuration using commands.

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

Deploy cluster nodes manually - GWLB-based deployment

This task allows you to deploy cluster nodes so they form a cluster in Azure using Gateway Load Balancer-based deployment.

Deploy the cluster nodes so they form a cluster.

Procedure

Step 1 Log in to the Azure Portal: https://portal.azure.com

Step 2 Create a Resource Group.

a. In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.

b. Choose the required **Region**.

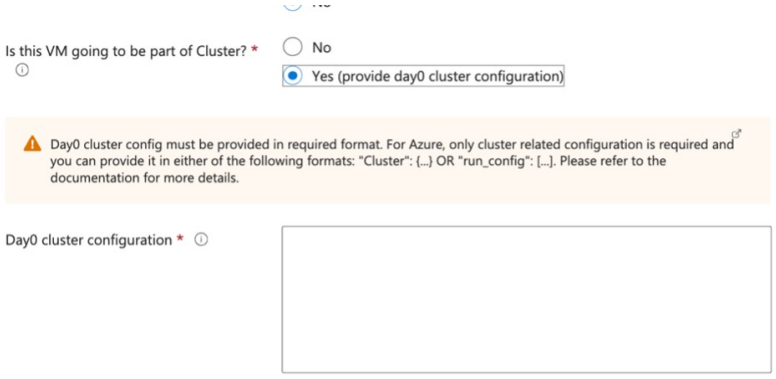
Step 3 Create a Virtual Network with the necessary subnets: Management, Data and Cluster Control Link (CCL).

Note Configure the CCL with the smallest subnet mask as required. Wider subnets can impact performance.

Refer to the Azure document for creating the Virtual Network and subnet: https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

Step 4 Go to the Marketplace and search for **Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG** and click **Create**.

Step 5 Fill the required details and choose **Yes** for **Is this VM going to be part of Cluster?**



Paste the following cluster-related configuration in the text box.

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name", //mandatory user input
"HealthProbePort": "port_number", //mandatory user input
"GatewayLoadBalancerIP": "ip_address",  //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

a) Click **Next** and select the **Virtual Network & Subnets**.

b) Click **Review + create**. Wait for the Threat Defense Virtual deployment to complete.

Step 6 Connect to the Threat Defense Virtual device and use the **show cluster info** command to confirm the cluster formation is successful.

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

Step 7 Configure the Azure Gateway Load Balancer. Refer to Auto Scale with Azure Gateway Load Balancer Use Case for more information.

Step 8 Add the control node to the Firewall Management Center. Refer to Add the cluster to the Management Center (manual deployment), on page 493.

Deploy cluster nodes manually - NLB-based deployment

Deploy cluster nodes manually to establish a functional cluster configuration in Azure using NLB-based deployment.

Deploy the cluster nodes so they form a cluster.

Procedure

Step 1 Log in to the Azure Portal: https://portal.azure.com

Step 2 Create a Resource Group.

a. In the **Basics** tab, choose the **Subscription** and **Resource Group** from the drop-down lists.

b. Choose the required **Region**.

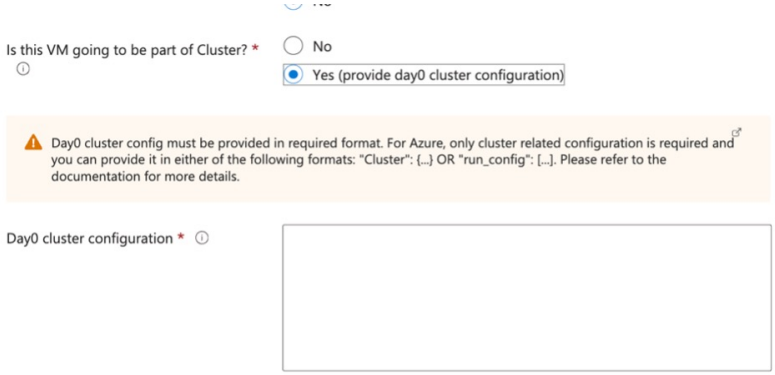
Step 3 Create a Virtual Network with the necessary subnets: Management, Inside, Outside and Cluster Control Link (CCL).

Note Configure the CCL with the smallest subnet mask as required. Wider subnets can impact performance.

Refer to the Azure document for creating the Virtual Network and subnet: https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

Step 4 Go to the Marketplace and search for **Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG** and click **Create**.

Step 5 Fill the required details and choose **Yes** for **Is this VM going to be part of Cluster?**



Paste the following cluster-related configuration in the text box.

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name" //mandatory user input
}
```

Step 6 Click **Next** and select the **Virtual Network & Subnets**.

Step 7 Click **Review + create**. Wait until the Threat Defense Virtual deployment is completed.

Step 8 Connect to the Threat Defense Virtual device and use the **show cluster info** command to confirm the cluster formation is successful.

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

Step 9 Add the control node to the Management Center. Refer to Add the cluster to the Management Center (manual deployment), on page 493.

Troubleshoot cluster deployment in Azure

This reference provides troubleshooting guidance for resolving common issues that may occur during cluster deployment in Azure, including traffic flow problems, cluster formation failures, and role assignment errors.

- Issue: No traffic flow

  Troubleshooting:

  - Check if the health probe status of the Threat Defense Virtual instances deployed with a GWLB is healthy.
  - If the Threat Defense Virtual instance's health probe status is unhealthy-
    - Check if the static route is configured in the Management Center Virtual.
    - Check if the default gateway is the data subnet's gateway IP address.
    - Check if the Threat Defense Virtual instance is receiving health probe traffic.
    - Check if the access list configured in the Management Center Virtual allows health probe traffic.

- Issue: Cluster is not formed

  Troubleshooting:

  - Check the IP address of the NVE-only cluster interface. Ensure that you can ping the NVE-only cluster interface of other nodes.
  - Check the IP address of the NVE-only cluster interfaces are part of the object group.
  - Ensure that the NVE interface is configured with the object group .

- Ensure that the cluster interface in the cluster group has the right VNI interface. This VNI interface has the NVE with the corresponding object group.
- Ensure that the nodes are pingable from each other. Since each node has its own cluster interface IP, these should be pingable from each other.
- Check if the CCL subnet's start and end address mentioned during template deployment is correct. The start address should begin with the first available IP address in the subnet. For example, if the subnet is 192.168.1.0/27. The start address should be 192.168.1.4 (the three IP addresses at the start are reserved by Azure).
- Check if the Management Center Virtual has a valid license.

- Issue: Role-related error while deploying resources again in the same resource group.

  Troubleshooting: Remove the roles given below by using these commands on the terminal.

  Error message:

```
"error": {
"code": "RoleAssignmentUpdateNotPermitted",
"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be
updated."}
```

  - **az role assignment delete --resource-group** <*Resource Group Name*> **--role "Storage Queue Data Contributor"**
  - **az role assignment delete --resource-group** <*Resource Group Name*> **--role "Contributor"**

Deploy the cluster in GCP

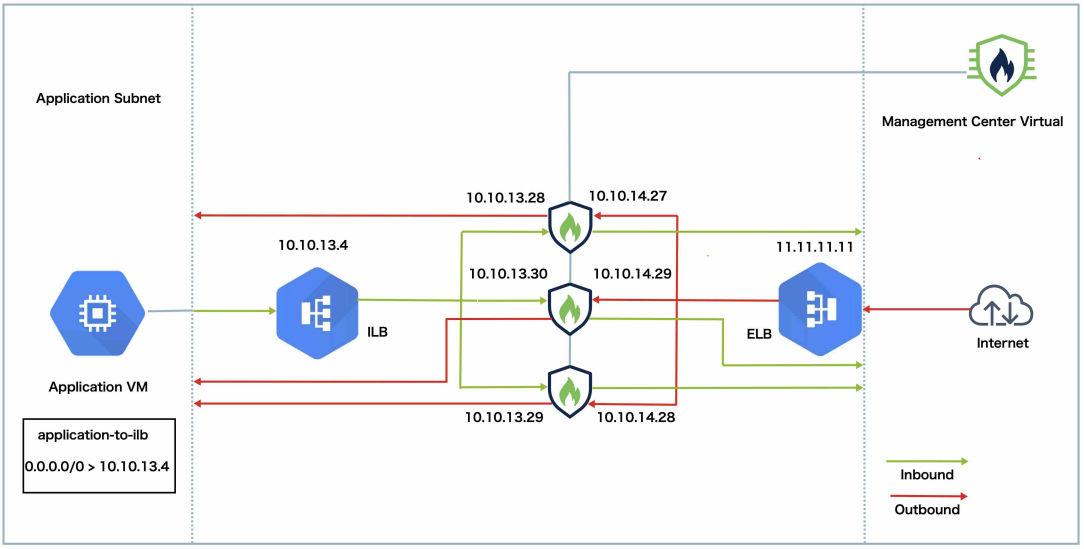
To deploy a cluster in GCP, you can either manually deploy or use an instance template to deploy an instance group. You can use the cluster with native GCP load balancers or non-native load balancers such as the Cisco Cloud Services Router.

Note Outbound traffic requires interface NAT and is limited to 64,000 connections.

Sample topology for GCP clustering autoscale solution

Understand the architecture and traffic flow of a typical GCP clustering autoscale deployment.

Figure 199: Sample Topology



The topology shows both inbound and outbound traffic flow.

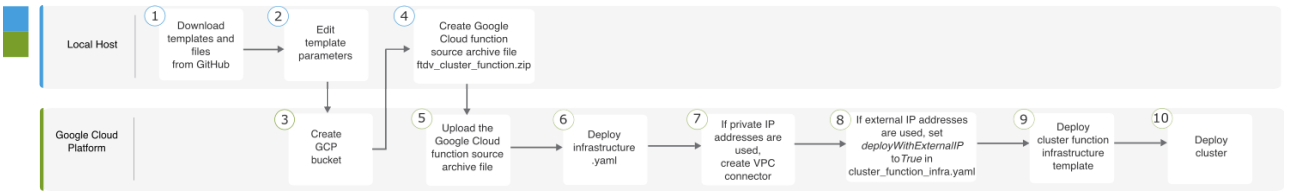
1. The Threat Defense Virtual cluster is placed between the internal and external load balancers. A Management Center Virtual instance is used to manage the cluster.
2. Inbound traffic from the internet goes to the external load balancer, which then transmits the traffic to the Threat Defense Virtual cluster.
3. The Threat Defense Virtual instance in the cluster inspects the traffic, and after inspection, forwards the traffic to the application VM.
4. Outbound traffic from the application VM goes to the internal load balancer. The load balancer forwards this traffic to the Threat Defense Virtual cluster, which sends it to the internet.

End-to-end process for deploying Threat Defense Virtual cluster in GCP

Provides a workflow to help users successfully deploy and verify a Threat Defense Virtual cluster on GCP using either template-based or manual deployment processes.

Template-based Deployment

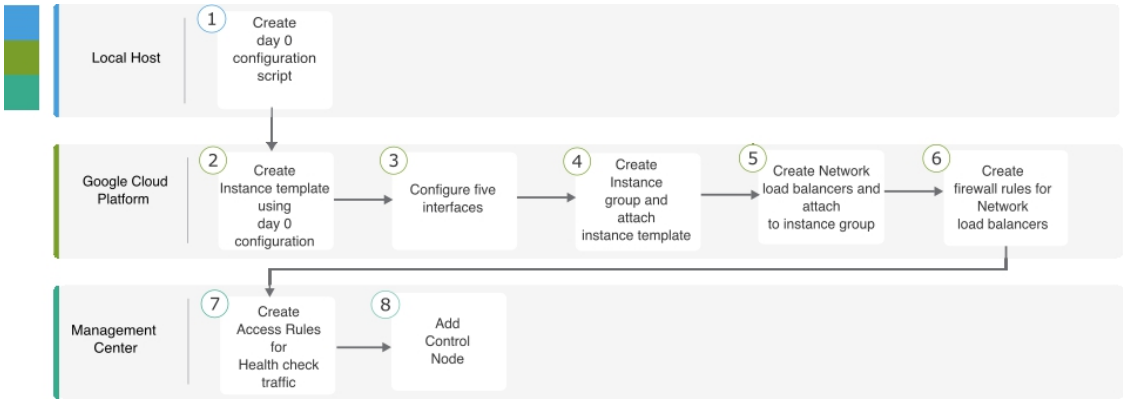
The following flowchart illustrates the workflow for template-based deployment of the Threat Defense Virtual cluster on GCP.



	Workspace	Steps
1	Local Host	Download templates and files from GitHub.
2	Local Host	Edit template parameters.
3	Google Cloud Platform	Create GCP bucket.
4	Local Host	Create Google Cloud function source archive file *ftdv_cluster_function.zip*.
5	Google Cloud Platform	Upload the Google function source archive file.
6	Google Cloud Platform	Deploy infrastructure.yaml.
7	Google Cloud Platform	If private IP addresses are used, create VPC connector.
8	Google Cloud Platform	If external IP addresses are used, set *deployWithExternalIP* to *True* in *cluster_function_infra.yaml*.
9	Google Cloud Platform	Deploy cluster function infrastructure template.
10	Google Cloud Platform	Deploy cluster.

Manual Deployment

The following flowchart illustrates the workflow for manual deployment of the Threat Defense Virtual cluster on GCP.



	Workspace	Steps
1	Local Host	Create day 0 configuration script.

	Workspace	Steps
2	Google Cloud Platform	Create instance template using day 0 configuration.
3	Google Cloud Platform	Configure the interfaces.
4	Google Cloud Platform	Create instance group and attach instance template.
5	Google Cloud Platform	Create NLB and attach to instance group.
6	Google Cloud Platform	Create firewall rules for NLB.
7	Management Center	Create access rules for health check traffic.
8	Management Center	Add control node.

Templates

The templates are available in GitHub. The parameter values are self-explanatory with the parameter names and values given in the template.

- Cluster deployment template for East-West traffic - deploy_ngfw_cluster_yaml
- Cluster deployment template for North-South traffic - deploy_ngfw_cluster.yaml

Deploy the instance group in GCP using an instance template

Deploy a scalable instance group in Google Cloud Platform using pre-configured instance templates to establish a Secure Firewall cluster with automated management capabilities.

Deploy the instance group in GCP using an instance template.

Before you begin

- Download the templates from GitHub to your local folder.
- Use Google Cloud Shell for deployment. Alternatively, you can use Google SDK on any macOS/Linux/Windows machine.
- To allow the cluster to auto-register with the Management Center, you need to create a user with administrative privileges on the Management Center that can use the REST API. See the *Cisco Secure Firewall Management Center Administration Guide*.
- Add an access policy in the Management Center that matches the name of the policy that you specified in *cluster_function_infra.yaml*.

Procedure

Step 1 Edit the **infrastructure.yaml**, **cluster_function_infra.yaml** and **deploy_ngfw_cluster.yaml** templates with the required *resourceNamePrefix* parameter (for example, ngfwvcls) and other required user inputs.

From Secure Firewall version 7.4.1, you can deploy the cluster without the diagnostic interface. To deploy the cluster with only the Outside, Inside, Management, and CCL interfaces, set the *withDiagnostic* variable to **False** in both the **infrastructure.yaml** and the **deploy_ngfw_cluster.yaml** files.

Note that there is a **deploy_ngfw_cluster.yaml** file in both the **east-west** and **north-south** folders in GitHub. Download the appropriate template as per your traffic flow requirement.

Step 2 Create a bucket using Google Cloud Shell to upload the Google cloud function source archive file *ftdv_cluster_function.zip*.

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

Ensure that the *resourceNamePrefix* variable here matches the *resourceNamePrefix* variable that you specified in **cluster_function_infra.yaml**.

Step 3 Create an archive file for the cluster infrastructure.

Example:

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

Step 4 Upload the Google source archive that you created earlier.

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

Step 5 Deploy infrastructure for the cluster.

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

Step 6 If you are using private IP addresses, perform the steps given below:

a) Launch and set up the Management Center Virtual with a Threat Defense Virtual management VPC.

b) Create a VPC connector to connect the Google Cloud functions with the Threat Defense Virtual management VPC.

gcloud compute networks VPC-access connectors create *VPC-connector-name* **--region us-central1 --subnet** *resourceNamePrefix***-ftdv-mgmt-subnet28**

Step 7 If the Management Center is remote from the Threat Defense Virtual, and the Threat Defense Virtual needs an external IP address, ensure that you set **deployWithExternalIP** to **True** in **cluster_function_infra.yaml**.

Step 8 Deploy the cluster function infrastructure.

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

Step 9 Deploy the cluster.

a. For North-South topology deployment:

gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

b. For East-West topology deployment:

gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

Manual cluster deployment in GCP

To deploy the cluster manually, prepare the day0 configuration, deploy each node, and then add the control node to the Firewall Management Center .

Create the Day0 configuration with a fixed configuration for GCP

The fixed configuration will auto-generate the cluster bootstrap configuration.

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
                "Diagnostic": "OFF",       //Optional user input from version 7.4.1 - use
to deploy cluster without Diagnostic interface
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
    }
}
```

For example:

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",     //mandatory user input
        "ClusterGroupName": "ftdv-cluster"               //mandatory user input
    }
}
```

Note If you are copying and pasting the configuration given above, ensure that you remove **//mandatory user input** from the configuration.

For the **CclSubnetRange** variable, note that you cannot use the first two IP addresses and the last two IP addresses in the subnet. See Reserved IP addresses in IPv4 subnets for more information. Ensure that you have at least 16 available IP addresses for clustering. Some examples of start and end IP addresses are given below.

Note All cluster infrastructure subnets must use /27 CIDR.

Table 35: Examples of start and end IP addresses

CIDR	Start IP Address	End IP Address
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253

Deploy cluster nodes manually

Deploy cluster nodes to form a functional cluster on Google Cloud Platform (GCP) with proper network load balancing and management integration.

Deploy the cluster nodes so they form a cluster. For clustering on GCP, you cannot use the 4 vCPU machine type. The 4 vCPU machine type only supports four interfaces, and five are needed. Use a machine type that supports five interfaces, such as c2-standard-8.

Procedure

Step 1 Create an instance template using the day 0 configuration (in the **Metadata** > **Startup Script** section) with 5 interfaces: outside, inside, management, diagnostic, and cluster control link.

See Secure Firewall Threat Defense Virtual getting started guides.

Step 2 Create an instance group, and attach the instance template.

Step 3 Create GCP network load balancers (internal and external), and attach the instance group.

Step 4 For GCP network load balancers, allow health checks in your security policy on the Management Center. Refer to Allow health checks for GCP network load balancers, on page 491.

Step 5 Add the control node to the Management Center. Refer to Add the cluster to the Management Center (manual deployment), on page 493.

Allow health checks for GCP network load balancers

Google Cloud provides health checks to determine if backends respond to traffic. This configuration allows health check traffic through firewall rules and access rules, redirects health check traffic to the Google metadata server using dynamic manual NAT rules, and sets up routing for GCP health checks across all interfaces used for health probes.

Configuration requirements

Refer to https://cloud.google.com/load-balancing/docs/health-checks to create firewall rules for network load balancers. Then in the Firewall Management Center, create access rules to allow the health check traffic. See https://cloud.google.com/load-balancing/docs/health-check-concepts for the required network ranges. See Access Control Rules, on page 1609.

You also need to configure dynamic manual NAT rules to redirect the health check traffic to the Google metadata server at 169.254.169.254. See Configure dynamic manual NAT, on page 1214.

You can set up a route for GCP health checks across all interfaces that are used to configure their health probes. You can achieve this by creating a route with a higher metric on interfaces where a route for GCP health checks is not already available.

North-South NAT rules sample configuration

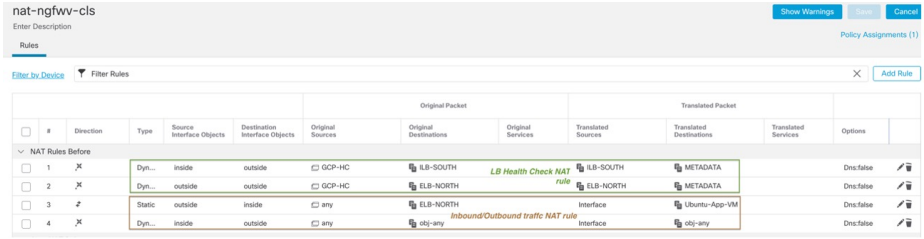
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



East-West NAT rules sample configuration

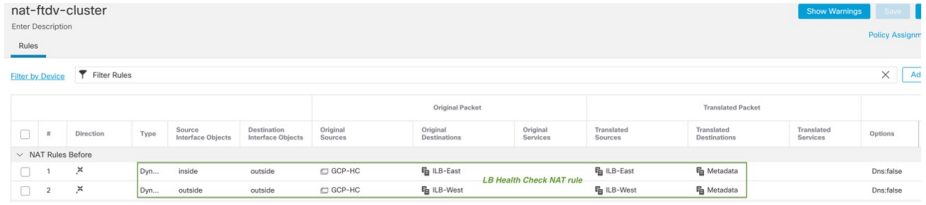
```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
```

```
network-object 35.191.0.0 255.255.0.0
network-object 130.211.0.0 255.255.252.0
network-object 209.85.204.0 255.255.252.0
network-object 209.85.152.0 255.255.252.0
```



North-South and East-West traffic routing configuration sample

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

If a default route is not available, then policy-based routing can be used to route the traffic for health checks.

Note Set the NAT > Translated destination port to 80.

Add the cluster to the Management Center (manual deployment)

This task registers a manually deployed cluster with the Firewall Management Center to enable centralized management and configuration of the cluster units.

Use this procedure to add the cluster to the Firewall Management Center if you manually deployed the cluster. If you used a template, the cluster will auto-register on the Firewall Management Center.

Add one of the cluster units as a new device to the Firewall Management Center; the Firewall Management Center automatically detects all other cluster members.

Before you begin

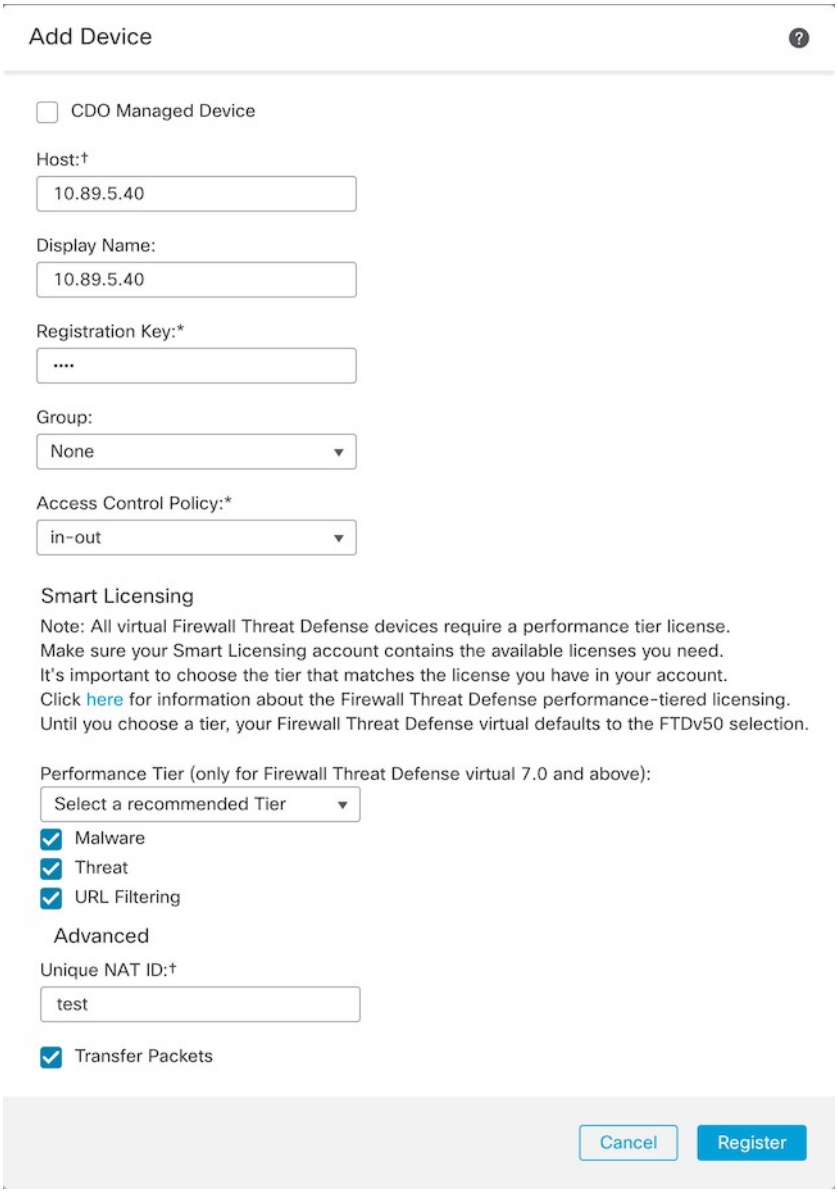
- All cluster units must be in a successfully formed cluster before adding the cluster to the Firewall Management Center. You should also check which unit is the control unit. Use the Firewall Threat Defense **show cluster info** command.

Follow these steps to add the cluster to the Management Center for manual deployment:

Procedure

Step 1 In the Firewall Management Center, choose **Devices** > **Device Management**, and then choose **Add** > **Add Device** to add the control unit using the unit's management IP address.

Figure 200: Add device



a) In the **Host** field, enter the IP address or hostname of the control unit.

We recommend adding the control unit for the best performance, but you can add any unit of the cluster.

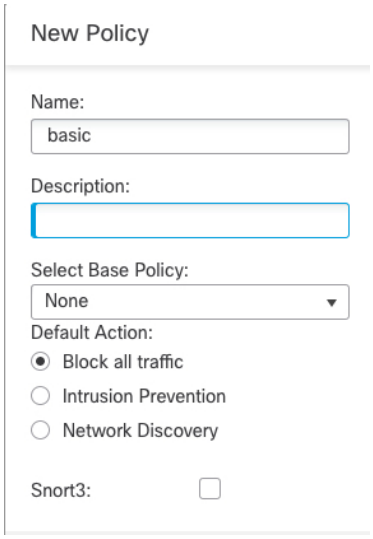
If you used a NAT ID during device setup, you may not need to enter this field. For more information, see NAT environments, on page 8.

b) In the **Display Name** field, enter a name for the control unit as you want it to display in the Firewall Management Center.

This display name is not for the cluster; it is only for the control unit you are adding. You can later change the name of other cluster members and the cluster display name.

c) In the **Registration Key** field, enter the same registration key that you used during device setup. The registration key is a one-time-use shared secret.
d) (Optional) Add the device to a device **Group**.
e) Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If you create a new policy, you create a basic policy only. You can later customize the policy as needed.



f) Choose licenses to apply to the device.
g) If you used a NAT ID during device setup, expand the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field.
h) Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

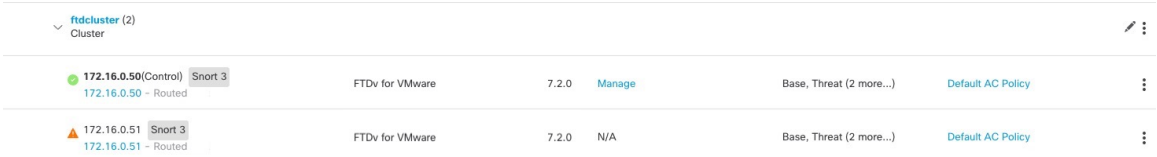
If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent.

i) Click **Register**.

The Firewall Management Center identifies and registers the control unit, and then registers all data units. If the control unit does not successfully register, then the cluster is not added. A registration failure can occur if the cluster was not up, or because of other connectivity issues. In this case, we recommend that you try re-adding the cluster unit.

The cluster name shows on the **Devices** > **Device Management** page; expand the cluster to see the cluster units.

Figure 201: Cluster management

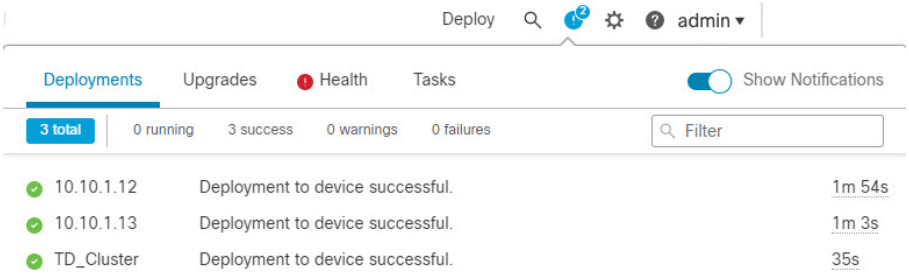


A unit that is currently registering shows the loading icon.

Figure 202: Node registration



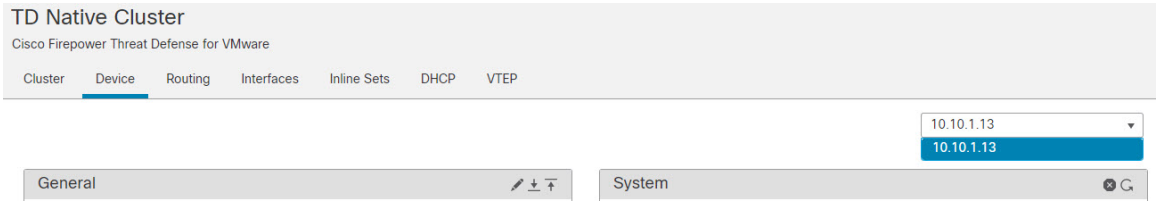
You can monitor cluster unit registration by clicking the **Notifications** icon and choosing **Tasks**. The Firewall Management Center updates the Cluster Registration task as each unit registers. If any units fail to register, see Reconcile Cluster Nodes, on page 504.



Step 2 Configure device-specific settings by clicking the **Edit** (✎) for the cluster.

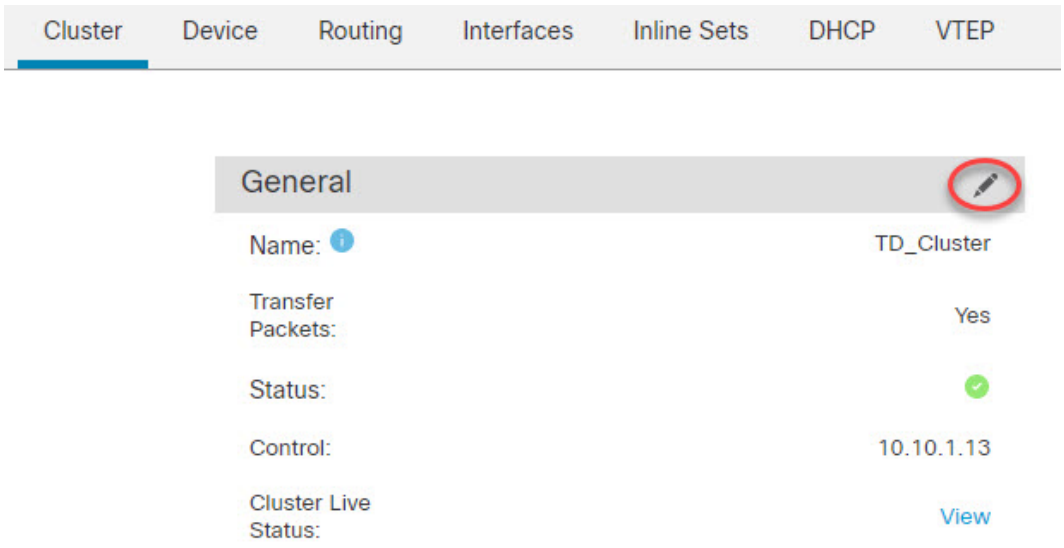
Most configuration can be applied to the cluster as a whole, and not nodes in the cluster. For example, you can change the display name per node, but you can only configure interfaces for the whole cluster.

Step 3 On the **Devices** > **Device Management** and then choose **Add**, **Cluster** screen, you see **General**, **License**, **System**, and **Health** settings.

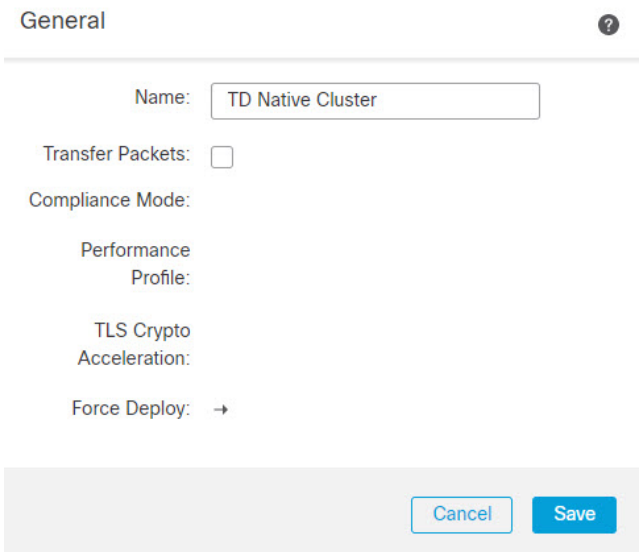


See these cluster-specific items:

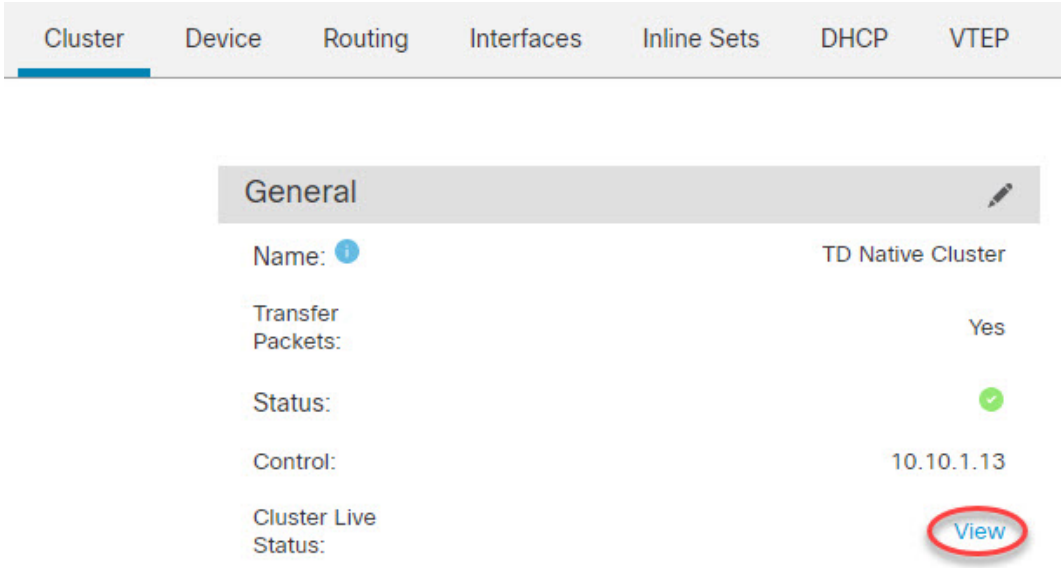
- **General** > **Name**—Change the cluster display name by clicking the **Edit** (✎).



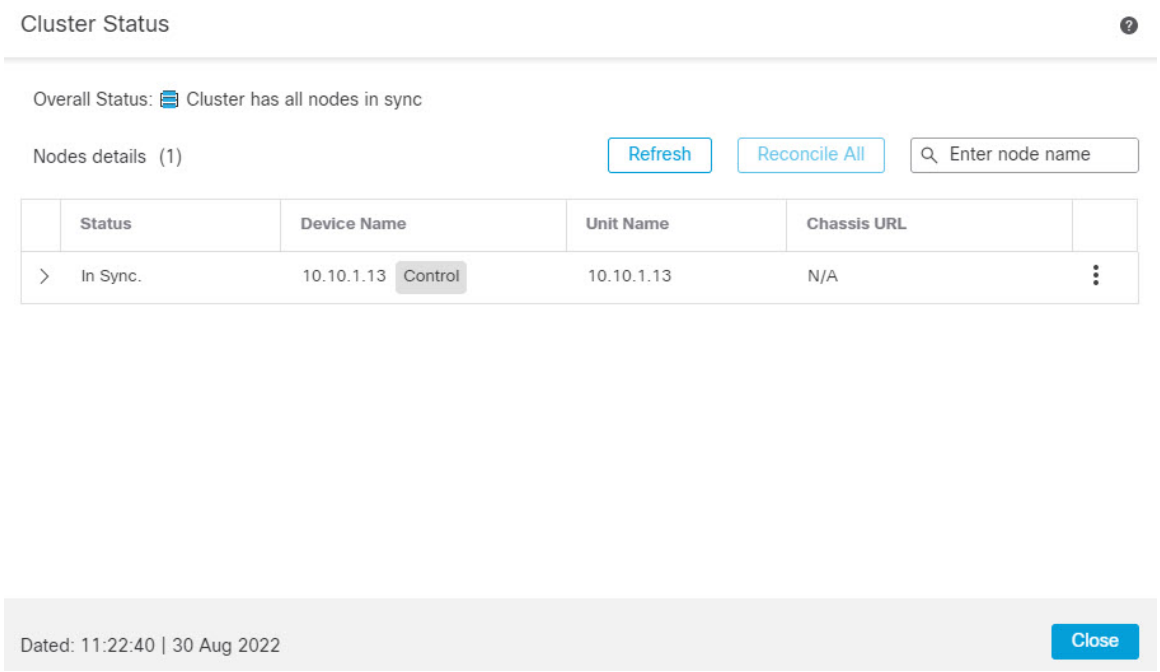
Then set the **Name** field.



- **General > Cluster Live Status**—Click the **View** link to open the **Cluster Status** dialog box.

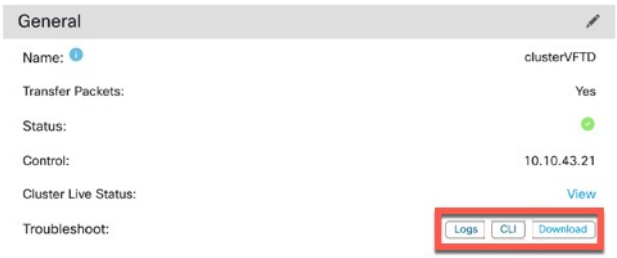


The **Cluster Status** dialog box also lets you retry data unit registration by clicking **Reconcile**.You can also ping the cluster control link from a node. See Perform a ping on the cluster control link, on page 367.



- **General > Troubleshoot**—You can generate and download troubleshooting logs, and you can view cluster CLIs. See Troubleshoot the cluster, on page 365.

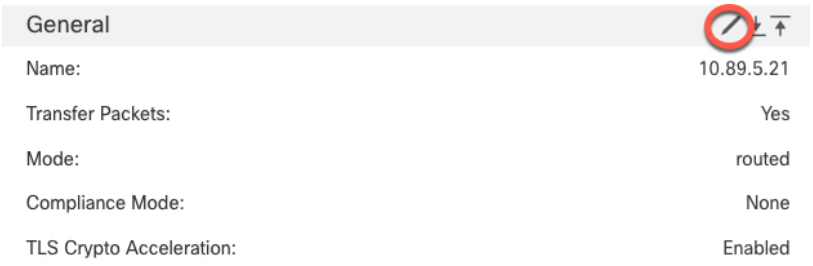
Figure 203: Troubleshoot



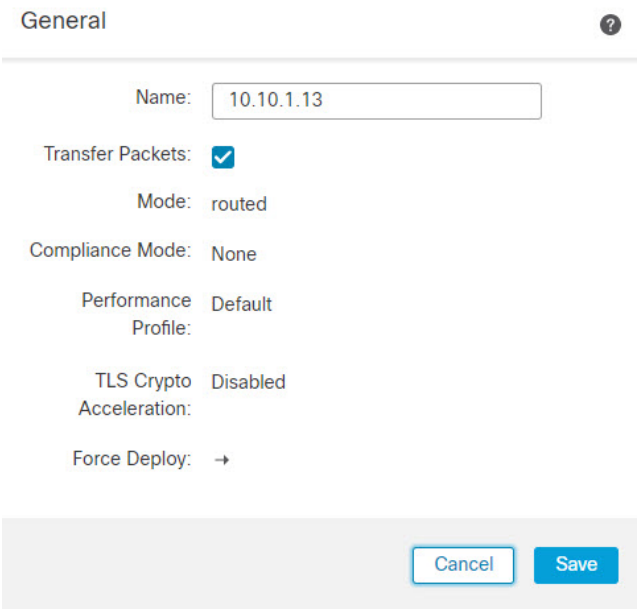
- **License**—Click **Edit** (✎) to set license entitlements.

Step 4 On the **Devices** > **Device Management** and then click **Add** > **Device**, you can choose each member in the cluster from the top right drop-down menu and configure these settings.

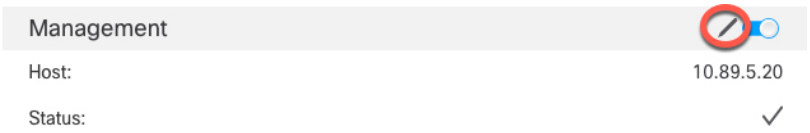
- **General > Name**—Change the cluster member display name by clicking the **Edit** (✎).



Then set the **Name** field.



- **Management > Host**—If you change the management IP address in the device configuration, you must match the new address in the Firewall Management Center so that it can reach the device on the network; edit the **Host** address in the **Management** area.



Edit cluster health monitor settings

This task allows you to modify cluster health monitor settings to control how cluster nodes monitor system health and automatically rejoin the cluster after failures.

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings for monitoring cluster node health. You can monitor any port-channel ID, any single physical interface ID, and the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link. It is always monitored.

When a topology change occurs (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature. Also, disable interface monitoring for any interfaces that are disabled. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management**.

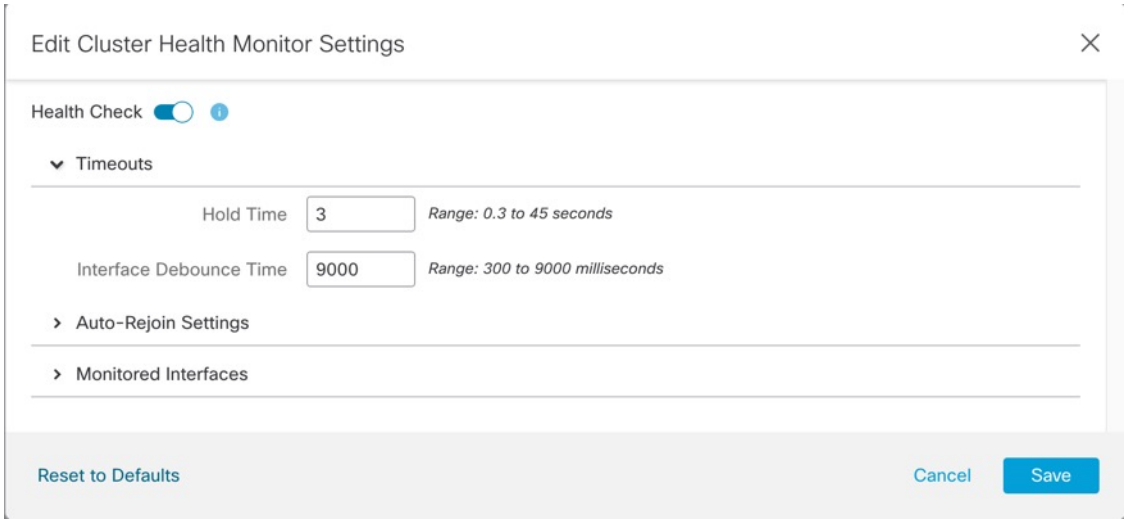
Step 2 Next to the cluster you want to modify, click **Edit** ( ).

Step 3 Click **Cluster**.

Step 4 In the **Cluster Health Monitor Settings** section, click **Edit** ( ).

Step 5 Disable the system health check by clicking the **Health Check** slider.

Figure 204: Disable the system health check



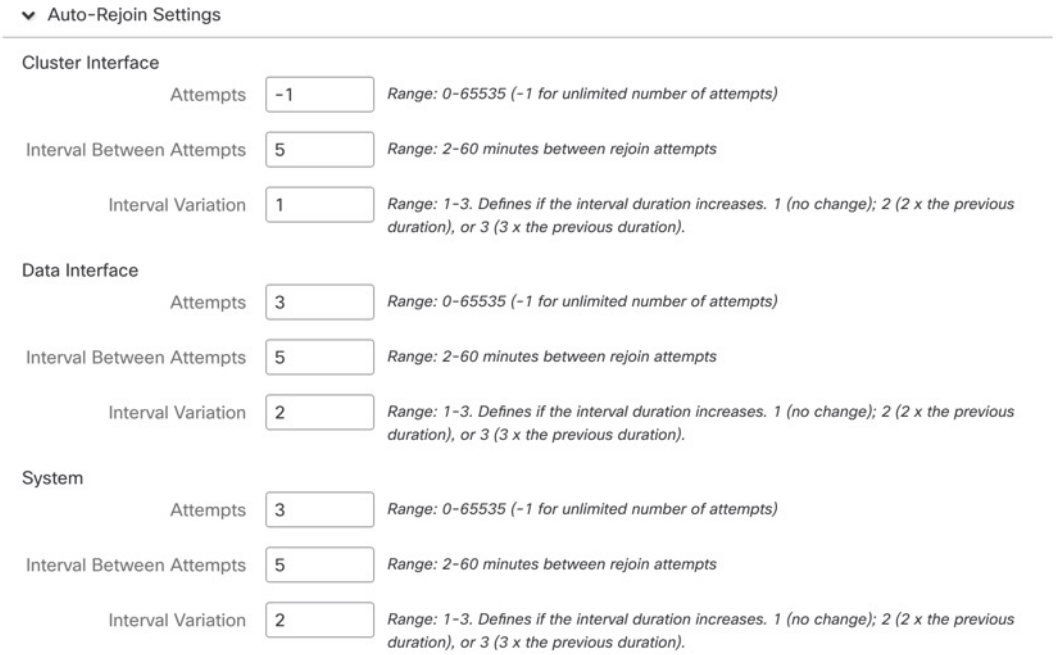
When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between 0.3 and 45 seconds. The default is 3 seconds.
- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the specified number of milliseconds before marking the interface as failed and removing the node from the cluster. If an EtherChannel transitions from a down state to an up state, such as after the switch reloads or enables an EtherChannel, a longer debounce time can prevent the interface from appearing failed on a cluster node if another cluster node bundles the ports more quickly.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 205: Configure Auto-Rejoin settings

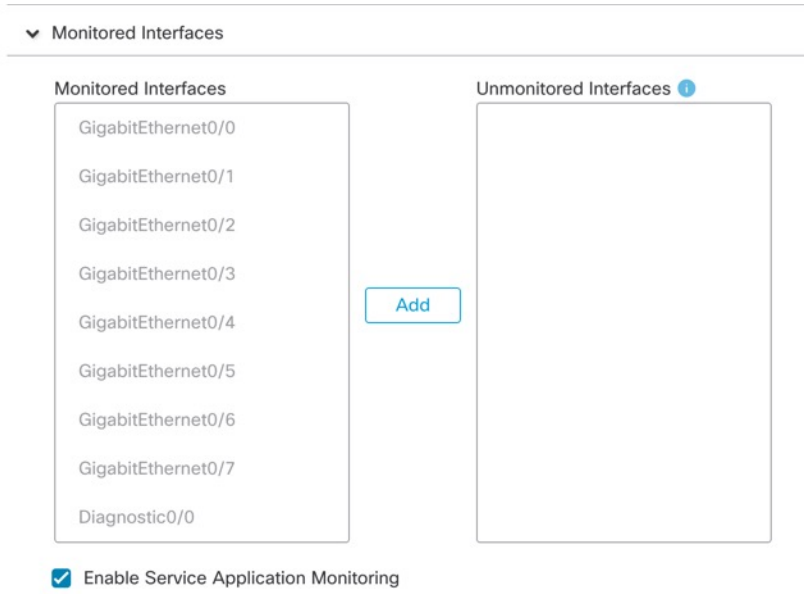


Set values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8 Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 206: Configure monitored interfaces



The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The time required to remove a member from the cluster depends on the type of interface and whether the node is established or is joining the cluster. By default, health check is enabled for all interfaces and the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save**.

Deploy configuration changes; see Deploy configuration changes, on page 135.

Manage cluster nodes

Explains how to add, remove, and configure cluster nodes in your deployment.

Disable clustering

Disable clustering to temporarily deactivate a node in preparation for deleting the node or for maintenance purposes.

You may want to deactivate a node to delete it or for temporary maintenance. This procedure temporarily deactivates a node, but the node will still appear in the Firewall Management Center device list. When a node becomes inactive, all data interfaces are shut down.

Note Do not power off the node without first disabling clustering.

Procedure

Step 1 For the unit you want to disable, choose **Devices** > **Device Management**, click the **More** (⋮), and choose **Disable Node Clustering**.

Step 2 Confirm that you want to disable clustering on the node.

The node will show **(Disabled)** next to its name in the **Devices** > **Device Management** list.

Step 3 To reenable clustering, refer to Rejoin the Cluster.

Rejoin the cluster

Rejoin a node to the cluster after it was removed because of failure or when clustering was manually disabled.

If a node was removed from the cluster, for example, due to a failed interface or if you manually disabled clustering, you must manually rejoin the cluster. Make sure the failure is resolved before you try to rejoin the cluster. Refer to Rejoining the cluster, on page 429 for more information about why a node can be removed from a cluster.

Procedure

Step 1 For the unit you want to reactivate, choose **Devices** > **Device Management**, click **More** (⋮), and choose **Enable Node Clustering**.

Step 2 Confirm that you want to enable clustering on the node.

Reconcile Cluster Nodes

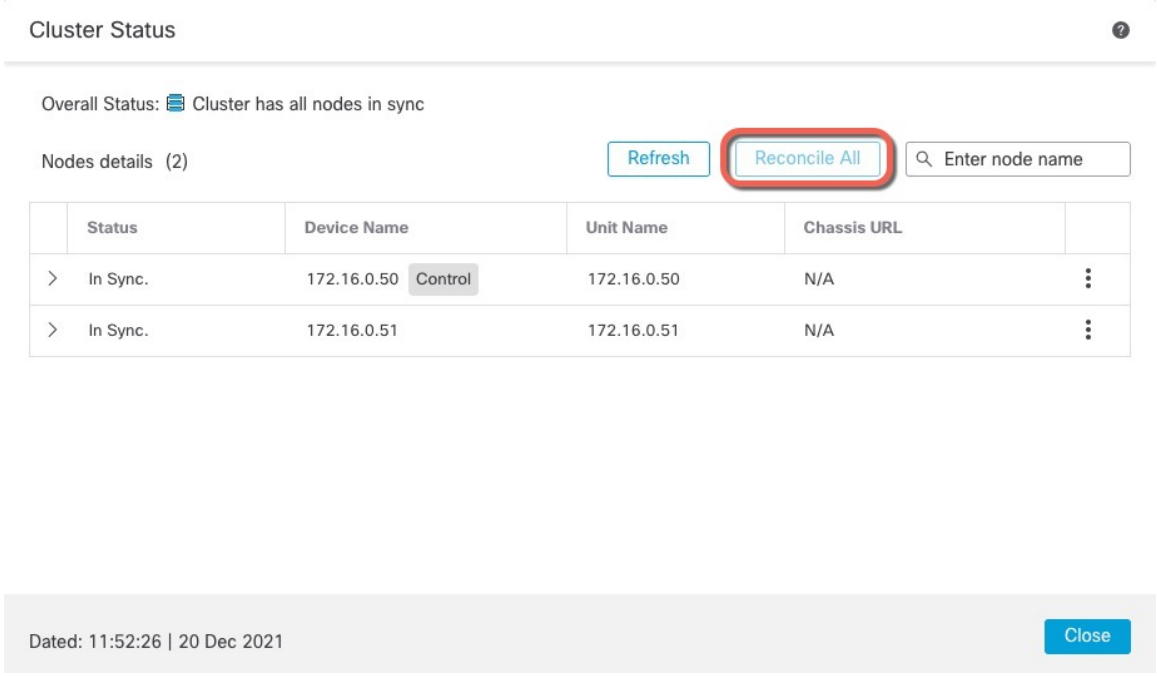
If a cluster node fails to register, you can reconcile the cluster membership from the device to the Firewall Management Center. For example, a data node might fail to register if the Firewall Management Center is occupied with certain processes, or if there is a network issue.

Procedure

Step 1 Choose **Devices** > **Device Management More** (⋮) for the cluster, and then choose **Cluster Live Status** to open the **Cluster Status** dialog box.

Step 2 Click **Reconcile All**.

Figure 207: Reconcile All



Delete (Unregister) the cluster or nodes and register with a new Firewall Management Center

This task allows you to move cluster nodes from one management center to another by safely removing them from their current management center and re-registering them with a new one.

You can unregister the cluster from the Firewall Management Center, which keeps the cluster intact. You might want to unregister the cluster if you want to add the cluster to a new Firewall Management Center.

You can also unregister a node from the Firewall Management Center without breaking the node from the cluster. Although the node is not visible in the Firewall Management Center, it is still part of the cluster, and it will continue to pass traffic and could even become the control node. You cannot unregister the current control node. You might want to unregister the node if it is no longer reachable from the Firewall Management Center, but you still want to keep it as part of the cluster while you troubleshoot management connectivity.

Unregistering a cluster:

- Severs all communication between the Firewall Management Center and the cluster.

- Removes the cluster from the **Device Management** page.
- Returns the cluster to local time management if the cluster's platform settings policy is configured to receive time from the Firewall Management Center using NTP.
- Leaves the configuration intact, so the cluster continues to process traffic.

  Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.

Registering the cluster again to the same or a different Firewall Management Center causes the configuration to be removed, so the cluster will stop processing traffic at that point; the cluster configuration remains intact so you can add the cluster as a whole. You can choose an access control policy at registration, but you will have to re-apply other policies after registration and then deploy the configuration before it will process traffic again.

Before you begin

This procedure requires CLI access to one of the nodes.

Procedure

Step 1 Choose **Devices** > **Device Management**, click **More** (⋮) for the cluster or node, and choose **Delete**.

Step 2 You are prompted to delete the cluster or node; click **Yes**.

Step 3 You can register the cluster with a new (or the same) Firewall Management Center by adding one of the cluster members as a new device.

Add one of the cluster nodes as a device. The system will discover the remaining nodes.

a) Connect to the CLI of a cluster node, and identify the new Firewall Management Center using the **configure manager add** command.
b) Choose **Devices** > **Device Management**, and then click **Add Device**.

Step 4 To re-add a deleted node, refer to Reconcile Cluster Nodes, on page 504.

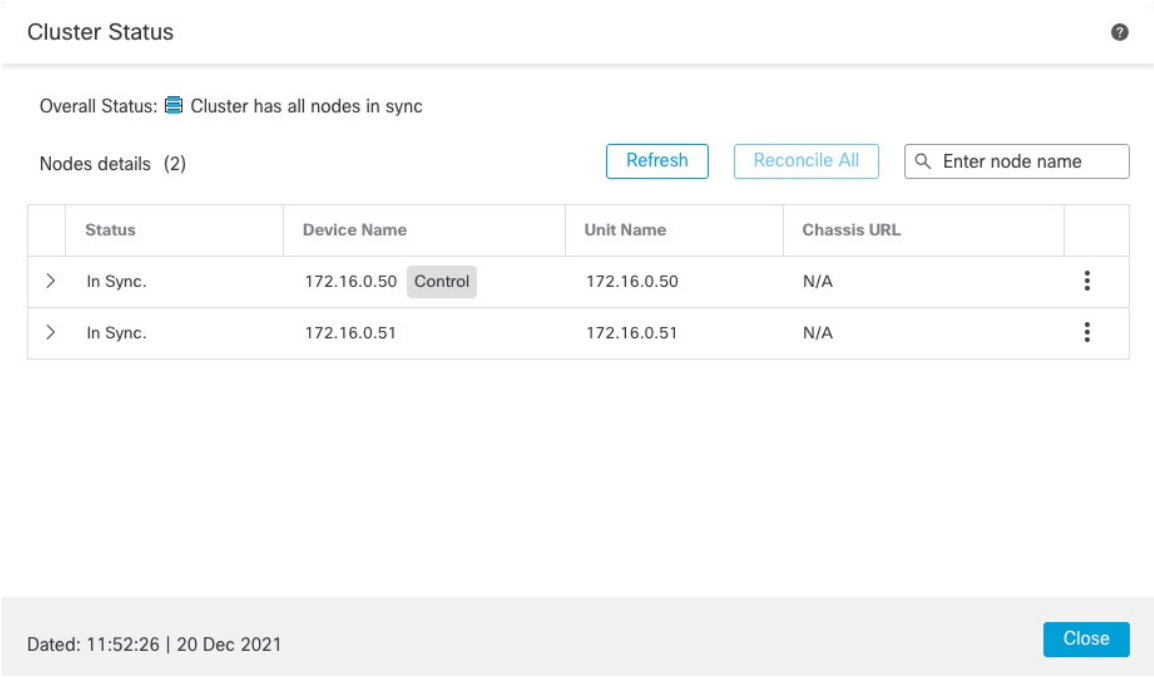
Monitor cluster status

You can monitor the cluster in the Firewall Management Center and at the Firewall Threat Defense CLI.

Monitor cluster status through these methods:

- **Cluster Status** dialog box, which is available from the **Devices** > **Device Management**, **More** (⋮) icon or from the **Devices** > **Device Management**, click **Add**, choose the **Cluster** page **General** area **Cluster Live Status** link.

Figure 208: Cluster status



The Control node has a graphic indicator identifying its role.

Cluster member **Status** includes these states:

- In Sync—The node is registered with the Firewall Management Center.
- Pending Registration—The node is part of the cluster, but has not yet registered with the Firewall Management Center. If a node fails to register, you can retry registration by clicking **Reconcile All**.
- Clustering is disabled—The node is registered with the Firewall Management Center, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the node from the cluster.
- Joining cluster...—The node is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the Firewall Management Center.

For each node, you can view the **Summary** or the **History**.

Figure 209: Node summary

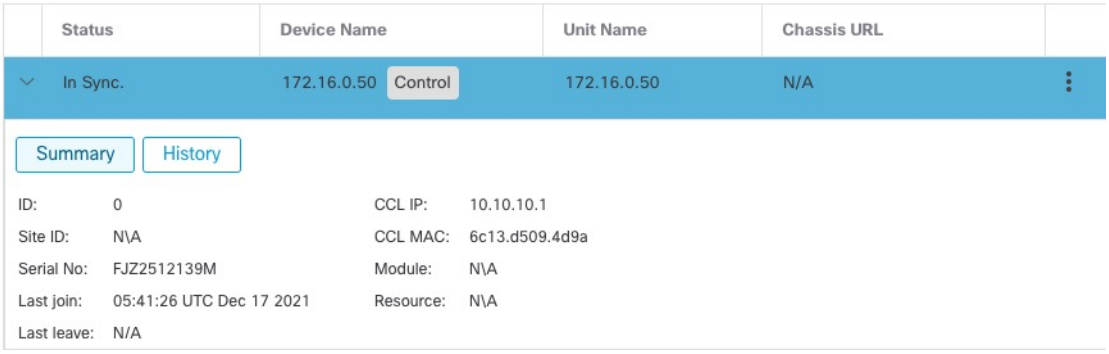
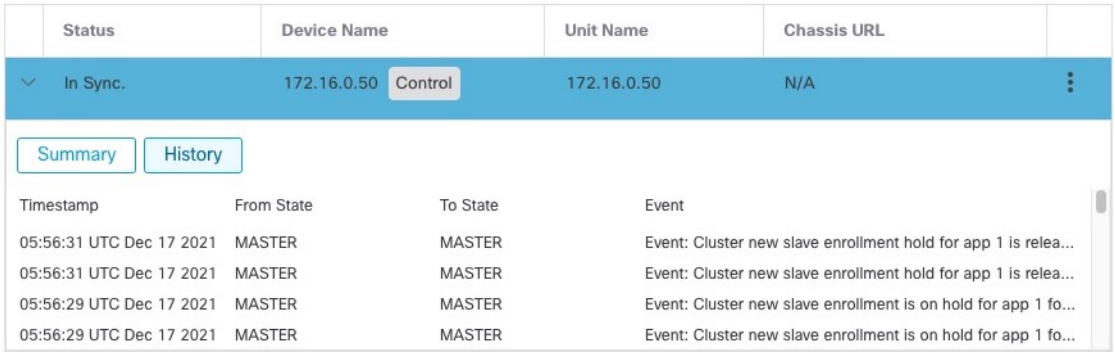


Figure 210: Node history



- **System** (⚙) > **Tasks** page.

  The **Tasks** page shows updates of the Cluster Registration task as each node registers.

- **Devices** > **Device Management** and then click **Add** > **Device** *cluster_name*.

  When you expand the cluster on the devices listing page, you can see all member nodes, including the control node shown with its role next to the IP address. For nodes that are still registering, you can see the loading icon.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  To view aggregated data for the entire cluster or other information, use the **show cluster** command.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  To view cluster information, use the **show cluster info** command.

Cluster health monitor

When a Firewall Threat Defense is the control node of a cluster, the Firewall Management Center collects various metrics periodically from the device metric data collector.

The cluster health monitor is comprised of these components:

- Overview dashboard: Displays information about the cluster topology, cluster statistics, and metric charts:
  - The topology section displays a cluster's live status, the health of individual threat defense, threat defense node type (control node or data node), and the status of the device. The status of the device could be *Disabled* (when the device leaves the cluster), *Added out of box* (in a public cloud cluster, the additional nodes that do not belong to the Firewall Management Center), or *Normal* (ideal state of the node).
  - The cluster statistics section displays current metrics of the cluster with respect to the CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.



Note The CPU and memory metrics display the individual average of the data plane and snort usage.

  - The metric charts, namely, CPU Usage, Memory Usage, Throughput, and Connections, diagrammatically display the statistics of the cluster over the specified time period.

- Load Distribution dashboard: Displays load distribution across the cluster nodes in two widgets:
  - The Distribution widget displays the average packet and connection distribution over the time range across the cluster nodes. This data depicts how the load is being distributed by the nodes. Using this widget, you can easily identify any abnormalities in the load distribution and rectify it.
  - The Node Statistics widget displays the node level metrics in table format. It displays metric data on CPU usage, memory usage, input rate, output rate, active connections, and NAT translations across the cluster nodes. This table view enables you to correlate data and easily identify any discrepancies.

- Member Performance dashboard: Displays current metrics of the cluster nodes. You can use the selector to filter the nodes and view the details of a specific node. The metric data include CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.
- CCL dashboard: Displays, graphically, the cluster control link data namely, the input, and output rate.
- Troubleshooting and Links: Provides convenient links to frequently used troubleshooting topics and procedures.
- Time range: An adjustable time window to constrain the information that appears in the various cluster metrics dashboards and widgets.
- Custom Dashboard: Displays data on both cluster-wide metrics and node-level metrics. However, node selection only applies for the threat defense metrics and not for the entire cluster to which the node belongs.

View the cluster health monitor

The cluster health monitor provides a detailed view of the health status of a cluster and its nodes. This cluster health monitor provides health status and trends of the cluster in an array of dashboards.

Before you begin

Ensure you have created a cluster from one or more devices in the Firewall Management Center.

Follow these steps to view the cluster health monitor:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**.

Use the Monitoring navigation pane to access node-specific health monitors.

Step 2 In the device list, click **Expand**(>) and **Collapse** (⌄) to expand and collapse the list of managed cluster devices.

Step 3 Click on the cluster name to view the cluster health statistics.

The cluster monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including its nodes, CPU, memory, input and output rates, connection statistics, and NAT translation information.
- Load Distribution: Traffic and packet distribution across the cluster nodes.
- Member Performance: Node-level statistics on CPU usage, memory usage, input throughput, output throughput, active connection, and NAT translation.
- CCL: Interface status and aggregate traffic statistics.

You can navigate through the various metrics dashboards by clicking on the labels. For a comprehensive list of the supported cluster metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

Step 4 Configure the time range from the drop-down in the upper-right corner.

The time range can reflect a period as short as the last hour (the default) or as long as two weeks. Select **Custom** from the drop-down to configure a custom start and end date.

Click the refresh icon to set auto refresh to 5 minutes or to toggle off auto refresh.

Step 5 Click on deployment icon for a deployment overlay on the trend graph, with respect to the selected time range.

The deployment icon indicates the number of deployments during the selected time-range. A vertical band indicates the deployment start and end time. For multiple deployments, multiple bands/lines appear. Click on the icon on top of the dotted line to view the deployment details.

Step 6 View the **Health Alerts** for the node in the alert notification at the top of page, directly to the right of the device name.

Hover your pointer over the **Health Alerts** to view the health summary of the node. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.

Step 7 View device monitor health and performance metrics in several predefined dashboards.

The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information.
- CPU: CPU utilization, including the CPU usage by process and by physical cores.

- Memory: Device memory utilization, including data plane and Snort memory usage.
- Interfaces: Interface status and aggregate traffic statistics.
- Connections: Connection statistics (such as elephant flows, active connections, peak connections, and so on) and NAT translation counts.
- Snort: Statistics that are related to the Snort process.
- ASP drops: Statistics related to the dropped packets against various reasons.

You can navigate through the various metrics dashboards by clicking on the labels. Refer to Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Step 8 Click the plus sign **Add New Dashboard**(+) in the upper right corner of the health monitor to create a custom dashboard by building your own variable set from the available metric groups.

For cluster-wide dashboard, choose Cluster metric group, and then choose the metric.

Cluster metrics

The cluster health monitor tracks statistics that are related to a cluster and its nodes, and aggregate of load distribution, performance, and CCL traffic statistics.

Table 36: Cluster Metrics

Metric	Description	Format
CPU	Average of CPU metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Memory	Average of memory metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Data Throughput	Incoming and outgoing data traffic statistics for a cluster.	bytes
CCL Throughput	Incoming and outgoing CCL traffic statistics for a cluster.	bytes
Connections	Count of active connections in a cluster.	number
NAT Translations	Count of NAT translations for a cluster.	number
Distribution	Connection distribution count in the cluster for every second.	number
Packets	Packet distribution count in the cluster for every second.	number

Troubleshoot the cluster

Use these methods to troubleshoot the devices and clusters:

- Use **Logs** to generates troubleshooting files for all nodes in the cluster. Use this option when you need one cluster-level collection instead of generating troubleshooting files from each node separately.
- Use **CLI** to run a predefined set of cluster diagnostic commands and displays the output. Use this option to check cluster configuration, member state, cluster health, control-plane transport statistics, packet drops, interface status, CPU usage, memory buffers, ARP entries, and reachability. The **CLI** option displays command output; it does not open an interactive CLI session.

Commands
show running-config cluster: Review the cluster group configuration, local unit, cluster interface, priority, health-check, auto-rejoin, and cLACP settings.
show cluster info: Confirm that clustering is enabled and identify the control node, member state, software version, serial number, CCL IP address, CCL MAC address, and last join or leave state.
show cluster info health: Check unit, interface, service, and overall cluster health.
show cluster info transport cp: Review control-plane transport counters, including reliable and unreliable message counters, errors, retransmits, drops, and buffer conditions.
show version: Capture platform, software, build, UUID, LSP, VDB, uptime, resource, and license context.
show asp drop: Identify accelerated security path packet or flow drop reasons and counters.
show counters: Review protocol, feature, and cluster CCL counters.
show arp: Verify ARP entries for interfaces that participate in cluster communication.
show int ip brief: Check interface IP addresses and administrative and line protocol status.
show blocks: Check buffer availability and failed allocations.
show cpu detailed: Check data path, control point, and total CPU usage.
show interface *ccl_interface*: Review interface state, MTU, MAC address, IP address, traffic counters, errors, and drops for the cluster-related interface.
ping *ccl_ip* **size** *ccl_mtu* **repeat 2**: Test reachability to a cluster peer by using the packet size selected by the tool.

- Use the **CCL Ping** when you need to test cluster control link connectivity between joined cluster nodes.
- Troubleshooting files—If a node fails to join the cluster, a troubleshooting file is automatically generated. You can also generate and download troubleshooting files from the **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area. For more information, refer to Generate troubleshooting files, on page 745.

You can also generate files from the **Device Management** page. Click **More** (⋮) and choose **Troubleshoot Files**.

- CLI output—Choose **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area, you can view a set of pre-defined CLI outputs that can help you troubleshoot the cluster. These commands are automatically run for the cluster:

  You can also enter any **show** command in the **Command** field.

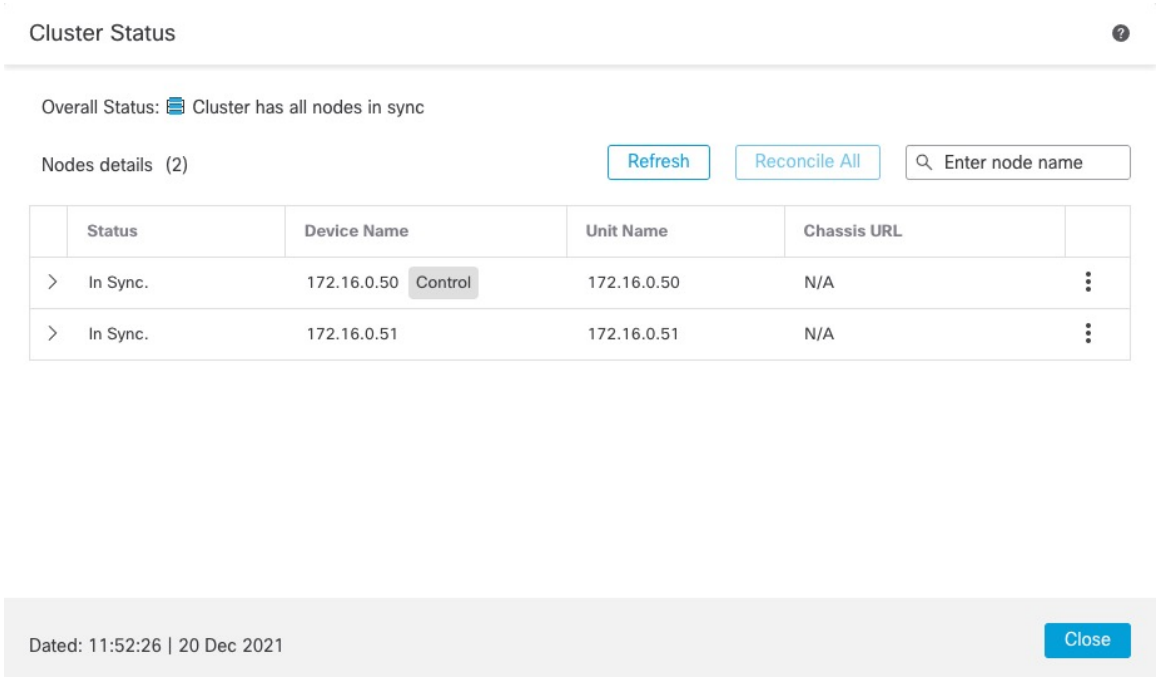
Perform a ping on the cluster control link

You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs.

Procedure

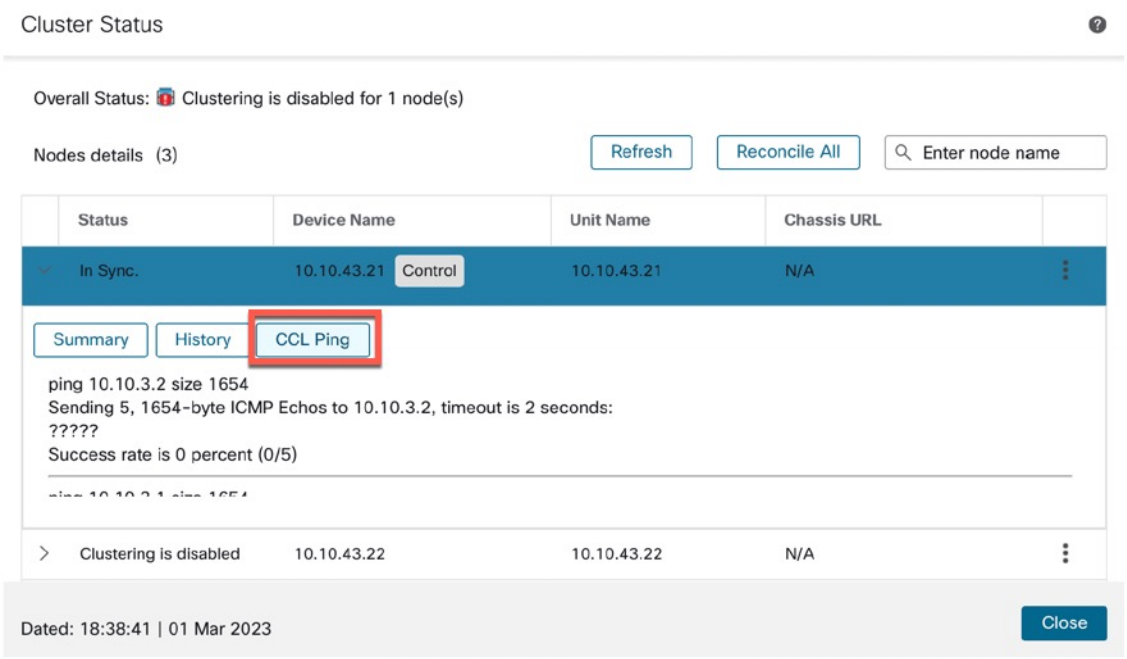
Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) icon next to the cluster, and choose **Cluster Live Status**.

Figure 211: Cluster status



Step 2 Expand one of the nodes, and click **CCL Ping**.

Figure 212: CCL ping



The node sends a ping on the cluster control link to every other node using a packet size that matches the maximum MTU.

Upgrade the cluster

This task upgrades a Firewall Threat Defense Virtual cluster to a new software version by updating the cloud instance template and performing a managed upgrade.

The cluster upgrade process involves updating both the cloud infrastructure template and the software package through the management center. The upgrade is performed one node at a time to maintain cluster availability.

Before you begin

- Before you upgrade a cluster in the public cloud, copy the target version image to your cloud image repository and update the image ID in the cluster deployment template (we actually recommend replacing the existing template with a modified copy). This ensures that after the upgrade, new instances — for example, instances launched during cluster scaling — will use the correct version. If the marketplace does not have the image you need, such as when the cluster has been patched, create a custom image from a snapshot of a standalone Firewall Threat Defense Virtual instance running the correct version, with no instance-specific (day 0) configurations.

Follow these steps to upgrade a Firewall Threat Defense Virtual cluster:

Procedure

Step 1 Upload the target image version to the cloud image storage.

Step 2 Update the cloud instance template of the cluster with the updated target image version.

a) Create a copy of the instance template with the target image version.

b) Attach the newly created template to cluster instance group.

Step 3 Upload the target image version upgrade package to the Firewall Management Center.

Step 4 Perform a readiness check on the cluster that you want to upgrade.

Step 5 After a successful readiness check, initiate the installation of the upgrade package.

Step 6 The Firewall Management Center upgrades the cluster nodes one at a time.

Step 7 The Firewall Management Center displays a notification after successful upgrade of the cluster.

There is no change to the serial number and UUID of the instance after the upgrade.

Reference for clustering

This section includes more information about how clustering operates.

Threat Defense features and clustering

Some Firewall Threat Defense features are not supported with clustering, and some are only supported on the control unit. Other features might have caveats for proper usage.

Unsupported features and clustering

Centralized features for clustering

These features are only supported on the control node, and are not scaled for the cluster.

Note Traffic for centralized features is forwarded from member nodes to the control node over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-control nodes before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the control node.

For centralized features, if the control node fails, all connections are dropped, and you have to re-establish the connections on the new control node.

Note To view FlexConfig features that are also centralized with clustering, for example RADIUS inspection, see the ASA general operations configuration guide. FlexConfig lets you configure many ASA features that are not present in the Firewall Management Center GUI. For more information, refer to FlexConfig policies, on page 921.

- These application inspections are supported:
  - DCERPC and ESMTP
  - NetBIOS and PPTP
  - RSH
  - SQLNET and SUNRPC
  - TFTP
  - XDMCP
- Static route monitoring
- Site-to-site VPN
- IGMP multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- PIM multicast control plane protocol processing (data plane forwarding is distributed across the cluster)
- Dynamic routing

Cisco Trustsec and clustering

Only the control node learns security group tag (SGT) information. The control node then populates the SGT to data nodes, and data nodes can make a match decision for SGT based on the security policy.

Connection settings and clustering

Connection limits are enforced cluster-wide. Each node has an estimate of the cluster-wide counter values based on broadcast messages. Due to efficiency considerations, the configured connection limit across the cluster might not be enforced exactly at the limit number. Each node may overestimate or underestimate the cluster-wide counter value at any given time. However, the information will get updated over time in a load-balanced cluster.

Dynamic routing and clustering

Dynamic routing and clustering are network configuration approaches that

- enable each node to run the routing protocol as a standalone router in Individual interface mode,
- allow routes to be learned by each node independently, and
- require separate router IDs for each node when communicating with external routers.

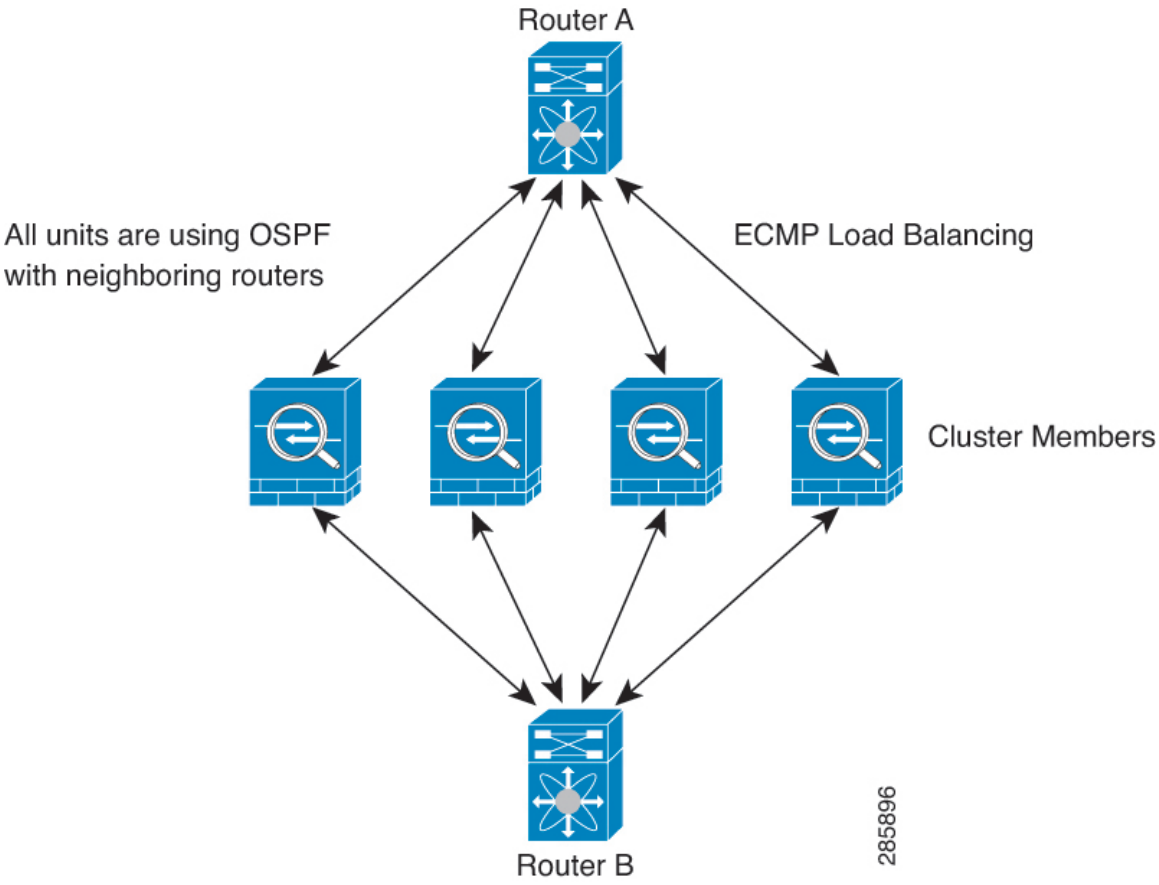
Routing behavior and load balancing

In Individual interface mode, ECMP is used to load balance traffic between multiple equal-cost paths. External routers can discover multiple paths to destinations through different cluster nodes.

Router A learns that there are 4 equal-cost paths to Router B, each through a node. ECMP is used to load balance traffic between the 4 paths. Each node picks a different router ID when communicating with external routers.

You must configure a cluster pool for the router ID so that each node has a separate router ID.

Figure 213: Dynamic routing in individual interface mode



FTP and clustering

- If FTP data channel and control channel flows are owned by different cluster members, then the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

NAT and clustering

Provides information about NAT behavior and limitations in clustering deployments.

NAT can affect the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different Firewall Threat Defenses in the cluster, because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When a packet arrives at the Firewall Threat Defense that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link. Note that the receiving node does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

If you still want to use NAT in clustering, then consider the following guidelines:

- No Proxy ARP—For individual interfaces, a proxy ARP reply is never sent for mapped addresses. This prevents the adjacent router from maintaining a peer relationship with an ASA that may no longer be in the cluster. The upstream router requires a static route or policy-based routing (PBR) with Object Tracking for the mapped addresses, which must point to the main cluster IP address.
- No interface PAT on an individual interface—Interface PAT is not supported for Individual interfaces.
- PAT with Port Block Allocation—See the following guidelines for this feature:
  - Maximum-per-host limit is not a cluster-wide limit, and is enforced on each node individually. Thus, in a 3-node cluster with the maximum-per-host limit configured as 1, if the traffic from a host is load-balanced across all 3 nodes, then it can get allocated 3 blocks with 1 in each node.
  - Port blocks created on the backup node from the backup pools are not accounted for when enforcing the maximum-per-host limit.
  - On-the-fly PAT rule modifications, where the PAT pool is modified with a completely new range of IP addresses, will result in xlate backup creation failures for the xlate backup requests that were still in transit while the new pool became effective. This behavior is not specific to the port block allocation feature, and is a transient PAT pool issue seen only in cluster deployments where the pool is distributed and traffic is load-balanced across the cluster nodes.
  - When operating in a cluster, you cannot simply change the block allocation size. The new size is effective only after you reload each device in the cluster. To avoid having to reload each device, we recommend that you delete all block allocation rules and clear all xlates related to those rules. You can then change the block size and recreate the block allocation rules.
- NAT pool address distribution for dynamic PAT—When you configure a PAT pool, the cluster divides each IP address in the pool into port blocks. By default, each block is 512 ports, but if you configure port block allocation rules, your block setting is used instead. These blocks are distributed evenly among the nodes in the cluster, so that each node has one or more blocks for each IP address in the PAT pool. Thus, you could have as few as one IP address in a PAT pool for a cluster, if that is sufficient for the number of PAT'ed connections you expect. Port blocks cover the 1024-65535 port range, unless you configure the option to include the reserved ports, 1-1023, on the PAT pool NAT rule.
- Reusing a PAT pool in multiple rules—To use the same PAT pool in multiple rules, you must be careful about the interface selection in the rules. You must either use specific interfaces in all rules, or "any" in all rules. You cannot mix specific interfaces and "any" across the rules, or the system might not be able to match return traffic to the right node in the cluster. Using unique PAT pools per rule is the most reliable option.
- No round-robin—Round-robin for a PAT pool is not supported with clustering.
- No extended PAT—Extended PAT is not supported with clustering.

- Dynamic NAT xlates managed by the control node—The control node maintains and replicates the xlate table to data nodes. When a data node receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the control node. The data node owns the connection.
- Stale xlates—The xlate idle time on the connection owner does not get updated. Thus, the idle time might exceed the idle timeout. An idle timer value higher than the configured timeout with a refcnt of 0 is an indication of a stale xlate.
- No static PAT for the following inspections—
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- If you have an extremely large number of NAT rules, over ten thousand, you should enable the transactional commit model using the **asp rule-engine transactional-commit nat** command in the device CLI. Otherwise, the node might not be able to join the cluster.

SIP inspection and clustering

A control flow can be created on any node (due to load balancing); its child data flows must reside on the same node.

SNMP and clustering

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new control node is elected, the poll to the new control node will fail.

When using SNMPv3 with clustering, if you add a new cluster node after the initial cluster formation, then SNMPv3 users are not replicated to the new node. You must remove the users, and re-add them, and then redeploy your configuration to force the users to replicate to the new node.

Syslog and clustering

- Each node in the cluster generates its own syslog messages. You can configure logging so that each node uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all nodes in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all nodes look as if they come from a single node. If you configure logging to use the local-node name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different nodes.

VPN and Clustering

Site-to-site VPN is a centralized feature; only the control node supports VPN connections.

Note Remote access VPN is not supported with clustering.

VPN functionality is limited to the control node and does not take advantage of the cluster high availability capabilities. If the control node fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control node is elected, you must reestablish the VPN connections.

For connections to an Individual interface when using PBR or ECMP, you must always connect to the Main cluster IP address, not a Local address.

VPN-related keys and certificates are replicated to all nodes.

Performance scaling factor

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately 80% of the maximum combined throughput.

Throughput calculation

For example, if your model can handle approximately 10 Gbps of traffic when running alone, then for a cluster of 8 units, the maximum combined throughput will be approximately 80% of 80 Gbps (8 units x 10 Gbps): 64 Gbps.

Control node election

Summary

The key components involved in the control node election process are:

- Cluster nodes: Communicate over the cluster control link and participate in the election process
- Election requests: Broadcast every 3 seconds by nodes when clustering is enabled
- Priority values: Set between 1 and 100 where 1 is the highest priority
- Control node: The elected node that coordinates cluster operations

Workflow

These stages describe how cluster nodes elect a control node:

1. When clustering is enabled for a node (or when it first starts up with clustering already enabled), the node broadcasts an election request every 3 seconds.
2. Any other nodes with a higher priority respond to the election request. The priority is set between 1 and 100, where 1 is the highest priority.
3. If after 45 seconds, a node does not receive a response from another node with a higher priority, then it becomes the control node.

Note If multiple nodes tie for the highest priority, the cluster node name and then the serial number is used to determine the control node.

4. If a node later joins the cluster with a higher priority, it does not automatically become the control node. The existing control node always remains as the control node unless it stops responding, at which point a new control node is elected.
5. In a "split brain" scenario when there are temporarily multiple control nodes, the node with highest priority retains the role while the other nodes return to data node roles.

Note You can manually force a node to become the control node. For centralized features, if you force a control node change, then all connections are dropped, and you have to re-establish the connections on the new control node.

High availability within the cluster

Clustering provides high availability by monitoring node and interface health and by replicating connection states between nodes.

Node health monitoring

Each node periodically sends a broadcast heartbeat packet over the cluster control link. If the control node does not receive any heartbeat packets or other packets from a data node within the configurable timeout period, then the control node removes the data node from the cluster. If the data nodes do not receive packets from the control node, then a new control node is elected from the remaining nodes.

Split brain scenario

If nodes cannot reach each other over the cluster control link because of a network failure and not because a node has actually failed, then the cluster may go into a "split brain" scenario where isolated data nodes will elect their own control nodes. For example, if a router fails between two cluster locations, then the original control node at location 1 will remove the location 2 data nodes from the cluster. Meanwhile, the nodes at location 2 will elect their own control node and form their own cluster. Note that asymmetric traffic may fail in this scenario. After the cluster control link is restored, then the control node that has the higher priority will keep the control node's role.

Interface monitoring

Each node monitors the link status of all named hardware interfaces in use, and reports status changes to the control node.

All physical interfaces are monitored; only named interfaces can be monitored. You can optionally disable monitoring per interface.

A node is removed from the cluster if its monitored interfaces fail. The node is removed after 500 milliseconds.

Status after failure

When a node in the cluster fails, the connections hosted by that node are seamlessly transferred to other nodes; state information for traffic flows is shared over the control node's cluster control link.

If the control node fails, then another member of the cluster with the highest priority (lowest number) becomes the control node.

The Firewall Threat Defense automatically tries to rejoin the cluster, depending on the failure event.

Note When the Firewall Threat Defense becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management interface can send and receive traffic.

Rejoining the cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

- Failed cluster control link when initially joining—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering.
- Failed cluster control link after joining the cluster—The Firewall Threat Defense automatically tries to rejoin every 5 minutes, indefinitely.
- Failed data interface—The Firewall Threat Defense automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the Firewall Threat Defense application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.
- Failed node—If the node was removed from the cluster because of a node health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the node will rejoin the cluster when it starts up again as long as the cluster control link is up. The Firewall Threat Defense application attempts to rejoin the cluster every 5 seconds.
- Internal error—Internal failures include: application sync timeout; inconsistent application statuses; and so on.
- Failed configuration deployment—If you deploy a new configuration from Firewall Management Center, and the deployment fails on some cluster members but succeeds on others, then the nodes that failed are removed from the cluster. You must manually rejoin the cluster by re-enabling clustering. If the deployment fails on the control node, then the deployment is rolled back, and no members are removed. If the deployment fails on all data nodes, then the deployment is rolled back, and no members are removed.

Data path connection state replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

Table 37: Features Replicated Across the Cluster

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	—
MAC address table	Yes	—
User Identity	Yes	—
IPv6 Neighbor database	Yes	—
Dynamic routing	Yes	—
SNMP Engine ID	**No**	—

How the cluster manages connections

Connections can be load-balanced to multiple nodes of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

Connection roles

See the following roles defined for each connection:

- Owner—Usually, the node that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new nodes receive packets from the connection, the director chooses a new owner from those nodes.
- Backup owner—The node that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then the first node to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

  As long as the director (see below) is not the same node as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

  For clustering on the Firepower 9300, which can include up to 3 cluster nodes in one chassis, if the backup owner is on the same chassis as the owner, then an additional backup owner will be chosen from another chassis to protect flows from a chassis failure.
- Director—The node that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and ports (see below for ICMP hash details), and sends a message to the director to register the new connection. If packets arrive at any node other than the owner, the node queries the director about which node is the owner so it can forward the packets. A connection has only one director. If a director fails, the owner chooses a new director.

  As long as the director is not the same node as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.

  ICMP/ICMPv6 hash details:

- For Echo packets, the source port is the ICMP identifier, and the destination port is 0.
- For Reply packets, the source port is 0, and the destination port is the ICMP identifier.
- For other packets, both source and destination ports are 0.

- Forwarder—A node that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner. A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.



Note We do not recommend disabling TCP sequence randomization when using clustering. There is a small chance that some TCP sessions won't be established, because the SYN/ACK packet might be dropped.

- Fragment Owner—For fragmented packets, cluster nodes that receive a fragment determine a fragment owner using a hash of the fragment source IP address, destination IP address, and the packet ID. All fragments are then forwarded to the fragment owner over the cluster control link. Fragments may be load-balanced to different cluster nodes, because only the first fragment includes the 5-tuple used in the switch load balance hash. Other fragments do not contain the source and destination ports and may be load-balanced to other cluster nodes. The fragment owner temporarily reassembles the packet so it can determine the director based on a hash of the source/destination IP address and ports. If it is a new connection, the fragment owner will register to be the connection owner. If it is an existing connection, the fragment owner forwards all fragments to the provided connection owner over the cluster control link. The connection owner will then reassemble all fragments.

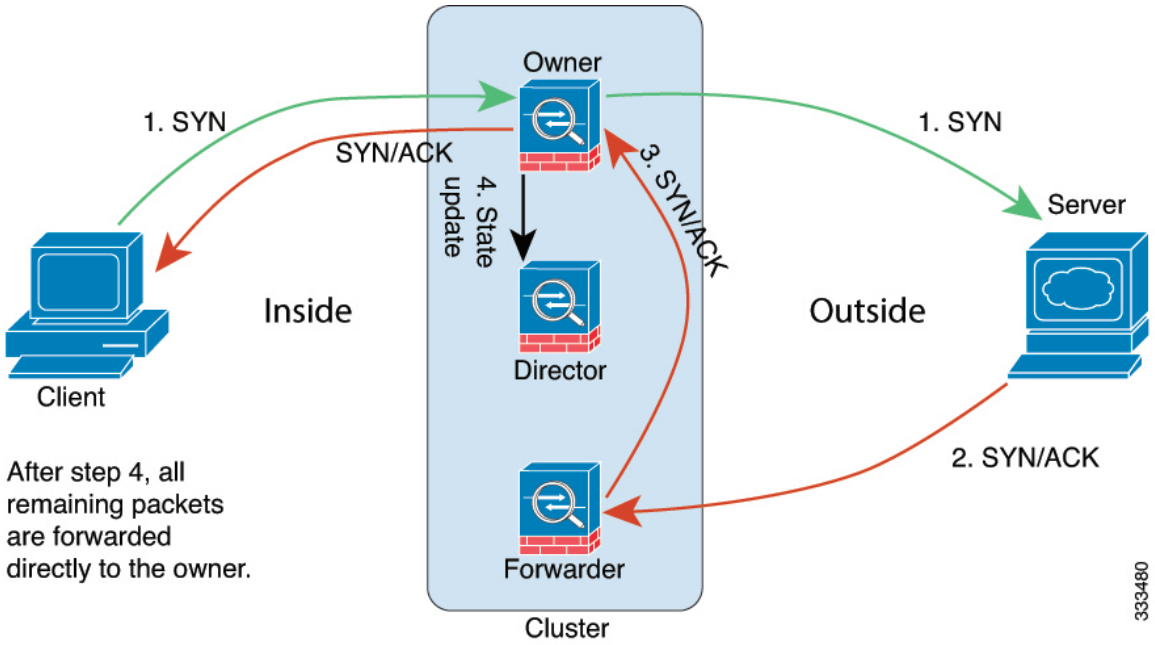
Port Address Translation Connections

New connection ownership

Traffic redirection is not supported in this release. When a new connection is directed to a node of the cluster via load balancing, that node owns both directions of the connection. All the subsequent packets for the same connection should arrive the same node. If any connection packets arrive at a different node, they will be dropped. If a reverse flow arrives at a different node, it will be dropped as well. For centralized features, if the connections do not arrive on the control node, they will be dropped.

Sample data flow for TCP

The following example shows the establishment of a new connection.

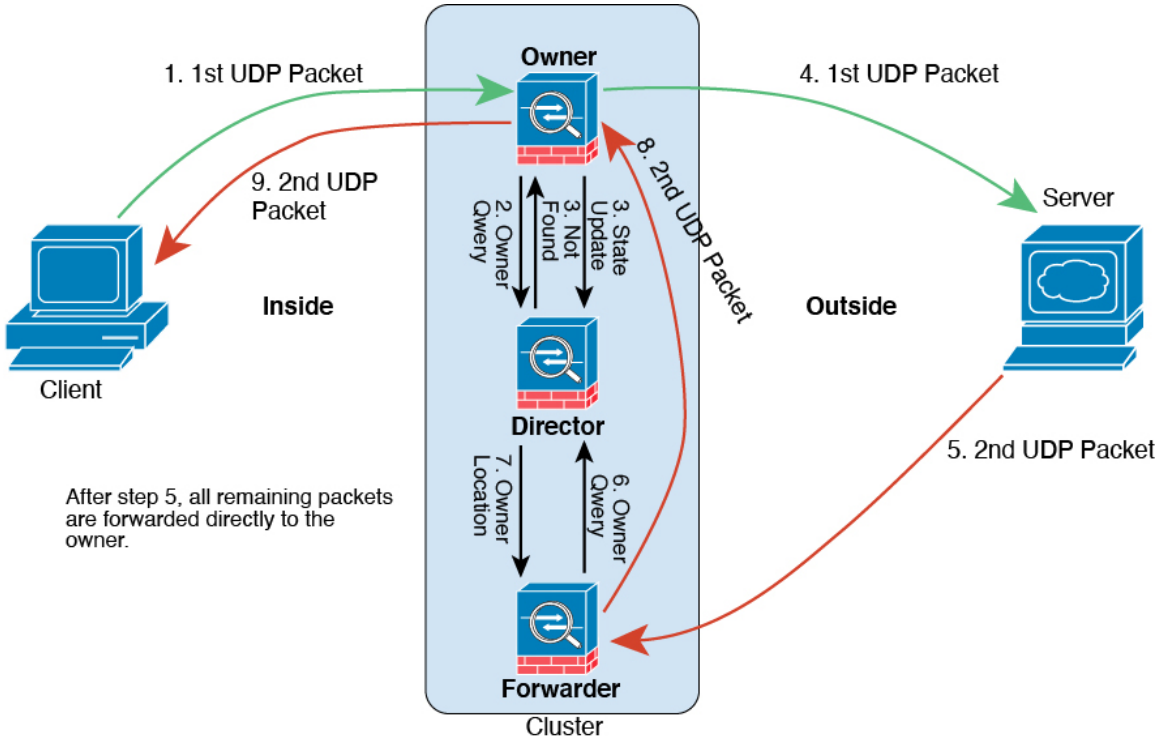


1. The SYN packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.
2. The SYN-ACK packet originates from the server and is delivered to a different Firewall Threat Defense (based on the load balancing method). This Firewall Threat Defense is the forwarder.
3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.
4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.
5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.
6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.
7. If packets are delivered to any additional nodes, it will query the director for the owner and establish a flow.
8. Any state change for the flow results in a state update from the owner to the director.

Sample data flow for ICMP and UDP

The following example shows the establishment of a new connection.

1. *Figure 214: ICMP and UDP Data Flow*



The first UDP packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method).

2. The node that received the first packet queries the director node that is chosen based on a hash of the source/destination IP address and ports.
3. The director finds no existing flow, creates a director flow and forwards the packet back to the previous node. In other words, the director has elected an owner for this flow.
4. The owner creates the flow, sends a state update to the director, and forwards the packet to the server.
5. The second UDP packet originates from the server and is delivered to the forwarder.
6. The forwarder queries the director for ownership information. For short-lived flows such as DNS, instead of querying, the forwarder immediately sends the packet to the director, which then sends it to the owner.
7. The director replies to the forwarder with ownership information.
8. The forwarder creates a forwarding flow to record owner information and forwards the packet to the owner.
9. The owner forwards the packet to the client.

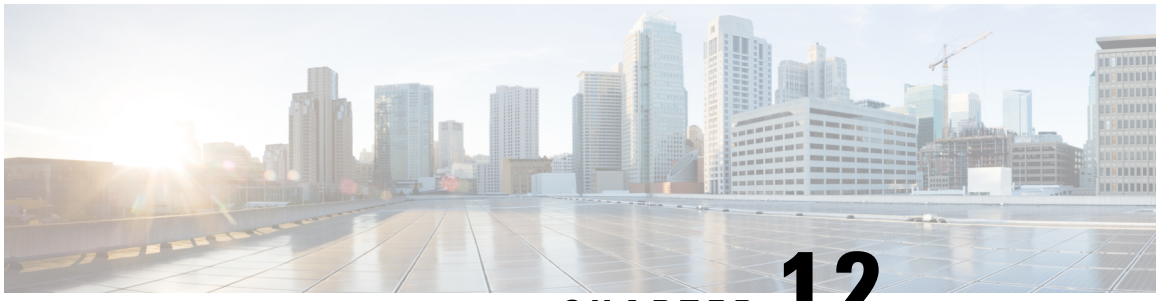
History for Threat Defense Virtual clustering in the public cloud

This reference provides the historical timeline and version information for Threat Defense Virtual clustering features introduced across different software releases and deployment platforms in public cloud environments.

Table 38: Feature history

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cluster control link ping tool.	7.2.6/7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** > **Cluster Live Status.**
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**
Cluster health monitor settings.	7.3.0	Any	You can now edit cluster health monitor settings. New/Modified screens: **Devices** > **Device Management** > **Cluster** > **Cluster Health Monitor Settings** **Note** If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.
Cluster health monitor dashboard.	7.3.0	Any	You can now view cluster health on the cluster health monitor dashboard. New/Modified screens: **System** > **Health** > **Monitor**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Clustering for the Firewall Threat Defense Virtual in Azure.	7.3.0	7.3.0	You can now configure clustering for up to 16 nodes the Firewall Threat Defense Virtual in Azure for the Azure Gateway Load Balancer or for external load balancers. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** Supported platforms: Firewall Threat Defense Virtual in Azure
Clustering for the Firewall Threat Defense Virtual in the Public Cloud (Amazon Web Services and Google Cloud Platform).	7.2.0	7.2.0	The Firewall Threat Defense Virtual supports Individual interface clustering for up to 16 nodes in the public cloud (AWS and GCP). New/Modified screens: • **Devices** > **Device Management** > **Add Device** • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** Supported platforms: Firewall Threat Defense Virtual in AWS and GCP



CHAPTER 12

Clustering: Firepower 4100/9300

Clustering lets you group multiple Firewall Threat Defense nodes together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

Note Some features are not supported when using clustering. See Unsupported features with clustering, on page 585.

- About clustering on the Firepower 4100/9300 chassis, on page 529
- Licenses for clustering, on page 534
- Requirements and prerequisites for clustering, on page 534
- Clustering guidelines and limitations, on page 538
- Configure clustering, on page 541
- FXOS: Remove a cluster node, on page 567
- Firewall Management Center: Manage cluster members, on page 569
- Firewall Management Center: Monitor the cluster, on page 574
- Troubleshoot the cluster, on page 581
- Examples for Clustering, on page 583
- Reference for clustering, on page 585
- History for clustering, on page 597

About clustering on the Firepower 4100/9300 chassis

When you deploy a cluster on the Firepower 4100/9300 chassis, it does the following:

- For native instance clustering: Creates a *cluster-control link* (by default, port-channel 48) for node-to-node communication.

  For multi-instance clustering: You should pre-configure subinterfaces on one or more cluster-type EtherChannels; each instance needs its own cluster control link.

  For a cluster isolated to security modules within one Firepower 9300 chassis, this link utilizes the Firepower 9300 backplane for cluster communications.

  For clustering with multiple chassis, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

- Creates the cluster bootstrap configuration within the application.

  When you deploy the cluster, the chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

- Assigns data interfaces to the cluster as *Spanned* interfaces.

  For a cluster isolated to security modules within one Firepower 9300 chassis, spanned interfaces are not limited to EtherChannels, like it is for clustering with multiple chassis. The Firepower 9300 supervisor uses EtherChannel technology internally to load-balance traffic to multiple modules on a shared interface, so any data interface type works for Spanned mode. For clustering with multiple chassis, you must use Spanned EtherChannels for all data interfaces.



Note Individual interfaces are not supported, with the exception of a management interface.

- Assigns a management interface to all units in the cluster.

Bootstrap configuration

A bootstrap configuration is a minimal cluster configuration that includes cluster name, cluster control link interface, and other cluster settings.

When you deploy the cluster, the Firepower 4100/9300 chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

Cluster members

Cluster members are security devices that work together to accomplish the sharing of the security policy and traffic flows.

Cluster member roles and management

One member of the cluster is the **control** unit. The control unit is determined automatically. All other members are **data** units.

You must perform all configuration on the control unit only; the configuration is then replicated to the data units.

Some features do not scale in a cluster, and the control unit handles all traffic for those features. .

Cluster control link

Cluster control link traffic includes both control and data traffic.

For native instance clustering: The cluster control link is automatically created using the Port-channel 48 interface.

For multi-instance clustering: You should pre-configure subinterfaces on one or more cluster-type EtherChannels; each instance needs its own cluster control link.

For a cluster isolated to security modules within one Firepower 9300 chassis, this interface has no member interfaces. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications. For clustering with multiple chassis, you must add one or more interfaces to the EtherChannel.

For a cluster with two chassis, do not directly connect the cluster control link from one chassis to the other chassis. If you directly connect the interfaces, then when one unit fails, the cluster control link fails, and thus the remaining healthy unit fails. If you connect the cluster control link through a switch, then the cluster control link remains up for the healthy unit.

Size the cluster control link

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features.

For example:

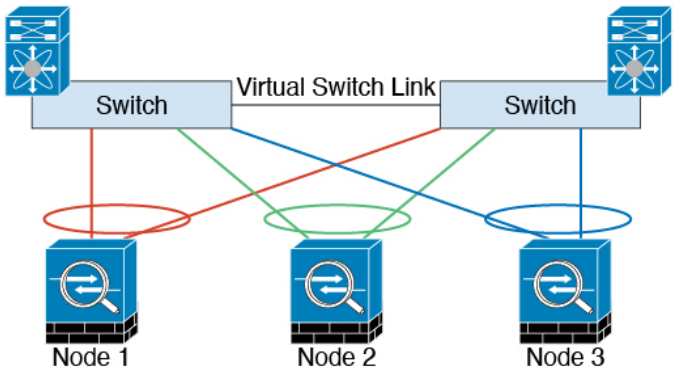
- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.

Note If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Cluster control link redundancy

The diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS), Virtual Port Channel (vPC), StackWise, or StackWise Virtual environment. All links in the EtherChannel are active. When the switch is part of a redundant system, then you can connect firewall interfaces within the same EtherChannel to separate switches in the redundant system. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.



Cluster control link reliability for inter-chassis clustering

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster control link network

The Firepower 4100/9300 chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. For multi-instance clusters, which typically use different VLAN subinterfaces of the same EtherChannel, the same IP address can be used for different clusters because of VLAN separation. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed.

Management network

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

Management interface

You must assign a Management type interface to the cluster. This interface is a special individual interface as opposed to a Spanned interface. The management interface lets you connect directly to each unit. This Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the Secure Firewall Management Center. It uses its own local authentication, IP address, and static routing.

Management interface configuration

Each cluster member uses a separate IP address on the management network that you set as part of the bootstrap configuration.

Cluster interfaces

For a cluster isolated to security modules within one Firepower 9300 chassis, you can assign either physical interfaces or EtherChannels (also known as port channels) to the cluster. The assigned interfaces are Spanned interfaces that load-balance traffic across all cluster members.

For clustering with multiple chassis, you can only assign data EtherChannels to the cluster. These Spanned EtherChannels include the same member interfaces on each chassis. On the upstream switch, all these interfaces are part of a single EtherChannel, so the switch does not recognize that it is connected to multiple devices.

You can use regular firewall interfaces or IPS-only interfaces (inline sets or passive interfaces).

Individual interfaces are not supported except for a management interface.

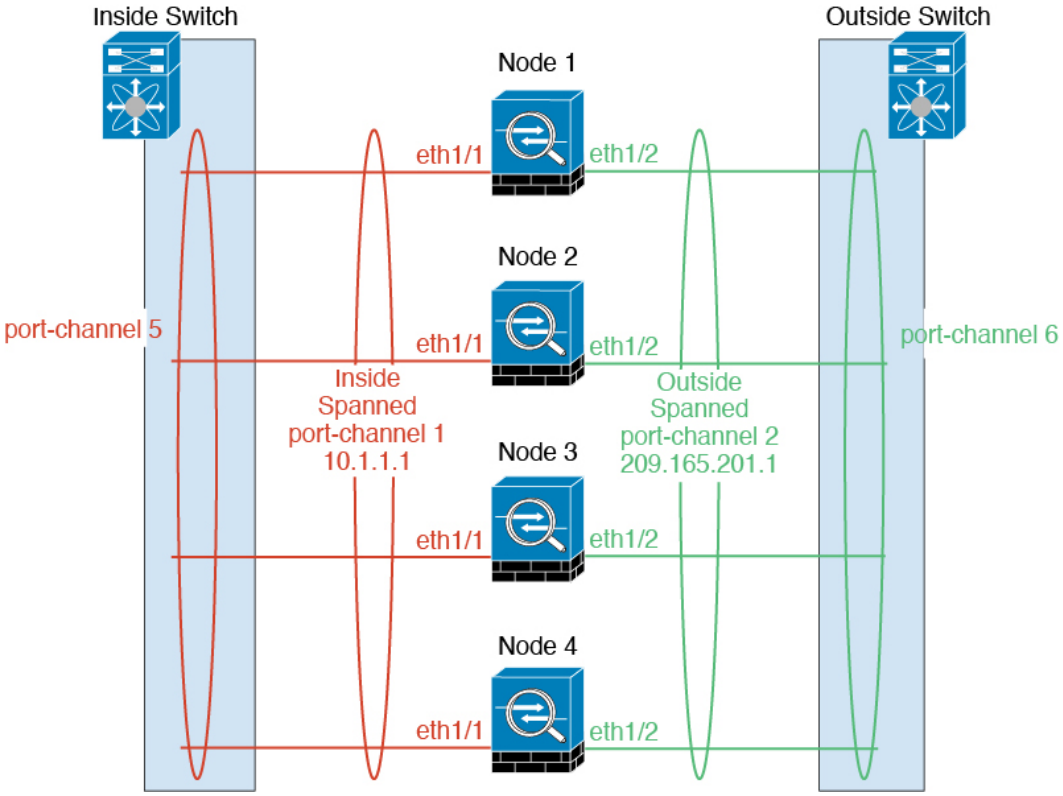
Spanned EtherChannels

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel.

For regular firewall interfaces:A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the BVI, not to the bridge group member interface.

The EtherChannel inherently provides load balancing as part of basic operation.

For multi-instance clusters, each cluster requires dedicated data EtherChannels; you cannot use shared interfaces or VLAN subinterfaces.



Connecting to a redundant switch system

We recommend connecting EtherChannels to a redundant switch system such as a VSS, vPC, StackWise, or StackWise Virtual system to provide redundancy for your interfaces.

Configuration replication

All nodes in the cluster share a single configuration. You can only make configuration changes on the control node (with the exception of the bootstrap configuration), and changes are automatically synced to all other nodes in the cluster.

Licenses for clustering

You assign feature licenses to the cluster as a whole, not to individual nodes. However, each node of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

Note APEX, PLUS, and VPN-Only licenses are not supported for clustering. Before you create a cluster, remove unsupported license assignments from the devices that will become cluster nodes.

When you add a cluster node to the Firewall Management Center, you can specify the feature licenses you want to use for the cluster. You can modify licenses for the cluster in the **Devices** > **Device Management** and the choose the **Add**, **Cluster** and then **License** area.

Note If you add the cluster before the Firewall Management Center is licensed (and running in Evaluation mode), then when you license the Firewall Management Center, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

Requirements and prerequisites for clustering

This topic provides the necessary prerequisites and hardware support details for configuring clustering on supported security appliances.

Cluster model support

The Firewall Threat Defense supports clustering on the following models:

- Firepower 9300— You can include up to 16 nodes in the cluster. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules. Supports clustering with multiple chassis and clustering isolated to security modules within one chassis.
- Firepower 4100—Supported for up to 16 nodes using clustering with multiple chassis.

User roles

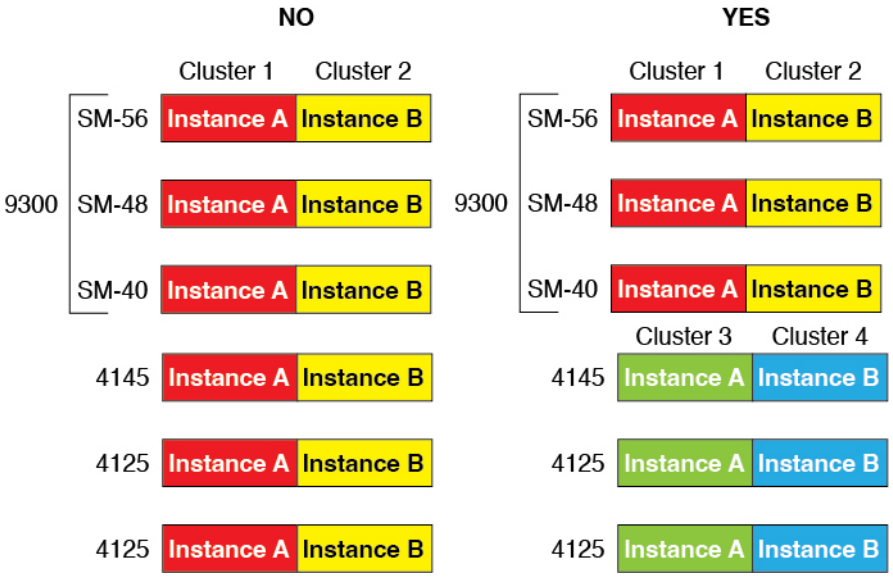
The following user roles are required to manage clustering configurations:

- Admin
- Access Admin
- Network Admin

Clustering hardware and software requirements

All chassis in a cluster:

- Native instance clustering—For the Firepower 4100: All chassis must be the same model. For the Firepower 9300: All security modules must be the same type. For example, if you use clustering, all modules in the Firepower 9300 must be SM-40s. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.
- Container instance clustering—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-48, and SM-40. Or you can create a cluster on a Firepower 4145 and a 4125.



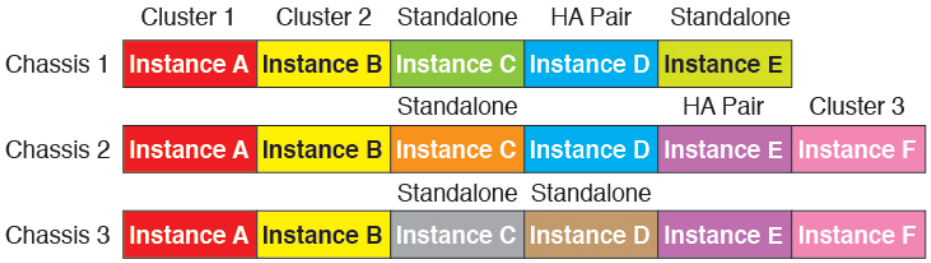
- Must run the identical FXOS and application software except at the time of an image upgrade. Mismatched software versions can lead to poor performance, so be sure to upgrade all nodes in the same maintenance window.
- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in clusters with multiple chassis. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the data nodes, and ending with the control node.
- Must use the same NTP server. For Firewall Threat Defense, the Firewall Management Center must also use the same NTP server. Do not set the time manually.

Multi-instance clustering requirements

- No intra-security-module/engine clustering—For a given cluster, you can only use a single container instance per security module/engine. You cannot add 2 container instances to the same cluster if they are running on the same module.



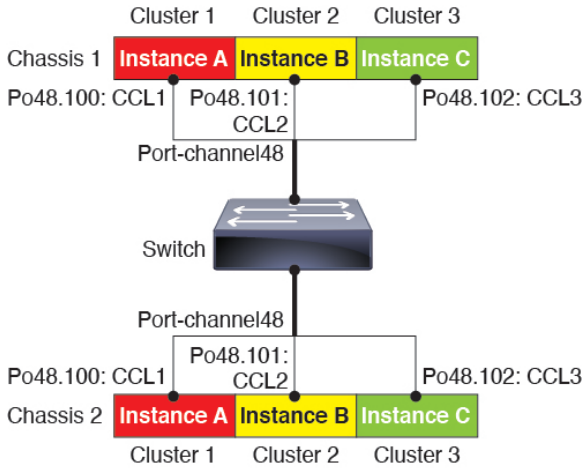
- Mix and match clusters and standalone instances—Not all container instances on a security module/engine need to belong to a cluster. You can use some instances as standalone or High Availability nodes. You can also create multiple clusters using separate instances on the same security module/engine.



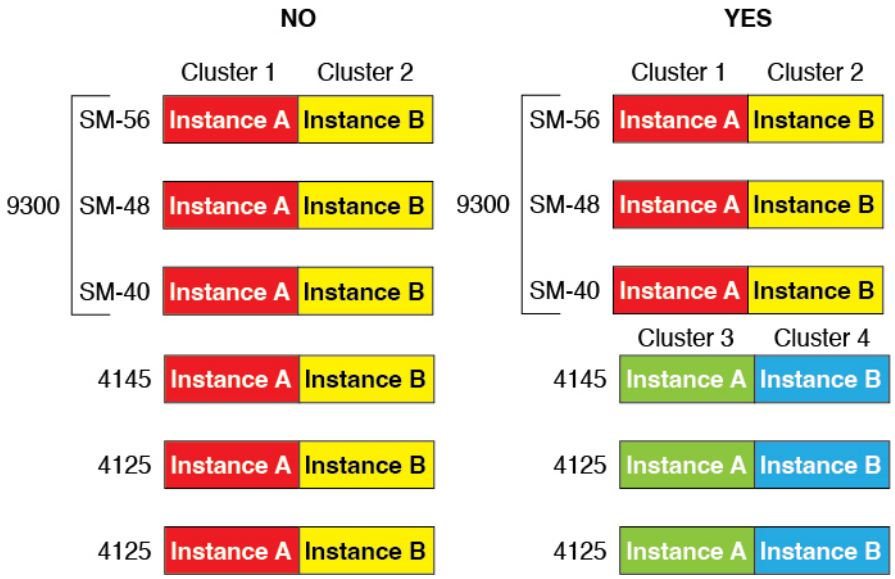
- All 3 modules in a Firepower 9300 must belong to the cluster—For the Firepower 9300, a cluster requires a single container instance on all 3 modules. You cannot create a cluster using instances on module 1 and 2, and then use a native instance on module 3, or example.



- Match resource profiles—We recommend that each node in the cluster use the same resource profile attributes; however, mismatched resources are allowed when changing cluster nodes to a different resource profile, or when using different models.
- Dedicated cluster control link—For clusters with multiple chassis, each cluster needs a dedicated cluster control link. For example, each cluster can use a separate subinterface on the same cluster-type EtherChannel, or use separate EtherChannels.



- No shared interfaces—Shared-type interfaces are not supported with clustering. However, the same Management and Eventing interfaces can used by multiple clusters.
- No subinterfaces—A multi-instance cluster cannot use FXOS-defined VLAN subinterfaces. An exception is made for the cluster control link, which can use a subinterface of the Cluster EtherChannel.
- Mix chassis models—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-48, and SM-40. Or you can create a cluster on a Firepower 4145 and a 4125.



- Maximum 6 nodes—You can use up to six container instances in a cluster.

Switch requirements

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 4100/9300 chassis.

- For supported switch characteristics, see Cisco FXOS Compatibility.

Clustering guidelines and limitations

Clustering is a deployment method that groups multiple security devices into a single logical unit to provide high availability and increased throughput.

Switches for Clustering

- Make sure connected switches match the MTU for both cluster data interfaces and the cluster control link interface. You should configure the cluster control link interface MTU to be at least 100 bytes higher than the data interface MTU, so make sure to configure the cluster control link connecting switch appropriately. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead. In addition, we do not recommend setting the cluster control link MTU between 2561 and 8362; due to block pool handling, this MTU size is not optimal for system operation.
- For Cisco IOS XR systems, if you want to set a non-default MTU, set the IOS XR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the **mtu-ignore** option is used. Note that the cluster device MTU should match the IOS XR *IPv4* MTU. This adjustment is not required for Cisco Catalyst and Cisco Nexus switches.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: **source-dest-ip** or **src-dst-mixed-ip-port** (see the Cisco Nexus OS and Cisco IOS-XE **port-channel load-balance** command). Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
- If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.
- Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
- Port-channel bundling downtime should not exceed the configured keepalive interval.
- On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

  router(config)# **port-channel** *id* **hash-distribution fixed**

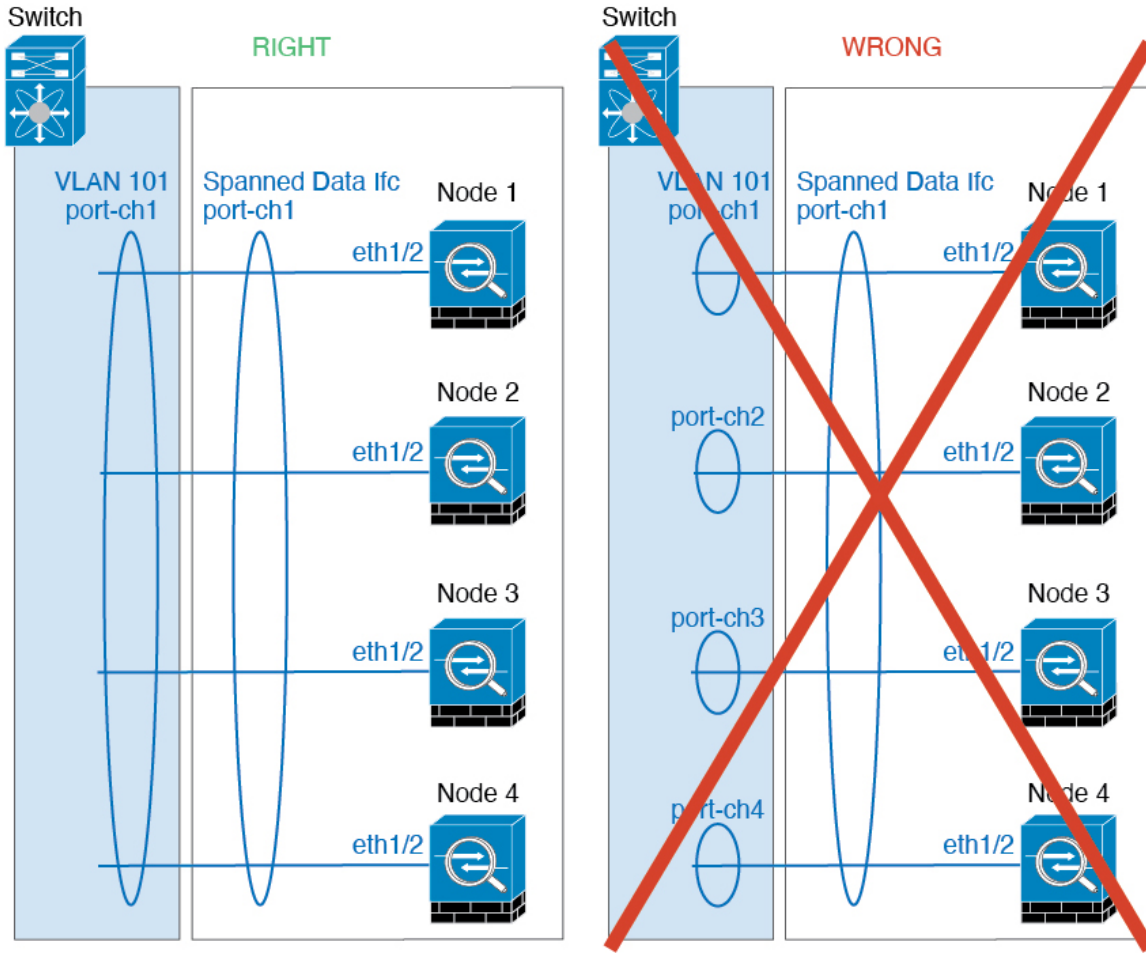
  Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

- Firepower 4100/9300 clusters support LACP graceful convergence. So you can leave LACP graceful convergence enabled on connected Cisco Nexus switches.
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. FXOS EtherChannels have the LACP rate set to fast by default.

Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

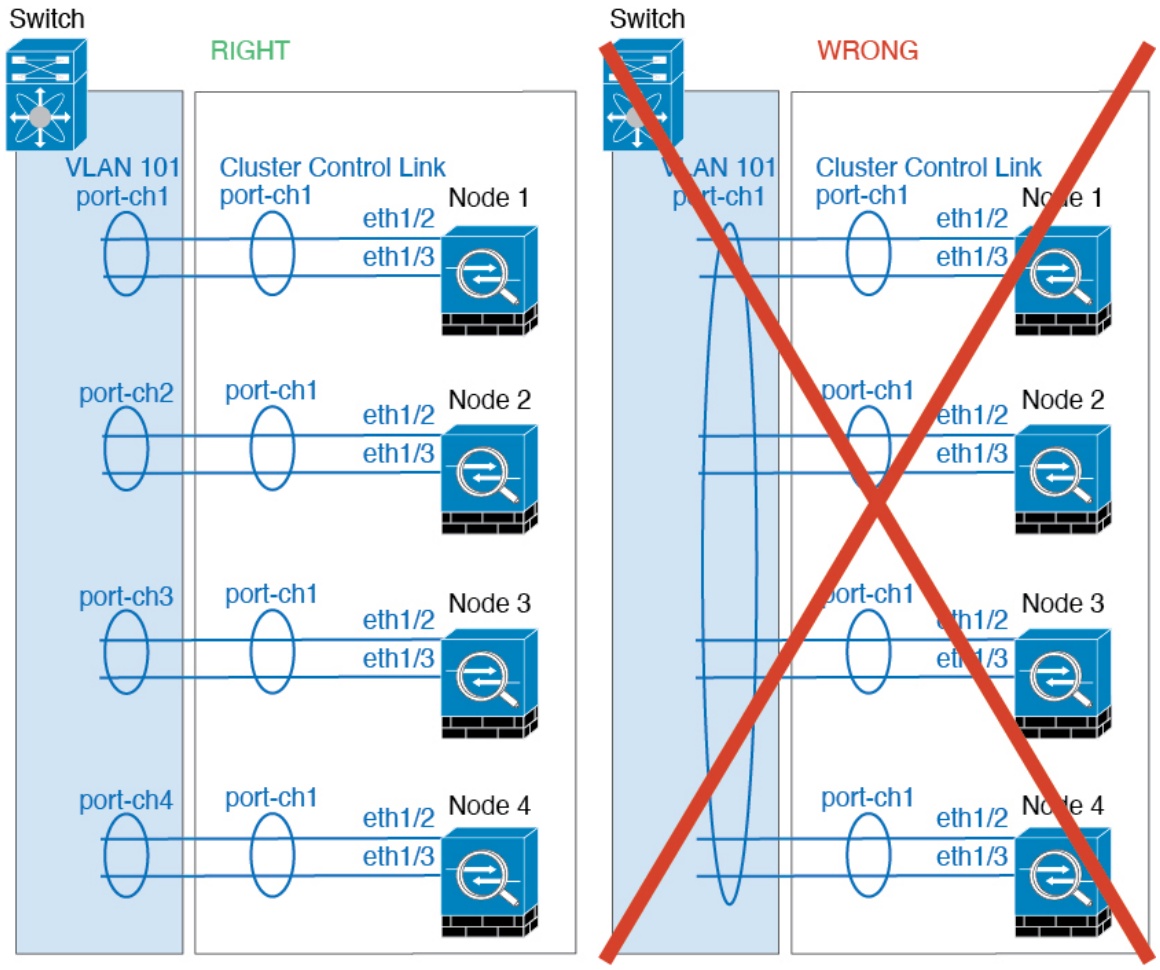
EtherChannels for Clustering

- In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the control unit switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.
- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  - Spanned EtherChannels—For cluster unit *Spanned* EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.



  - Device-local EtherChannels—For cluster unit *Device-local* EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels

on the switch; do not combine multiple cluster unit EtherChannels into one EtherChannel on the switch.



Additional Guidelines

- When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the Firepower 4100/9300 chassis or the switch, adding an additional switch to form a VSS, vPC, StackWise, or StackWise Virtual) you should disable the health check feature, and also disable interface monitoring for the disabled interfaces . When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.
- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang connections; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel interface, when the syslog server port is down, and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the cluster. These messages can result in some units of the cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.

- We recommend connecting EtherChannels to a VSS, vPC, StackWise, or StackWise Virtual for redundancy.
- Within a chassis, you cannot cluster some security modules and run other security modules in standalone mode; you must include all security modules in the cluster.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

Defaults

- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is set to unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is set to 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Configure clustering

You can easily deploy the cluster from the Firepower 4100/9300 supervisor. All initial configuration is automatically generated for each unit. You can then add the units to the Firewall Management Center and group them into a cluster.

FXOS: Add a Firewall Threat Defense cluster

A cluster is a deployment configuration that allows you to group security modules to increase capacity and redundancy.

Cluster Deployment Modes

In native mode: You can add a cluster to a single Firepower 9300 chassis that is isolated to security modules within the chassis, or you can use multiple chassis.

In multi-instance mode: You can add one or more clusters to a single Firepower 9300 chassis that are isolated to security modules within the chassis (you must include an instance on each module), or add one or more clusters on multiple chassis.

For clusters on multiple chassis, you must configure each chassis separately. Add the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment

Create a Firewall Threat Defense cluster

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For clustering on multiple chassis, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, or for container instances, a container instance in each slot, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300 chassis.
- For container instances, if you do not want to use the default profile, add a resource profile according to Add a resource profile for container instances , on page 264.
- For container instances, before you can install a container instance for the first time, you must reinitialize the security module/engine so that the disk has the correct formatting. Choose **Security Modules** or **Security Engine**, and click the Reinitialize icon (). An existing logical device will be deleted and then reinstalled as a new device, losing any local application configuration. If you are replacing a native instance with container instances, you will need to delete the native instance in any case. You cannot automatically migrate a native instance to a container instance.
- Gather the following information:
  - Management interface ID, IP addresses, and network mask
  - Gateway IP address
  - Firewall Management Center IP address and/or NAT ID of your choosing
  - DNS server IP address
  - Firewall Threat Defense hostname and domain name

Procedure

Step 1 Configure interfaces.

a) Add at least one Data type interface or EtherChannel (also known as a port-channel) before you deploy the cluster. See Add an EtherChannel (port channel), on page 261 or Configure a physical interface, on page 259.

For clustering on multiple chassis, all data interfaces must be Spanned EtherChannels with at least one member interface. Add the same EtherChannels on each chassis. Combine the member interfaces from all cluster units into a single EtherChannel on the switch. See Clustering guidelines and limitations, on page 538 for more information about EtherChannels.

For multi-instance clustering, you cannot use FXOS-defined VLAN subinterfaces or data-sharing interfaces in the cluster. Only application-defined subinterfaces are supported. See FXOS interfaces and application interfaces, on page 226 for more information.

b) Add a Management type interface or EtherChannel. See Add an EtherChannel (port channel), on page 261 or Configure a physical interface, on page 259.

The management interface is required. Note that this management interface is not the same as the chassis management interface that is used only for chassis management (in FXOS, you might see the chassis management interface displayed as MGMT, management0, or other similar names).

For clustering on multiple chassis, add the same Management interface on each chassis.

For multi-instance clustering, you can share the same management interface across multiple clusters on the same chassis, or with standalone instances.

c) For clustering on multiple chassis, add a member interface to the cluster control link EtherChannel (by default, port-channel 48). See Add an EtherChannel (port channel), on page 261.

Do not add a member interface for a cluster isolated to security modules within one Firepower 9300 chassis. If you add a member, the chassis assumes this cluster will be using multiple chassis, and will only allow you to use Spanned EtherChannels, for example.

On the **Interfaces** tab, the port-channel 48 cluster type interface shows the **Operation State** as **failed** if it does not include any member interfaces. For a cluster isolated to security modules within one Firepower 9300 chassis, this EtherChannel does not require any member interfaces, and you can ignore this Operational State.

Add the same member interfaces on each chassis. The cluster control link is a device-local EtherChannel on each chassis. Use separate EtherChannels on the switch per device. See Clustering guidelines and limitations, on page 538 for more information about EtherChannels.

For multi-instance clustering, you can create additional Cluster type EtherChannels. Unlike the Management interface, the cluster control link is not sharable across multiple devices, so you will need a Cluster interface for each cluster. However, we recommend using VLAN subinterfaces instead of multiple EtherChannels; see the next step to add a VLAN subinterface to the Cluster interface.

d) For multi-instance clustering, add VLAN subinterfaces to the cluster EtherChannel so you have a subinterface for each cluster. See Add a VLAN subinterface for container instances, on page 263.

If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster.

e) (Optional) Add an eventing interface. See Add an EtherChannel (port channel), on page 261 or Configure a physical interface, on page 259.

This interface is a secondary management interface for the Firewall Threat Defense devices. To use this interface, you must configure its IP address and other parameters at the Firewall Threat Defense CLI. For example, you can separate management traffic from events (such as web events). See the **configure network** commands in the Firewall Threat Defense command reference.

For clustering on multiple chassis, add the same eventing interface on each chassis.

Step 2 Choose **Logical Devices**.

Step 3 Click **Add** > **Cluster**, and set the following parameters:

Figure 215: Native Cluster

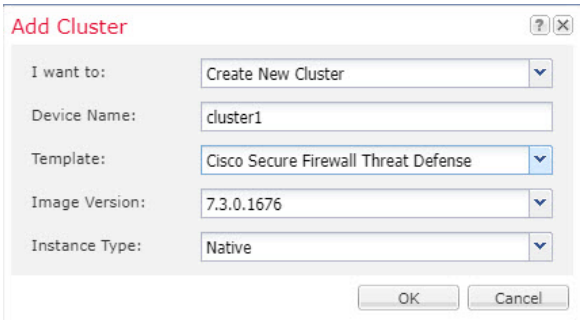
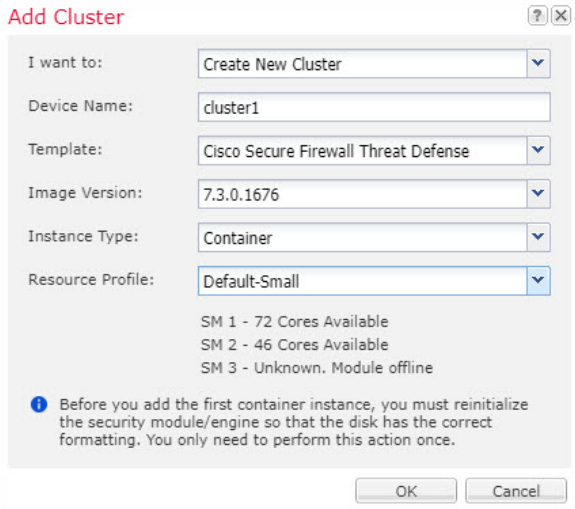


Figure 216: Multi-Instance Cluster



a) Choose **I want to:** > **Create New Cluster**
b) Provide a **Device Name**.

   This name is used internally by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

c) For the **Template**, choose **Cisco Firepower Threat Defense**.
d) Choose the **Image Version**.
e) For the **Instance Type**, choose either **Native** or **Container**.

   A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.

f) (Container Instance only) For the **Resource Type**, choose one of the resource profiles from the drop-down list.

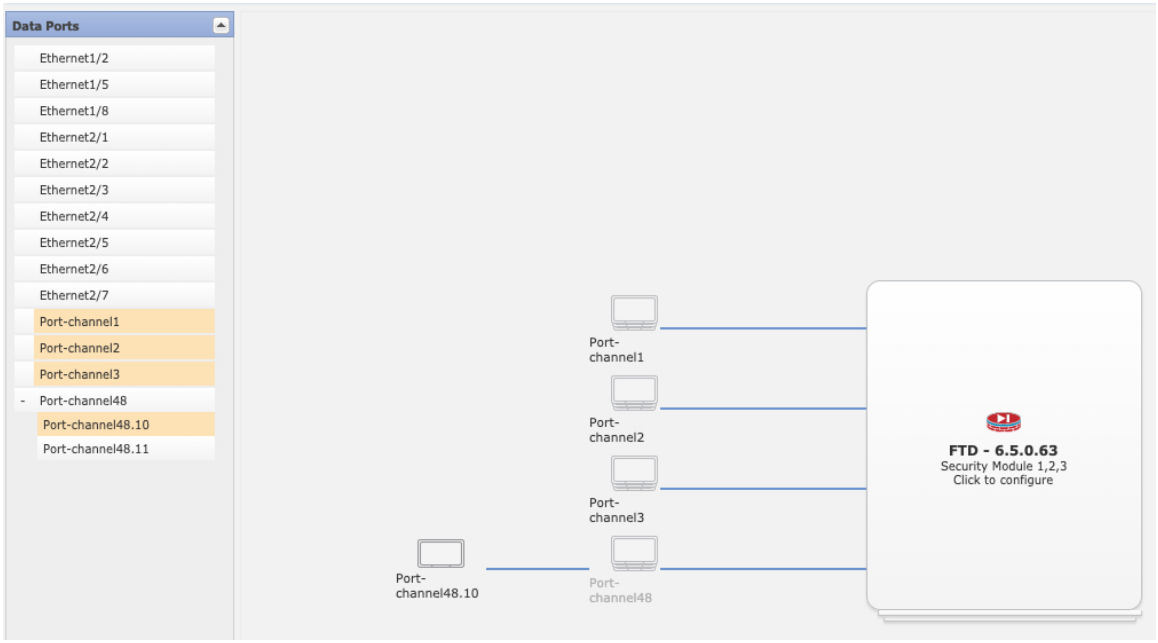
   For the Firepower 9300, this profile will be applied to each instance on each security module. You can set different profiles per security module later in this procedure; for example, if you are using different security module types, and you want to use more CPUs on a lower-end model. We recommend choosing the correct profile before you create the cluster. If you need to create a new profile, cancel out of the cluster creation, and add one using Add a resource profile for container instances , on page 264.

Note If you assign a different profile to instances in an established cluster, which allows mismatched profiles, then apply the new profile on the data nodes first; after they reboot and come back up, you can apply the new profile to the control node.

g) Click **OK**.

You see the Provisioning - *device name* window.

Step 4 Choose the interfaces you want to assign to this cluster.



For native mode clustering: All valid interfaces are assigned by default. If you defined multiple Cluster type interfaces, deselect all but one.

For multi-instance clustering: Choose each data interface you want to assign to the cluster, and also choose the Cluster type port-channel or port-channel subinterface.

Step 5 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 6 On the **Cluster Information** page, complete the following.

Figure 217: Native Cluster

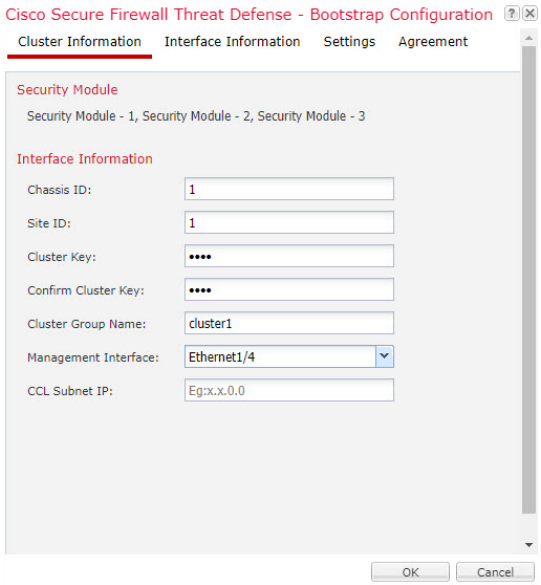
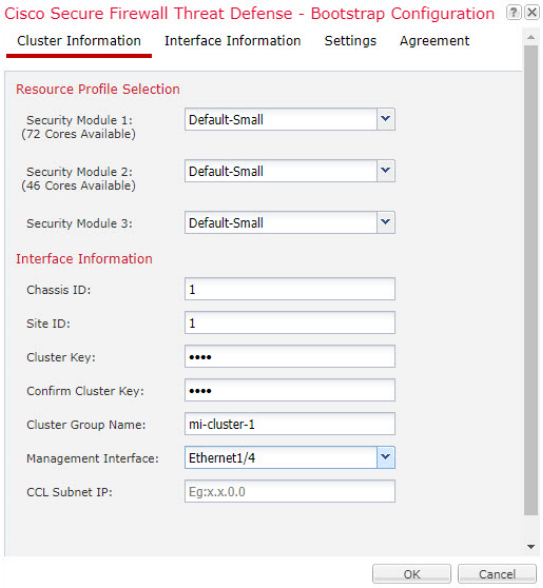


Figure 218: Multi-Instance Cluster



a) (Container Instance for the Firepower 9300 only) In the **Security Module (SM) and Resource Profile Selection** area, you can set a different resource profile per module; for example, if you are using different security module types, and you want to use more CPUs on a lower-end model.

b) For clustering on multiple chassis, in the **Chassis ID** field, enter a chassis ID. Each chassis in the cluster must use a unique ID.

   This field only appears if you added a member interface to cluster control link Port-Channel 48.

c) For inter-site clustering, in the **Site ID** field, enter the site ID for this chassis between 1 and 8. FlexConfig feature. Additional inter-site cluster customizations to enhance redundancy and stability, such as director

localization, site redundancy, and cluster flow mobility, are only configurable using the Firewall Management Center FlexConfig feature.

d) In the **Cluster Key** field, configure an authentication key for control traffic on the cluster control link.

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This option does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

e) Set the **Cluster Group Name**, which is the cluster group name in the logical device configuration.

The name must be an ASCII string from 1 to 38 characters.



Important From 2.4.1, spaces in cluster group name will be considered as special characters and may result in error while deploying the logical devices. To avoid this issue, you must rename the cluster group name without a space.

f) Choose the **Management Interface**.

This interface is used to manage the logical device. This interface is separate from the chassis management port.

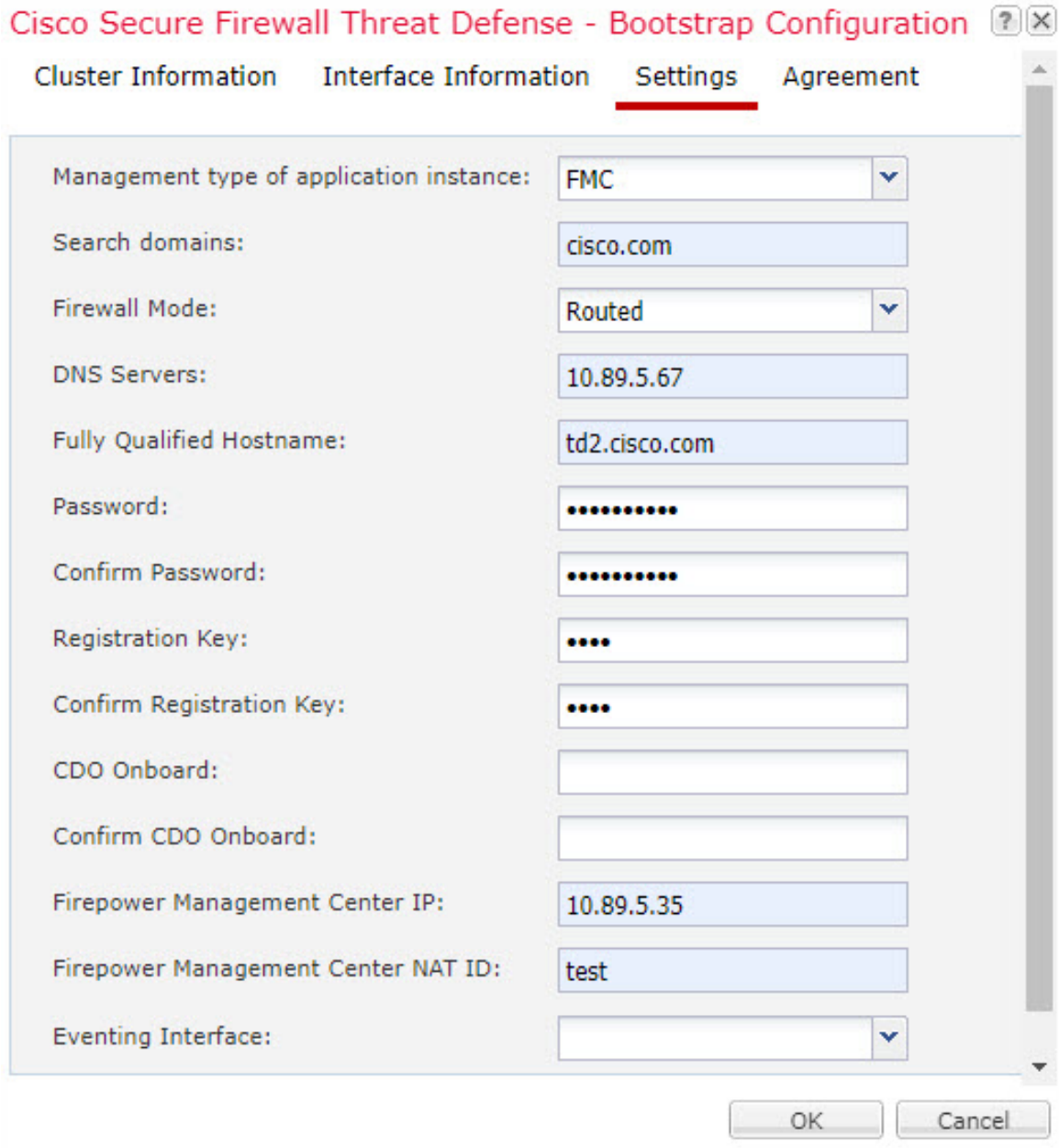
If you assign a Hardware Bypass-capable interface as the Management interface, you see a warning message to make sure your assignment is intentional.

g) (Optional) Set the **CCL Subnet IP** as ***a.b*.0.0**.

By default, the cluster control link uses the 127.2.0.0/16 network. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. In this case, specify any /16 network address on a unique network for the cluster, except for loopback (127.0.0.0/8), multicast (224.0.0.0/4), and internal (169.254.0.0/16) addresses. If you set the value to 0.0.0.0, then the default network is used.

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis_id.slot_id*.

Step 7 On the **Settings** page, complete the following.



a) In the **Registration Key** field, enter the key to be shared between the Firewall Management Center and the cluster members during registration.

   You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the Firewall Management Center when you add the Firewall Threat Defense.

b) Enter a **Password** for the Firewall Threat Defense admin user for CLI access.

c) In the **Firepower Management Center IP** field, enter the IP address of the managing Firewall Management Center. If you do not know the Firewall Management Center IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

d) (Optional) For a container instance, **Permit Expert mode from FTD SSH sessions**: **Yes** or **No**. Expert Mode provides Firewall Threat Defense shell access for advanced troubleshooting.

If you choose **Yes** for this option, then users who access the container instance directly from an SSH sesssion can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.

Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the Firewall Threat Defense CLI.

e) (Optional) In the **Search Domains** field, enter a comma-separated list of search domains for the management network.

f) (Optional) From the **Firewall Mode** drop-down list, choose **Transparent** or **Routed**.

In routed mode, the Firewall Threat Defense is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

g) (Optional) In the **DNS Servers** field, enter a comma-separated list of DNS servers.

The Firewall Threat Defense uses DNS if you specify a hostname for the Firewall Management Center, for example.

h) (Optional) In the **Firepower Management Center NAT ID** field, enter a passphrase that you will also enter on the Firewall Management Center when you add the cluster as a new device.

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the Firewall Management Center specifies the device IP address, and the device specifies the Firewall Management Center IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The Firewall Management Center and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

i) (Optional) In the **Fully Qualified Hostname** field, enter a fully qualified name for the Firewall Threat Defense device.

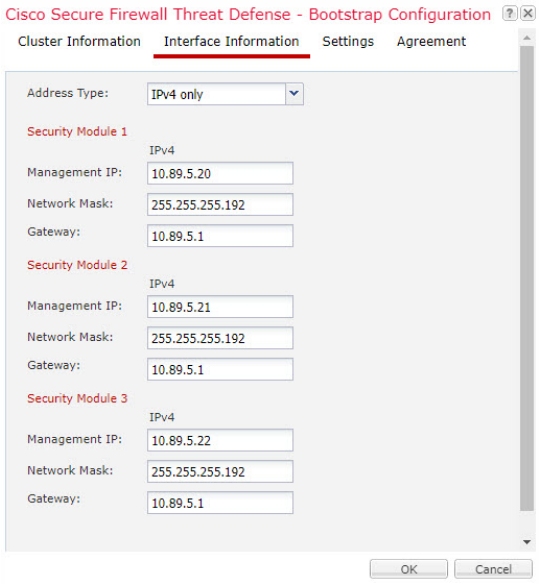
Valid characters are the letters from a to z, the digits from 0 to 9, the dot (.), and the hyphen (-); maximum number of characters is 253.

j) (Optional) From the **Eventing Interface** drop-down list, choose the interface on which events should be sent. If not specified, the management interface will be used.

To specify a separate interface to use for events, you must configure an interface as a *firepower-eventing* interface. If you assign a Hardware Bypass-capable interface as the Eventing interface, you see a warning message to make sure your assignment is intentional.

Step 8 On the **Interface Information** page, configure a management IP address for each security module in the cluster. Select the type of address from the **Address Type** drop-down list and then complete the following for each security module.

Note You must set the IP address for all 3 module slots in a chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.



a) In the **Management IP** field, configure an IP address.

Specify a unique IP address on the same network for each module.

b) Enter a **Network Mask** or **Prefix Length**.

c) Enter a **Network Gateway** address.

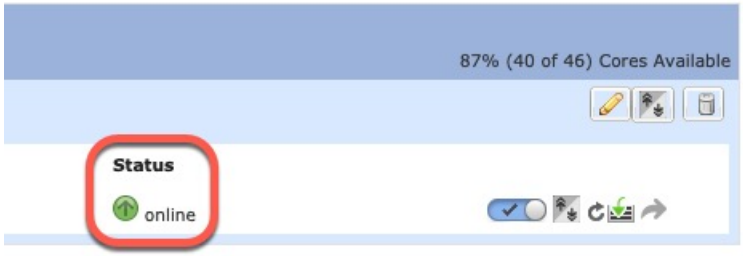
Step 9 On the **Agreement** tab, read and accept the end user license agreement (EULA).

Step 10 Click **OK** to close the configuration dialog box.

Step 11 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can add the remaining cluster chassis, or for a cluster isolated to security modules within one Firepower 9300 chassis, start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.





Step 12 For clustering on multiple chassis, add the next chassis to the cluster:

a) On the first chassis of the Firewall Chassis Manager, click the **Show Configuration icon** at the top right; copy the displayed cluster configuration.

b) Connect to the Firewall Chassis Manager on the next chassis, and add a logical device according to this procedure.

c) Choose **I want to:** > **Join an Existing Cluster**.

d) Click **OK**.

e) In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK**.

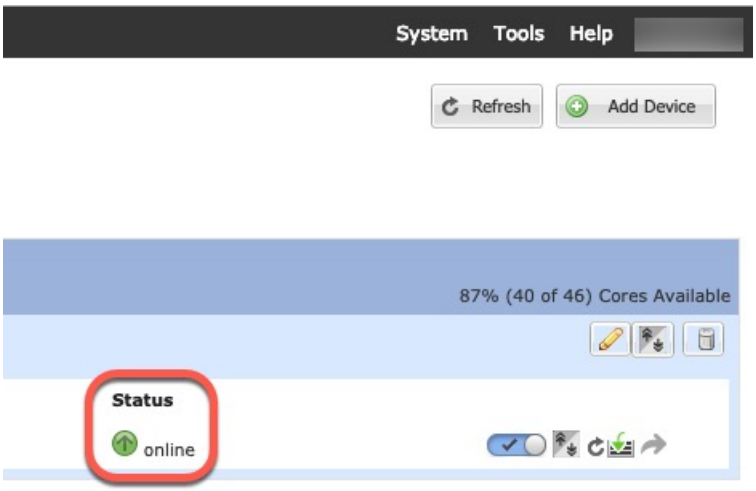
f) Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:

- **Chassis ID**—Enter a unique chassis ID.
- **Site ID**—For inter-site clustering, enter the site ID for this chassis between 1 and 8. Additional inter-site cluster customizations to enhance redundancy and stability, such as director localization, site redundancy, and cluster flow mobility, are only configurable using the Firewall Management Center FlexConfig feature.
- **Cluster Key**—(Not prefilled) Enter the same cluster key.
- **Management IP**—Change the management address for each module to be a unique IP address on the same network as the other cluster members.

Click **OK**.

g) Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online**, you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



Step 13 Add each unit separately to the Firewall Management Center using the management IP addresses, and then group them into a cluster at the web interface.

All cluster units must be in a successfully-formed cluster on FXOS prior to adding them to Firewall Management Center.

Step 14 Add the control unit to the Firewall Management Center using the management IP address.

All cluster units must be in a successfully-formed cluster on FXOS prior to adding them to Firewall Management Center.

The Firewall Management Center then automatically detects the data units.

Add more cluster nodes

Add or replace the Firewall Threat Defense cluster node in an existing cluster. When you add a new cluster node in FXOS, the Firewall Management Center adds the node automatically.

Note The FXOS steps in this procedure only apply to adding a new chassis ; if you are adding a new module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

Before you begin

- In the case of a replacement, you must delete the old cluster node from the Firewall Management Center . When you replace it with a new node, it is considered to be a new device on the Firewall Management Center .
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

Procedure

Step 1 If you previously upgraded the Firewall Threat Defense image using the Firewall Management Center , perform the following steps *on each chassis in the cluster* .

When you upgraded from the Firewall Management Center , the startup version in the FXOS configuration was not updated, and the standalone package was not installed on the chassis. Both of these items need to be set manually so the new node can join the cluster using the correct image version.



Note If you only applied a patch release, you can skip this step. Cisco does not provide standalone packages for patches.

a) Install the running Firewall Threat Defense image on the chassis using the **System** > **Updates** page.

b) Click **Logical Devices** and click the Set Version icon ( ) . For a Firepower 9300 with multiple modules, set the version for each module.

The **Startup Version** shows the original package you deployed with. The **Current Version** shows the version you upgraded to.

c) In the **New Version** drop-down menu, choose the version that you uploaded. This version should match the **Current Version** displayed, and will set the startup version to match the new version.

d) On the new chassis, make sure the new image package is installed.

Step 2 In an existing cluster chassis Firewall Chassis Manager , click **Logical Devices** .

Step 3 Click the **Show Configuration icon** at the top right; copy the displayed cluster configuration.

Step 4 Connect to the Firewall Chassis Manager on the new chassis, and click **Add** > **Cluster** .

Step 5 For the **Device Name** , provide a name for the logical device, and click **OK** ..

Step 6 In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK** .

Step 7 Click the device icon in the center of the screen. The cluster information is partly pre-filled, but you must fill in the following settings:

Figure 219: Cluster Information

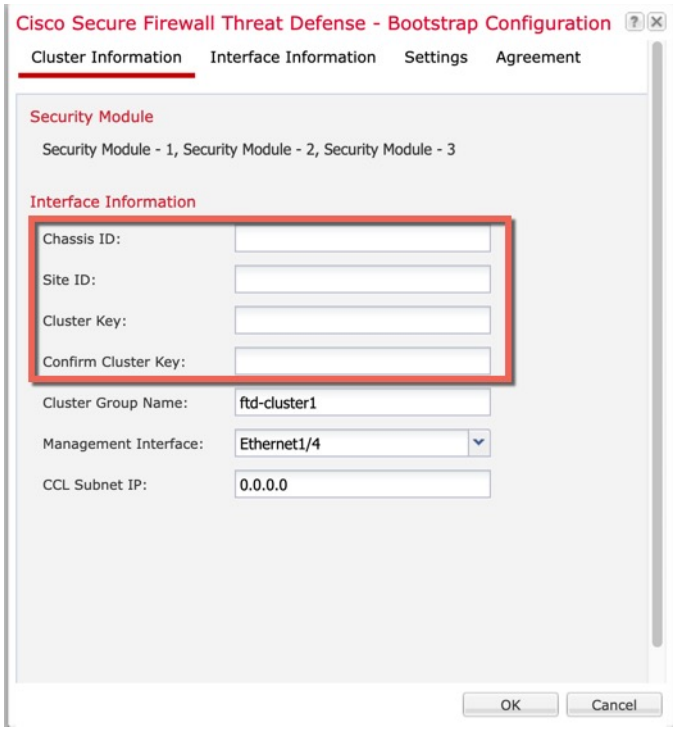


Figure 220: Interface Information

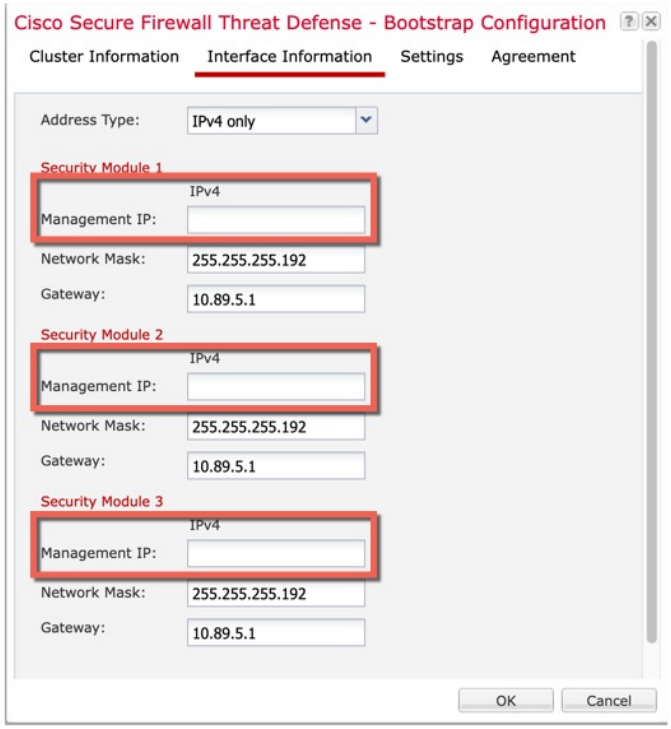
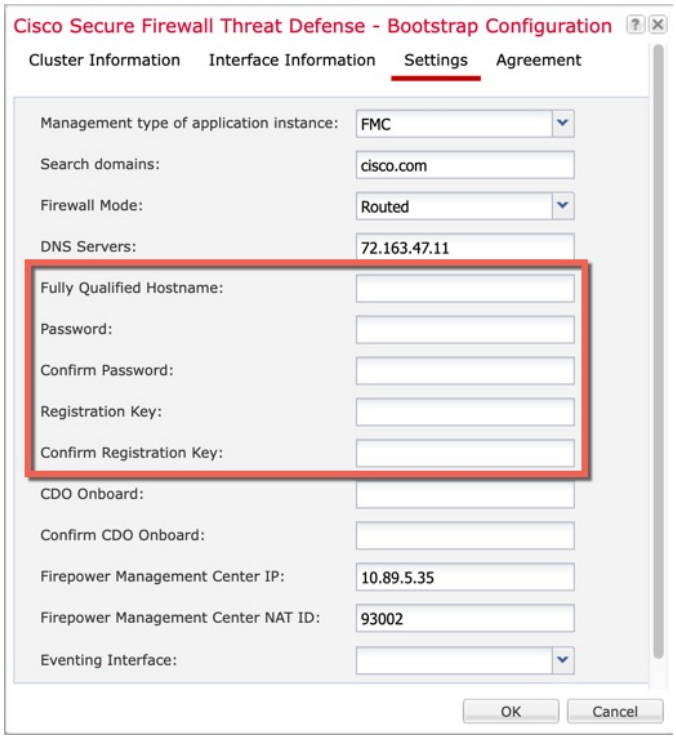


Figure 221: Settings

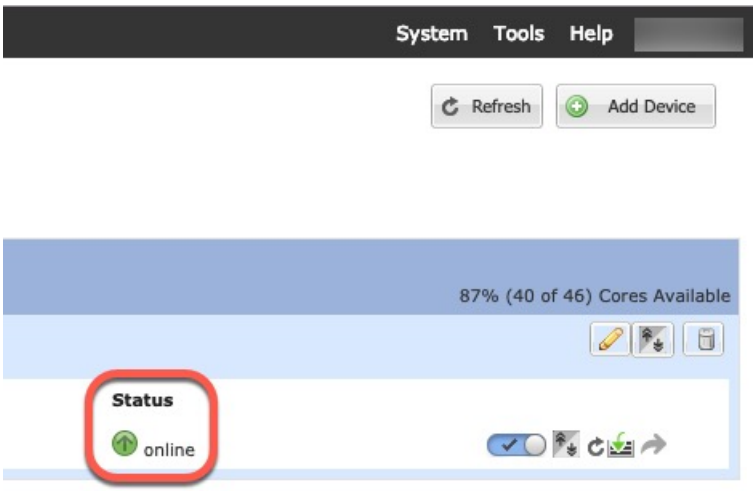


- **Chassis ID** —Enter a unique chassis ID.
- **Site ID** —For inter-site clustering, enter the site ID for this chassis between 1 and 8. This feature is only configurable using the Firewall Management Center FlexConfig feature.
- **Cluster Key** —Enter the same cluster key.
- **Management IP** —Change the management address for each module to be a unique IP address on the same network as the other cluster members.
- **Fully Qualified Hostname** —Enter the same hostname.
- **Password** —Enter the same password.
- **Registration Key** —Enter the same registration key.

Click **OK** .

Step 8 Click **Save** .

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online** , you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



What to do next

1. To add another chassis to the cluster, repeat the procedure in Create a Firewall Threat Defense cluster , on page 541 except you must configure the following settings to be unique; otherwise, use the same configuration for both chassis.
   - Chassis ID
   - Management IP addresses

   Also be sure to set the startup version to the currently running version on the cluster nodes.
2. In the Firewall Management Center , choose **Devices** > **Device Management** , and select the **Add** > **Device** to add the new logical device.
3. Choose **Add** > **Cluster** .
4. Choose the current control unit from the drop-down list.

   When you choose a control unit that is already in a cluster, then the existing cluster name is auto-filled, and all eligible data units are added to the box, including the new unit you just added to the Firewall Management Center .
5. Click **Add** , and then **Deploy** . The cluster is updated to include the new member.

Firewall Management Center: Add a cluster

Add one of the cluster units as a new device to the Secure Firewall Management Center; the Firewall Management Center auto-detects all other cluster members.

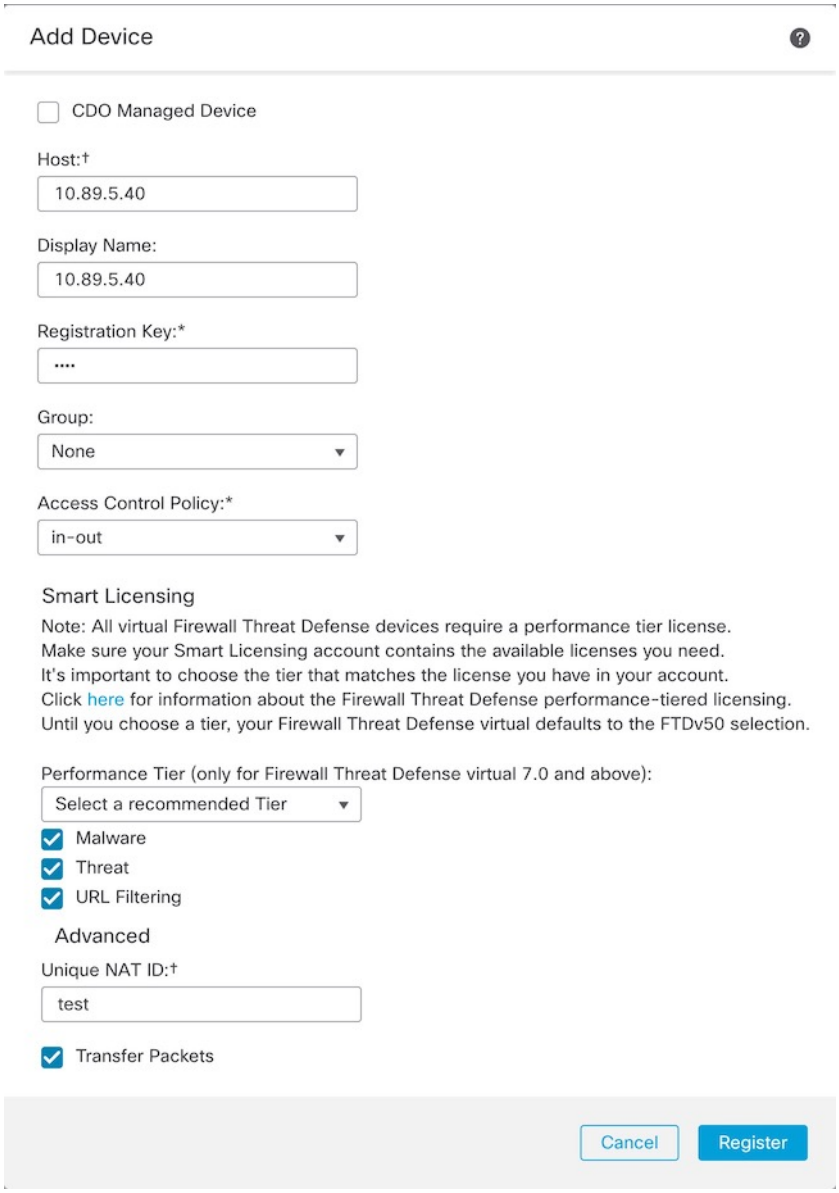
Before you begin

- All cluster units must be in a successfully-formed cluster on FXOS prior to adding the cluster to the Firewall Management Center. You should also check which unit is the control unit. Refer to the Firewall Chassis Manager **Logical Devices** screen or use the Firewall Threat Defense **show cluster info** command.

Procedure

Step 1 In the Firewall Management Center, choose **Devices** > **Device Management**, and then choose **Add** > **Add Device** to add the control unit using the unit's management IP address you assigned when you deployed the cluster.

Figure 222: Add Device



a) In the **Host** field, enter the IP address or hostname of the control unit.

We recommend adding the control unit for the best performance, but you can add any unit of the cluster.

If you used a NAT ID during device setup, you may not need to enter this field. For more information, see NAT environments, on page 8.

b) In the **Display Name** field, enter a name for the control unit as you want it to display in the Firewall Management Center.

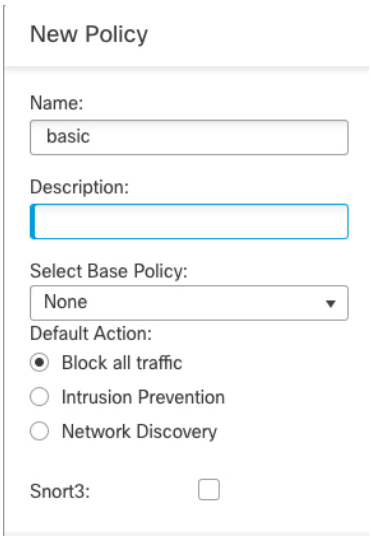
This display name is not for the cluster; it is only for the control unit you are adding. You can later change the name of other cluster members and the cluster display name.

c) In the **Registration Key** field, enter the same registration key that you used when you deployed the cluster in FXOS. The registration key is a one-time-use shared secret.

d) (Optional) Add the device to a device **Group**.

e) Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If you create a new policy, you create a basic policy only. You can later customize the policy as needed.



f) Choose licenses to apply to the device.

g) If you used a NAT ID during device setup, expand the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field.

h) Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent.

i) Click **Register**.

The Firewall Management Center identifies and registers the control unit, and then registers all data units. If the control unit does not successfully register, then the cluster is not added. A registration failure can occur if the cluster was not up on the chassis, or because of other connectivity issues. In this case, we recommend that you try re-adding the cluster unit.

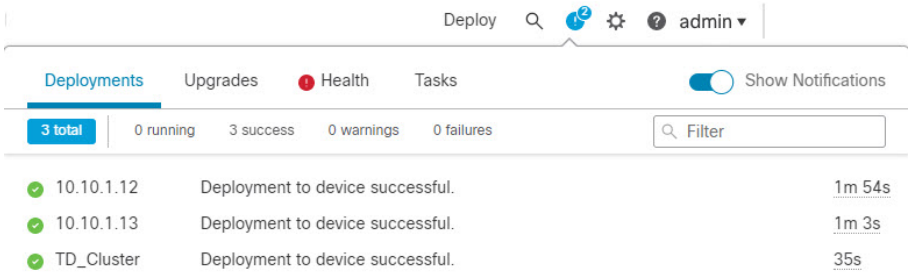
The cluster name shows on the **Devices** > **Device Management** page; expand the cluster to see the cluster units.



A unit that is currently registering shows the loading icon.



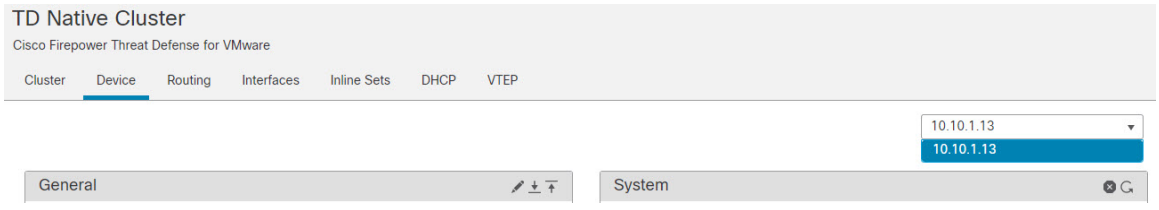
You can monitor cluster unit registration by clicking the **Notifications** icon and choosing **Tasks**. The Firewall Management Center updates the Cluster Registration task as each unit registers. If any units fail to register, see Reconcile cluster members, on page 574.



Step 2 Configure device-specific settings by clicking the **Edit** (✎) for the cluster.

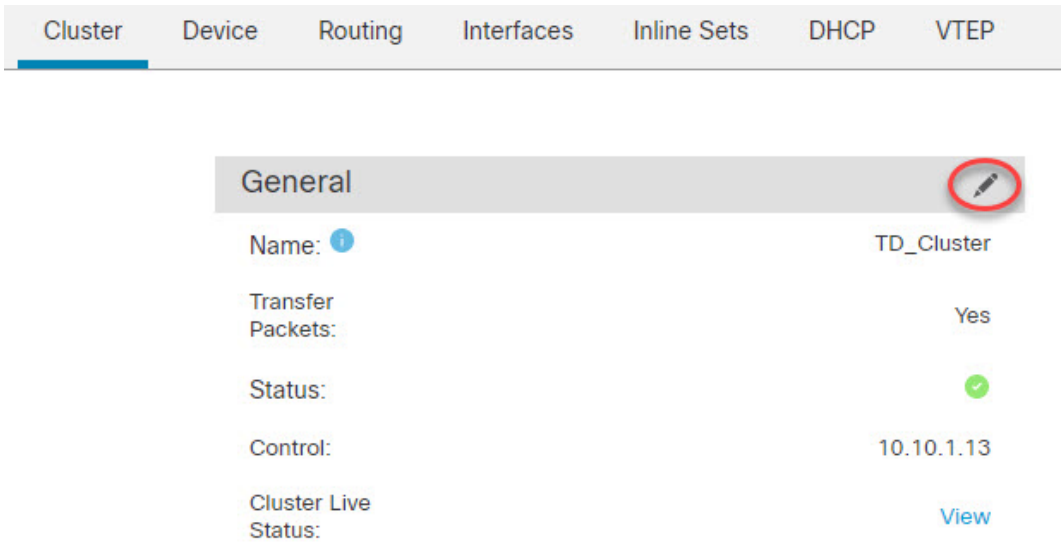
Most configuration can be applied to the cluster as a whole, and not member units in the cluster. For example, you can change the display name per unit, but you can only configure interfaces for the whole cluster.

Step 3 On the **Devices** > **Device Management**and choose the **Add**, **Cluster** screen, you see **General**, **License**, **System**, and **Health** settings.

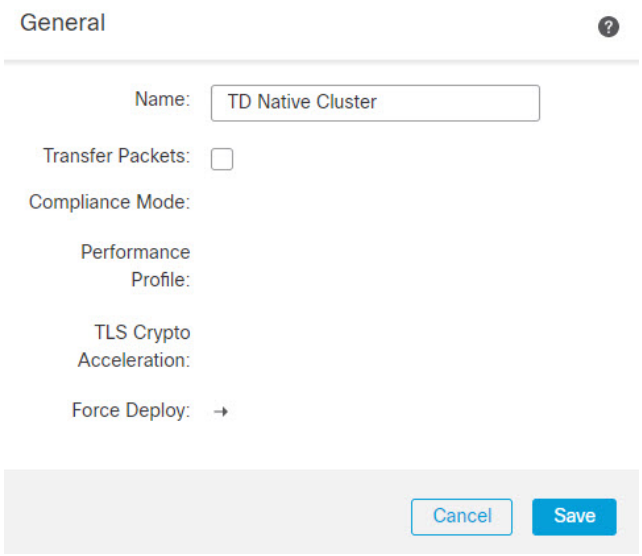


See the following cluster-specific items:

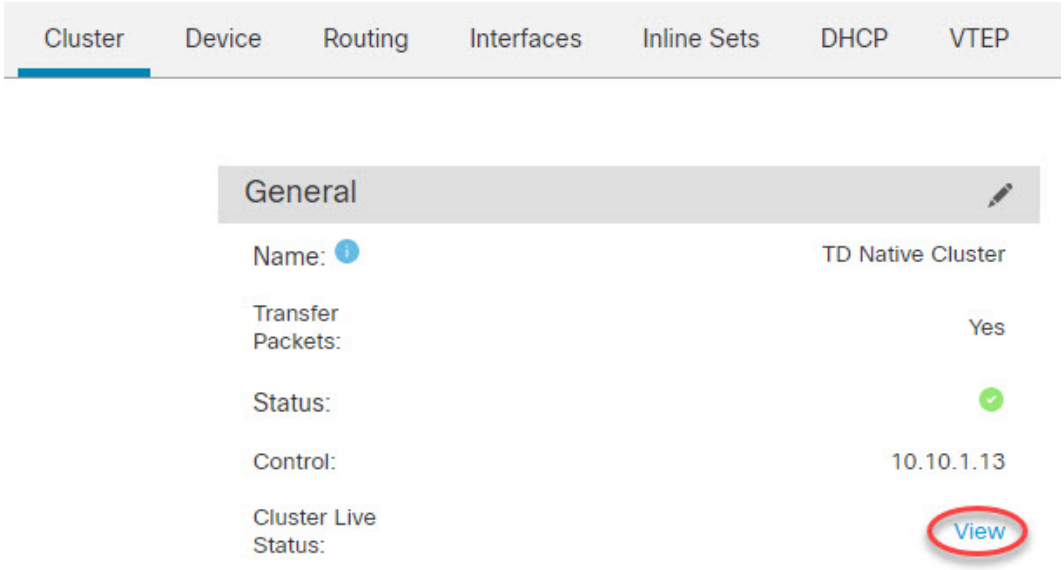
- **General** > **Name**—Change the cluster display name by clicking the **Edit** (✎).



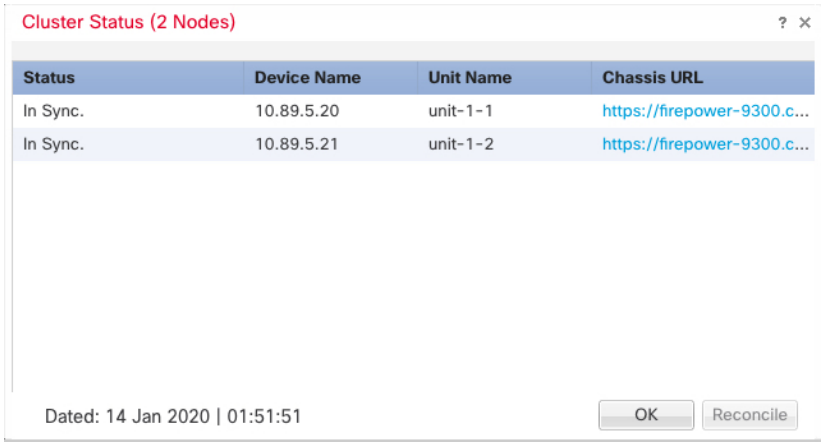
Then set the **Name** field.



- **General > View cluster status**—Click the **View cluster status** link to open the **Cluster Status** dialog box.

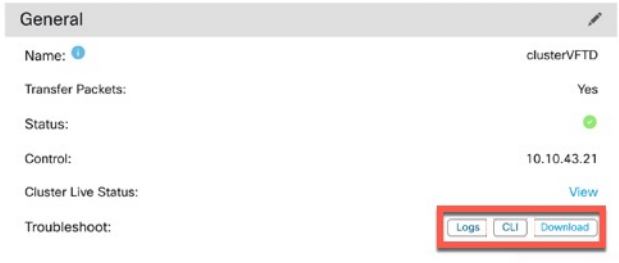


The **Cluster Status** dialog box also lets you retry data unit registration by clicking **Reconcile**.



- **General** > **Troubleshoot**—You can generate and download troubleshooting logs, and you can view cluster CLIs. See Troubleshoot the cluster, on page 365.

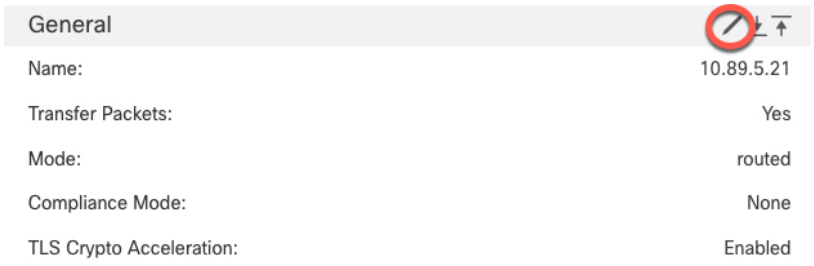
Figure 223: Troubleshoot



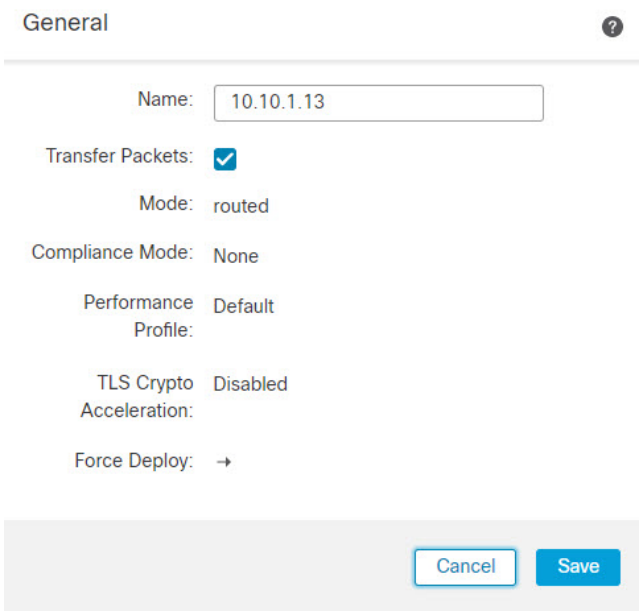
- **License**—Click **Edit** (✎) to set license entitlements.

Step 4 On the **Devices** > **Device Management** and then choose **Add Device**, you can choose each member in the cluster from the top right drop-down menu and configure the following settings.

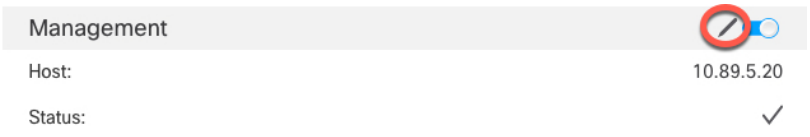
- **General > Name**—Change the cluster member display name by clicking the **Edit** ( ).



Then set the **Name** field.



- **Management > Host**—If you change the management IP address in the device configuration, you must match the new address in the Firewall Management Center so that it can reach the device on the network; edit the **Host** address in the **Management** area.



Firewall Management Center: Configure cluster, data interfaces

This procedure configures basic parameters for each data interface that you assigned to the cluster when you deployed it in FXOS. For clustering on multiple chassis, data interfaces are always Spanned EtherChannel

interfaces. For the cluster control link interface for a cluster isolated to security modules within one Firepower 9300 chassis, you must increase the MTU from the default.

Note When using Spanned EtherChannels for clustering on multiple chassis, the port-channel interface will not come up until clustering is fully enabled. This requirement prevents traffic from being forwarded to a unit that is not an active unit in the cluster.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) next to the cluster.

Step 2 Click **Interfaces**.

Step 3 Configure the cluster control link.

For clustering on multiple chassis, set the cluster control link MTU to be at least 100 bytes higher than the highest MTU of the data interfaces. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead. We suggest setting the MTU to the maximum of 9184; the minimum value is 1400 bytes. For example, because the maximum MTU is 9184, then the highest data interface MTU can be 9084, while the cluster control link can be set to 9184.

For native clusters: The cluster control link interface is Port-Channel48 by default. If you don't know which interface is the cluster control link, check the FXOS configuration for chassis for the Cluster-type interface assigned to the cluster.

a) Click **Edit** (✎) for the cluster control link interface.
b) On the **General** page, in the **MTU** field, enter a value between 1400 and 9184but not between 2561 and 8362. Due to block pool handling, this MTU size is not optimal for system operation. We suggest using the maximum, 9184.
c) Click **OK**.

Step 4 Configure data interfaces.

a) (Optional) For regular firewall interfaces, configure VLAN subinterfaces on the data interface. The rest of this procedure applies to the subinterfaces. See Add a subinterface, on page 669.
b) Click **Edit** (✎) for the data interface.
c) Configure the name and other parameters. For regular firewall interfaces, see Configure routed mode interfaces, on page 690 or, for transparent mode, Bridge group interfaces, on page 695. For IPS-only interfaces, see Inline Sets and Passive Interfaces, on page 727..

Note If the cluster control link interface MTU is not at least 100 bytes higher than the data interface MTU, you will see an error that you must reduce the MTU of the data interface. See, Step 3, on page 563 to increase the cluster control link MTU, after which you can continue configuring the data interfaces.

d) For clustering on multiple chassis, set a unique. manual global MAC address for the EtherChannel. Click **Advanced**, and in the **Active Mac Address** field, enter a MAC address in H.H.H format, where H is a 16-bit hexadecimal digit.

For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.

Do not set the **Standby Mac Address**; it is ignored.

You must configure a unique MAC address not currently in use on your network for a Spanned EtherChannel to avoid potential network connectivity problems. With a manually-configured MAC address, the MAC address stays with the current control unit. If you do not configure a MAC address, then if the control unit changes, the new control unit uses a new MAC address for the interface, which can cause a temporary network outage.

e) Click **OK**. Repeat the above steps for other data interfaces.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Firewall Management Center: Configure Cluster Health Monitor Settings

This task allows you to modify cluster health monitor settings to control how cluster nodes monitor system health and automatically rejoin the cluster after failures.

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings for monitoring cluster node health. You can monitor any port-channel ID, any single physical interface ID, and the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link. It is always monitored.

When a topology change occurs (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature. Also, disable interface monitoring for any interfaces that are disabled. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management**.

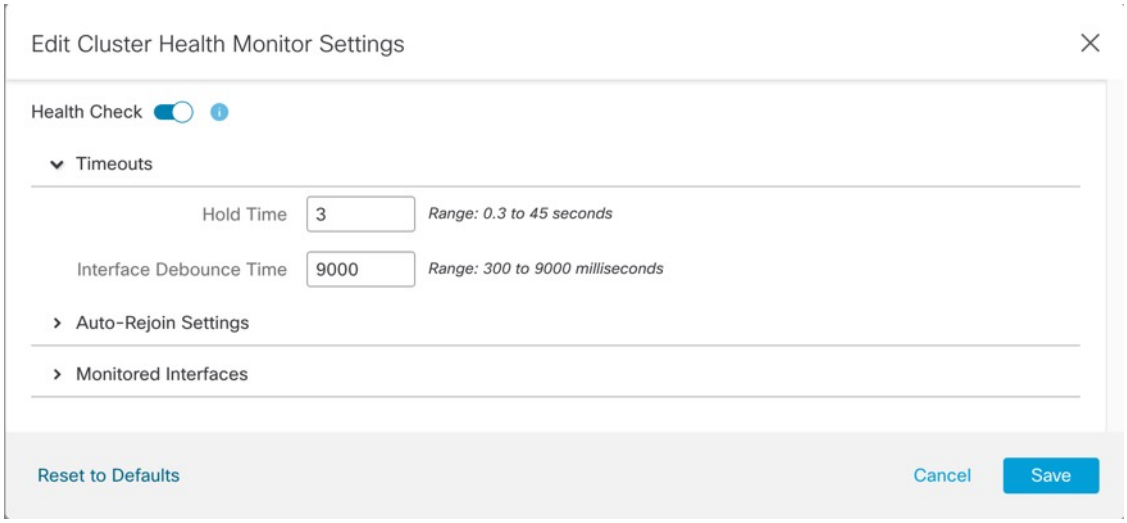
Step 2 Next to the cluster you want to modify, click **Edit** ( ).

Step 3 Click **Cluster**.

Step 4 In the **Cluster Health Monitor Settings** section, click **Edit** ( ).

Step 5 Disable the system health check by clicking the **Health Check** slider.

Figure 224: Disable the system health check



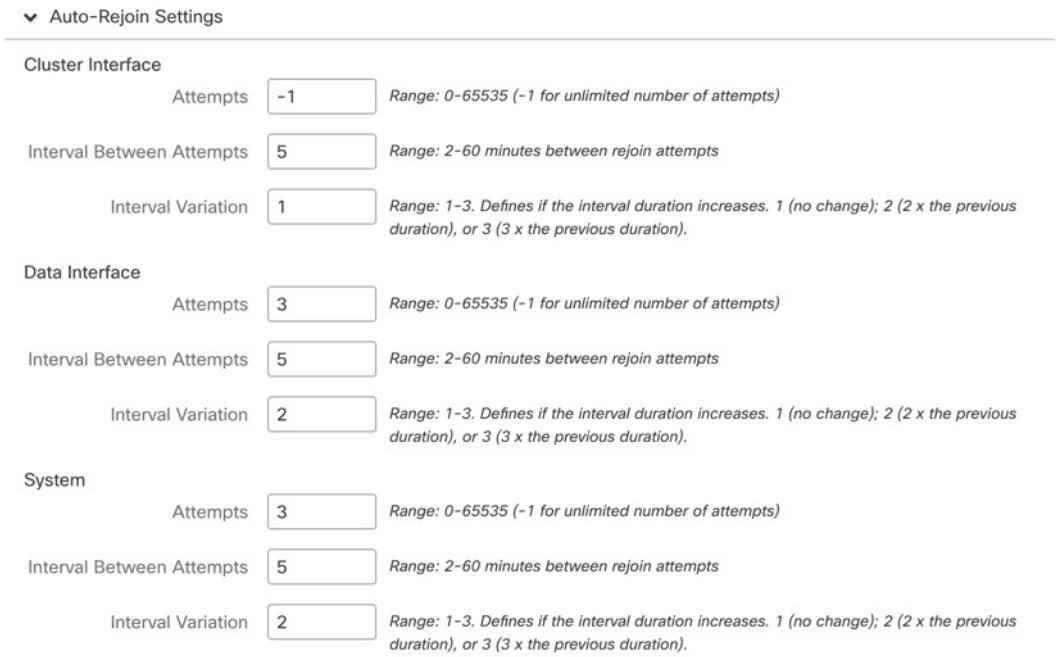
When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between 0.3 and 45 seconds. The default is 3 seconds.
- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the specified number of milliseconds before marking the interface as failed and removing the node from the cluster. If an EtherChannel transitions from a down state to an up state, such as after the switch reloads or enables an EtherChannel, a longer debounce time can prevent the interface from appearing failed on a cluster node if another cluster node bundles the ports more quickly.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 225: Configure Auto-Rejoin settings

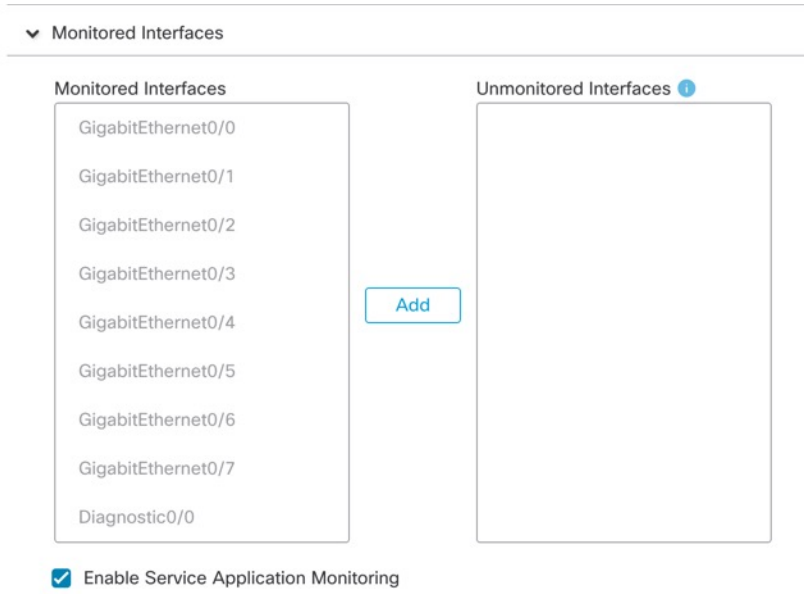


Set values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8 Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 226: Configure monitored interfaces



The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The time required to remove a member from the cluster depends on the type of interface and whether the node is established or is joining the cluster. By default, health check is enabled for all interfaces and the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save**.

Deploy configuration changes; see Deploy configuration changes, on page 135.

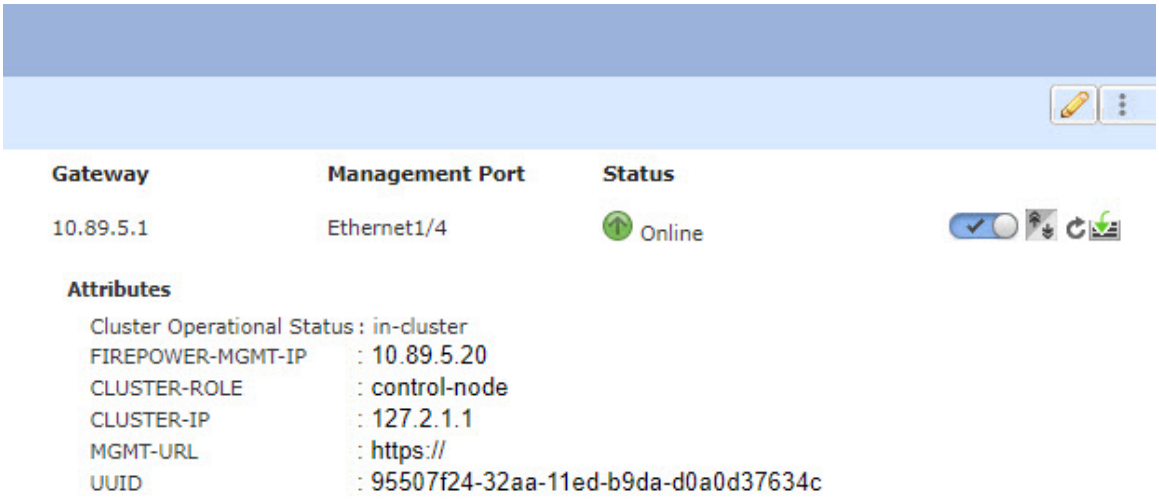
FXOS: Remove a cluster node

The following sections describe how to remove nodes temporarily or permanently from the cluster.

Temporary removal

A cluster node will be automatically removed from the cluster due to a hardware or network failure, for example. This removal is temporary until the conditions are rectified, and it can rejoin the cluster. You can also manually disable clustering.

To check whether a device is currently in the cluster, check the cluster status on the Firewall Chassis Manager **Logical Devices** page:



For Firewall Threat Defense using the Firewall Management Center, you should leave the device in the Firewall Management Center device list so that it can resume full functionality after you reenable clustering.

- Disable clustering in the application—You can disable clustering using the application CLI. Enter the **cluster remove unit** *name* command to remove any node other than the one you are logged into. The bootstrap configuration remains intact, as well as the last configuration synced from the control node, so you can later re-add the node without losing your configuration. If you enter this command on a data node to remove the control node, a new control node is elected.

  When a device becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, re-enable clustering. The Management interface remains up using the IP address the node received from the bootstrap configuration. However if you reload, and the node is still inactive in the cluster , the Management interface is disabled.

  To reenable clustering, on the Firewall Threat Defense enter **cluster enable**.

- Disable the application instance—In the Firewall Chassis Manager on the **Logical Devices** page, click the **Slider enabled** ( ). You can later reenable it using the **Slider disabled** ( ).

- Shut down the security module/engine—In the Firewall Chassis Manager on the **Security Module/Engine** page, click the **Power Off icon**.

- Shut down the chassis—In the Firewall Chassis Manager on the **Overview** page, click the **Shut Down icon**.

Permanent removal

You can permanently remove a cluster node using the following methods.

For Firewall Threat Defense using the Firewall Management Center, be sure to remove the node from the Firewall Management Center device list after you disable clustering on the chassis.

- Delete the logical device—In the Firewall Chassis Manager on the **Logical Devices** page, click the **Delete** ( ). You can then deploy a standalone logical device, a new cluster, or even add a new logical device to the same cluster.
- Remove the chassis or security module from service—If you remove a device from service, you can add replacement hardware as a new node of the cluster.

Firewall Management Center: Manage cluster members

After you deploy the cluster, you can change the configuration and manage cluster members.

Add a new cluster member

When you add a new cluster member in FXOS, the Secure Firewall Management Center adds the member automatically.

Before you begin

- Make sure the interface configuration is the same on the replacement unit as for the other chassis.

Follow these steps to add a new cluster member:

Procedure

Step 1 Add the new unit to the cluster in FXOS. Refer to the FXOS configuration guide.

Wait for the new unit to be added to the cluster. Refer to the Firewall Chassis Manager **Logical Devices** screen or use the Firewall Threat Defense **show cluster info** command to view cluster status.

Step 2 The new cluster member is added automatically. To monitor the registration of the replacement unit, view the following:

- **Cluster Status** dialog box (which is available from the **Devices** > **Device Management**, **More** ( ) icon or from the **Devices** > **Device Management** and choose the **Add**, **Cluster** tab **General** area **Cluster Live Status** link)—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the Firewall Management Center attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking **Reconcile**.
- System status **Tasks** —The Firewall Management Center shows all registration events and failures.
- **Devices** > **Device Management** and then choose **Add Device**—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.

Replace a cluster member

You can replace a cluster member in an existing cluster. The Firewall Management Center auto-detects the replacement unit. However, you must manually delete the old cluster member in the Firewall Management Center. This procedure also applies to a unit that was reinitialized; in this case, although the hardware remains the same, it appears to be a new member.

Before you begin

- Make sure the interface configuration is the same on the replacement unit as for other chassis.

Follow these steps to replace a cluster member:

Procedure

Step 1 For a new chassis, if possible, backup and restore the configuration from the old chassis in FXOS.

If you are replacing a module in a Firepower 9300, you do not need to perform these steps.

If you do not have a backup FXOS configuration from the old chassis, first perform the steps in Add a new cluster member, on page 569.

For information about all of the below steps, refer to the FXOS configuration guide.

a) Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis.
b) Import the configuration file to the replacement chassis.
c) Accept the license agreement.
d) If necessary, upgrade the logical device application instance version to match the rest of the cluster.

Step 2 In the Firewall Management Center for the old unit, choose **Devices** > **Device Management**, **More** (⋮) > **Delete** .



Step 3 Confirm that you want to delete the unit.

The unit is removed from the cluster and from the Firewall Management Center devices list.

Step 4 The new or reinitialized cluster member is added automatically. To monitor the registration of the replacement unit, view the following:

- **Cluster Status** dialog box (**Devices** > **Device Management**, **More** (⋮) icon or **Devices** > **Device Management** and then choose **Add**, **Cluster** page, **General** area, **Cluster Live Status** link)—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the Firewall Management Center attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking **Reconcile All**.

- Click **System** (⚙), and then click **Tasks**—The Firewall Management Center shows all registration events and failures.
- **Devices** > **Device Management**, and then click **Add** > **Device**—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.

Deactivate a member

You may want to deactivate a member in preparation for deleting the unit, or temporarily for maintenance. This procedure is meant to temporarily deactivate a member; the unit will still appear in the Firewall Management Center device list.

Note When a unit becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, reenable clustering. The Management interface remains up using the IP address the unit received from the bootstrap configuration. However if you reload, and the unit is still inactive in the cluster, the management interface is disabled. You must use the console for any further configuration.

Procedure

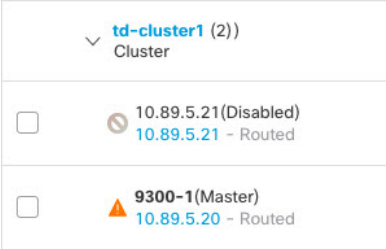
Step 1 For the unit you want to deactivate, choose **Devices** > **Device Management**, **More** (⋮), and then **Disable Clustering**.



You can also deactivate a unit from the **Cluster Status** dialog box (**Devices** > **Device Management**, **More** (⋮), and **Cluster Live Status**).

Step 2 Confirm that you want to disable clustering on the unit.

The unit will show **(Disabled)** next to its name in the **Devices** > **Device Management** list.



Step 3 To re-enable clustering, refer to Rejoin the cluster, on page 572.

Rejoin the cluster

If a unit was removed from the cluster, for example for a failed interface or if you manually disabled clustering, you must manually rejoin the cluster. Make sure the failure is resolved before you try to rejoin the cluster. See Rejoining the cluster, on page 592 for more information about why a unit can be removed from a cluster.

Procedure

Step 1 For the unit you want to reactivate, choose **Devices** > **Device Management**, **More** (⋮) > **Enable Clustering**.



You can also reactivate a unit from the **Cluster Status** dialog box (**Devices** > **Device Management**, **More** (⋮) > **Cluster Live Status**).

Step 2 Confirm that you want to enable clustering on the unit.

Delete (Unregister) a data node

If you need to permanently remove a cluster node (for example, if you remove a module on the Firepower 9300, or remove a chassis), then you should unregister it from the Firewall Management Center.

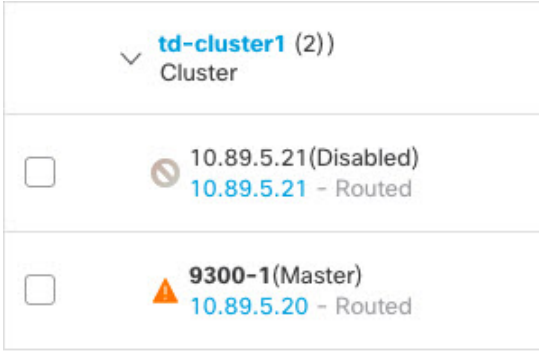
Do not unregister the node if it is still a healthy part of the cluster, or if you only want to disable the node temporarily. To remove it permanently from the cluster in FXOS, see FXOS: Remove a cluster node, on page 567. If you unregister it from the Firewall Management Center, and it is still part of the cluster, it will continue to pass traffic, and could even become the control node—a control node that the Firewall Management Center can no longer manage.

Before you begin

To manually deactivate the node, see Deactivate a member, on page 571. Before you unregister a node, the node must be inactive, either manually or because of a health failure.

Procedure

Step 1 Make sure the node is ready to be unregistered from the Firewall Management Center. On **Devices** > **Device Management**, make sure the node shows **(Disabled)**.



You can also view each node's status on the **Cluster Status** dialog box available from **More** (⋮). If the status is stale, click **Reconcile All** on the **Cluster Status** dialog box to force an update.

Step 2 In the Firewall Management Center for the data node you want to delete, choose **Devices** > **Device Management** and then click **Add** > **DeviceMore** (⋮) > **Delete**.



Step 3 Confirm that you want to delete the node.

The node is removed from the cluster and from the Firewall Management Center devices list.

Change the control unit

The best method to change the control unit is to disable clustering on the control unit, wait for a new control election, and then re-enable clustering.

Caution If you must specify the *exact* unit you want to become the control unit, use the procedure in this section. Note that for centralized features, if you force a control unit change, then all connections are dropped, and you have to re-establish the connections on the new control unit.

Procedure

Step 1 Open the **Cluster Status** dialog box by choosing **Devices** > **Device Management**, **More** (⋮) > **Cluster Live Status**.

You can also access the **Cluster Status** dialog box from **Devices** > **Device Management** and choose the **Add**, **Cluster** page, **General** area, and **Cluster Live Status** link.

Step 2 For the unit you want to become the control unit, choose **More** (⋮) > **Change Role to Control**.

Step 3 You are prompted to confirm the role change. Check the check box, and click **OK**.

Reconcile cluster members

If a cluster member fails to register, you can reconcile the cluster membership from the chassis to the Secure Firewall Management Center. For example, a data unit might fail to register if the Firewall Management Center is occupied with certain processes, or if there is a network issue.

Procedure

Step 1 Choose **Devices** > **Device Management**, **More** (⋮) for the cluster, and then choose **Cluster Live Status** to open the **Cluster Status** dialog box.

You can also open the **Cluster Status** dialog box from the **Devices** > **Device Management** page **General** area, **Cluster Live Status** link.

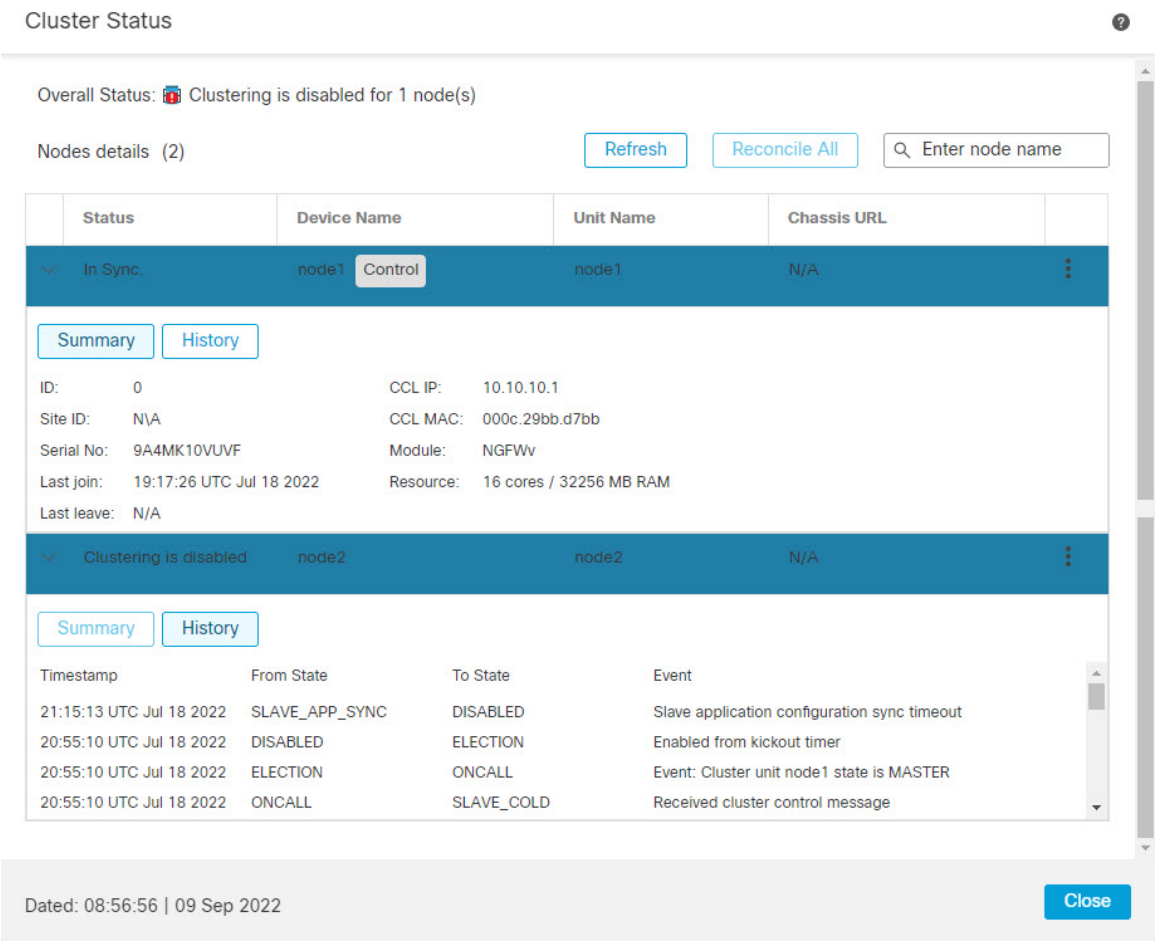
Step 2 Click **Reconcile All**.

For more information about the cluster status, refer to Firewall Management Center: Monitor the cluster, on page 574.

Firewall Management Center: Monitor the cluster

You can monitor the cluster in Secure Firewall Management Center and at the Firewall Threat Defense CLI.

- **Cluster Status** dialog box, which is available from the **Devices** > **Device Management**, **More** (⋮) icon or from the **Devices** > **Device Management** and then chose **Add**, **Cluster** page, **General** area, and **Cluster Live Status** link.



The Control unit has a graphic indicator identifying its role.

Cluster member **Status** includes the following states:

- In Sync.—The unit is registered with the Firewall Management Center.
- Pending Registration—The unit is part of the cluster, but has not yet registered with the Firewall Management Center. If a unit fails to register, you can retry registration by clicking **Reconcile All**.
- Clustering is disabled—The unit is registered with the Firewall Management Center, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the unit from the cluster.
- Joining cluster...—The unit is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the Firewall Management Center.

For each unit, you can view the **Summary** or the **History**.

For each unit from the **More** (⋮) menu , you can perform the following status changes:

- **Disable Clustering**
- **Enable Clustering**

- **Change Role to Control**

- Click **System** (⚙), and then click **Tasks**.

  The **Tasks** page shows updates of the Cluster Registration task as each unit registers.

- **Devices** > **Device Management** and then choose **Add Device** *cluster_name*.

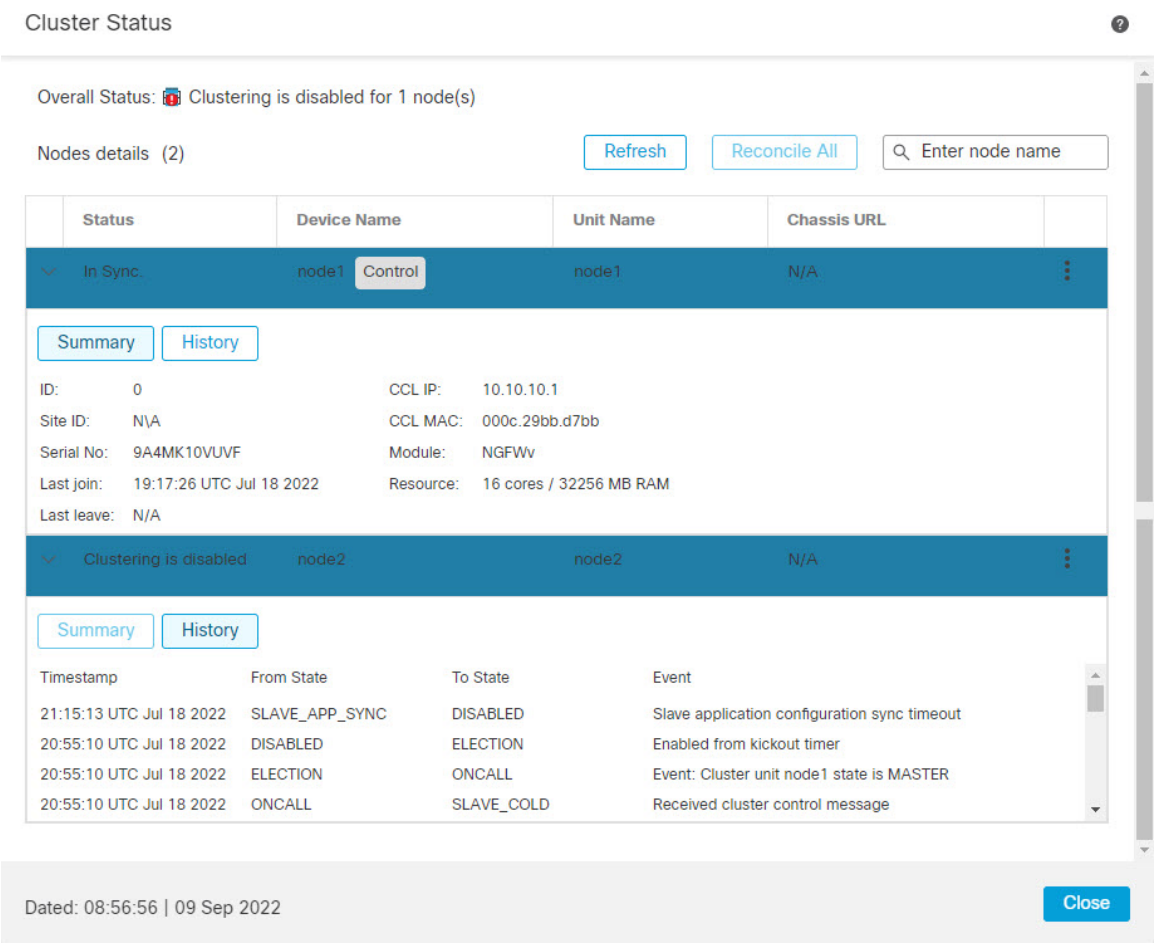
  When you expand the cluster on the devices listing page, you can see all member units, including the control unit shown with its role next to the IP address. For units that are still registering, you can see the loading icon.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  To view aggregated data for the entire cluster or other information, use the **show cluster** command.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  To view cluster information, use the **show cluster info** command.



The Control unit has a graphic indicator identifying its role.

Cluster member **Status** includes these states:

- In Sync.—The unit is registered with the Firewall Management Center.
- Pending Registration—The unit is part of the cluster, but has not yet registered with the Firewall Management Center. If a unit fails to register, you can retry registration by clicking **Reconcile All**.
- Clustering is disabled—The unit is registered with the Firewall Management Center, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the unit from the cluster.
- Joining cluster...—The unit is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the Firewall Management Center.

For each unit, you can view the **Summary** or the **History**.

For each unit from the **More** (⋮) menu, you can perform these status changes:

- **Disable Clustering**
- **Enable Clustering**
- **Change Role to Control**

Tasks page

Click **System** (⚙), and then click **Tasks**.

The **Tasks** page shows updates of the Cluster Registration task as each unit registers.

Device management page

Devices > **Device Management** and then choose **Add Device** *cluster_name*.

When you expand the cluster on the devices listing page, you can see all member units, including the control unit shown with its role next to the IP address. For units that are still registering, you can see the loading icon.

CLI commands for cluster monitoring

show cluster {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

To view aggregated data for the entire cluster or other information, use the **show cluster** command.

show cluster info [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

To view cluster information, use the **show cluster info** command.

Cluster Health Monitor Dashboard

When a Firewall Threat Defense is the control node of a cluster, the Firewall Management Center collects various metrics periodically from the device metric data collector.

The cluster health monitor is comprised of these components:

- Overview dashboard: Displays information about the cluster topology, cluster statistics, and metric charts:
  - The topology section displays a cluster's live status, the health of individual threat defense, threat defense node type (control node or data node), and the status of the device. The status of the device could be *Disabled* (when the device leaves the cluster), *Added out of box* (in a public cloud cluster, the additional nodes that do not belong to the Firewall Management Center), or *Normal* (ideal state of the node).
  - The cluster statistics section displays current metrics of the cluster with respect to the CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.



Note The CPU and memory metrics display the individual average of the data plane and snort usage.

  - The metric charts, namely, CPU Usage, Memory Usage, Throughput, and Connections, diagrammatically display the statistics of the cluster over the specified time period.

- Load Distribution dashboard: Displays load distribution across the cluster nodes in two widgets:
  - The Distribution widget displays the average packet and connection distribution over the time range across the cluster nodes. This data depicts how the load is being distributed by the nodes. Using this widget, you can easily identify any abnormalities in the load distribution and rectify it.
  - The Node Statistics widget displays the node level metrics in table format. It displays metric data on CPU usage, memory usage, input rate, output rate, active connections, and NAT translations across the cluster nodes. This table view enables you to correlate data and easily identify any discrepancies.

- Member Performance dashboard: Displays current metrics of the cluster nodes. You can use the selector to filter the nodes and view the details of a specific node. The metric data include CPU usage, memory usage, input rate, output rate, active connections, and NAT translations.
- CCL dashboard: Displays, graphically, the cluster control link data namely, the input, and output rate.
- Troubleshooting and Links: Provides convenient links to frequently used troubleshooting topics and procedures.
- Time range: An adjustable time window to constrain the information that appears in the various cluster metrics dashboards and widgets.
- Custom Dashboard: Displays data on both cluster-wide metrics and node-level metrics. However, node selection only applies for the threat defense metrics and not for the entire cluster to which the node belongs.

Viewing cluster health

The cluster health monitor provides a detailed view of the health status of a cluster and its nodes. This cluster health monitor provides health status and trends of the cluster in an array of dashboards.

Before you begin

Ensure you have created a cluster from one or more devices in the Firewall Management Center.

Follow these steps to view the cluster health monitor:

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**.

Use the Monitoring navigation pane to access node-specific health monitors.

Step 2 In the device list, click **Expand**(>) and **Collapse** (⌄) to expand and collapse the list of managed cluster devices.

Step 3 Click on the cluster name to view the cluster health statistics.

The cluster monitor reports health and performance metrics in several predefined dashboards by default. The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including its nodes, CPU, memory, input and output rates, connection statistics, and NAT translation information.
- Load Distribution: Traffic and packet distribution across the cluster nodes.
- Member Performance: Node-level statistics on CPU usage, memory usage, input throughput, output throughput, active connection, and NAT translation.
- CCL: Interface status and aggregate traffic statistics.

You can navigate through the various metrics dashboards by clicking on the labels. For a comprehensive list of the supported cluster metrics, refer to Cisco Secure Firewall Threat Defense Health Metrics.

Step 4 Configure the time range from the drop-down in the upper-right corner.

The time range can reflect a period as short as the last hour (the default) or as long as two weeks. Select **Custom** from the drop-down to configure a custom start and end date.

Click the refresh icon to set auto refresh to 5 minutes or to toggle off auto refresh.

Step 5 Click on deployment icon for a deployment overlay on the trend graph, with respect to the selected time range.

The deployment icon indicates the number of deployments during the selected time-range. A vertical band indicates the deployment start and end time. For multiple deployments, multiple bands/lines appear. Click on the icon on top of the dotted line to view the deployment details.

Step 6 View the **Health Alerts** for the node in the alert notification at the top of page, directly to the right of the device name.

Hover your pointer over the **Health Alerts** to view the health summary of the node. The popup window shows a truncated summary of the top five health alerts. Click on the popup to open a detailed view of the health alert summary.

Step 7 View device monitor health and performance metrics in several predefined dashboards.

The metrics dashboards include:

- Overview: Highlights key metrics from the other predefined dashboards, including CPU, memory, interfaces, connection statistics; plus disk usage and critical process information.
- CPU: CPU utilization, including the CPU usage by process and by physical cores.

- Memory: Device memory utilization, including data plane and Snort memory usage.
- Interfaces: Interface status and aggregate traffic statistics.
- Connections: Connection statistics (such as elephant flows, active connections, peak connections, and so on) and NAT translation counts.
- Snort: Statistics that are related to the Snort process.
- ASP drops: Statistics related to the dropped packets against various reasons.

You can navigate through the various metrics dashboards by clicking on the labels. Refer to Cisco Secure Firewall Threat Defense Health Metrics for a comprehensive list of the supported device metrics.

Step 8 Click the plus sign **Add New Dashboard**(+) in the upper right corner of the health monitor to create a custom dashboard by building your own variable set from the available metric groups.

For cluster-wide dashboard, choose Cluster metric group, and then choose the metric.

Cluster metrics

The cluster health monitor tracks statistics that are related to a cluster and its nodes, and aggregate of load distribution, performance, and CCL traffic statistics.

Table 39: Cluster Metrics

Metric	Description	Format
CPU	Average of CPU metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Memory	Average of memory metrics on the nodes of a cluster (individually for data plane and snort).	percentage
Data Throughput	Incoming and outgoing data traffic statistics for a cluster.	bytes
CCL Throughput	Incoming and outgoing CCL traffic statistics for a cluster.	bytes
Connections	Count of active connections in a cluster.	number
NAT Translations	Count of NAT translations for a cluster.	number
Distribution	Connection distribution count in the cluster for every second.	number
Packets	Packet distribution count in the cluster for every second.	number

Troubleshoot the cluster

Use these methods to troubleshoot the devices and clusters:

- Use **Logs** to generates troubleshooting files for all nodes in the cluster. Use this option when you need one cluster-level collection instead of generating troubleshooting files from each node separately.
- Use **CLI** to run a predefined set of cluster diagnostic commands and displays the output. Use this option to check cluster configuration, member state, cluster health, control-plane transport statistics, packet drops, interface status, CPU usage, memory buffers, ARP entries, and reachability. The **CLI** option displays command output; it does not open an interactive CLI session.

Commands
show running-config cluster: Review the cluster group configuration, local unit, cluster interface, priority, health-check, auto-rejoin, and cLACP settings.
show cluster info: Confirm that clustering is enabled and identify the control node, member state, software version, serial number, CCL IP address, CCL MAC address, and last join or leave state.
show cluster info health: Check unit, interface, service, and overall cluster health.
show cluster info transport cp: Review control-plane transport counters, including reliable and unreliable message counters, errors, retransmits, drops, and buffer conditions.
show version: Capture platform, software, build, UUID, LSP, VDB, uptime, resource, and license context.
show asp drop: Identify accelerated security path packet or flow drop reasons and counters.
show counters: Review protocol, feature, and cluster CCL counters.
show arp: Verify ARP entries for interfaces that participate in cluster communication.
show int ip brief: Check interface IP addresses and administrative and line protocol status.
show blocks: Check buffer availability and failed allocations.
show cpu detailed: Check data path, control point, and total CPU usage.
show interface *ccl_interface*: Review interface state, MTU, MAC address, IP address, traffic counters, errors, and drops for the cluster-related interface.
ping *ccl_ip* **size** *ccl_mtu* **repeat 2**: Test reachability to a cluster peer by using the packet size selected by the tool.

- Use the **CCL Ping** when you need to test cluster control link connectivity between joined cluster nodes.
- Troubleshooting files—If a node fails to join the cluster, a troubleshooting file is automatically generated. You can also generate and download troubleshooting files from the **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area. For more information, refer to Generate troubleshooting files, on page 745.

You can also generate files from the **Device Management** page. Click **More** (⋮) and choose **Troubleshoot Files**.

- CLI output—Choose **Devices** > **Device Management** and then choose **Add**, **ClusterGeneral** area, you can view a set of pre-defined CLI outputs that can help you troubleshoot the cluster. These commands are automatically run for the cluster:

  You can also enter any **show** command in the **Command** field.

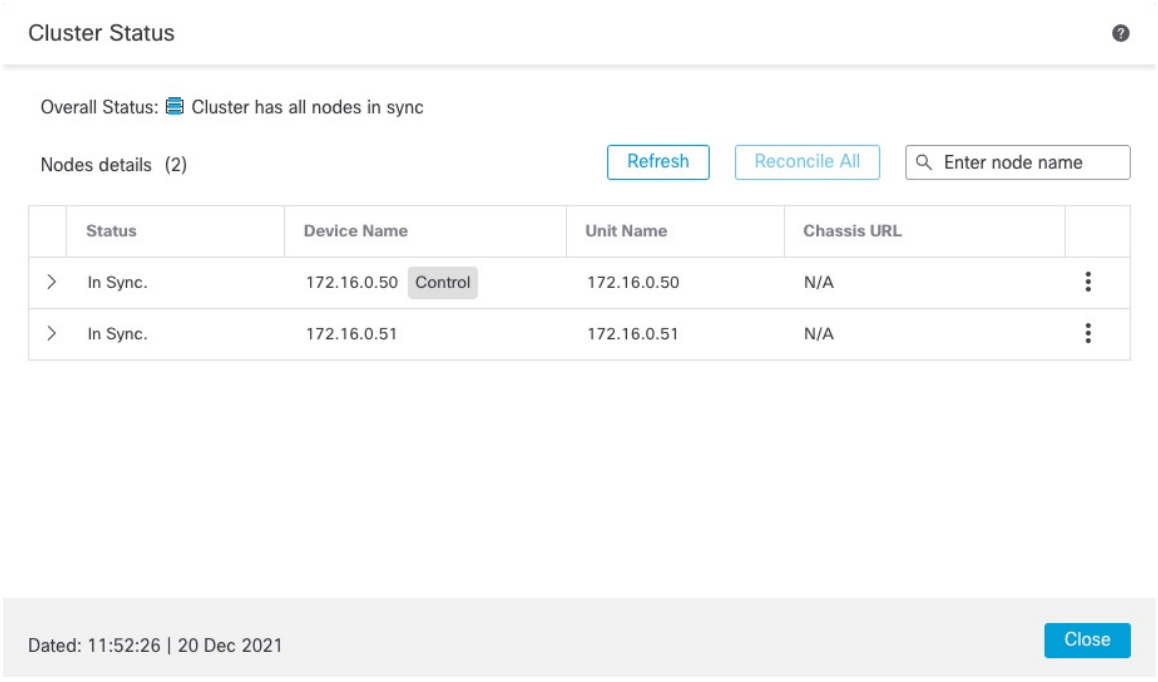
Perform a ping on the cluster control link

You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs.

Procedure

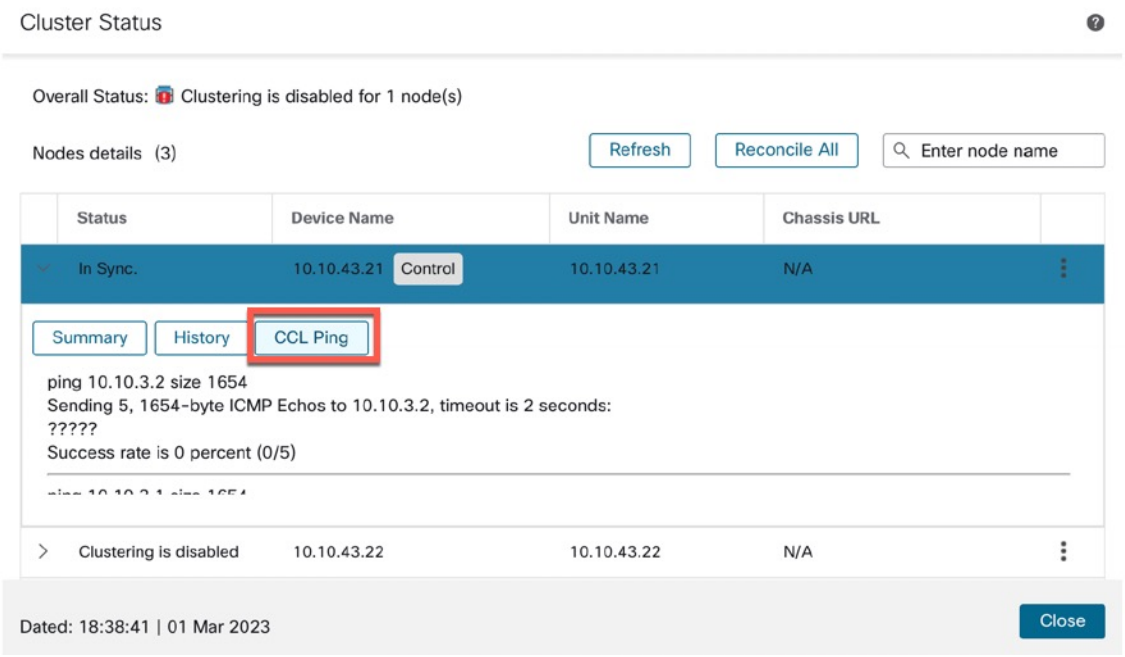
Step 1 Choose **Devices** > **Device Management**, click the **More** (⋮) icon next to the cluster, and choose **Cluster Live Status**.

Figure 227: Cluster status



Step 2 Expand one of the nodes, and click **CCL Ping**.

Figure 228: CCL ping



The node sends a ping on the cluster control link to every other node using a packet size that matches the maximum MTU.

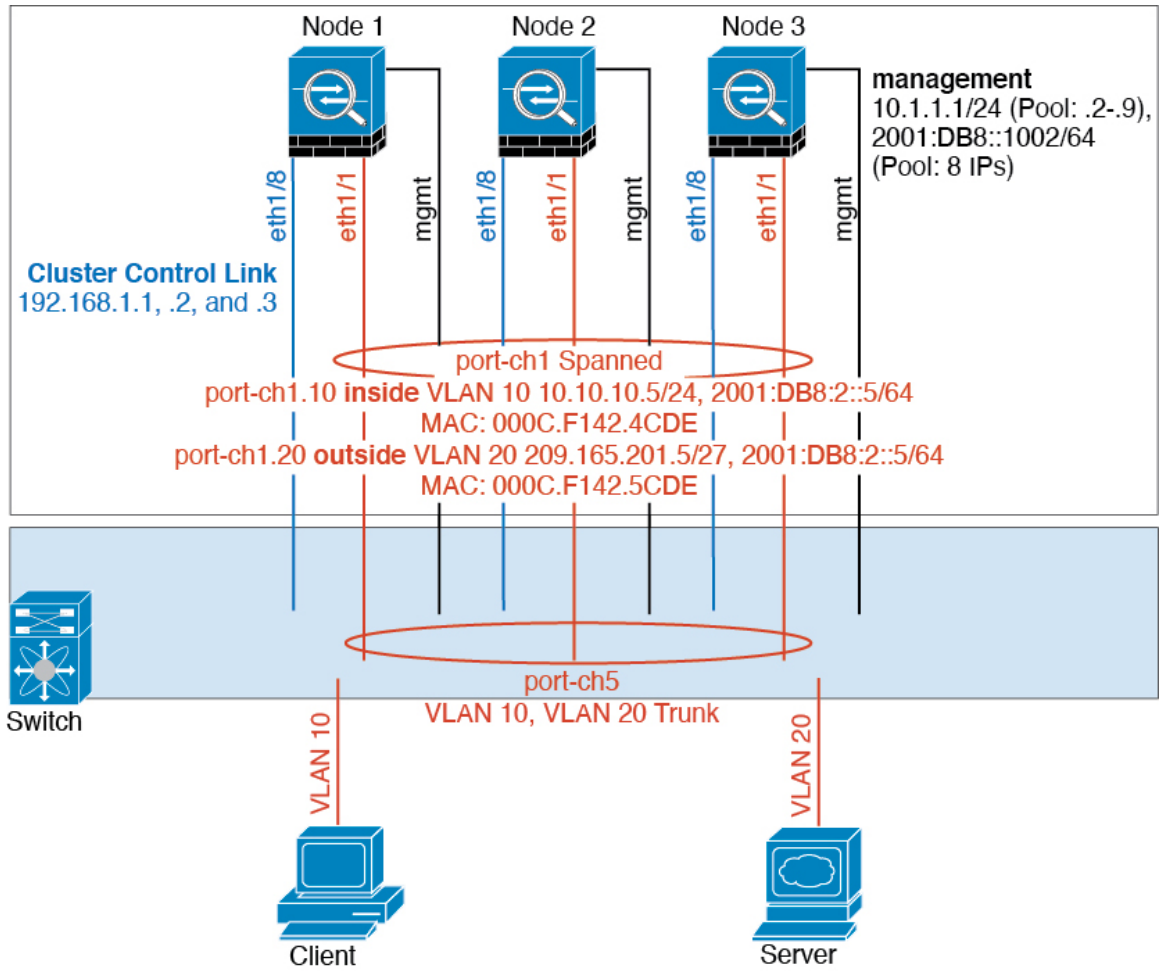
Examples for Clustering

These examples include typical deployments.

Firewall on a stick

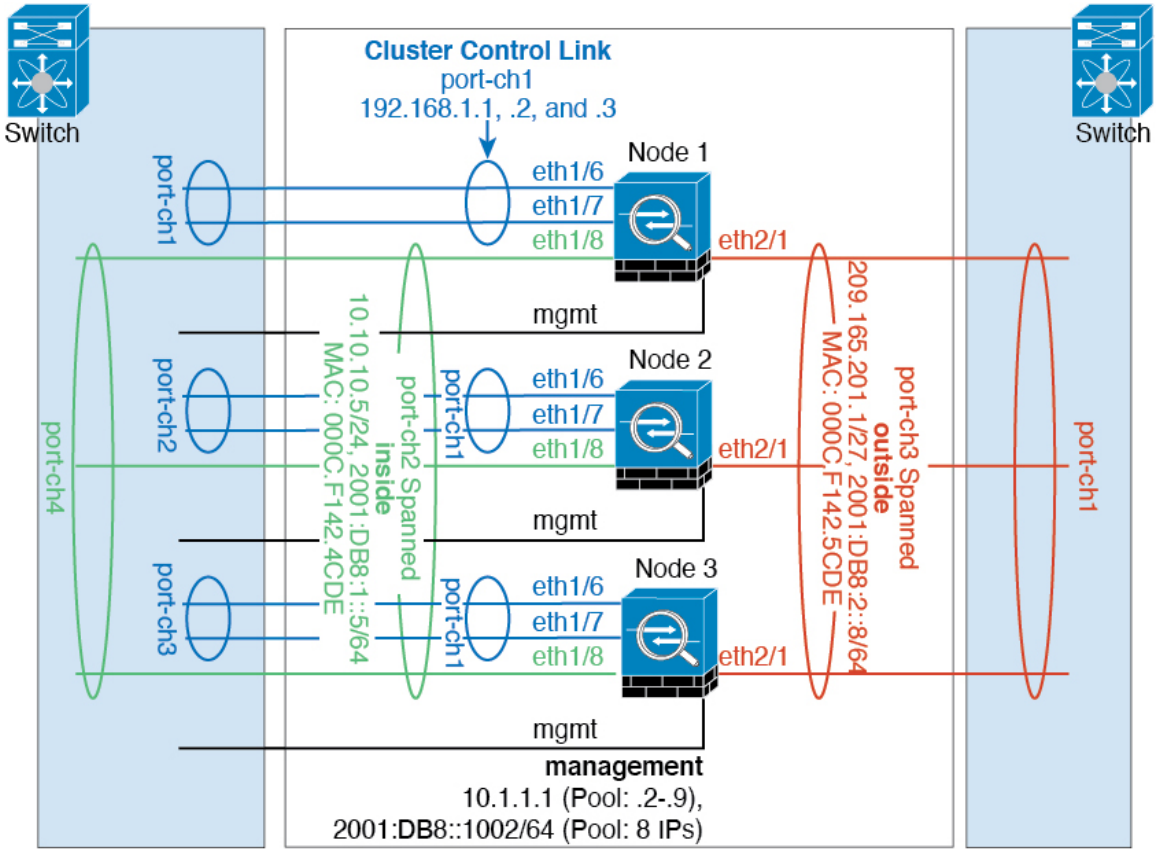
Data traffic from different security domains are associated with different VLANs. For example, VLAN 10 for the inside network and VLAN 20 for the outside network. Each Threat Defense has a single physical port connected to the external switch or router. Trunking is enabled so that all packets on the physical link are 802.1q encapsulated. The Threat Defense is the firewall between VLAN 10 and VLAN 20.

When using Spanned EtherChannels, all data links are grouped into one EtherChannel on the switch side. If the Threat Defense becomes unavailable, the switch will rebalance traffic between the remaining units.



Traffic segregation

Provides the necessary bootstrap and interface configurations to implement traffic segregation using spanned EtherChannels in a cluster environment.



As shown in the diagram above, there is one Spanned EtherChannel on the left side that connects to the inside switch, and the other on the right side to outside switch. You can also create VLAN subinterfaces on each EtherChannel if desired.

Reference for clustering

This section includes more information about how clustering operates.

Firewall Threat Defense features and clustering

Some Firewall Threat Defense features are not supported with clustering, and some are only supported on the control unit. Other features might have caveats for proper usage.

Unsupported features with clustering

These features cannot be configured with clustering enabled, and the commands will be rejected.

Note To view FlexConfig features that are also not supported with clustering, for example WCCP inspection, see the ASA general operations configuration guide. FlexConfig lets you configure many ASA features that are not present in the Firewall Management Center GUI. See FlexConfig policies, on page 921.

- Remote access VPN (SSL VPN and IPsec VPN)
- DHCP client, server, and proxy. DHCP relay is supported.
- Virtual Tunnel Interfaces (VTIs)
- High Availability
- Integrated Routing and Bridging
- Firewall Management Center UCAPL/CC mode
- DHCP client, server, and proxy. DHCP relay is supported.

Centralized features for clustering

The following features are only supported on the control unit, and are not scaled for the cluster.



Note Traffic for centralized features is forwarded from member units to the control unit over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-control units before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the control unit.

For centralized features, if the control unit fails, all connections are dropped, and you have to re-establish the connections on the new control unit.

- Site-to-site VPN
- The following application inspections:
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- Dynamic routing
- Static route monitoring

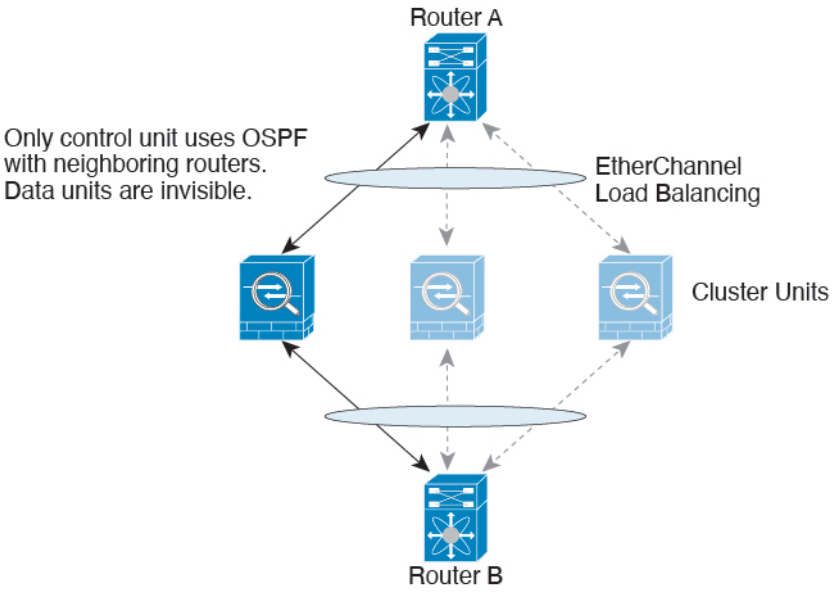
Connection settings

Connection limits are enforced cluster-wide. Each node has an estimate of the cluster-wide counter values based on broadcast messages. Due to efficiency considerations, the configured connection limit across the cluster might not be enforced exactly at the limit number. Each node may overestimate or underestimate the cluster-wide counter value at any given time. However, the information will get updated over time in a load-balanced cluster.

Dynamic routing and clustering

The routing process only runs on the control unit, and routes are learned through the control unit and replicated to secondaries. If a routing packet arrives at a data unit, it is redirected to the control unit.

Figure 229: Dynamic Routing



After the data units learn the routes from the control unit, each unit makes forwarding decisions independently.

The OSPF LSA database is not synchronized from the control unit to data units. If there is a control unit switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.

FTP and clustering

- If FTP data channel and control channel flows are owned by different cluster members, then the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

Multicast routing and clustering

The control unit handles all multicast routing packets and data packets until fast-path forwarding is established. After the connection is established, each data unit can forward multicast data packets.

NAT and clustering

NAT can affect the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different Firewall Threat Defenses in the cluster, because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When

a packet arrives at the Firewall Threat Defense that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link. Note that the receiving node does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

If you still want to use NAT in clustering, then consider the following guidelines:

- PAT with Port Block Allocation—See the following guidelines for this feature:
  - Maximum-per-host limit is not a cluster-wide limit, and is enforced on each node individually. Thus, in a 3-node cluster with the maximum-per-host limit configured as 1, if the traffic from a host is load-balanced across all 3 nodes, then it can get allocated 3 blocks with 1 in each node.
  - Port blocks created on the backup node from the backup pools are not accounted for when enforcing the maximum-per-host limit.
  - On-the-fly PAT rule modifications, where the PAT pool is modified with a completely new range of IP addresses, will result in xlate backup creation failures for the xlate backup requests that were still in transit while the new pool became effective. This behavior is not specific to the port block allocation feature, and is a transient PAT pool issue seen only in cluster deployments where the pool is distributed and traffic is load-balanced across the cluster nodes.
  - When operating in a cluster, you cannot simply change the block allocation size. The new size is effective only after you reload each device in the cluster. To avoid having to reload each device, we recommend that you delete all block allocation rules and clear all xlates related to those rules. You can then change the block size and recreate the block allocation rules.
- NAT pool address distribution for dynamic PAT—When you configure a PAT pool, the cluster divides each IP address in the pool into port blocks. By default, each block is 512 ports, but if you configure port block allocation rules, your block setting is used instead. These blocks are distributed evenly among the nodes in the cluster, so that each node has one or more blocks for each IP address in the PAT pool. Thus, you could have as few as one IP address in a PAT pool for a cluster, if that is sufficient for the number of PAT'ed connections you expect. Port blocks cover the 1024-65535 port range, unless you configure the option to include the reserved ports, 1-1023, on the PAT pool NAT rule.
- Reusing a PAT pool in multiple rules—To use the same PAT pool in multiple rules, you must be careful about the interface selection in the rules. You must either use specific interfaces in all rules, or "any" in all rules. You cannot mix specific interfaces and "any" across the rules, or the system might not be able to match return traffic to the right node in the cluster. Using unique PAT pools per rule is the most reliable option.
- No round-robin—Round-robin for a PAT pool is not supported with clustering.
- No extended PAT—Extended PAT is not supported with clustering.
- Dynamic NAT xlates managed by the control node—The control node maintains and replicates the xlate table to data nodes. When a data node receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the control node. The data node owns the connection.
- Stale xlates—The xlate idle time on the connection owner does not get updated. Thus, the idle time might exceed the idle timeout. An idle timer value higher than the configured timeout with a refcnt of 0 is an indication of a stale xlate.
- No static PAT for the following inspections—
  - FTP

- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- If you have an extremely large number of NAT rules, over ten thousand, you should enable the transactional commit model using the **asp rule-engine transactional-commit nat** command in the device CLI. Otherwise, the node might not be able to join the cluster.

SIP inspection and clustering

A control flow can be created on any node (due to load balancing); its child data flows must reside on the same node.

SNMP and clustering

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new control node is elected, the poll to the new control node will fail.

When using SNMPv3 with clustering, if you add a new cluster node after the initial cluster formation, then SNMPv3 users are not replicated to the new node. You must remove the users, and re-add them, and then redeploy your configuration to force the users to replicate to the new node.

Syslog and clustering

- Each node in the cluster generates its own syslog messages. You can configure logging so that each node uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all nodes in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all nodes look as if they come from a single node. If you configure logging to use the local-node name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different nodes.

TLS/SSL connections and clustering

The decryption states of TLS/SSL connections are not synchronized, and if the connection owner fails, then the decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

Cisco TrustSec and clustering

Only the control node learns security group tag (SGT) information. The control node then populates the SGT to data nodes, and data nodes can make a match decision for SGT based on the security policy.

VPN and clustering

Site-to-site VPN is a centralized feature; only the control unit supports VPN connections.

Note Remote access VPN is not supported with clustering.

VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities. If the control unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control unit is elected, you must reestablish the VPN connections.

When you connect a VPN tunnel to a Spanned interface address, connections are automatically forwarded to the control unit.

VPN-related keys and certificates are replicated to all units.

Performance scaling factor

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately 80% of the maximum combined throughput.

For example, for TCP throughput, the Firepower 9300 with 3 SM-40 modules can handle approximately 135 Gbps of real world firewall traffic when running alone. For 2 chassis, the maximum combined throughput will be approximately 80% of 270 Gbps (2 chassis x 135 Gbps): 216 Gbps.

Control unit election

The control unit election is a automated process where cluster members determine which unit manages centralized features.

Election process and rules

Members of the cluster communicate over the cluster control link to elect a control unit as follows:

1. When you deploy the cluster, each unit broadcasts an election request every 3 seconds.
2. Any other units with a higher priority respond to the election request; the priority is set when you deploy the cluster and is not configurable.
3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes the control unit.
4. If a unit later joins the cluster with a higher priority, it does not automatically become the control unit; the existing control unit always remains as the control unit unless it stops responding, at which point a new control unit is elected.
5. In a *split brain* scenario when there are temporarily multiple control units, then the unit with highest priority retains the role while the other units return to data unit roles.

Note You can manually force a unit to become the control unit. For centralized features, if you force a control unit change, then all connections are dropped, and you have to re-establish the connections on the new control unit.

High availability within the cluster

Clustering provides high availability by monitoring chassis, unit, and interface health and by replicating connection states between units.

Chassis-application monitoring

Chassis-application health monitoring is always enabled. The Firepower 4100/9300 chassis supervisor checks the Firewall Threat Defense application periodically (every second). If the Firewall Threat Defense device is up and cannot communicate with the Firepower 4100/9300 chassis supervisor for 3 seconds, the Firewall Threat Defense device generates a syslog message and leaves the cluster.

If the Firepower 4100/9300 chassis supervisor cannot communicate with the application after 45 seconds, it reloads the Firewall Threat Defense device. If the Firewall Threat Defense device cannot communicate with the supervisor, it removes itself from the cluster.

Unit health monitoring

Each unit periodically sends a broadcast keepaliveheartbeat packet over the cluster control link. If the control node does not receive any keepaliveheartbeat packets or other packets from a data node within the configurable timeout period, then the control node removes the data node from the cluster. If the data nodes do not receive packets from the control node, then a new control node is elected from the remaining node.

If nodes cannot reach each other over the cluster control link because of a network failure and not because a node has actually failed, then the cluster may go into a "split brain" scenario where isolated data nodes will elect their own control nodes. For example, if a router fails between two cluster locations, then the original control node at location 1 will remove the location 2 data nodes from the cluster. Meanwhile, the nodes at location 2 will elect their own control node and form their own cluster. Note that asymmetric traffic may fail in this scenario. After the cluster control link is restored, then the control node that has the higher priority will keep the control node's role. See Control unit election, on page 590 for more information.

Interface monitoring

Each node monitors the link status of all hardware interfaces in use, and reports status changes to the control node. For clustering on multiple chassis, Spanned EtherChannels use the cluster Link Aggregation Control Protocol (cLACP). Each chassis monitors the link status and the cLACP protocol messages to determine if the port is still active in the EtherChannel, and informs the Firewall Threat Defense application if the interface is down. When you enable health monitoring, all physical interfaces are monitored by default (including the main EtherChannel for EtherChannel interfaces). Only named interfaces that are in an Up state can be monitored. For example, all member ports of an EtherChannel must fail before a *named* EtherChannel is removed from the cluster. You can optionally disable monitoring per interface.

If a monitored interface fails on a particular node, but it is active on other nodes, then the node is removed from the cluster. The amount of time before the Firewall Threat Defense device removes a node from the cluster depends on whether the node is an established member or is joining the cluster. The Firewall Threat Defense device does not monitor interfaces for the first 90 seconds that a node joins the cluster. Interface status changes during this time will not cause the Firewall Threat Defense device to be removed from the cluster. For an established member, the node is removed after 500 ms.

For clustering on multiple chassis, if you add or delete an EtherChannel from the cluster, interface health-monitoring is suspended for 95 seconds to ensure that you have time to make the changes on each chassis.

Decorator application monitoring

When you install a decorator application on an interface, such as the Radware DefensePro application, then both the Firewall Threat Defense device and the decorator application must be operational to remain in the cluster. The unit does not join the cluster until both applications are operational. Once in the cluster, the unit monitors the decorator application health every 3 seconds. If the decorator application is down, the unit is removed from the cluster.

Status after failure

When a node in the cluster fails, the connections hosted by that node are seamlessly transferred to other nodes; state information for traffic flows is shared over the control node's cluster control link.

If the control node fails, then another member of the cluster with the highest priority (lowest number) becomes the control node.

The Firewall Threat Defense automatically tries to rejoin the cluster, depending on the failure event.

Note When the Firewall Threat Defense becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management interface can send and receive traffic.

Rejoining the cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

Rejoining scenarios and automatic retry behavior

- Failed cluster control link when initially joining—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering.
- Failed cluster control link after joining the cluster—The Firewall Threat Defense automatically tries to rejoin every 5 minutes, indefinitely.
- Failed data interface—The Firewall Threat Defense automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the Firewall Threat Defense application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.
- Failed node—If the node was removed from the cluster because of a node health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the node will rejoin the cluster when it starts up again as long as the cluster control link is up. The Firewall Threat Defense application attempts to rejoin the cluster every 5 seconds.
- Internal error—Internal failures include: application sync timeout; inconsistent application statuses; and so on.
- Failed configuration deployment—If you deploy a new configuration from Firewall Management Center, and the deployment fails on some cluster members but succeeds on others, then the nodes that failed are removed from the cluster. You must manually rejoin the cluster by re-enabling clustering. If the deployment fails on the control node, then the deployment is rolled back, and no members are removed. If the deployment fails on all data nodes, then the deployment is rolled back, and no members are removed.

- Failed Chassis-Application Communication—When the Firewall Threat Defense application detects that the chassis-application health has recovered, it tries to rejoin the cluster automatically.

Data path connection state replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

Table 40: Features Replicated Across the Cluster

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	—
MAC address table	Yes	—
User Identity	Yes	—
IPv6 Neighbor database	Yes	—
Dynamic routing	Yes	—
SNMP Engine ID	**No**	—

How the cluster manages connections

Connections can be load-balanced to multiple nodes of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

Connection roles

See the following roles defined for each connection:

- Owner—Usually, the node that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new nodes receive packets from the connection, the director chooses a new owner from those nodes.
- Backup owner—The node that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then the first node to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

  As long as the director (see below) is not the same node as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

For clustering on the Firepower 9300, which can include up to 3 cluster nodes in one chassis, if the backup owner is on the same chassis as the owner, then an additional backup owner will be chosen from another chassis to protect flows from a chassis failure.

- Director—The node that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and ports (see below for ICMP hash details), and sends a message to the director to register the new connection. If packets arrive at any node other than the owner, the node queries the director about which node is the owner so it can forward the packets. A connection has only one director. If a director fails, the owner chooses a new director.

  As long as the director is not the same node as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.

  ICMP/ICMPv6 hash details:

  - For Echo packets, the source port is the ICMP identifier, and the destination port is 0.
  - For Reply packets, the source port is 0, and the destination port is the ICMP identifier.
  - For other packets, both source and destination ports are 0.

- Forwarder—A node that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner. A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.



Note We do not recommend disabling TCP sequence randomization when using clustering. There is a small chance that some TCP sessions won't be established, because the SYN/ACK packet might be dropped.

- Fragment Owner—For fragmented packets, cluster nodes that receive a fragment determine a fragment owner using a hash of the fragment source IP address, destination IP address, and the packet ID. All fragments are then forwarded to the fragment owner over the cluster control link. Fragments may be load-balanced to different cluster nodes, because only the first fragment includes the 5-tuple used in the switch load balance hash. Other fragments do not contain the source and destination ports and may be load-balanced to other cluster nodes. The fragment owner temporarily reassembles the packet so it can determine the director based on a hash of the source/destination IP address and ports. If it is a new connection, the fragment owner will register to be the connection owner. If it is an existing connection, the fragment owner forwards all fragments to the provided connection owner over the cluster control link. The connection owner will then reassemble all fragments.

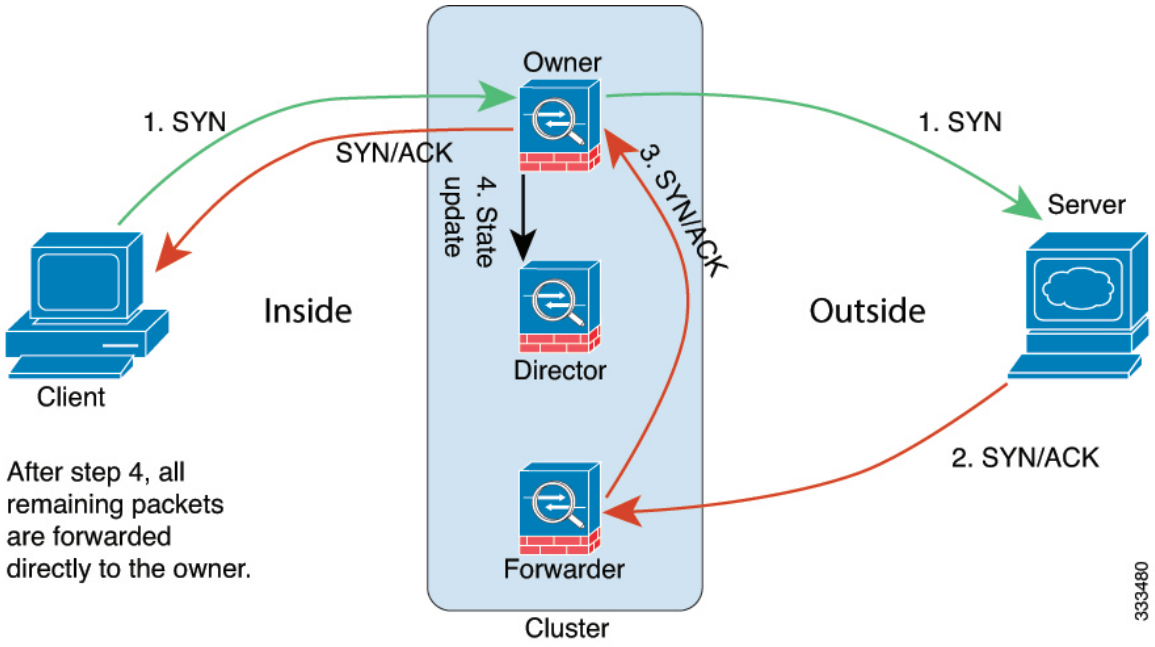
Port Address Translation Connections

New connection ownership

When a new connection is directed to a node of the cluster via load balancing, that node owns both directions of the connection. If any connection packets arrive at a different node, they are forwarded to the owner node over the cluster control link. If a reverse flow arrives at a different node, it is redirected back to the original node.

Sample data flow for TCP

The following example shows the establishment of a new connection.

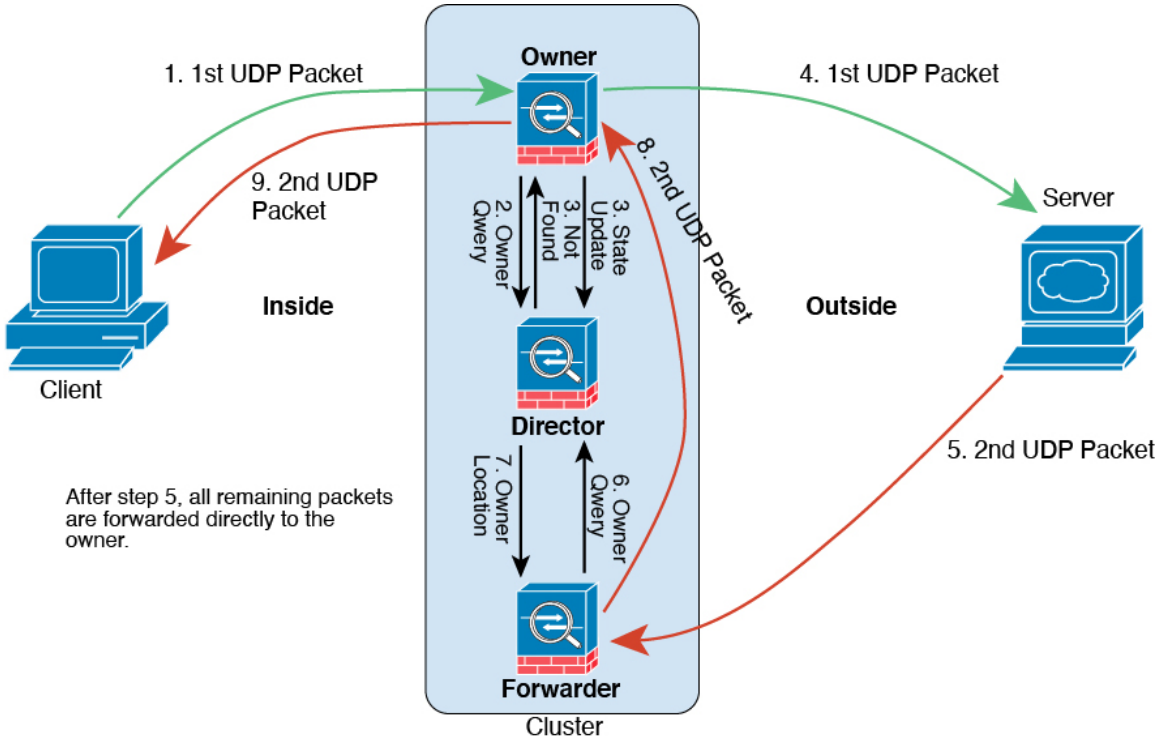


1. The SYN packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.
2. The SYN-ACK packet originates from the server and is delivered to a different Firewall Threat Defense (based on the load balancing method). This Firewall Threat Defense is the forwarder.
3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.
4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.
5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.
6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.
7. If packets are delivered to any additional nodes, it will query the director for the owner and establish a flow.
8. Any state change for the flow results in a state update from the owner to the director.

Sample data flow for ICMP and UDP

The following example shows the establishment of a new connection.

1. ***Figure 230: ICMP and UDP Data Flow***



The first UDP packet originates from the client and is delivered to one Firewall Threat Defense (based on the load balancing method).

2. The node that received the first packet queries the director node that is chosen based on a hash of the source/destination IP address and ports.
3. The director finds no existing flow, creates a director flow and forwards the packet back to the previous node. In other words, the director has elected an owner for this flow.
4. The owner creates the flow, sends a state update to the director, and forwards the packet to the server.
5. The second UDP packet originates from the server and is delivered to the forwarder.
6. The forwarder queries the director for ownership information. For short-lived flows such as DNS, instead of querying, the forwarder immediately sends the packet to the director, which then sends it to the owner.
7. The director replies to the forwarder with ownership information.
8. The forwarder creates a forwarding flow to record owner information and forwards the packet to the owner.
9. The owner forwards the packet to the client.

History for clustering

Table 41:

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cluster control link ping tool.	7.2.6/7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** > **Cluster Live Status.**
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**
Cluster health monitor settings.	7.3.0	Any	You can now edit cluster health monitor settings. New/Modified screens: **Devices** > **Device Management** > **Cluster** > **Cluster Health Monitor Settings** **Note** If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.
Cluster health monitor dashboard.	7.3.0	Any	You can now view cluster health on the cluster health monitor dashboard. New/Modified screens: **System** > **Health** > **Monitor**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for 16-node clusters.	7.2.0	7.2.0	You can now configure 16 node clusters for the Firepower 4100/9300. Previously, the maximum was 6 units. New/Modified screens: none. Supported platforms: Firepower 4100/9300
Cluster deployment for firewall changes completes faster.	7.1.0	7.1.0	Cluster deployment for firewall changes now completes faster. New/Modified screens: none.
Improved PAT port block allocation for clustering.	7.0.0	7.0.0	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command using FlexConfig. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/Modified commands: **cluster-member-limit** (FlexConfig), **show nat pool cluster** [**summary**], **show nat pool ip detail**
Cluster deployment for Snort changes completes faster, and fails faster when there is an event.	6.7.0	6.7.0	Cluster deployment for Snort changes now completes faster. Also, when a cluster has an event that causes a Firewall Management Center deployment to fail, the failure now occurs more quickly. New/Modified screens: none.
Improved cluster management.	6.7.0	6.7.0	Firewall Management Center has improved cluster management functionality that formerly you could only accomplish using the CLI, including: • Enable and disable cluster units • Show cluster status from the Device Management page, including History and Summary per unit • Change the role to the control unit New/Modified screens: • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** > **General** area **> Cluster Live Status** link **Cluster Status** Supported platforms: Firepower 4100/9300

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multi-instance clustering.	6.6.0	6.6.0	You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. New/Modified FXOS commands: **set port-type cluster** New/modified Firepower Chassis Manager screens: • **Logical Devices** > **Add Cluster** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu**Subinterface Type field** Supported platforms: Firewall Threat Defense on the Firepower 4100/9300
Configuration sync to data units in parallel.	6.6.0	6.6.0	The control unit now syncs configuration changes with data units in parallel by default. Formerly, synching occurred sequentially. New/Modified screens: none.
Messages for cluster join failure or eviction added to **show cluster history**.	6.6.0	6.6.0	New messages were added to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. New/Modified commands: **show cluster history** New/Modified screens: none.
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	6.5.0	6.5.0	If you enable Dead Connection Detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. New/Modified commands: **show conn** (output only). Supported platforms: Firewall Threat Defense on the Firepower 4100/9300

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Adding clusters is easier.	6.3.0	6.3.0	You can now add any unit of a cluster to the Firewall Management Center, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster. Adding a cluster unit is also now automatic. Note that you must delete a unit manually. New/Modified screens: **Devices** > **Device Management** > **Add** drop-down menu **Device** > **Add Device** dialog box **Devices** > **Device Management** > **Cluster** tab**General** area**Cluster Registration Status** **Current Cluster Summary** link **Cluster Status** dialog box Supported platforms: Firewall Threat Defense on the Firepower 4100/9300
Support for site-to-site VPN with clustering as a centralized feature.	6.2.3.3	6.2.3.3	You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the control unit supports VPN connections. Supported platforms: Firewall Threat Defense on the Firepower 4100/9300
Automatically rejoin the cluster after an internal failure.	6.2.3	6.2.3	Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New/Modified command: **show cluster info auto-join** No modified screens. Supported platforms: Firewall Threat Defense on the Firepower 4100/9300
Clustering on multiple chassis for 6 modules; Firepower 4100 support.	6.2.0	6.2.0	With FXOS 2.1.1, you can now enable clustering on multiple chassis of the Firepower 9300 and 4100. For the Firepower 9300, you can include up to 6 modules. For example, you can use 1 module in 6 chassis, or 2 modules in 3 chassis, or any combination that provides a maximum of 6 modules. For the Firepower 4100, you can include up to 6 chassis. **Note** Inter-site clustering is also supported. However, customizations to enhance redundancy and stability, such as site-specific MAC and IP addresses, director localization, site redundancy, and cluster flow mobility, are only configurable using the FlexConfig feature. No modified screens. Supported platforms: Firewall Threat Defense on the Firepower 4100/9300

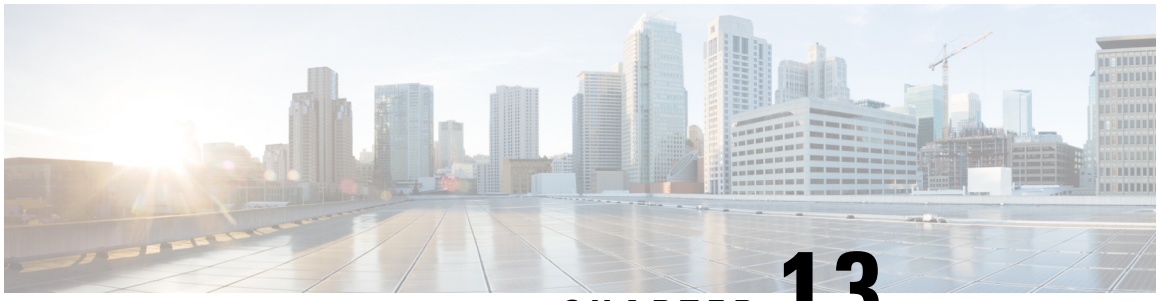
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Clustering on multiple modules with one Firepower 9300 chassis.	6.0.1	6.0.1	You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. New/Modified screens: **Devices** > **Device Management** > **Add** > **Add Cluster** **Devices** > **Device Management** > **Cluster** Supported platforms: Firewall Threat Defense on the Firepower 9300



PART III

Interfaces and Device Settings

- Interface Overview, on page 605
- Regular Firewall Interfaces, on page 649
- Inline Sets and Passive Interfaces, on page 727
- Device Settings, on page 743
- DHCP and DDNS, on page 827
- Platform Settings, on page 847
- FlexConfig policies, on page 921



CHAPTER 13

Interface Overview

The Firewall Threat Defense device includes data interfaces that you can configure in different modes, as well as a management interface.

- Management interface, on page 605
- Interface Mode and Types, on page 607
- Security zones and interface groups, on page 607
- Auto-MDI/MDIX feature, on page 609
- Redundant interfaces (deprecated), on page 609
- Default settings for interfaces, on page 609
- Create security zone and interface group objects, on page 610
- Enable the physical interface and configure Ethernet settings, on page 611
- Configure EtherChannel interfaces, on page 614
- Sync Interface Changes with the Firewall Management Center, on page 622
- Network module management for Secure Firewall 3100/4200, on page 625
- Merge the management and diagnostic interfaces, on page 640
- History for interfaces, on page 645

Management interface

A management interface is a shared physical interface that enables communication between the diagnostic logical interface and the management logical interface on security appliances.

Interface configuration details

In Version 7.3 and earlier, the physical management interface is shared between the Diagnostic logical interface and the Management logical interface. In Version 7.4 and later, the diagnostic interface is merged with management for a simplified user experience.

Management interface

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. It uses its own IP address and static routing.

Management interface configuration and monitoring

You can configure its settings at the CLI using the **configure network** command. You can also view its status on the **Devices** > **Device Management** page. If you change the IP address at the CLI after you add it to the Firewall Management Center, you can match the IP address in the Secure Firewall Management Center in the **Devices** > **Device Management** area.

You can alternatively manage the Firewall Threat Defense using a data interface instead of the management interface.

Diagnostic interface

Diagnostic interface shares a physical port with the Management interface but requires different IP addresses on the same network. A diagnostic interface allows only management traffic.

Legacy diagnostic interface support

For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available.

If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically.

If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. To manually merge the Management and Diagnostic interfaces, see Merge the management and diagnostic interfaces, on page 640. Configurations that prevent an automatic merge include these:

- A data interface named "management"—This name is reserved for use with the merged Management interface.
- IP Address on Diagnostic
- DNS enabled on Diagnostic
- Syslog, SNMP, RADIUS or AD (for remote access VPN) source interface is Diagnostic
- RADIUS or AD (for remote access VPN) with no source interface specified, and there is at least one interface configured as management-only (including Diagnostic)—The default route lookup for these services has changed from the management-only routing table to the data routing table, with no fallback to management. Therefore, you cannot use a management-only interface other than Management.
- Static routes on Diagnostic
- Dynamic routing on Diagnostic
- HTTP server on Diagnostic
- ICMP on Diagnostic
- DDNS for Diagnostic
- FlexConfig using Diagnostic

For more information about how the legacy Diagnostic interface operates, see the 7.3 version of this guide.

Interface Mode and Types

You can deploy Firewall Threat Defense interfaces in two modes: Regular firewall mode and IPS-only mode. You can include both firewall and IPS-only interfaces on the same device.

Regular Firewall Mode

Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this traffic according to your security policy.

The types of firewall interfaces you can configure depends on the firewall mode set for the device: routed or transparent mode. See Transparent or Routed Firewall Mode, on page 71 for more information.

- Routed mode interfaces (routed firewall mode only)—Each interface that you want to route between is on a different subnet.
- Bridge group interfaces (routed and transparent firewall mode)—You can group together multiple interfaces on a network, and the Firewall Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. In routed mode, the Firewall Threat Defense device routes between BVIs and regular routed interfaces. In transparent mode, each bridge group is separate and cannot communicate with each other.

IPS-Only Mode

You can configure your device in either a passive or inline IPS deployment. In a passive deployment, you deploy the system out-of-band from the flow of network traffic. In an inline deployment, you configure the system transparently on a network segment by binding two interfaces together.

Security zones and interface groups

You can assign each interface to a security zone, an interface group, or both. You then apply your security policy based on zones or groups. For example, you can assign the "inside" interface on one or more devices to the "inside" zone, and the "outside" interfaces to the "outside" zone. You can then configure your access control policy to enable traffic to go from the inside zone to the outside zone for every device using the same zones.

Security zones and interface groups functionality

To view the interfaces that belong to each object, choose **Objects** > **Object Management** and click **Interface**. This page lists the security zones and interface groups configured on your managed devices. You can expand each interface object to view the type of interfaces in each interface object.

Note Policies that apply to **any** zone (a global policy) apply to interfaces in zones as well as any interfaces that are not assigned to a zone.

Note The Management interface does not belong to a zone or interface group.

Security zones and interface groups have different membership and usage characteristics:

- Security zones—An interface can belong to only one security zone.
- Interface groups—An interface can belong to multiple interface groups (and to one security zone).

  You can use interface groups in NAT policies, prefilter policies, and QoS policies, as well as features that let you specify the interface name directly, such as Syslog servers or DNS servers.

Some policies only support security zones, while other policies support zones and groups. Unless you need the functionality an interface group provides, you should default to using security zones because security zones are supported for all features.

You cannot change an existing security zone to an interface group or vice-versa. Instead, you must create a new interface object.

Note Although tunnel zones are not interface objects, you can use them in place of security zones in certain configurations; see Using tunnel zones to apply access control at the tunnel level, on page 1970.

Interface objects are categorized by these types:

- Passive—For IPS-only passive or ERSPAN interfaces.
- Inline—For IPS-only inline set interfaces.
- Switched—For regular firewall bridge group interfaces.
- Routed—For regular firewall routed interfaces.
- ASA—(Security zones only) For legacy ASA FirePOWER device interfaces.
- Management—(Interface groups only) For management-only interfaces.
- Loopback—(Interface groups only) For loopback interfaces.

All interfaces in an interface object must be of the same type. After you create an interface object, you cannot change the type of interfaces it contains.

The interface (or zone name) itself does not provide any default behavior in regarding the security policy. We recommend using names that are self-describing to avoid mistakes in future configuration. A good name signifies a logical segment or traffic specification, for example:

- Names of internal interfaces—InsideV110, InsideV160, InsideV195
- Names of DMZ interfaces—DMZV11, DMZV12, DMZV-TEST
- Names of external interfaces—Outside-ASN78, Outside-ASN91

Auto-MDI/MDIX feature

Auto-MDI/MDIX is a feature that eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. The feature is enabled by default with auto-negotiation on RJ-45 interfaces and requires either speed or duplex to be set to auto-negotiate. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Redundant interfaces (deprecated)

Redundant interfaces were supported for the ASA 5500-X platforms only. We don't recommend configuring them for other platforms.

Default settings for interfaces

This section lists default settings for interfaces.

Default state of interfaces

The default state of an interface depends on the type.

- Physical interfaces—Disabled. The exception is the Management interface that is enabled for initial setup. Physical interfaces includes switch ports.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- EtherChannel port-channel interfaces (ISA 3000)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Firepower and Secure Firewall models)—Disabled.

Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and in the Firewall Management Center. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and Firewall Management Center.

Default speed and duplex

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

By default, the speed and duplex for fiber (SFP) interfaces are set to the maximum speed, with auto-negotiation enabled. If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the Threat Defense interface as well. For example,

N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, you must disable the default auto-negotiation on the platform and the switch for the port to be connected.

For the Secure Firewall 3100/4200 the speed is set to detect the installed SFP speed.

Create security zone and interface group objects

Create empty interface objects that can be populated with interfaces later, or create security zones while configuring interfaces to provide logical grouping and management of device interfaces.

Add security zones and interface groups to which you can assign device interfaces.

Tip You can create empty interface objects and add interfaces to them later. To add an interface, the interface must have a name. You can also create security zones (but not interface groups) while configuring interfaces.

Before you begin

Understand the usage requirements and restrictions for each type of interface object. See Security zones and interface groups, on page 607.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Interface**.

Step 2 Click **Add** > **Security Zone** or **Add** > **Interface Group**.

Step 3 Enter a **Name**.

Do not use the same name as a network or port object. These object names are deployed to the device, and duplicate names result in a failed deployment.

Step 4 Choose an **Interface Type**.

Step 5 (Optional) From the **Device** > **Interfaces** drop-down list, choose a device that contains interfaces you want to add.

You do not need to assign interfaces on this screen; you can instead assign interfaces to the zone or group when you configure the interface.

Step 6 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Enable the physical interface and configure Ethernet settings

Before you begin

If you changed the physical interfaces on the device after you added it to the Firewall Management Center , you need to refresh the interface listing by clicking **Sync Interfaces from device** on the top left of **Interfaces** . For the 3100 /4200 , which supports hot swapping, see Network module management for Secure Firewall 3100/4200, on page 625 before you change interfaces on a device.

This section describes how to:

- Enable the physical interface. By default, physical interfaces are disabled (with the exception of the Management interface).
- Set a specific speed and duplex. By default, speed and duplex are set to Auto.

This procedure only covers a small subset of interface settings. Refrain from setting other parameters at this point. For example, you cannot name an interface that you want to use as part of an EtherChannel interface. The exact interface options vary depending on your model and interface type.

Note For the Firepower 4100/9300 , you configure basic interface settings in FXOS. See Configure a physical interface, on page 259 for more information.

Note For switch ports, see Configure switch ports, on page 650 .

You can also click the **Virtual Tunnels** tab to view details of dynamic and static VTIs of route-based VPNs on the device. For more information, see View virtual tunnel interface details, on page 1388 .

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** ( ) for the interface you want to edit.

Step 3 Enable the interface by checking the **Enabled** check box.

a) (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 4 (Optional) Set the duplex and speed by clicking **Hardware Configuration** > **Speed** .

- **Duplex** —Choose **Full** or **Half** . SFP interfaces only support **Full** duplex.
- **Speed** —Choose a speed (varies depending on the model). For SFPs, choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always full, autonegotiation is enabled, and FEC is set to auto. For dual-speed transceivers, the lower speed is used. This option is

useful if you later change the network module to a different model, and want the speed to update automatically. Some switches and transceivers don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.

Note You cannot modify the speed of a high availability or a cluster control link interface.

- **Auto-negotiation** —Set the interface to negotiate the link status and flow control.

  Except for the 1100 and 2100 , autonegotiation is set separately from the speed. Some switches don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.

- **Forward Error Correction Mode** —For 25Gbps and higher interfaces, enable Forward Error Correction (FEC).

  For an EtherChannel member interface, configure FEC before adding it to the EtherChannel. If you remove the interface from EtherChannel and then reboot, reconfigure the FEC for the interface.

  Some switches don't support auto mode for FEC, especially for larger interfaces. Be sure to manually configure the setting, depending on the switch support. We don't recommend disabling FEC because the EtherChannel may not function correctly.

  The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 42: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC *x* M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

Note From Version 7.4.2, Firewall Threat Defense supports the SFP 10G_25G_CSR_S module. To avoid link-down issues after a reboot, Forward Error Correction (FEC) must be enabled on these interfaces.

Step 5 (Optional) Enable Link Layer Discovery Protocol (LLDP) by clicking **Hardware Configuration** > **Network Connectivity** .

- **Enable LLDP Receive** —Enables the firewall to receive LLDP packets from its peers.
- **Enable LLDP Transmit** —Enables the firewall to send LLDP packets to its peers.

Step 6 (Optional) Enable pause (XOFF) frames for flow control by clicking **Hardware Configuration** > **Network Connectivity** , and checking **Flow Control Send** .

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the threat defense port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.



Note The Firewall Threat Defense supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 7 In the **Mode** drop-down list, choose one of the following:

- **None** —Choose this setting for regular firewall interfaces and inline sets. The mode will automatically be changed to Routed, Switched, or Inline based on further configuration.
- **Passive** —Choose this setting for passive IPS-only interfaces.
- **Erspan** —Choose this setting for ERSPAN passive IPS-only interfaces.

Step 8 In the **Priority** field, enter a number ranging from 0–65535.

This value is used in the policy based routing configuration. The priority is used to determine how you want to distribute the traffic across multiple egress interfaces.

Step 9 Click **OK** .

Click **Save**.

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Continue configuring interfaces.

- Regular Firewall Interfaces, on page 649
- Inline Sets and Passive Interfaces, on page 727

Configure EtherChannel interfaces

This section tells how to configure EtherChannel interfaces.

Note For the Firepower 4100/9300, you configure EtherChannels in FXOS. Refer to Add an EtherChannel (port channel), on page 261 for more information.

About EtherChannels

This section describes EtherChannels.

EtherChannels

An 802.3ad EtherChannel is a logical interface, called a port-channel interface) that consists of a bundle of individual Ethernet links, known as a channel group. This approach increases the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Channel group interfaces

Channel group interfaces enable EtherChannel aggregation with specific capacity and configuration requirements. Understanding these interface specifications ensures proper EtherChannel deployment and performance.

Each channel group can have up to 8 active interfaces, except for the ISA 3000, which support 16 active interfaces. On switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group. Only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

The EtherChannel aggregates traffic across all the available active interfaces in the channel. A proprietary hash algorithm selects the interface, using criteria such as source or destination MAC addresses, IP addresses, TCP and UDP port numbers, and VLAN numbers.

EtherChannel connection to other devices

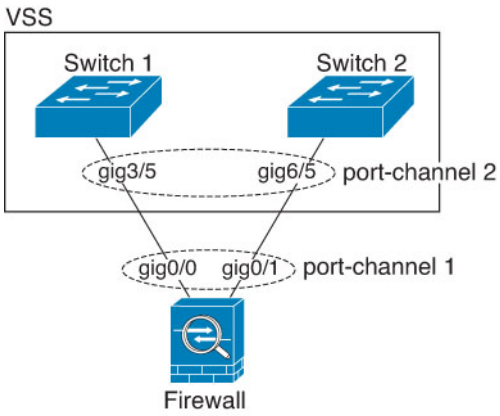
An EtherChannel connection to other devices requires the connected device to support 802.3ad EtherChannels for compatibility.

EtherChannel connection requirements and configurations

The device to which you connect the Firewall Threat Defense EtherChannel must also support 802.3ad EtherChannels. For example, you can connect to the Catalyst 6500 switch or the Cisco Nexus 7000.

When the switch is part of a Virtual Switching System (VSS) or Virtual Port Channel (vPC), you can connect Firewall Threat Defense interfaces within the same EtherChannel to separate switches in the VSS/vPC. The switch interfaces are members of the same EtherChannel port-channel interface because the separate switches act like a single switch.

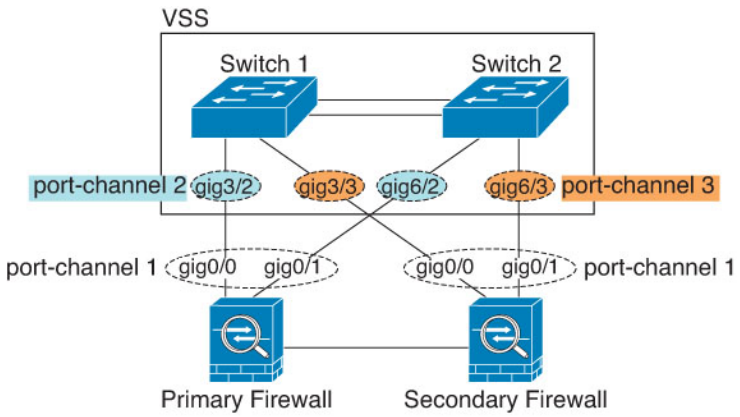
Figure 231: Connecting to a VSS/vPC



Note If the Firewall Threat Defense device is in transparent firewall mode, and you place the Firewall Threat Defense device between two sets of VSS/vPC switches, then be sure to disable Unidirectional Link Detection (UDLD) on any switch ports connected to the Firewall Threat Defense device with an EtherChannel. If you enable UDLD, then a switch port may receive UDLD packets sourced from both switches in the other VSS/vPC pair. The receiving switch will place the receiving interface in a down state with the reason "UDLD Neighbor mismatch".

If you use the Firewall Threat Defense device in an Active/Standby failover deployment, you need to create separate EtherChannels on the switches in the VSS/vPC, one for each Firewall Threat Defense device. On each Firewall Threat Defense device, a single EtherChannel connects to both switches. Even if you could group all switch interfaces into a single EtherChannel connecting to both Firewall Threat Defense devices,the EtherChannel would not be established because of the separate Firewall Threat Defense system IDs. Also, using a single EtherChannel would not be desirable because you do not want traffic sent to the standby Firewall Threat Defense device.

Figure 232: Active/Standby failover and VSS/vPC



Link aggregation control protocol

The Link Aggregation Control Protocol (LACP) is a network protocol that aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP interface configuration modes

You can configure each physical interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- Passive—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel. Not supported on hardware models.
- On—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. "On" mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

Load balancing

Load balancing is a distribution mechanism that distributes packets to interfaces in the EtherChannel and ensures transparent failover when active interfaces go down by rebalancing traffic between remaining links.

Load balancing operation details

The Firewall Threat Defense device distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (this criteria is configurable). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a *hash_value* **mod** *active_links* result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

EtherChannel MAC address

An EtherChannel MAC address is a network identifier that is shared by all interfaces in the EtherChannel group. This makes the EtherChannel transparent to network applications and users by presenting one logical connection.

All interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links.

Platform-specific MAC address behavior

MAC address assignment for EtherChannel interface varies by hardware platform.

Firepower and Secure Firewall Hardware

The port-channel interface uses the MAC address of the internal interface Internal-Data 0/1. You can manually configure a MAC address for the port-channel interface if needed. All EtherChannel interfaces on a chassis use the same MAC address, so be aware that if you use SNMP polling, for example, multiple interfaces will have the same MAC address.



Note Member interfaces only use the Internal-Data 0/1 MAC address after a reboot. Prior to rebooting, the member interface uses its own MAC address. If you add a new member interface after a reboot, you will have to perform another reboot to update its MAC address.

Guidelines for EtherChannels and redundant interfaces

Provides essential configuration rules and limitations for implementing EtherChannels and redundant interfaces to maintain network stability and high availability.

Bridge Group

In routed mode, Firewall Management Center -defined EtherChannels are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.

High availability

- When you use an EtherChannel interface as a High availability link, it must be pre-configured on both units in the High availability pair; you cannot configure it on the primary unit and expect it to replicate to the secondary unit because the High availability link itself is required for replication .
- If you use an EtherChannel interface for the state link, no special configuration is required; the configuration can replicate from the primary unit as normal. For the Firepower 4100/9300 chassis , all interfaces, including EtherChannels, need to be pre-configured on both units.
- You can monitor EtherChannel interfaces for High availability . When an active member interface fails over to a standby interface, this activity does not cause the EtherChannel interface to appear to be failed when being monitored for device-level High availability . Only when all physical interfaces fail does the

EtherChannel interface appear to be failed (for an EtherChannel interface, the number of member interfaces allowed to fail is configurable) .

- If you use an EtherChannel interface for a High availability or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a High availability link. To alter the configuration, you need to temporarily disable High availability , which prevents High availability from occurring for the duration.

Model Support

- You cannot add EtherChannels in the Firewall Management Center for the Firepower 4100/9300 or the Firewall Threat Defense Virtual . The Firepower 4100/9300 supports EtherChannels, but you must perform all hardware configuration of EtherChannels in FXOS on the chassis.
- You cannot use Firepower 1010 or Secure Firewall 1210/1220 switch ports or VLAN interfaces in EtherChannels.

Clustering

- To configure a spanned EtherChannel or an individual cluster interface, see the clustering chapter.

General Redundant Interface Guidelines

- You can configure up to 8 redundant interface pairs.
- All the Firewall Threat Defense configuration refers to the logical redundant interface instead of the member physical interfaces.
- You cannot use a redundant interface as part of an EtherChannel, nor can you use an EtherChannel as part of a redundant interface. You cannot use the same physical interfaces in a redundant interface and an EtherChannel interface. You can, however, configure both types on the Firewall Threat Defense device if they do not use the same physical interfaces.
- If you shut down the active interface, then the standby interface becomes active.
- Redundant interfaces do not support the Management *slot* / *port* interfaces as members. You can, however, set a redundant interface comprised of non- Management interfaces as management-only.

General EtherChannel Guidelines

- You can configure up to 48 EtherChannels, depending on how many interfaces are available on your model.
- Each channel group can have up to 8 active interfaces, except for ASA models and the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.
- When you add the first member interface, it sets the required hardware properties of all member interfaces.
    - The media type of member interfaces can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix RJ-45 and SFP interfaces.

  - All interfaces must be set to the same speed and duplex.
  - The first interface sets the speed *capacity* , which cannot be changed later.

- The device to which you connect the Firewall Threat Defense EtherChannel must also support 802.3ad EtherChannels.
- The Firewall Threat Defense device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS **vlan dot1Q tag native** command, then the Firewall Threat Defense device will drop the tagged LACPDUs.
- The LACP rate depends on the model. When you set the rate (normal or fast), the device requests that rate from the connecting switch.
- In Cisco IOS software versions earlier than 15.1(1)S2, Firewall Threat Defense does not support connecting an EtherChannel to a switch stack. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time.
- Match the speed, duplex, and auto-negotiation settings on every EtherChannel member interface and its corresponding peer port. For a 10/100-Mbps member link, use auto-negotiation at both ends, or use the same fixed speed and duplex settings at both ends. If one end is fixed at full duplex while the other end uses auto-negotiation, the auto-negotiating side defaults to half duplex, resulting in a duplex mismatch.
- All the Firewall Threat Defense configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

Configure an EtherChannel

Create an EtherChannel port-channel interface to aggregate multiple physical interfaces into a single logical interface for increased bandwidth and redundancy.

This section describes how to create an EtherChannel port-channel interface, assign interfaces to the EtherChannel, and customize the EtherChannel.

Note For the Firepower 4100/9300, you configure EtherChannels in FXOS. See Add an EtherChannel (port channel), on page 261 for more information.

Before you begin

- When you add the first member interface, it sets the required hardware properties of all member interfaces. See Guidelines for EtherChannels and redundant interfaces, on page 617 for more details about member interface requirements.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.

Note If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

Follow these steps to configure an EtherChannel:

Procedure

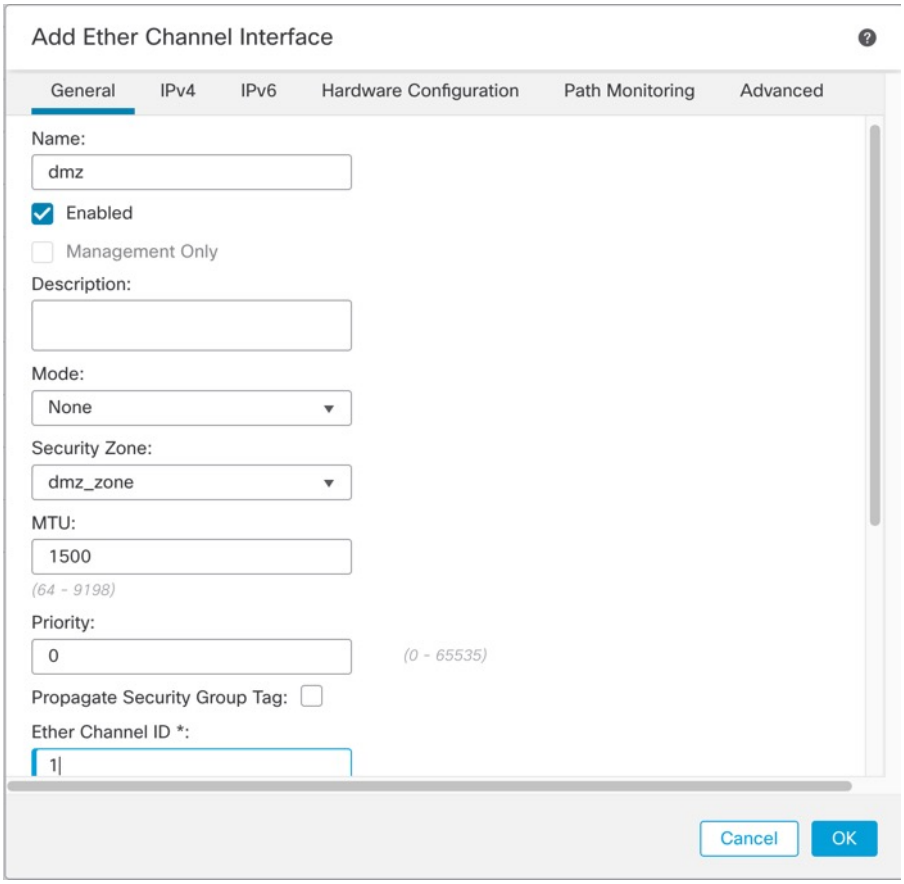
Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Enable the member interfaces according to Enable the physical interface and configure Ethernet settings, on page 611.

Step 3 Click **Add Interfaces** > **Ether Channel Interface**.

Step 4 On the **General** tab, set the **Ether Channel ID** to a number between 1 and 48 (1 and 8 for the Firepower 1010).

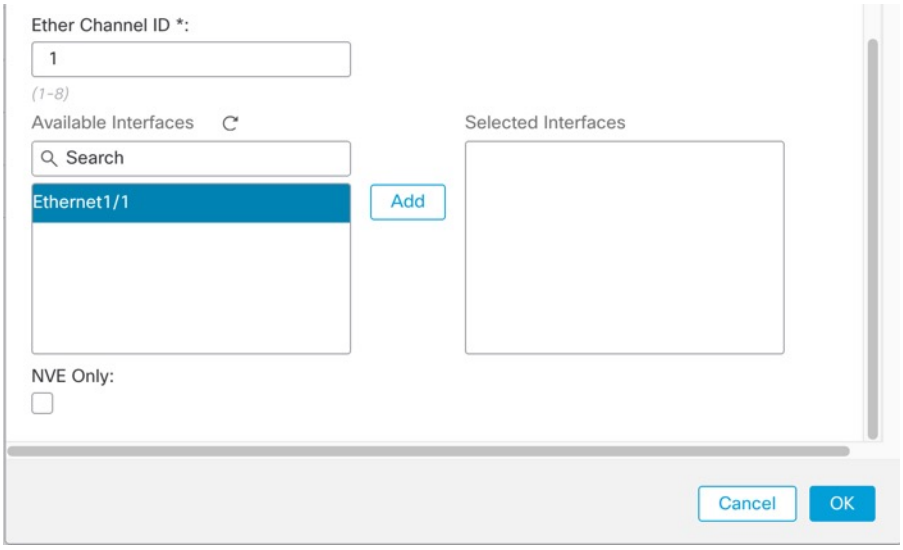
Figure 233: Add EtherChannel interface



Step 5 In the **Available Interfaces** area, click an interface and then click **Add** to move it to the **Selected Interfaces** area. Repeat for all interfaces that you want to make members.

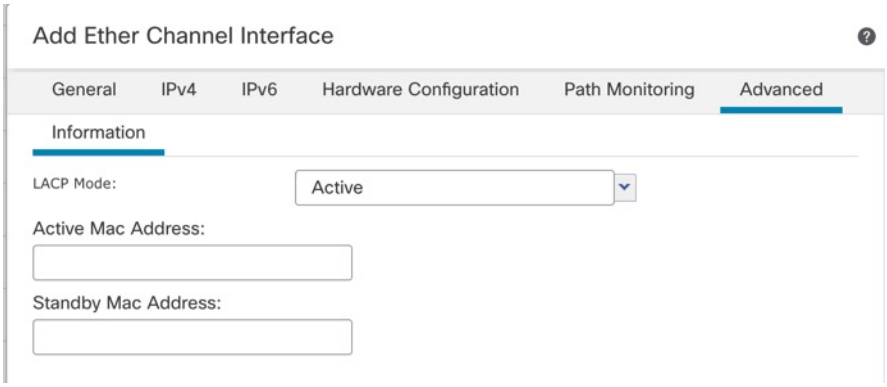
Make sure all interfaces are the same type and speed capability.

Figure 234: Available interfaces



Step 6 (Optional) Click the **Advanced** tab to customize the EtherChannel. Set the following parameters on the **Information** sub-tab:

Figure 235: Advanced



- (ISA 3000 only) **Load Balancing**—Select the criteria used to load balance the packets across the group channel interfaces. By default, the Firewall Threat Defense device balances the packet load on interfaces according to the source and destination IP address of the packet. If you want to change the properties on which the packet is categorized, choose a different set of criteria. For example, if your traffic is biased heavily towards the same source and destination IP addresses, then the traffic assignment to interfaces in the EtherChannel will be unbalanced. Changing to a different algorithm can result in more evenly distributed traffic. For more information about load balancing, see Load balancing, on page 616.
- **LACP Mode**—Choose Active, Passive, or On. We recommend using Active mode (the default). Passive mode is only available for the ISA 3000 only.
- (Secure Firewall 3100/4200 only) **LACP Rate**—Choose Default, Normal, or Fast. The defualt is Normal (also known as slow). Sets the LACP data unit receive rate for a physical interface in the channel group. We recommend that you set the same rate on both sides.

- (ISA 3000 only) **Active Physical Interface: Range**—From the left drop-down list, choose the minimum number of active interfaces required for the EtherChannel to be active, between 1 and 16. The default is 1. From the right drop-down list, choose the maximum number of active interfaces allowed in the EtherChannel, between 1 and 16. The default is 16. If your switch does not support 16 active interfaces, be sure to set this command to 8 or fewer.
- **Active MAC Address**—Set a manual MAC address if desired. The mac_address is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

Step 7 Click the **Hardware Configuration** tab and set the Duplex and Speed for all member interfaces.

Step 8 Click **OK**.

Step 9 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

For regular firewall interfaces:

- Add a VLAN subinterface. See Add a subinterface, on page 669.
- Configure the routed or transparent mode interface parameters: Configure routed mode interfaces, on page 690 or Bridge group interfaces, on page 695. For IPS-only interfaces, see Inline Sets and Passive Interfaces, on page 727.

Sync Interface Changes with the Firewall Management Center

Synchronize interface changes to ensure the Firewall Management Center and device configurations remain aligned when physical interfaces are added or removed.

Interface changes on the device can cause the Firewall Management Center and the device to get out of sync. The Firewall Management Center can detect interface changes by one of these methods:

- Event sent from the device
- Synchronize when you deploy from the Firewall Management Center

  If the Firewall Management Center detects interface changes when it attempts to deploy, the deployment will fail. You must first accept the interface changes.
- Manual synchronization

There are two types of interface changes performed outside of Firewall Management Center that need to be synchronized:

- Addition or deletion of physical interfaces—Adding a new interface, or deleting an unused interface has minimal impact on the Firewall Threat Defense configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the Firewall Threat Defense configuration, including access rules, NAT, SSL, identity rules,

VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the Firewall Management Center.

When the Firewall Management Center detects changes, the **Interface** page shows status (removed, changed, or added) to the left of each interface.

- Firewall Management Center access interface changes—If you configure a data interface for managing management center using the **configure network management-data-interface** command, you must manually make matching configuration changes in management center and then acknowledge the changes. These interface changes cannot be made automatically.

This procedure describes how to manually sync interface changes if required and how to acknowledge the detected changes. If interface changes are temporary, you should not save the changes in the Firewall Management Center; you should wait until the device is stable, and then re-sync.

Before you begin

- User roles:
  - Admin
  - Access Admin
  - Network Admin

Follow these steps to sync interface changes with the Firewall Management Center:

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 If required, click **Sync Device** on the top left of **Interfaces**.

Step 3 After the changes are detected, see these steps.

Addition or Deletion of Physical Interfaces

a) You will see a red banner on **Interfaces** indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

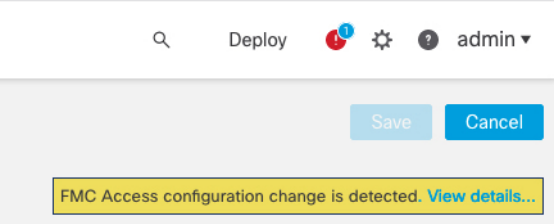
If there are any errors, you need to change your policy and rerun the validation.

c) Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

FMC Access Interface Changes

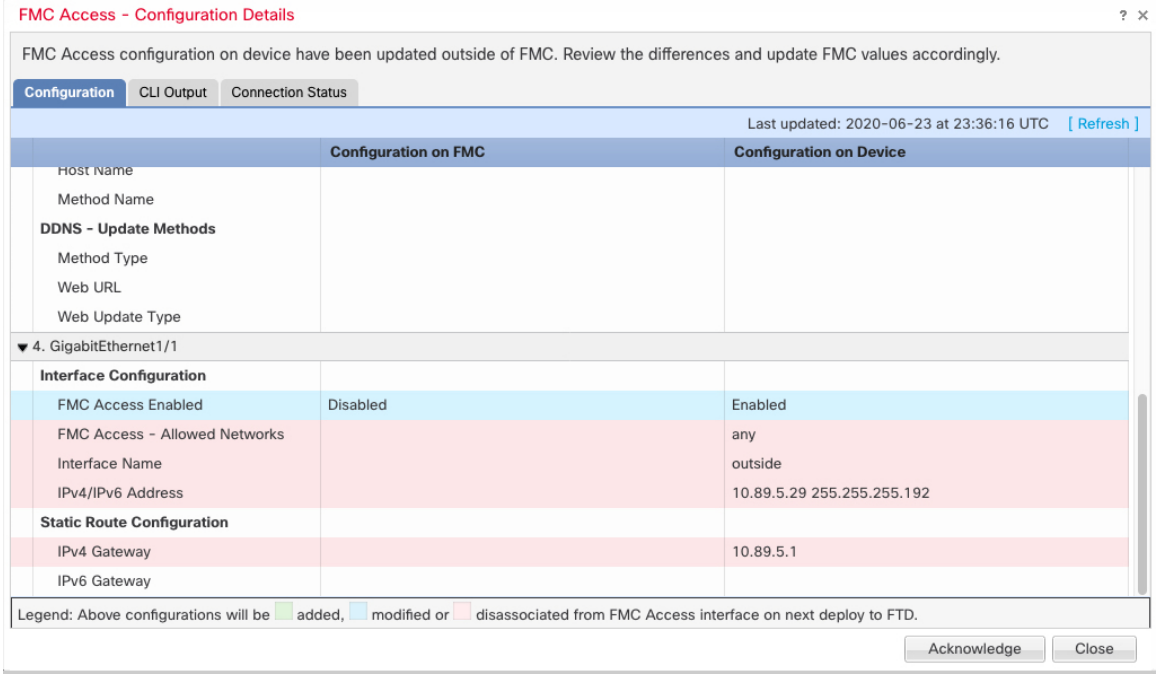
a) You will see a yellow banner in the top right of the **Device** page indicating that the Firewall Management Center access configuration has changed. Click the **View details** link to view the interface changes.



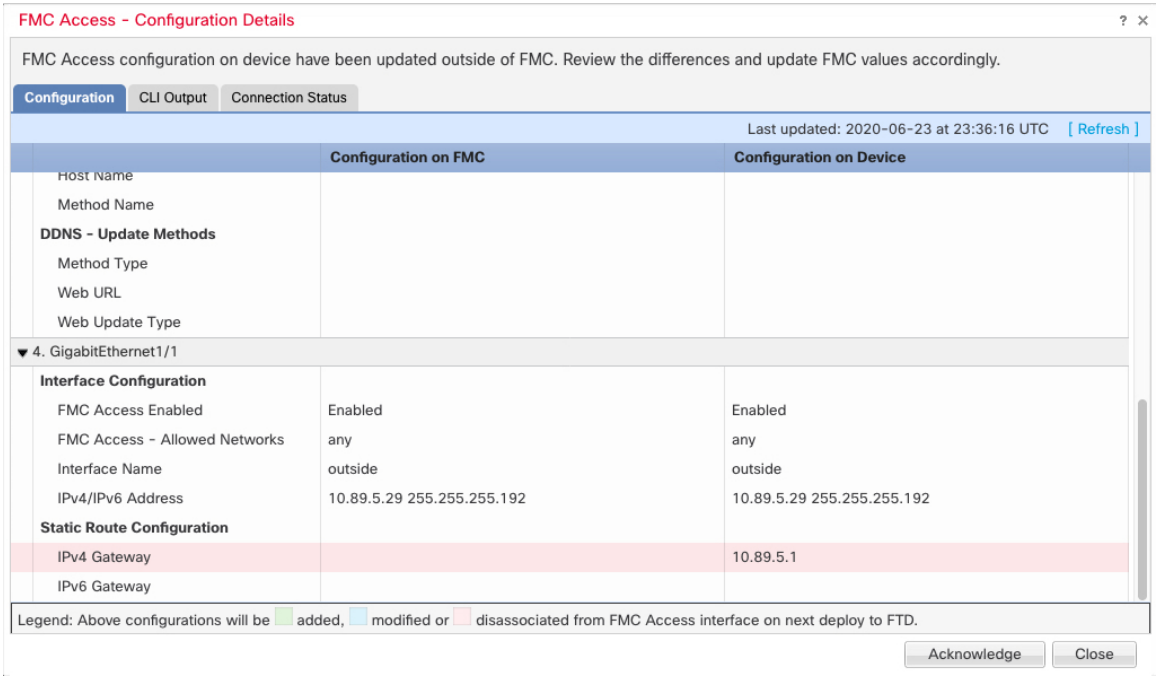
The **FMC Access - Configuration Details** dialog box opens.

b) Take note of all highlighted configurations, especially the pink highlighted ones. You need to match any values on the Firewall Threat Defense by manually configuring them on the Firewall Management Center.

For example, the pink highlights show configuration that exists on the Firewall Threat Defense but not yet on the Firewall Management Center.



This example shows this page after configuring the interface in Firewall Management Center; the interface settings match, and the pink highlight was removed.



c) Click **Acknowledge**.

We recommend that you do not click **Acknowledge** until you have finished the Firewall Management Center configuration, and are ready to deploy. Clicking **Acknowledge** removes the block on deployment. The next time you deploy, the Firewall Management Center configuration will overwrite any remaining conflicting settings on the Firewall Threat Defense. It is your responsibility to manually fix the configuration in the Firewall Management Center before you re-deploy.

d) You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

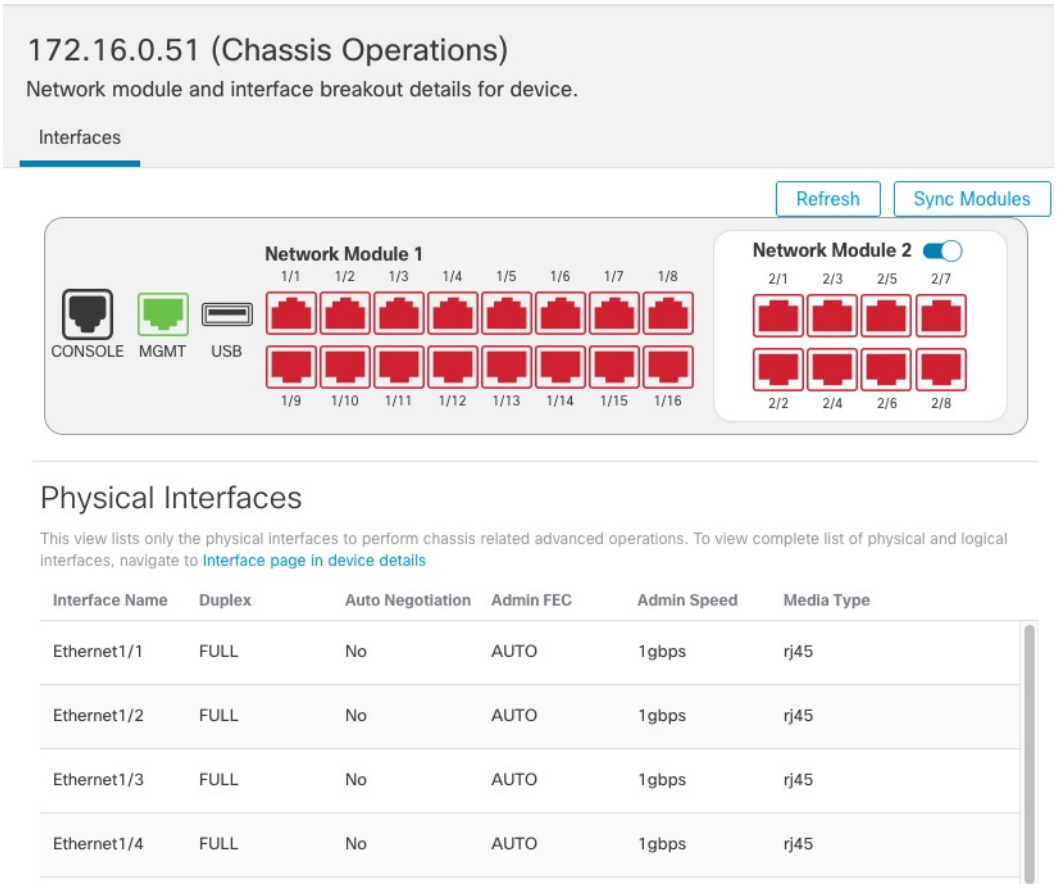
Network module management for Secure Firewall 3100/4200

If you install a network module before powering on the device, the network module becomes enabled and ready for use automatically.

Network module management operations

To view physical interface details for the device, and to manage the network module, open the **Chassis Operations** page. From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit. The **Chassis Operations** page opens for the device.

Figure 236: Chassis operations



Click **Refresh** to refresh interface status. Click **Sync Modules** if you made a hardware change on the device that you need to detect.

If you need to make changes to your network module installation after initial bootup, then see the following procedures.

Configure breakout ports

This task configures breakout ports to create smaller ports from 40GB or higher interfaces, allowing you to split a single high-capacity interface into multiple physical Ethernet ports that can be used like any other physical Ethernet port, including being added to EtherChannels.

You can configure smaller breakout ports for each 40GB or higher interface. This procedure tells you how to break out and rejoin the ports. The breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels. For example, you can break out four 10GB ports from a 40GB interface. The exact size and number of ports depends on your model.

Changes are immediate; you do not need to deploy to the device. After you break or rejoin, you cannot roll back to the previous interface state.

Before you begin

- You must use a supported breakout cable. See the hardware installation guide for more information.

- The interface cannot be in use for the following before breaking or rejoining:
  - Failover link
  - Cluster control link
  - Have a subinterface
  - EtherChannel member
  - BVI member
  - Manager access interface
- Breaking or rejoining an interface that is used directly in your security policy can impact the configuration; however, the action is not blocked.

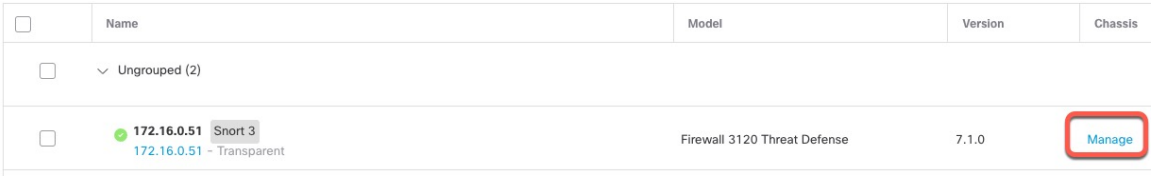
Follow these steps to configure breakout ports:

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column.

For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 237: Manage chassis



The **Chassis Operations** page opens for the device (in multi-instance mode, this page is called **Chassis Manager**). This page shows physical interface details for the device.

Step 2 Break out ports from a 40GB or higher interface.

a) Click **Break** ( ) to the right of the interface.

Click **Yes** on the confirmation dialog box. If the interface is in use, you will see an error message. You must resolve any use cases before you can retry the breakout.

For example, to break out the Ethernet2/1 40GB interface, the resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

On the interfaces graphic, a port that is broken out has this appearance:

Figure 238: Breakout ports



b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 239: Go to interface page



c) At the top of the **Interfaces** page, click **Click to know more**.

The **Interface Changes** dialog box opens.

Figure 240: View interface changes

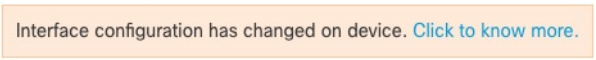
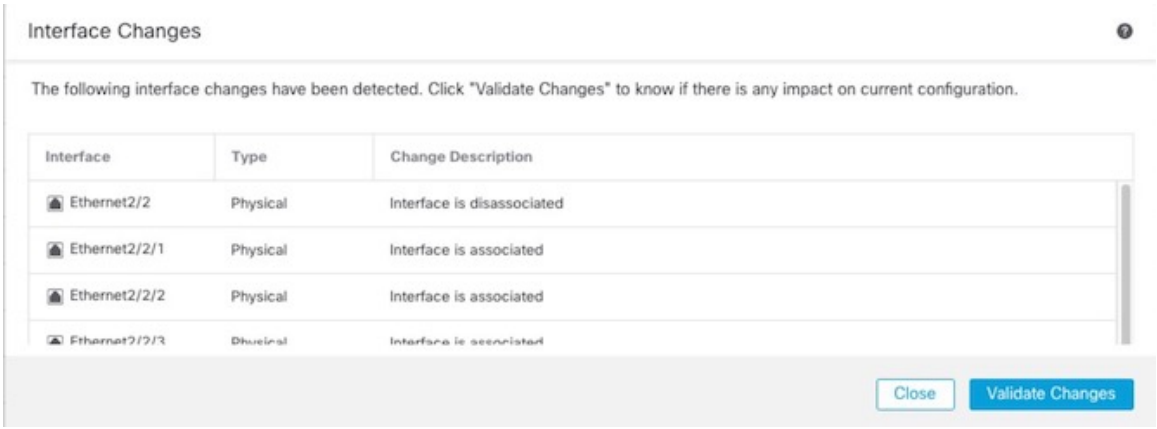


Figure 241: Interface changes



d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, change your policy and rerun the validation.

Replacing the parent interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Step 3 Rejoin breakout ports.

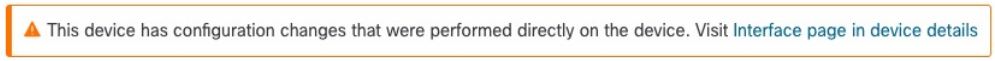
You must rejoin all child ports for the interface.

a) Click **Join** ( ) to the right of the interface.

Click **Yes** on the confirmation dialog box. If any child ports are in use, you will see an error message. You must resolve any use cases before you can retry the rejoin.

b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 242: Go to interface page



c) At the top of the **Interfaces** page, click **Click to know more**.

The **Interface Changes** dialog box opens.

Figure 243: View interface changes

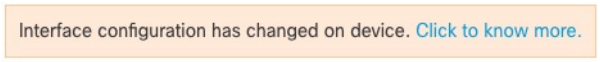
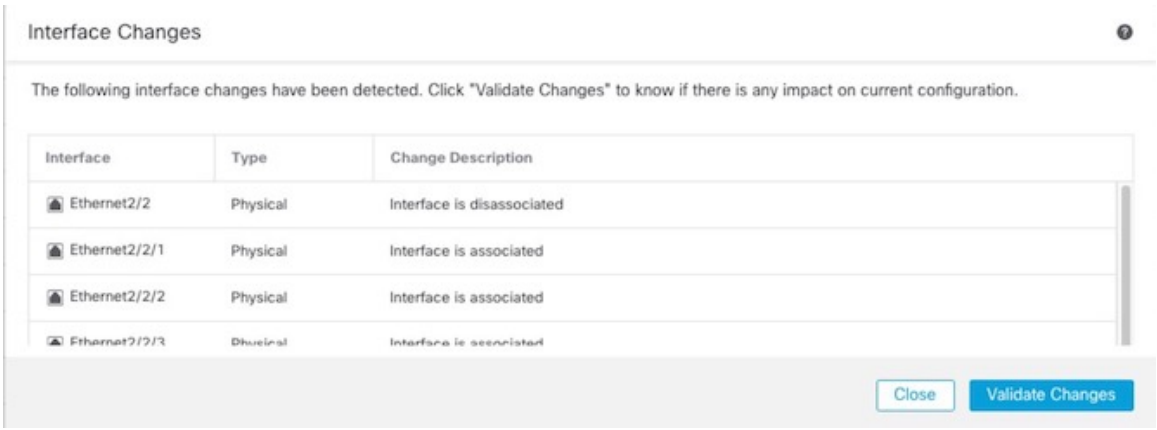


Figure 244: Interface changes



d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Replacing the child interfaces that are used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Add a network module

This task enables you to add network module functionality to a firewall that is already operational, expanding its interface capabilities.

Adding a new module requires a reboot of the firewall system.

Procedure

Step 1 Install the network module according to the hardware installation guide.

For clustering or High Availability, install the network module on all nodes.

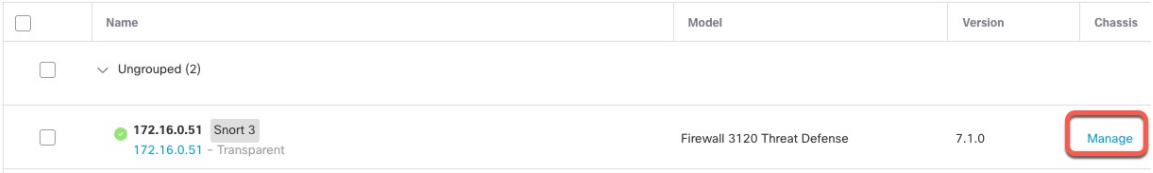
Step 2 Reboot the firewall; see Shut down or restart the device, on page 55.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node or active unit (see Switch the Active Peer in the Firewall Threat Defense High Availability Pair, on page 312), and reboot the former control node/active unit.

Step 3 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column.

For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 245: Manage chassis

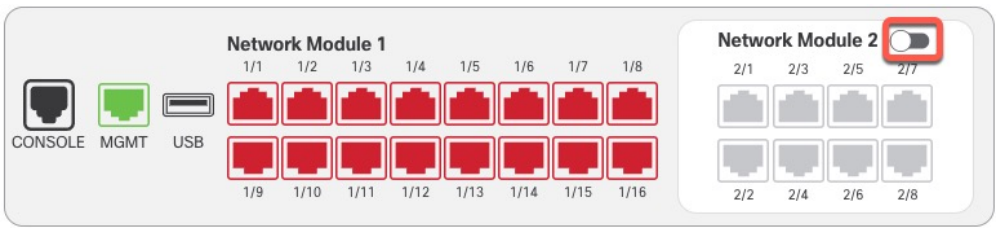


The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 4 Click **Sync Modules** to update the page with the new network module details.

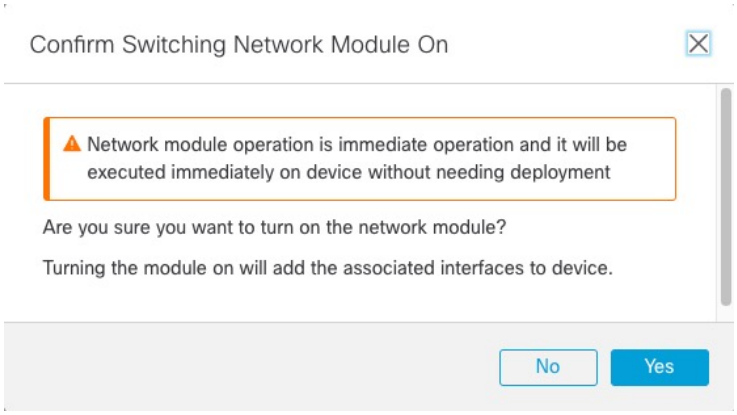
Step 5 On the interfaces graphic, click the slider ( ) to enable the network module.

Figure 246: Enable the network module



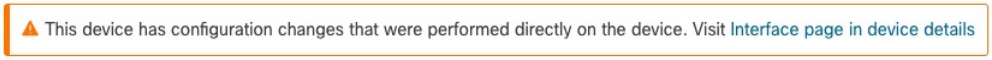
Step 6 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 247: Confirm enable



Step 7 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

Figure 248: Go to interface page



Step 8 (Optional) At the top of the **Interfaces** page, you see a message that the interface configuration has changed. You can click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 249: View interface changes

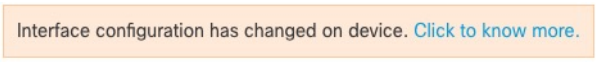
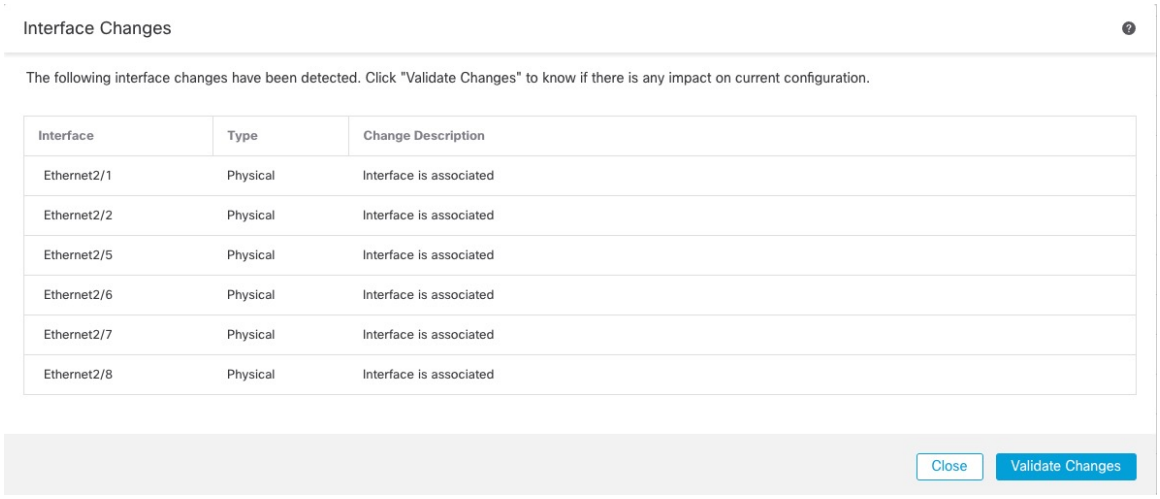


Figure 250: Interface changes



Click **Close** to return to the **Interfaces** page. (Because you are adding a new module, there shouldn't be any configuration impact, so you do not need to click **Validate Changes**.)

Step 9 Click **Save** to save the interface changes to the firewall.

Hot swap the network module

You can hot swap a network module for a new module of the same type without having to reboot.

You must shut down the current module to remove it safely. This procedure describes how to shut down the old module, install a new module, and enable it.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit. You cannot disable a network module if the cluster control link/failover link is on the module.

Procedure

Step 1 For clustering or High Availability, perform the following steps.

- **Clustering**—Ensure the unit you want to perform the hot swap on is a data node; then break the node so it is no longer in the cluster.

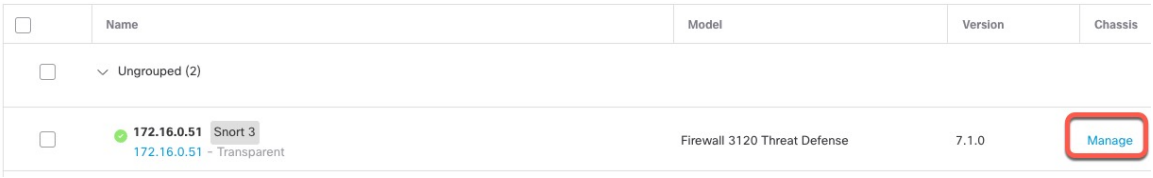
  You will add the node back to the cluster after you perform the hot swap. Alternatively, you can perform all operations on the control node, and the network module changes will sync to all data nodes. However, you will lose use of those interfaces on all nodes during the hot swap.

- **High Availability**—To avoid failing over when you disable the network module:
  - If the failover link is on the network module, you must break High Availability. See Break a high availability pair, on page 316. Disabling the network module with an active failover link is not allowed.
  - Disable interface monitoring for interfaces on the network module. See Configure standby IP addresses and interface monitoring, on page 309.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column.

For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

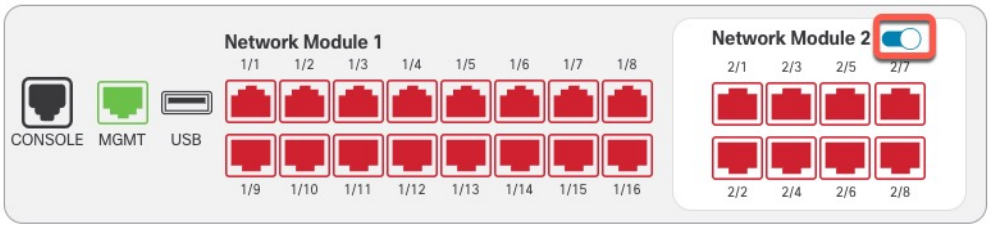
Figure 251: Manage chassis



The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider ( ) to disable the network module.

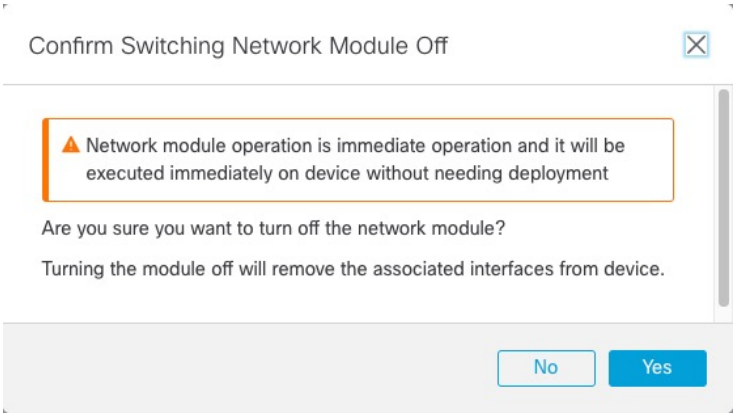
Figure 252: Disable the network module



Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

Step 4 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

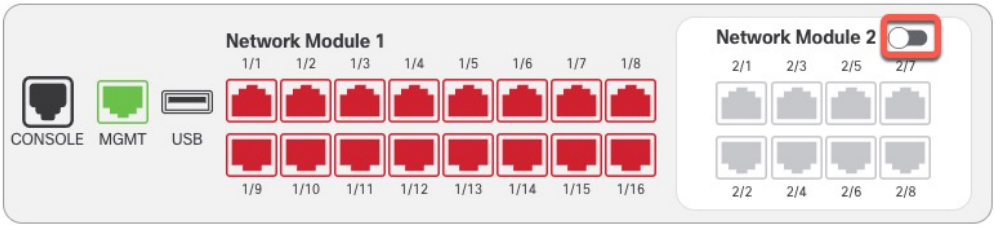
Figure 253: Confirm disable



Step 5 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

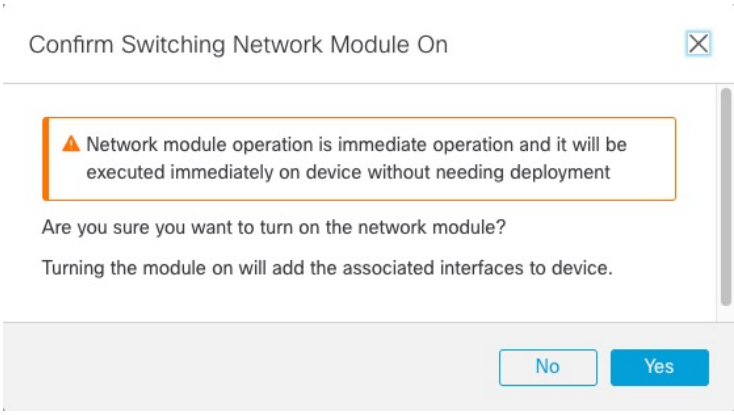
Step 6 In the Firewall Management Center, enable the new module by clicking the slider ( ).

Figure 254: Enable the network module



Step 7 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 255: Confirm enable



Step 8 For clustering or High Availability, perform the following steps.

- **Clustering**—Add the node back to the cluster.
- **High Availability**—
  - If you broke High Availability, then reform High Availability. See Add a high availability pair, on page 306.
  - Reenable interface monitoring for interfaces on the network module. See Configure standby IP addresses and interface monitoring, on page 309.

Replace the network module with a different type

Replace an existing network module with a different type to accommodate new interface requirements or hardware upgrades.

If you replace a network module with a different type, then a reboot is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present.

For clustering or High Availability, you can only perform chassis operations on the control node or active unit.

Before you begin

For High Availability, you cannot disable a network module if the failover link is on the module. You will have to break the high availability pair (see Break a high availability pair, on page 316), which means you will have downtime when you reboot the active unit. After the units finish rebooting, you can reform High Availability.

Follow these steps to replace the network module with a different type:

Procedure

Step 1 For clustering or High Availability, perform the following steps.

- **Clustering**—To avoid downtime, you can break each node one at a time so it is no longer in the cluster when you perform the network module replacement.

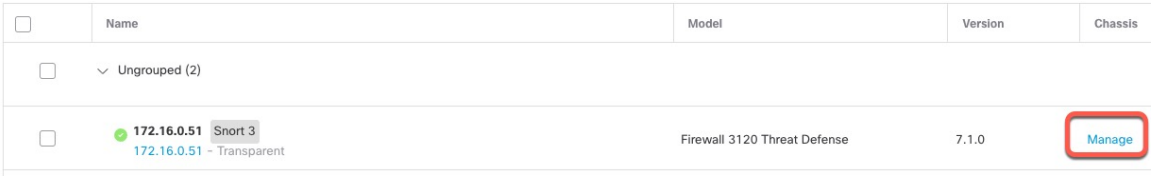
  Add the node back to the cluster after the replacement.

- **High Availability**—To avoid failing over when you replace the network module, disable interface monitoring for interfaces on the network module. See Configure standby IP addresses and interface monitoring, on page 309.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column.

For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 256: Manage chassis



The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider ( ) to disable the network module.

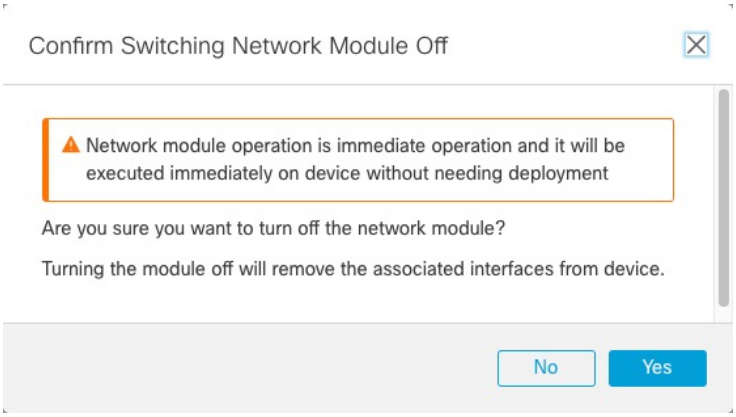
Figure 257: Disable the network module



Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

a) You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 258: Confirm disable



Step 4 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

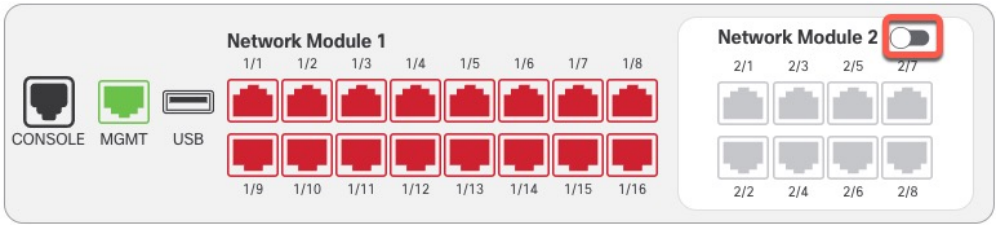
Reboot the firewall. Refer to Shut down or restart the device, on page 55 for guidance.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node or active unit (see Switch the Active Peer in the Firewall Threat Defense High Availability Pair, on page 312), and reboot the former control node/active unit.

Step 5 In the Firewall Management Center, click **Sync Modules** to update the page with the new network module details.

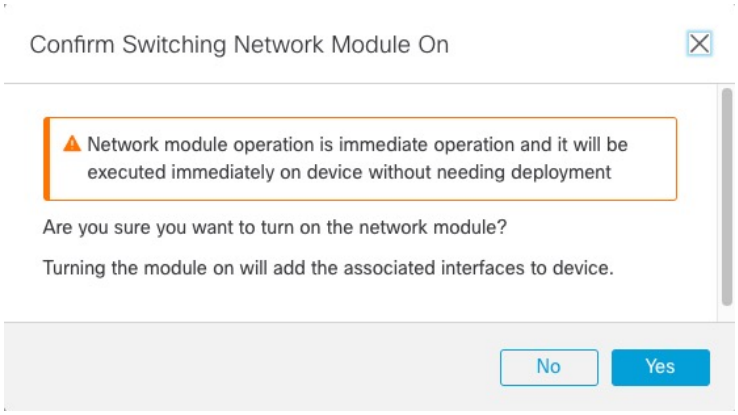
Step 6 Enable the new module by clicking the slider ( ).

Figure 259: Enable the network module



a) Click **Yes** when prompted to confirm that you want to turn the network module on.

Figure 260: Confirm enable



Step 7 Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 261: Go to interface page



Step 8 If the network module has *fewer* interfaces:

a) At the top of the **Interfaces** page, click **Click to know more**.

The **Interface Changes** dialog box opens.

Figure 262: View interface changes

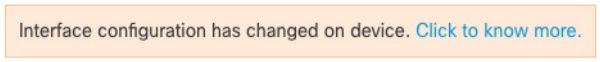
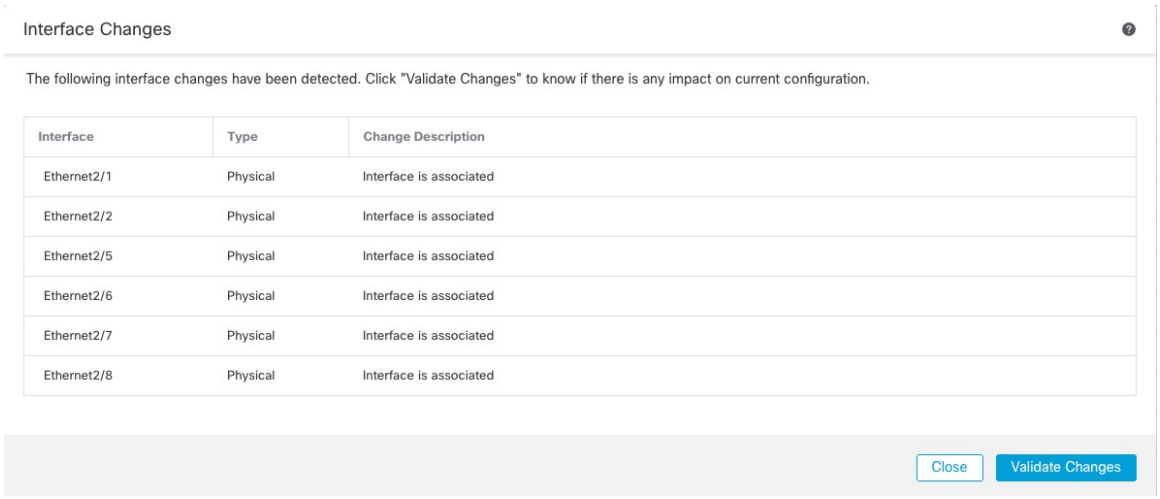


Figure 263: Interface changes



b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 9 To change the interface speed, see Enable the physical interface and configure Ethernet settings, on page 611.

The default speed is set to Detect SFP, which detects the correct speed from the SFP installed. You only need to fix the speed if you manually set the speed to a particular value and you now need a new speed.

Click **Save** to save the interface changes to the firewall.

What to do next

- If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.
- For clustering, add the node back to the cluster.
- For high availability, reenable interface monitoring for interfaces on the network module. See Configure standby IP addresses and interface monitoring, on page 309.

Remove the network module

Remove a network module permanently from the chassis when it is no longer needed or requires replacement.

If you want to permanently remove the network module, follow these steps. Removing a network module requires a reboot.

For clustering or High Availability, you can only perform chassis operations on the control node or active unit.

Before you begin

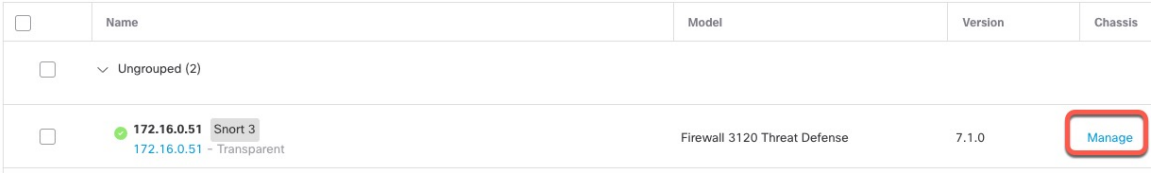
For clustering or High Availability, make sure the cluster or failover link is not on the network module.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column.

For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

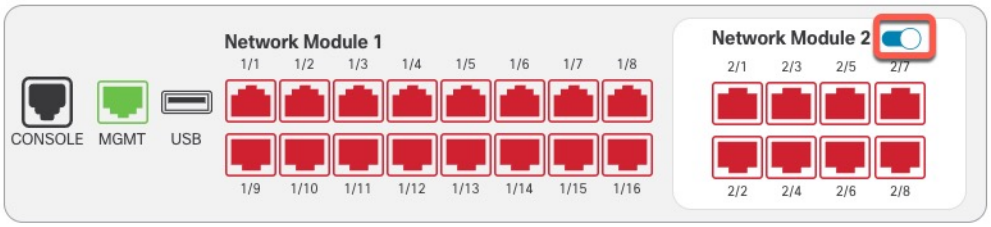
Figure 264: Manage chassis



The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

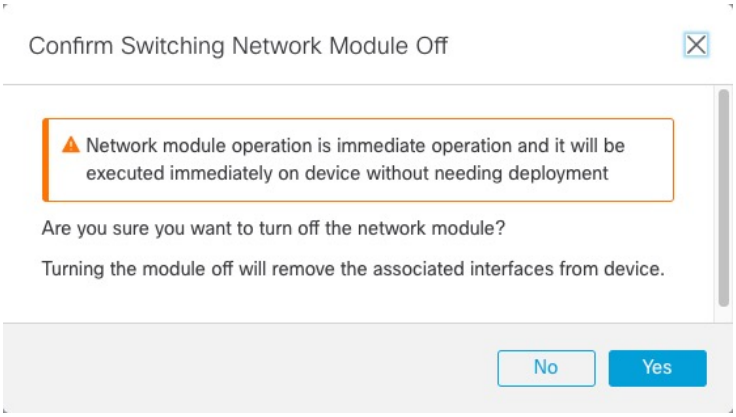
Step 2 On the interfaces graphic, click the slider ( ) to disable the network module.

Figure 265: Disable the network module



Step 3 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 266: Confirm disable



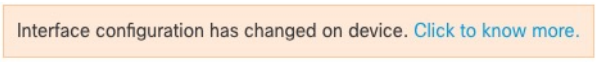
Step 4 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

Figure 267: Go to interface page



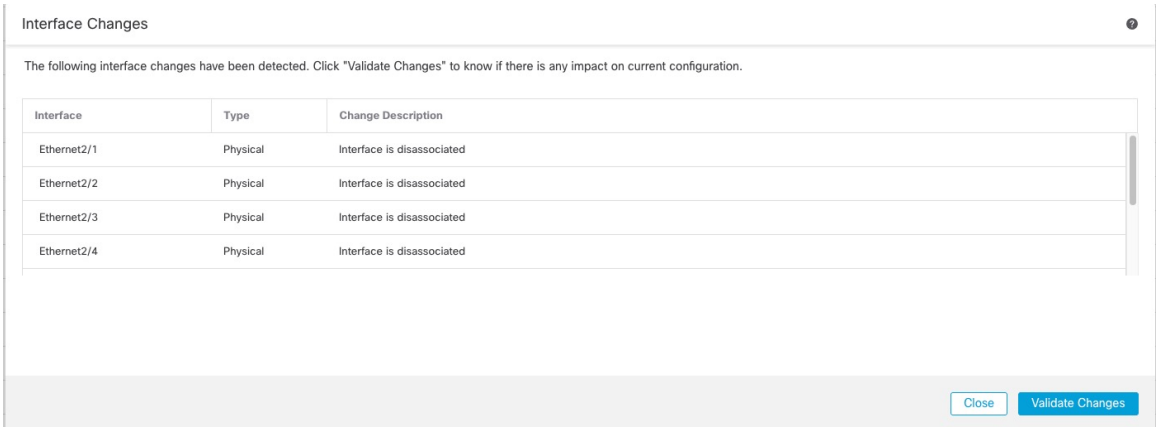
Step 5 At the top of the **Interfaces** page, you see a message that the interface configuration has changed.

Figure 268: View interface changes



a) Click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 269: Interface changes



b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 6 Click **Save** to save the interface changes to the firewall.

Step 7 If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

Step 8 Reboot the firewall; see Shut down or restart the device, on page 55.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control node or active unit (see Switch the Active Peer in the Firewall Threat Defense High Availability Pair, on page 312), and reboot the former control node/active unit.

Merge the management and diagnostic interfaces

This task merges the Management and Diagnostic interfaces on devices that have existing Diagnostic interface configurations that prevent automatic merging.

Starting with version 7.4, Firewall Threat Defense supports a merged Management and Diagnostic interface. "If your configuration uses the Diagnostic interface, the interfaces are not merged automatically. You must perform this procedure to complete the merge. This procedure requires you to acknowledge configuration changes and, in some cases, manually fix the configuration.

The Backup/Restore and Firewall Management Center configuration rollback functions save and restore the merged state, whether it is non-merged or merged. For example, if you merge the interfaces and then restore an old non-merged configuration, the restored configuration will be in a non-merged state.

This table shows the available configuration on the legacy Diagnostic interface, and how the merge is completed.

Before you begin

- To view the current mode of the device, enter the **show management-interface convergence** command at the Firewall Threat Defense CLI. The following output shows that the Management interfaces are merged:

```
> show management-interface convergence
management-interface convergence
>
```

  The following output shows that the Management interfaces are not merged:

```
> show management-interface convergence
no management-interface convergence
>
```

- For High Availability pairs and clusters, perform this task on the active/control unit. The merged configuration will be replicated automatically to the standby/data units.

Follow these steps to merge the Management and Diagnostic interfaces:

Procedure

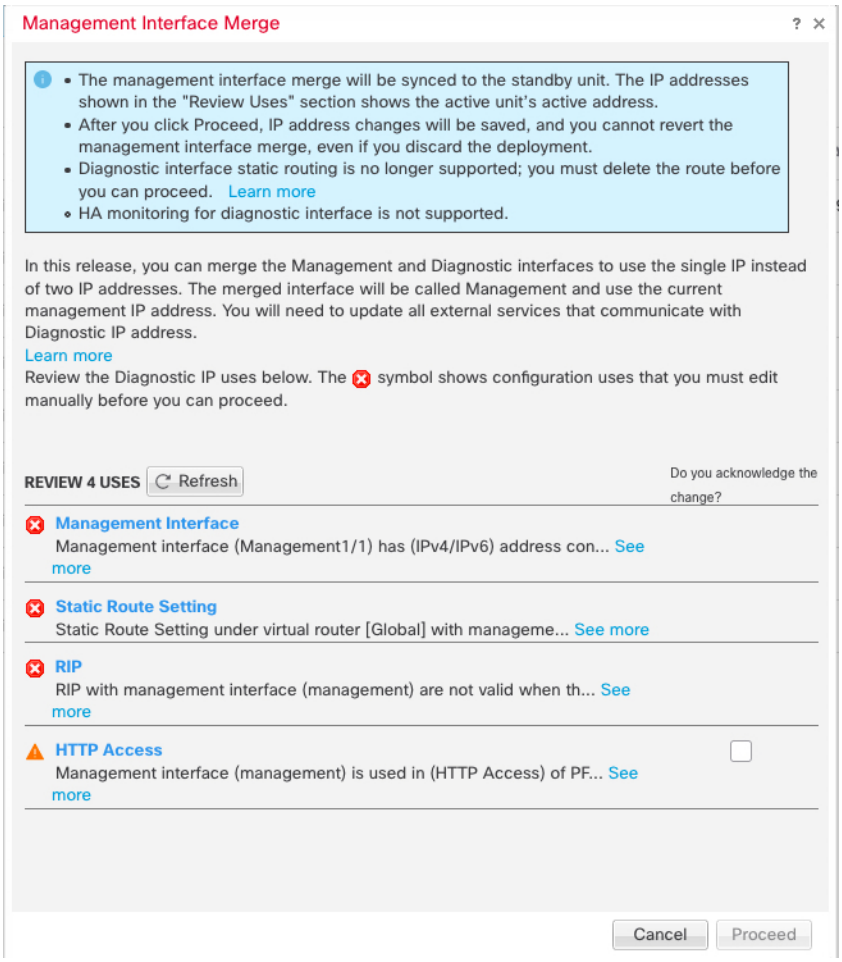
Step 1 Choose **Devices** > **Device Management**, and click **Edit** ( ) for your Firewall Threat Defense. The **Interfaces** page is selected by default. .

Step 2 Edit the Diagnostic interface, and remove the IP address.

You cannot complete the merge until after you have removed the Diagnostic IP address.

Step 3 Click **Management Interface Merge** in the **Management Interface action needed** area.

The **Management Interface Merge** dialog box shows all the occurrences of the Diagnostic interface in the configuration. For any occurrences that require you to manually remove or change the configuration, they will appear with a warning icon. Platform Settings that will no longer work on your device are marked with a caution icon and require your acknowledgement.



Step 4 If you need to manually remove or change any listed configurations, do the following.

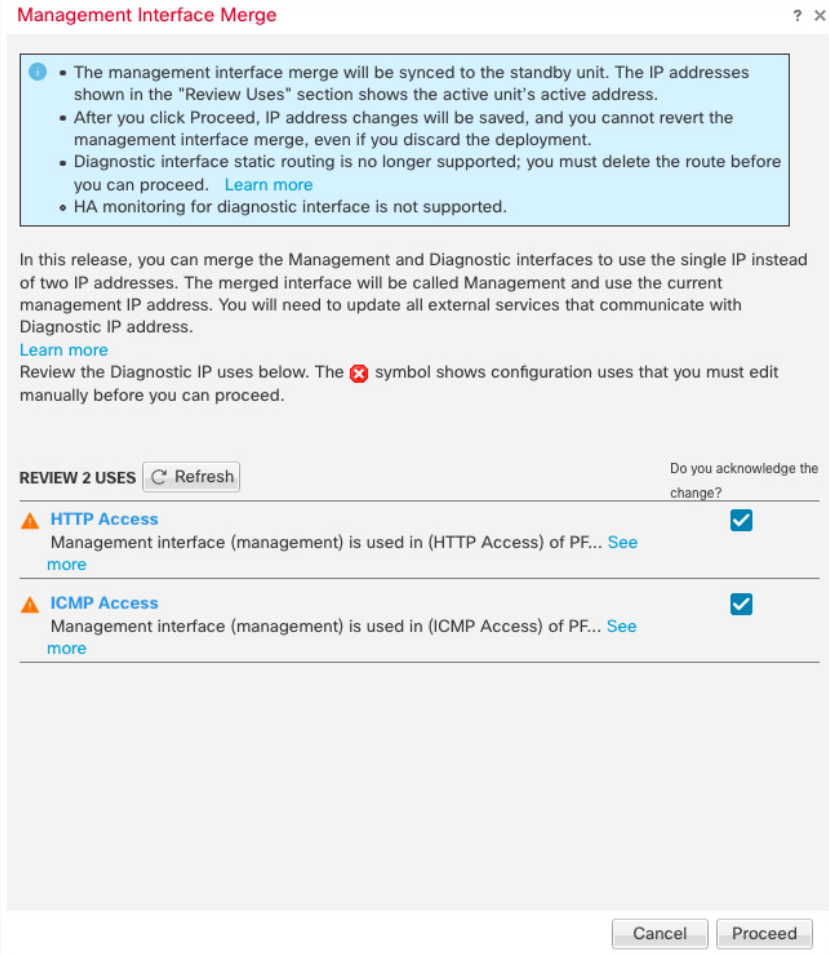
a) Click **Cancel** to close the **Management Interface Merge** dialog box.

b) Navigate to the feature area. You can then delete the item, or choose a data interface instead.

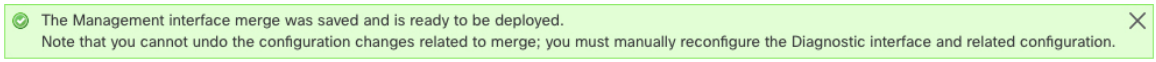
c) Reopen the **Management Interface Merge** dialog box.

There should no longer be any warnings.

Step 5 For each configuration caution, click the box in **Do you acknowledge the change?** column, and then click **Proceed**.



After the configuration is merged, you see a success banner:



Step 6 Deploy the new merged configuration.

Caution After you deploy the merged configuration, you can unmerge the interfaces from Firewall Management Center; however the Diagnostic interface will have to be reconfigured manually. See Unmerge the management interface, on page 644. Also, if you restore a configuration that is unmerged, or roll back to an unmerged configuration, then the device will revert to that unmerged configuration.

After the merge, the Management interface is shown on the **Interfaces** page, although it is read-only.

Step 7 After the merge, if you had any external services that communicated with the Diagnostic interface, you need to change their configuration to use the Management interface IP address.

For example:

- SNMP client

- RADIUS server—RADIUS servers often verify the IP address for incoming traffic, so you need to change that IP address to the Management address. Moreover, for a High Availability pair, you need to allow both the primary and secondary Management IP addresses; the Diagnostic interface used to support a single "floating" IP address that stayed with the active unit, but Management does not support that functionality.

Unmerge the management interface

This task separates the merged Management and Diagnostic interface into two distinct interfaces. This is useful when migrating network configurations or when separate interface management is required for specific network architectures.

The Firewall Threat Defense 7.4 and later supports a merged Management and Diagnostic interface. If you need to unmerge your interfaces, perform this procedure. We recommend using unmerged mode temporarily while you migrate your network to a merged mode deployment. Separate Management and Diagnostic interfaces may not be supported in all future releases.

Unmerging the interfaces does not restore your original Diagnostic configuration (if you upgraded and then merged your interfaces). You will need to reconfigure the Diagnostic interface manually. Also, the Management interface will now be named "management"; you cannot rename it "diagnostic."

Alternatively, if you used the Backup function to save an old unmerged configuration, you can restore that configuration or you can use the or Firewall Management Center configuration rollback feature, and the device will be in an unmerged state with the Diagnostic configuration intact.

Before you begin

- To view the current mode of the device, enter the **show management-interface convergence** command at the Firewall Threat Defense CLI. The following output shows that the Management interfaces are merged:

```
> show management-interface convergence
management-interface convergence
>
```

  The following output shows that the Management interfaces are not merged:

```
> show management-interface convergence
no management-interface convergence
>
```

- For High Availability pairs and clusters, perform this task on the active/control unit. The merged configuration will be replicated automatically to the standby/data units.

Follow these steps to unmerge the Management Interface:

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** ( ) for your Firewall Threat Defense. The **Interfaces** page is selected by default.

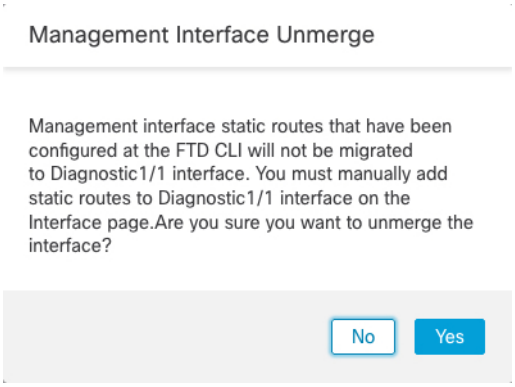
Step 2 For the Management interface, click **Unmerge Management Interface** ( ).

Figure 270: Management interface selection



Step 3 Click **Yes** to confirm that you want to unmerge the interface.

Figure 271: Unmerge confirmation



Step 4 Deploy the new unmerged configuration.

Note If you restore a configuration that is merged, or roll back to a merged configuration, then the device will revert to that merged configuration.

After the merge, the Management interface is no longer shown on the **Interfaces** page.

History for interfaces

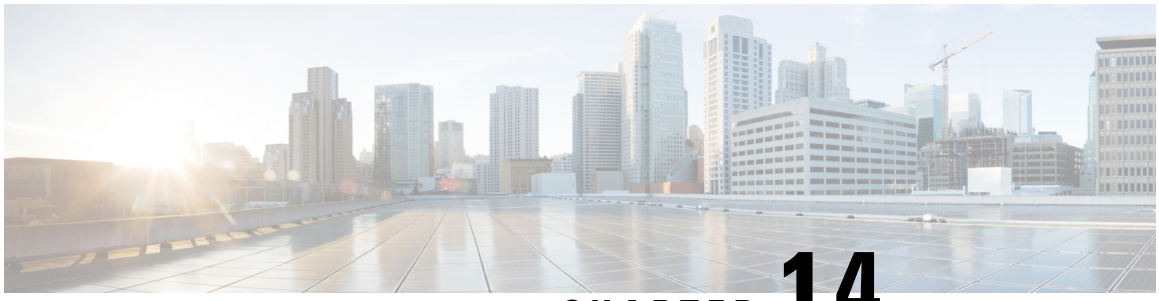
This reference provides the complete version history for interface-related features, enhancements, and changes across different versions of the Secure Firewall system.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Loopback and Management type interface group objects	7.4.0	7.4.0	You can now create interface group objects that include only management-only interfaces or only loopback interfaces. You can then use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are supported for any feature that supports loopback interfaces. Note that DNS does not support management interfaces. New/Modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged Management and Diagnostic interfaces	7.4.0	7.4.0	For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically. If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Note that support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. New/Modified screens: **Devices** > **Device Management** > **Interfaces** New/Modified commands: **show management-interface convergence**
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to Clause 108 RS-FEC from Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers	7.2.4	7.2.4	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to Clause 108 RS-FEC instead of Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers.
LLDP support for the Firepower 2100, Secure Firewall 3100	7.2.0	7.2.0	You can enable Link Layer Discovery Protocol (LLDP) for Firepower 2100 and Secure Firewall 3100 interfaces. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Network Connectivity** New/Modified commands: **show LLDP status**, **show LLDP neighbors**, **show LLDP statistics**
Pause Frames for Flow Control for the Secure Firewall 3100	7.2.0	7.2.0	If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Network Connectivity**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for hot swapping the network module for the Secure Firewall 3100	7.1.0	7.1.0	You can add or remove the network module on the Secure Firewall 3100 while the firewall is powered up. To replace a module with another module of the same type, you do not need to reboot. After initial bootup, adding a module, permanently removing a module, or replacing a module with a new type requires a reboot. New/Modified screens: **Devices** > **Device Management** > **Chassis Operations**
Support for Forward Error Correction for the Secure Firewall 3100	7.1.0	7.1.0	Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction (FEC). FEC is enabled by default and set to Auto. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **Hardware Configuration**
Support for setting the speed based on the SFP for the Secure Firewall 3100	7.1.0	7.1.0	The Secure Firewall 3100 supports speed detection for interfaces based on the SFP installed. Detect SFP is enabled by default. This option is useful if you later change the network module to a different model, and want the speed to update automatically. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **Hardware Configuration**
LLDP support for the Firepower 1100.	7.1.0	7.1.0	You can enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **LLDP** New/Modified commands: **show LLDP status**, **show LLDP neighbors**, **show LLDP statistics**
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved.	7.1.0	7.1.0	Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in Firewall Management Center, hardware changes are detected more effectively. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Speed** Supported platforms: Firepower 1000, 2100, Secure Firewall 3100

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Firepower 1100/2100 series fiber interfaces now support disabling auto-negotiation.	6.7.0	6.7.0	You can now configure a Firepower 1100/2100 series fiber interface to disable flow control and link status negotiation. Previously, when you set the fiber interface speed (1000 or 10000 Mbps) on these devices, flow control and link status negotiation was automatically enabled. You could not disable it. Now, you can deselect **Auto-negotiation** and set the speed to 1000 to disable flow control and link status negotiation. You cannot disable negotiation at 10000 Mbps. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Speed**



CHAPTER 14

Regular Firewall Interfaces

This chapter includes regular firewall Firewall Threat Defense interface configuration including EtherChannels, VLAN subinterfaces, IP addressing, and more.

Note For initial interface configuration on the Firepower 4100/9300, see Configure interfaces, on page 259.

- Requirements and prerequisites for regular firewall interfaces, on page 649
- Configure switch ports, on page 650
- Loopback interfaces, on page 661
- Guidelines for Loopback Interfaces, on page 662
- Configure a loopback interface, on page 662
- Rate-Limit traffic to the loopback interface, on page 663
- VLAN subinterfaces and 802.1Q trunking, on page 667
- Configure VXLAN Interfaces, on page 671
- Configure routed and transparent mode interfaces, on page 686
- Advanced interface settings, on page 711
- History for Regular Firewall Interfaces, on page 723

Requirements and prerequisites for regular firewall interfaces

This reference provides the requirements and prerequisites for configuring regular firewall interfaces, including supported models and required user roles.

Model support

Firewall Threat Defense

User roles

- Admin
- Access Admin
- Network Admin

Configure switch ports

For supported platforms, you can configure each interface to run as a regular firewall interface or as a Layer 2 hardware switch port. This section includes tasks for starting your switch port configuration, including enabling or disabling the switch mode and creating VLAN interfaces and assigning them to switch ports. This section also describes how to customize Power over Ethernet (PoE) on supported interfaces.

About switch ports

This section describes the switch ports for models with Layer 2 switches.

Switch ports and interfaces

Switch ports and firewall operate at different OSI layers to handle traffic forwarding.

Port and interface types

For each physical interface, you can set its operation as a firewall interface or as a switch port. This information describes physical interface and port types as well as logical VLAN interfaces to which you assign switch ports:

- Physical firewall interface—In routed mode, these interfaces forward traffic between networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces are bridge group members that forward traffic between the interfaces on the same network at Layer 2, using the configured security policy to apply firewall services. In routed mode, you can also use Integrated Routing and Bridging with some interfaces as bridge group members and others as Layer 3 interfaces. By default, the Ethernet 1/1 interface is configured as a firewall interface. You can also configure these interfaces to be IPS-only (passive interfaces).
- Physical switch port—Switch ports forward traffic at Layer 2, using the switching function in hardware. Switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the Firewall Threat Defense security policy. Access ports accept only untagged traffic, and you can assign them to a single VLAN. Trunk ports accept untagged and tagged traffic, and can belong to more than one VLAN. By default, Ethernet 1/2 and subsequent ports are configured as access switch ports on VLAN 1. You cannot configure the Management interface as a switch port.
- Logical VLAN interface—These interfaces operate the same as physical firewall interfaces, with the exception that you cannot create subinterfaces, IPS-only interfaces (inline sets and passive interfaces), or EtherChannel interfaces. When a switch port needs to communicate with another network, then the Firewall Threat Defense device applies the security policy to the VLAN interface and routes to another logical VLAN interface or firewall interface. You can even use Integrated Routing and Bridging with VLAN interfaces as bridge group members. Traffic between switch ports on the same VLAN are not subject to the Firewall Threat Defense security policy, but traffic between VLANs in a bridge group are subject to the security policy, so you may choose to layer bridge groups and switch ports to enforce the security policy between certain segments.

Power Over Ethernet

PoE is available on Ethernet 1/7 and Ethernet 1/8 using IEEE 802.3af (PoE) and 802.3at (PoE+) up to 30 watts per port.



Note PoE is not supported on the 1010E.

PoE+ uses Link Layer Discovery Protocol (LLDP) to negotiate the power level. Power is only supplied when needed.

If you shut down the interface, then you disable power to the device.

Auto-MDI/MDIX feature

Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase.

Auto-MDI/MDIX configuration details

For all switch ports, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. The interface enables Auto-MDI/MDIX when either the speed or duplex is set to auto-negotiate. If you set both the speed and duplex to fixed values, auto-negotiation is disabled, and Auto-MDI/MDIX is also disabled. When the speed and duplex are set to 1000 and full, the interface always auto-negotiates. Auto-MDI/MDIX enabled in this state, and disabling it is not possible.

Prerequisites for switch ports

This reference provides model support and other prerequisites for switch ports.

Model support

- Firepower 1010

Guidelines for switch ports

Context mode restrictions

Multiple context mode is not supported on several firewall models, with specific exceptions for the Secure Firewall 1210/1220.

- The Firepower 1010 does not support multiple context mode.
- The Secure Firewall 1210/1220 does not support multiple context mode.

High availability and clustering limitations

Do not use switch port functionality when using High availability because switch ports operate in hardware and continue to pass traffic on both active and standby units.

- No cluster support.
- Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. High availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High availability network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching

capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot. Theoretically, you can put a single switch port on a VLAN and successfully use High availability, but a simpler setup is to use physical firewall interfaces instead.

- You can only use a firewall interface as the failover link.

Logical VLAN interfaces (SVIs) configuration requirements

Ensure unique VLAN IDs between logical VLAN interfaces and VLAN subinterfaces on firewall interfaces to prevent conflicts.

- If you also use VLAN subinterfaces on a firewall interface, you cannot use the same VLAN ID as for a logical VLAN interface.
- MAC Addresses:
  - Routed firewall mode—All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See Configure the MAC address, on page 718.
  - Transparent firewall mode—Each VLAN interface has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See Configure the MAC address, on page 718.

Bridge groups restrictions

You cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.

VLAN interface and switch port unsupported features

VLAN interfaces and switch ports do not support these features.

- Dynamic routing
- Multicast routing
- Equal-Cost Multi-Path routing (ECMP)
- Inline sets or Passive interfaces
- EtherChannels—Switch ports cannot be part of an EtherChannel. PoE is also not supported on a port in an EtherChannel.
- Failover and state link
- Security group tagging (SGT)

Other guidelines and limitations

Configure a maximum of 60 named interfaces and ensure the Management interface is not configured as a switch port.

Default settings

Know the default interface assignments for each firewall model to properly plan your configuration.

- Ethernet 1/1 is a firewall interface.

- Ethernet 1/2 through Ethernet 1/8 are switch ports assigned to VLAN 1.
- Default Speed and Duplex—By default, the speed and duplex are set to auto-negotiate.

Configure switch ports and power over ethernet

To configure switch ports and PoE, complete the following tasks.

Enable or disable switch port mode

Set each interface independently to be either a firewall interface or a switch port based on your network requirements.

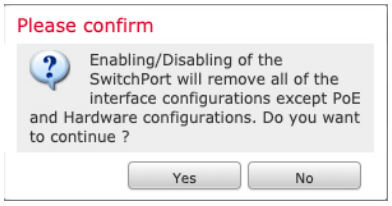
You can set each interface independently to be either a firewall interface or a switch port. By default, Ethernet 1/1 is a firewall interface, and the remaining Ethernet interfaces are configured as switch ports.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Set the switch port mode by clicking the slider in the **SwitchPort** column so it shows as **Slider enabled** ( ) or **Slider disabled** ( ).

By default, switch ports are set to access mode in VLAN 1. You must manually add a logical VLAN 1 interface (or whichever VLAN you set for these switch ports) for traffic to be routed and to participate in the Firewall Threat Defense security policy (see Configure a VLAN interface, on page 653). You cannot set the Management interface to switch port mode. When you change the switch port mode, all unsupported configuration is removed:



In addition, the interface is disabled if it was already enabled. Be sure to reenable the interface.

Configure a VLAN interface

Configure VLAN interfaces to enable traffic routing and participation in the Firewall Threat Defense security policy.

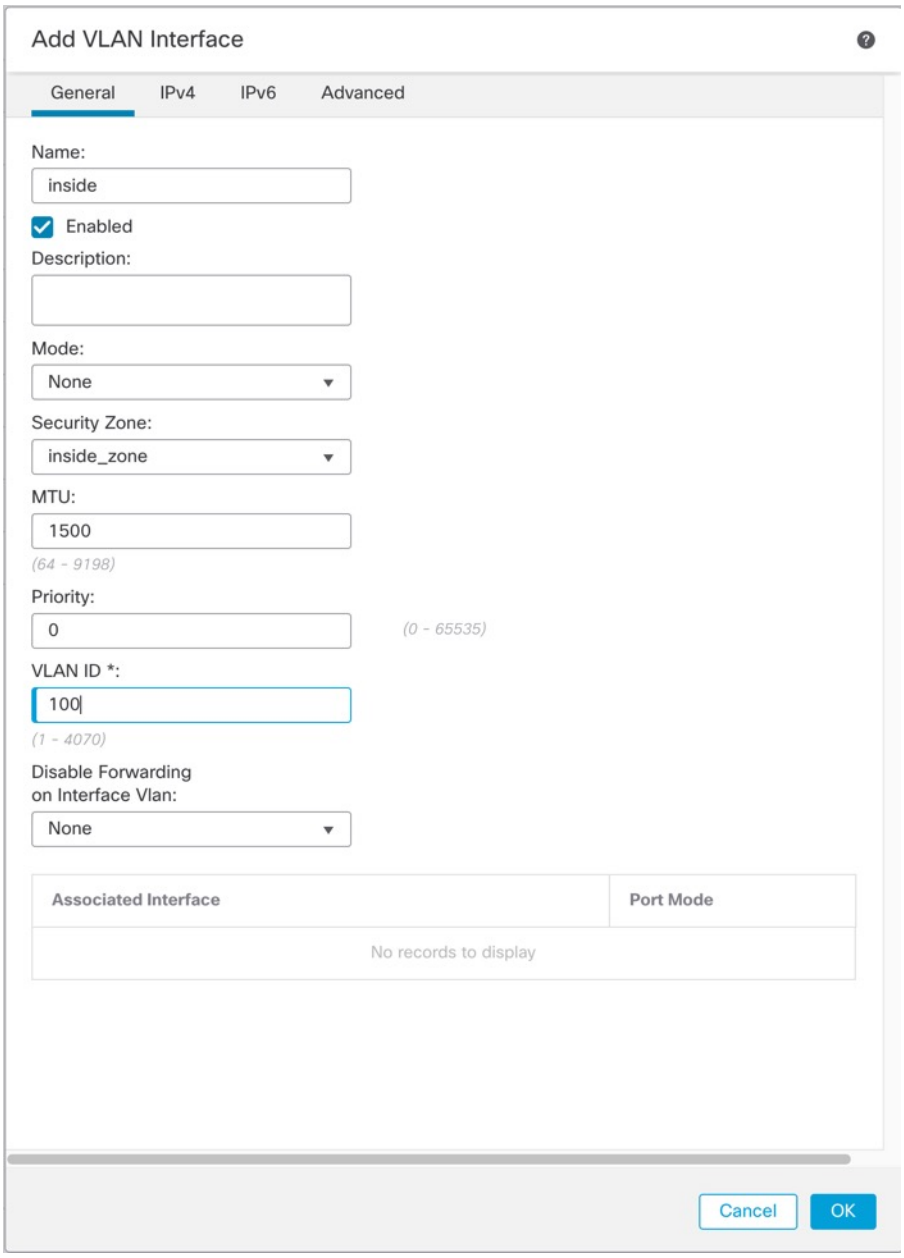
By default, switch ports are assigned to VLAN1; however, you must manually add the logical VLAN1 interface (or whichever VLAN you set for these switch ports) for traffic to be routed and to participate in the Firewall Threat Defense security policy.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Add Interfaces** > **VLAN Interface**.

Step 3 On **General**, set the following VLAN-specific parameters:



If you are editing an existing VLAN interface, the **Associated Interface** table shows switch ports on this VLAN.

a) Set the **VLAN ID** between 1 and 4070, excluding IDs in the range 3968 to 4047, which are reserved for internal use.

You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

b) (Optional) Choose a VLAN ID for **Disable Forwarding on Interface VLAN** to disable forwarding to another VLAN.

For example, you have one VLAN assigned to the outside for internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can disable forwarding on the home VLAN. The business network can access the home network, but the home network cannot access the business network.

Step 4 To complete the interface configuration, see one of these procedures:

- Configure routed mode interfaces, on page 690
- Configure general bridge group member interface parameters, on page 695

Step 5 Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure switch ports as access ports

Configure switch ports as access ports to assign them to a single VLAN for network segmentation and traffic management.

To assign a switch port to a single VLAN, configure it as an access port. Access ports accept only untagged traffic. By default, Ethernet 1/2 through Ethernet 1/8 switch ports are enabled and assigned to VLAN 1.

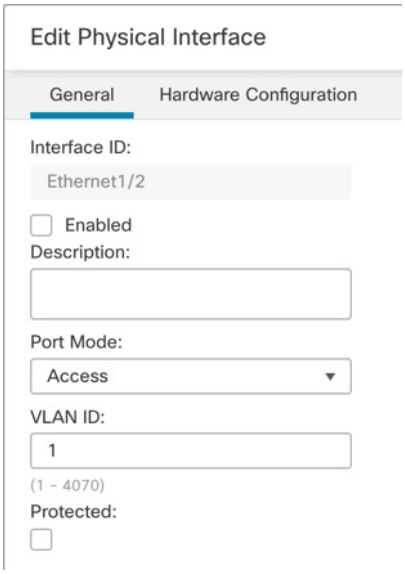
Note The device does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the Firewall Threat Defense does not end up in a network loop.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Figure 272: Edit physical interface



Step 3 Enable the interface by checking the **Enabled** check box.

Step 4 (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5 Set the **Port Mode** to **Access**.

Step 6 In the **VLAN ID** field, set the VLAN for this switch port, between 1 and 4070.

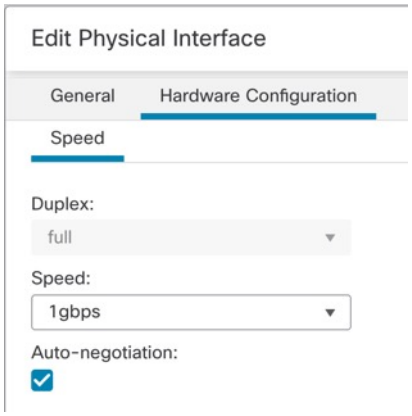
The default VLAN ID is 1.

Step 7 (Optional) Check the **Protected** check box to set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN.

You might want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you enable **Protected** on each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Step 8 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.

Figure 273: Hardware configuration



Check the **Auto-negotiation** check box (the default) to auto-detect the speed and duplex. If you uncheck it, you can set the speed and duplex manually:

- **Duplex**—Choose **Full** or **Half**.
- **Speed**—Choose **10mbps**, **100mbps**, or **1gbps**.

Note If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the Threat Defense interface as well. For example, N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, you must disable the default auto-negotiation on the platform and the switch for the port to be connected.

Step 9 Click **OK**.

Click **Save**.

What to do next

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure switch ports as trunk ports

This task creates a trunk port that can carry multiple VLANs using 802.1Q tagging.

This procedure describes how to create a trunk port that can carry multiple VLANs using 802.1Q tagging. Trunk ports accept untagged and tagged traffic. Traffic on allowed VLANs pass through the trunk port unchanged.

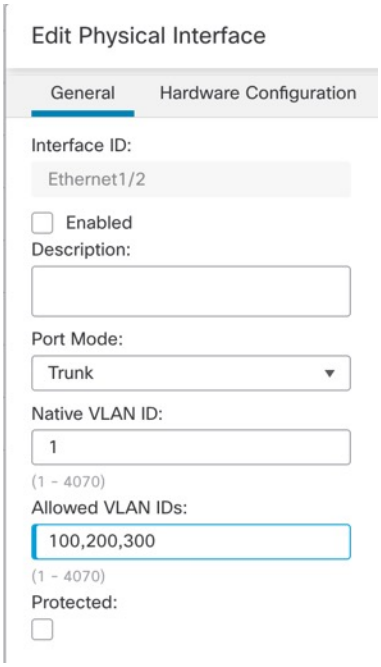
When the trunk receives untagged traffic, it tags it to the native VLAN ID so that the Firewall Threat Defense device can forward the traffic to the correct switch ports or can route it to another firewall interface. When the Firewall Threat Defense device sends native VLAN ID traffic out of the trunk port, it removes the VLAN tag. Be sure to set the same native VLAN on the trunk port on the other switch so that the untagged traffic will be tagged to the same VLAN.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Figure 274: Set trunk port mode



Step 3 Enable the interface by checking the **Enabled** check box.

Step 4 (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5 Set the **Port Mode** to **Trunk**.

Step 6 Set the VLAN IDs:

a) In the **Native VLAN ID** field, set the native VLAN for this switch port, between 1 and 4070.

The default native VLAN ID is 1.

Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.

b) In the **Allowed VLAN IDs** field, enter the VLANs for this trunk port between 1 and 4070.

You can identify up to 20 IDs in one of these ways:

- A single number (n)
- A range (n-x)

- Numbers and ranges separated by commas, for example:

  5,7-10,13,45-100

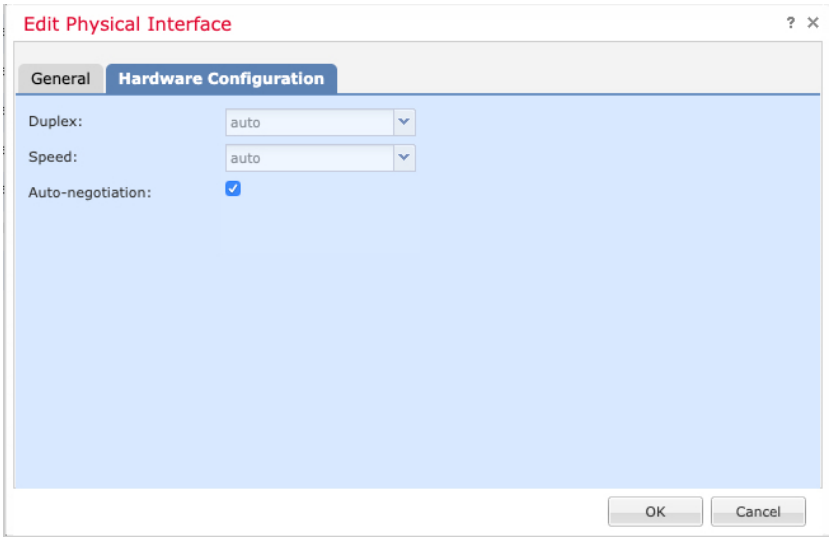
  You can enter spaces instead of commas.

If you include the native VLAN in this field, it is ignored; the trunk port always removes the VLAN tagging when sending native VLAN traffic out of the port. Moreover, it will not receive traffic that still has native VLAN tagging.

Step 7 (Optional) Check the **Protected** check box to set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN.

You might want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you enable **Protected** on each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Step 8 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.



Check the **Auto-negotiation** check box (the default) to auto-detect the speed and duplex. If you uncheck it, you can set the speed and duplex manually:

- **Duplex**—Choose **Full** or **Half**.
- **Speed**—Choose **10mbps**, **100mbps**, or **1gbps**.

If a peer switch connecting to the port over a 50G cable does not support auto-negotiation, ensure to disable auto-negotiation on the switch and the Threat Defense interface as well. For example, N9K-C93400LD-H1 does not support auto-negotiation on a 50G cable. Hence, you must disable the default auto-negotiation on the platform and the switch for the port to be connected.

Step 9 Click **OK**.

Click **Save**.

What to do next

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure Power over Ethernet

Configure Power over Ethernet (PoE) settings to control power delivery to connected devices and optimize power allocation.

Power over Ethernet (PoE) ports provide power for devices such as IP phones or wireless access points. PoE is enabled by default. This procedure describes how to disable and enable PoE and how to set optional parameters.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for Ethernet1/7 or 1/8 .

Step 3 Click **PoE**.

Figure 275: PoE



Step 4 Check the **Enable PoE** check box.

PoE is enabled by default.

Step 5 Choose autonegotiation or manual power.

- **Auto Negotiate Consumption Wattage**—Delivers power automatically to the powered device using a wattage appropriate to the class of the powered device. The firewall uses LLDP to further negotiate the correct wattage. When you connect a device of a certain class, it will be provisioned up to the maximum for that class in case it ever needs to use more power. For example, if you add a class 4 device that requests 12.95W, it will be allocated 30W even if it doesn't currently use all that power. Some devices can renegotiate power needs. If you know your device needs less power than is allocated, you can instead set the **Consumption Wattage** manually to free up the power for other devices.
- **Consumption Wattage**—Uncheck the **Auto Negotiate Consumption Wattage** check box to set the manual wattage to manually specify the wattage in milliwatts, from 4000 to 30000. Use this option if

you want to set the watts manually and disable LLDP negotiation. For manual allocation, the class will show in **show power inline** output as *n/a* because the class is not used to decide the power consumption.

View the current PoE status using the **show power inline** command.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Loopback interfaces

A loopback interface is a software-only interface that emulates a physical interface. This interface is reachable on IPv4 and IPv6 through multiple physical interfaces. The loopback interface helps to overcome path failures. It is accessible from any physical interface. If one interface goes down, you can access the loopback interface from another.

Loopback interfaces can be used for:

- AAA
- BGP
- DNS
- HTTP
- ICMP
- IPsec flow offload—Secure Firewall /3100/4200 only
- NetFlow
- SNMP
- SSH
- Static and dynamic VTI tunnels
- Syslog

The Firewall Threat Defense can distribute the loopback address using dynamic routing protocols, or you can configure a static route on the peer device to reach the loopback IP address through one of the Firewall Threat Defense's physical interfaces. You cannot configure a static route on the Firewall Threat Defense that specifies the loopback interface.

Related Topics

Guidelines for Loopback Interfaces, on page 662
Configure a loopback interface, on page 662

Guidelines for Loopback Interfaces

This topic outlines the specific constraints and supported configurations for loopback interfaces in various network environments.

Firewall Mode

- Supported in routed mode only.

High availability and Clustering

- No clustering support.

Additional Guidelines and Limitations

- TCP sequence randomization is always disabled for traffic from the physical interface to the loopback interface.

Configure a loopback interface

Configure a loopback interface to provide a virtual interface that remains active regardless of physical interface status, commonly used for routing protocols and management purposes.

Loopback interfaces are virtual interfaces that provide stable IP addresses for device management and routing protocols. They remain active as long as the device is operational, making them ideal for network management tasks.

Before you begin

Follow these steps to add a loopback interface for a device:

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 From the **Add Interfaces** drop-down list, choose **Loopback Interface**.

Step 3 In the **General** tab, configure the following parameters:

a) **Name**—Enter a name for the loopback interface.
b) **Enabled**—Check the check box to enable the loopback interface.
c) **Loopback ID**—Enter the loopback ID between 1 to 1024.
d) **Description**—Enter a description for the loopback interface.

Step 4 Configure the routed mode interface parameters. See Configure routed mode interfaces, on page 690.

Rate-Limit traffic to the loopback interface

You should rate-limit traffic going to the loopback interface IP address to prevent excessive load on the system. You can add a connection limit rule to the global service policy.

Rate-limiting protects the system from Denial of Service (DoS) attacks and ensures stable performance by controlling the number of connections to critical interface addresses.

Before you begin

Follow these steps to rate-limit traffic to the loopback interface:

Procedure

Step 1 Create an extended access list identifying traffic to the loopback interface IP address(es).

a. Choose **Objects** > **Object Management** > **Access List** > **Extended**.

b. Click **Add Extended Access List** to create a new ACL.

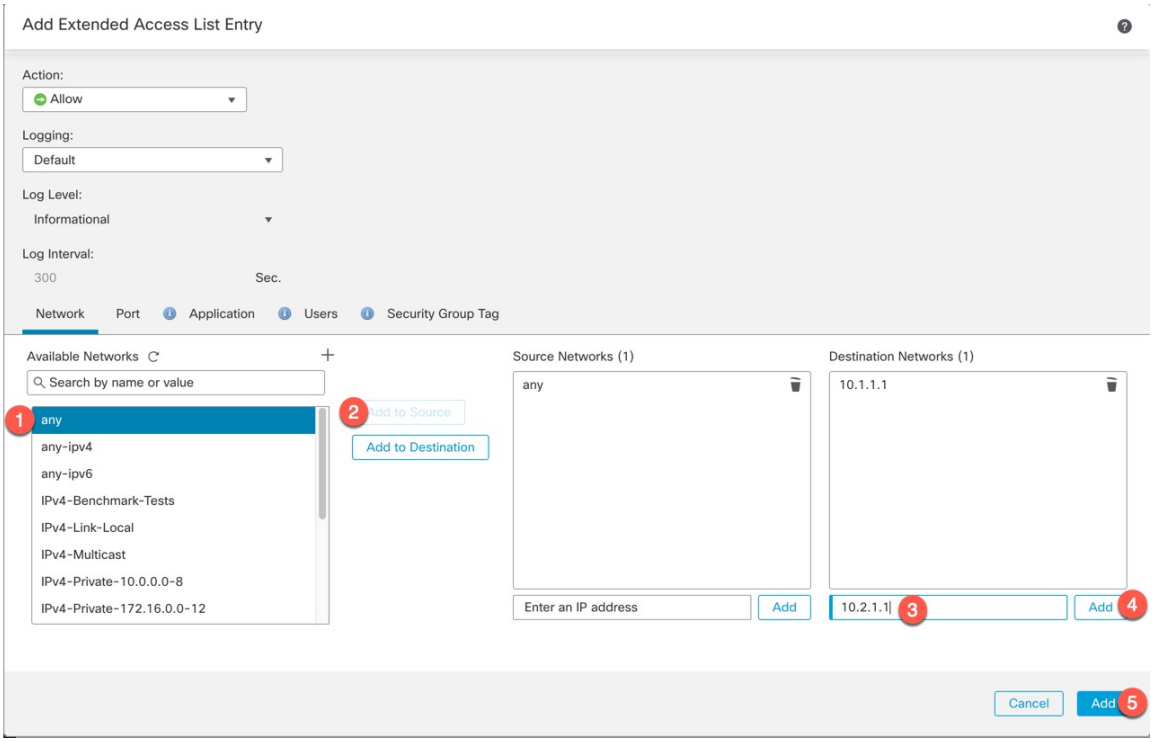
c. In the **New Extended Access List Object** dialog box, enter a name for the ACL (no spaces allowed), and click **Add** to create a new entry.

Figure 276: Name ACL and add entry



d. Configure the source (any) and destination addresses (loopback IP addresses) on the **Network** tab.

Figure 277: Source and destination networks



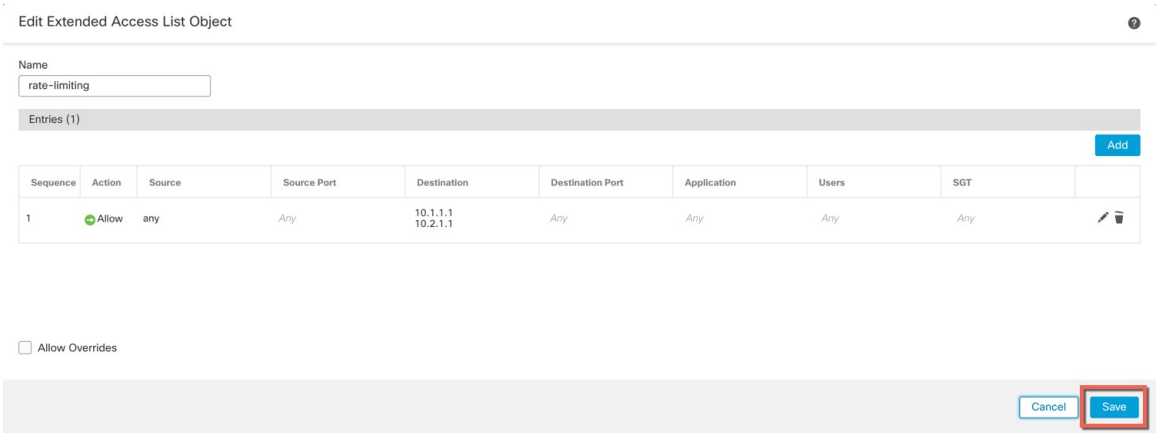
Note Keep the default **Action** as **Allow** (match) and other settings as-is.

- Source—Select **any** from the **Available Networks** list, and click **Add to Source**. You can also narrow this access list by specifying the source IP addresses instead of **any**.
- Destination—Type an address in the edit box below the **Destination Networks** list and click **Add**. Repeat for each loopback interface.

e. Click **Add** to add the entry to the ACL.

f. Click **Save** to save the ACL.

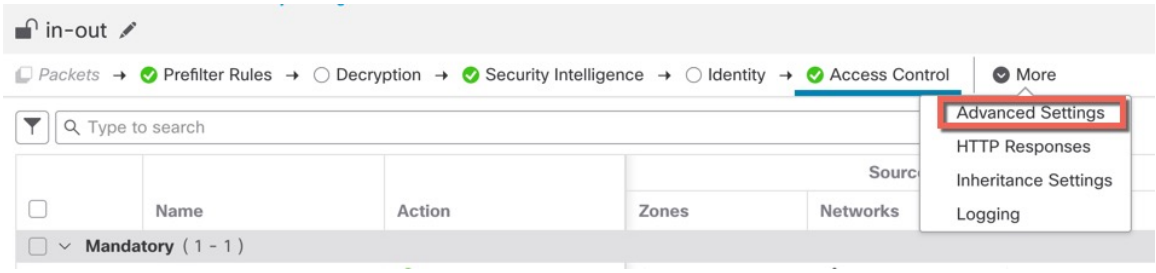
Figure 278: Save ACL



Step 2 Choose **Policies** > **Access Control heading** > **Access Control**, and click **Edit** (✎) for the access control policy assigned to your device.

Step 3 Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Figure 279: Advanced settings



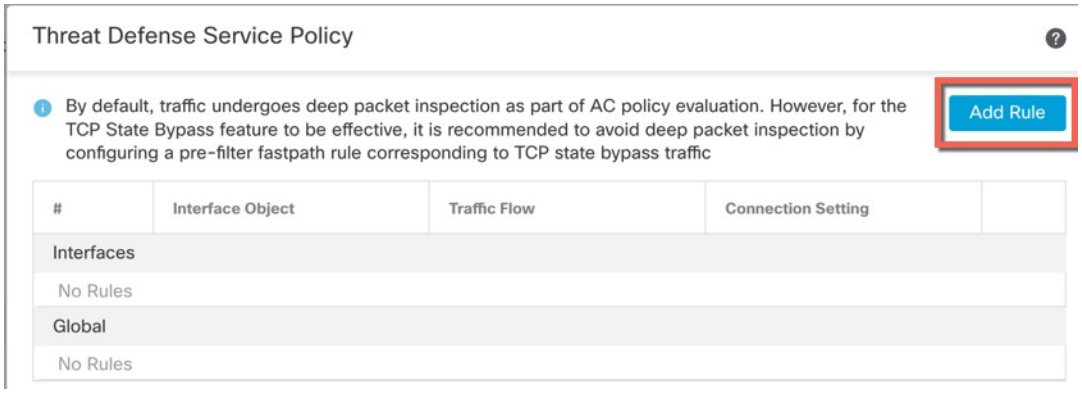
Step 4 Click **Edit** (✎) in the **Threat Defense Service Policy** group.

Figure 280: Threat defense service policy



Step 5 Click **Add Rule** to create a new rule.

Figure 281: Add rule



The service policy rule wizard opens to step you through the process of configuring the rule.

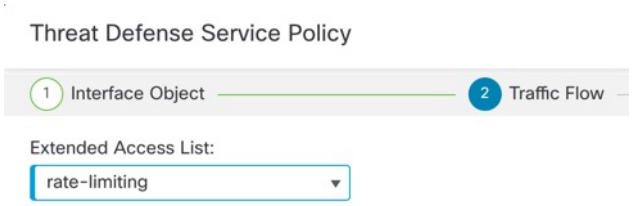
Step 6 In the **Interface Object** step, click **Global** to create a global rule, which applies to all interfaces, then click **Next**.

Figure 282: Global policy



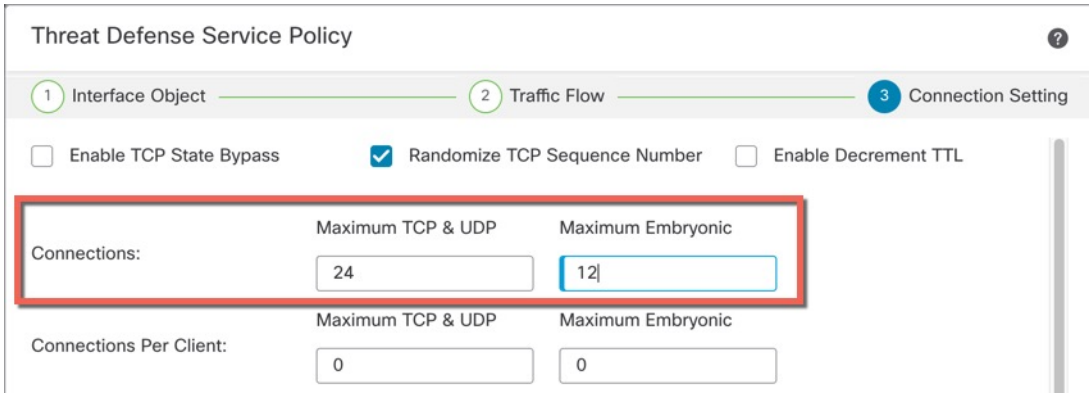
Step 7 In the **Traffic Flow** step, select the extended access list object you created in Step 1, on page 663, and then click **Next**.

Figure 283: Choose extended access list



Step 8 In the **Connection Setting** step, set the **Connections** limits.

Figure 284: Set connection limits



Set the **Maximum TCP & UDP** connections to the expected number of connections for the loopback interface, and the **Maximum Embryonic** connections to a lower number. For example, you can set it to 5/2, or 10/5, or 1024/512, depending on the expected loopback interface sessions you need.

Setting the embryonic connection limit enables TCP Intercept, which protects the system from a DoS attack perpetrated by flooding an interface with TCP SYN packets.

Step 9 Click **Finish** to save your changes.

Click **OK**.

Click **Save** on the **Advanced Settings** window.

What to do next

Deploy the changes to the affected devices.

VLAN subinterfaces and 802.1Q trunking

VLAN subinterfaces let you divide a physical, redundant, or EtherChannel interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs let you keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Guidelines for VLAN subinterfaces

Model support

- 1010—VLAN subinterfaces are not supported on switch ports or VLAN interfaces.

High availability and clustering

Do not use a subinterface for the failover or state link or for the cluster control link. The exception is for multi-instance mode: you can use a *chassis*-defined subinterface for these links.

Additional guidelines

- Preventing untagged packets on the physical interface—If you use subinterfaces, disable the physical interface from passing traffic. The physical interface transmits untagged packets. This behavior also applies to the active physical interface in a redundant interface pair and also to EtherChannel links. For the subinterface to pass traffic, the physical, redundant, or EtherChannel interface must be enabled. If you want to let the physical, redundant, or EtherChannel interface pass untagged packets, you can configure the name as usual.
- Configure subinterfaces only on non-Management interfaces. Avoid using the dedicated Management interface configured at the CLI or a data interface used for manager access.
- All subinterfaces on the same parent interface must be either members of bridge groups or routed interfaces; you cannot mix and match.
- The Firewall Threat Defense does not support the Dynamic Trunking Protocol (DTP), so configure the connected switch port to trunk unconditionally.
- Assign unique MAC addresses to the subinterfaces that are defined on the Firewall Threat Defense. Subinterfaces use the same burned-in MAC address of the parent interface by default. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense.

Note If you manually assign a MAC address, be sure to assign MAC addresses to all subinterfaces on the same physical interface to avoid unexpected behavior and outages.

Maximum number of VLAN subinterfaces by device model

Your device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface.

This table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Secure Firewall 4200	1024

Model	Maximum VLAN Subinterfaces
Firepower 4100	1024
Firepower 9300	1024
Firewall Threat Defense Virtual	50
ISA 3000	100

Add a subinterface

This task enables you to add subinterfaces to physical, redundant, or port-channel interfaces for network segmentation using VLAN tagging.

Add one or more subinterfaces to a physical, redundant, or port-channel interface.

For the Firepower 4100/9300, you can configure subinterfaces in FXOS for use with container instances; see Add a VLAN subinterface for container instances, on page 263. These subinterfaces appear in the Firewall Management Center interface list. You can also add subinterfaces in Firewall Management Center, but only on parent interfaces that do not already have subinterfaces defined in FXOS.

Note The parent physical interface passes untagged packets. You may not want to pass untagged packets, so be sure not to include the parent interface in your security policy.

Procedure

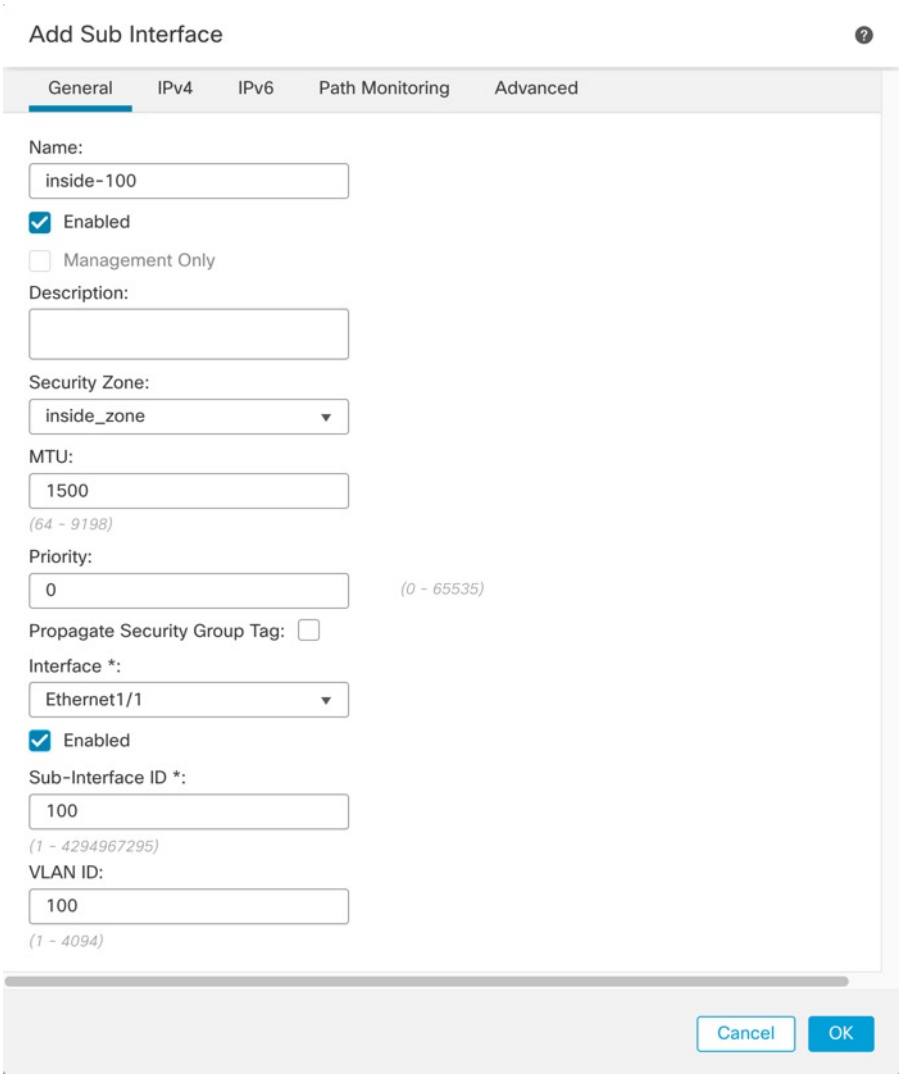
Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Enable the parent interface according to Enable the physical interface and configure Ethernet settings, on page 611.

Step 3 Click **Add Interfaces** > **Sub Interface**.

Step 4 On **General**, set these parameters:

Figure 285: Add subinterface



a) **Interface**—Choose the physical, redundant, or port-channel interface to which you want to add the subinterface.

b) **Sub-Interface ID**—Enter the subinterface ID as an integer between 1 and 4294967295. The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.

c) **VLAN ID**—Enter the VLAN ID between 1 and 4094 that will be used to tag the packets on this subinterface.

   This VLAN ID must be unique.

Step 5 Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Step 7 Configure the routed or transparent mode interface parameters. See Configure routed mode interfaces, on page 690 or Bridge group interfaces, on page 695.

Configure VXLAN Interfaces

This chapter tells how to configure Virtual eXtensible LAN (VXLAN) interfaces. VXLAN interfaces act as Layer 2 virtual networks over Layer 3 physical networks to stretch Layer 2 networks.

VXLAN interfaces

Virtual Extensible Local Area Network (VXLAN) is a network encapsulation protocol that provides flexible placement of multitenant segments throughout the data center. VXLAN offers higher scalability, supporting up to 16 million Layer 2 segments. VXLAN delivers Ethernet Layer 2 network services similar to VLAN and provides greater extensibility and flexibility.

Additional information

For detailed information about VXLAN, see RFC 7348.

encapsulation

The Firewall Threat Defense supports two types of VXLAN encapsulation:

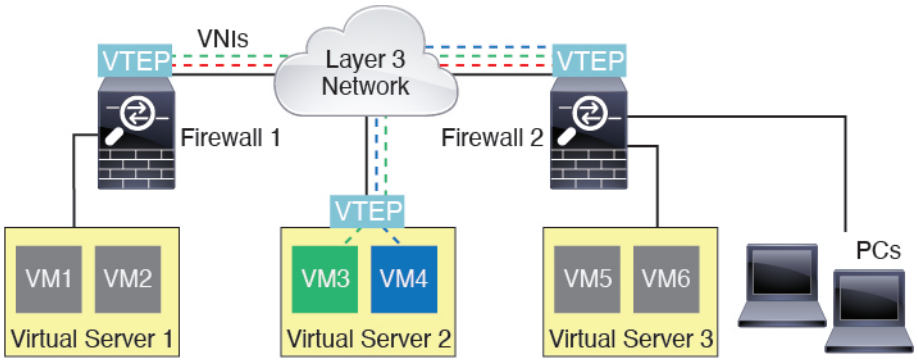
- VXLAN (all models)—VXLAN uses MAC Address-in-User Datagram Protocol (MAC-in-UDP) encapsulation. The original Layer 2 frame has a VXLAN header added and is then placed in a UDP-IP packet.
- Geneve (Firewall Threat Defense Virtual only)—Geneve has a flexible inner header that is not limited to the MAC address. Geneve encapsulation is required for transparent routing of packets between an Amazon Web Services (AWS) Gateway Load Balancer and appliances, and for sending extra information.

VXLAN tunnel endpoints

A VXLAN tunnel endpoint (VTEP) devices performs VXLAN encapsulation and decapsulation. Each VTEP has two interface types: one or more virtual interfaces called VXLAN Network Identifier (VNI) interfaces to which you apply your security policy, and a regular interface called the VTEP source interface that tunnels the VNI interfaces between VTEPs. The VTEP source interface is attached to the transport IP network for VTEP-to-VTEP communication.

VTEP network communication

This figure shows two Firewall Threat Defenses and Virtual Server 2 acting as VTEPs across a Layer 3 network, extending the VNI 1, 2, and 3 networks between sites. The Firewall Threat Defenses act as bridges or gateways between VXLAN and non-VXLAN networks.



The underlying IP network between VTEPs is independent of the VXLAN overlay. Encapsulated packets are routed based on the outer IP address header, which has the initiating VTEP as the source IP address and the terminating VTEP as the destination IP address. For VXLAN encapsulation: The destination IP address can be a multicast group when the remote VTEP is not known. With Geneve, the Firewall Threat Defense only supports static peers. The destination port for VXLAN is UDP port 4789 by default (user configurable). The destination port for Geneve is 6081.

VTEP source interface

A VTEP source interface is a regular interface (physical, EtherChannel, or even VLAN) that you plan to associate with all VNI interfaces. You can configure one VTEP source interface per Firewall Threat Defense Virtual.

VTEP source interface characteristics

The VTEP source interface can be devoted wholly to VXLAN traffic, although it is not restricted to that use. You can use the interface to handle regular traffic and apply a security policy to it. However, for VXLAN traffic, you must apply all security policies to the VNI interfaces. The VTEP interface serves as a physical port only.

In transparent firewall mode, the VTEP source interface is not part of a BVI. You must configure an IP address for it, similar to how the management interface is configured.

Because you can only configure one VTEP source interface, you cannot configure both VXLAN and Geneve interfaces on the same device. There is an exception for Firewall Threat Defense Virtual clustering on AWS or Azure, where you can have two VTEP source interfaces: a VXLAN interface is used for the cluster control link, and a Geneve (AWS) or VXLAN (Azure) interface can be used for the Gateway Load Balancer.

VNI interfaces

A VNI interface is a virtual interface that keeps network traffic separated on a given physical interface by using tagging. VNI interfaces are similar to VLAN interfaces. You can apply your security policy directly to each interface.

VNI interface configuration details

You can add only one VTEP interface. All VNI interfaces are associated with the same VTEP interface. There is an exception for Firewall Threat Defense Virtual clustering on AWS or Azure. For AWS clustering, you can have two VTEP source interfaces: a VXLAN interface is used for the cluster control link, and a Geneve interface can be used for the AWS Gateway Load Balancer. For Azure clustering, you can have two VTEP

source interfaces: a VXLAN interface is used for the cluster control link, and a second VXLAN interface can be used for the Azure Gateway Load Balancer.

How VXLAN and Geneve packets are processed

Summary

The key components involved in VXLAN and Geneve packet processing are:

- VTEP source interface: Performs encapsulation and decapsulation of VXLAN and Geneve traffic
- Inner MAC frame: The original packet payload that gets encapsulated
- Outer frame: The encapsulated packet with VXLAN or Geneve headers
- Remote VTEP: The destination endpoint for encapsulated traffic

Workflow

These stages describe how VXLAN and Geneve packet processing work:

1. Traffic entering and exiting the VTEP source interface is subject to VXLAN processing, specifically encapsulation or decapsulation.

   Encapsulation processing includes these tasks:

   - The VTEP source interface encapsulates the inner MAC frame with the VXLAN header.
   - The UDP checksum field is set to zero.
   - The Outer frame source IP is set to the VTEP interface IP.
   - The Outer frame destination IP is decided by a remote VTEP IP lookup.

   Decapsulation: the Firewall Threat Defense only decapsulates a VXLAN packet if:

   - It is a UDP packet with the destination port set to 4789 (this value is user configurable).
   - The ingress interface is the VTEP source interface.
   - The ingress interface IP address is the same as the destination IP address.
   - The VXLAN packet format is compliant with the standard.

2. Traffic entering and exiting the VTEP source interface is subject to Geneve processing, specifically encapsulation or decapsulation.

   Encapsulation processing includes these tasks:

   - The VTEP source interface encapsulates the inner MAC frame with the Geneve header.
   - The UDP checksum field is set to zero.
   - The Outer frame source IP is set to the VTEP interface IP.
   - The Outer frame destination IP is set the peer IP address that you configured.

   Decapsulation; the Firewall Threat Defense only decapsulates a Geneve packet if:

- It is a UDP packet with the destination port set to 6081 (this value is user configurable).
- The ingress interface is the VTEP source interface.
- The ingress interface IP address is the same as the destination IP address.
- The Geneve packet format is compliant with the standard.

Peer VTEPs

A peer VTEP is a VXLAN Tunnel Endpoint that enables the Firewall Threat Defense to send packets to devices behind remote VTEPs.

When the Firewall Threat Defense sends a packet to a device behind a peer VTEP, the Firewall Threat Defense needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

The Firewall Threat Defense maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

VXLAN peer configuration methods

There are two ways in which the Firewall Threat Defense can find this information:

- A single peer VTEP IP address can be statically configured on the Firewall Threat Defense.

  For IPv4: The Firewall Threat Defense then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

  For IPv6: The Firewall Threat Defense then sends an IPv6 Neighbor Solicitation message to the IPv6 solicited-node multicast address. The peer VTEP responds with an IPv6 Neighbor Advertisement message with its link-local address.

- A group of peer VTEP IP addresses can be statically configured on the Firewall Threat Defense.

  For IPv4: The Firewall Threat Defense then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC addresses.

  For IPv6: The Firewall Threat Defense then sends an IPv6 Neighbor Solicitation message to the IPv6 solicited-node multicast address. The peer VTEP responds with an IPv6 Neighbor Advertisement message with its link-local address.

- A multicast group can be configured on each VNI interface (or on the VTEP as a whole).

  For IPv4: The Firewall Threat Defense sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the Firewall Threat Defense to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

  For IPv6: The Firewall Threat Defense sends a Multicast Listener Discovery (MLD) Report message through the VTEP source interface to indicate that the Firewall Threat Defense is listening on the VTEP interface for the multicast address traffic.

  This option is not supported with Geneve.

Geneve peer configuration

The Firewall Threat Defense Virtual only supports statically defined peers. You can define the Firewall Threat Defense Virtual peer IP address on the AWS Gateway Load Balancer. Because the Firewall Threat Defense Virtual never initiates traffic to the Gateway Load Balancer, you do not also have to specify the Gateway Load Balancer IP address on the Firewall Threat Defense Virtual. It learns the peer IP address when it receives Geneve traffic. Multicast groups are not supported with Geneve.

VXLAN use cases

This section describes the use cases for implementing VXLAN on the Firewall Threat Defense.

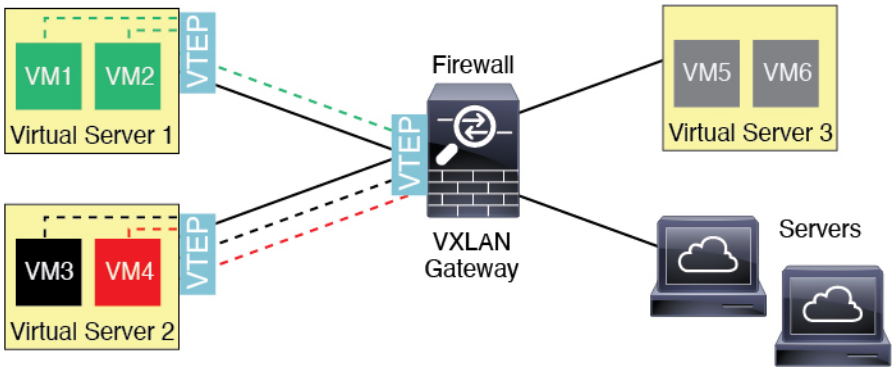
VXLAN bridge or gateway overview

A VTEP acts as a bridge or gateway between end nodes, such as VMs, servers, and PCs, and the VXLAN overlay network.

VXLAN Packet Processing

For incoming frames received with VXLAN encapsulation over the VTEP source interface, the Firewall Threat Defense strips out the VXLAN header and forwards it to a physical interface connected to a non-VXLAN network based on the destination MAC address of the inner Ethernet frame.

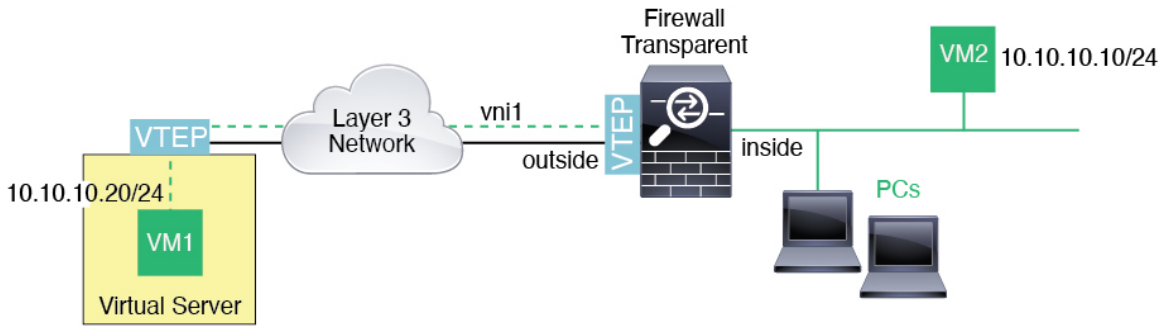
The Firewall Threat Defense always processes VXLAN packets rather than forwarding them untouched between two other VTEPs.



VXLAN bridge

A VXLAN bridge is a network configuration where the Firewall Threat Defense connects a remote VXLAN segment to a local segment.

When you use a bridge group (transparent firewall mode, or optionally routed mode), the Firewall Threat Defense can serve as a VXLAN bridge between a (remote) VXLAN segment and a local segment where both are in the same network. In this case, one member of the bridge group is a regular interface while the other member is a VNI interface.

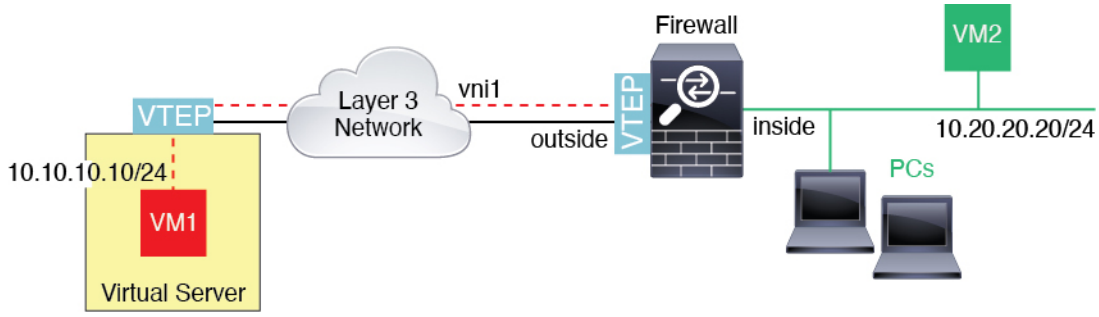


VXLAN gateway (routed mode)

The Firewall Threat Defense functions as a router between VXLAN and non-VXLAN domains, connecting devices on different networks.

VXLAN Gateway Visual Representation

This figure illustrates the VXLAN gateway connectivity.



Router Between VXLAN Domains

A VXLAN-stretched Layer 2 domain enables a VM to utilize a Firewall Threat Defense as its default gateway regardless of physical proximity.

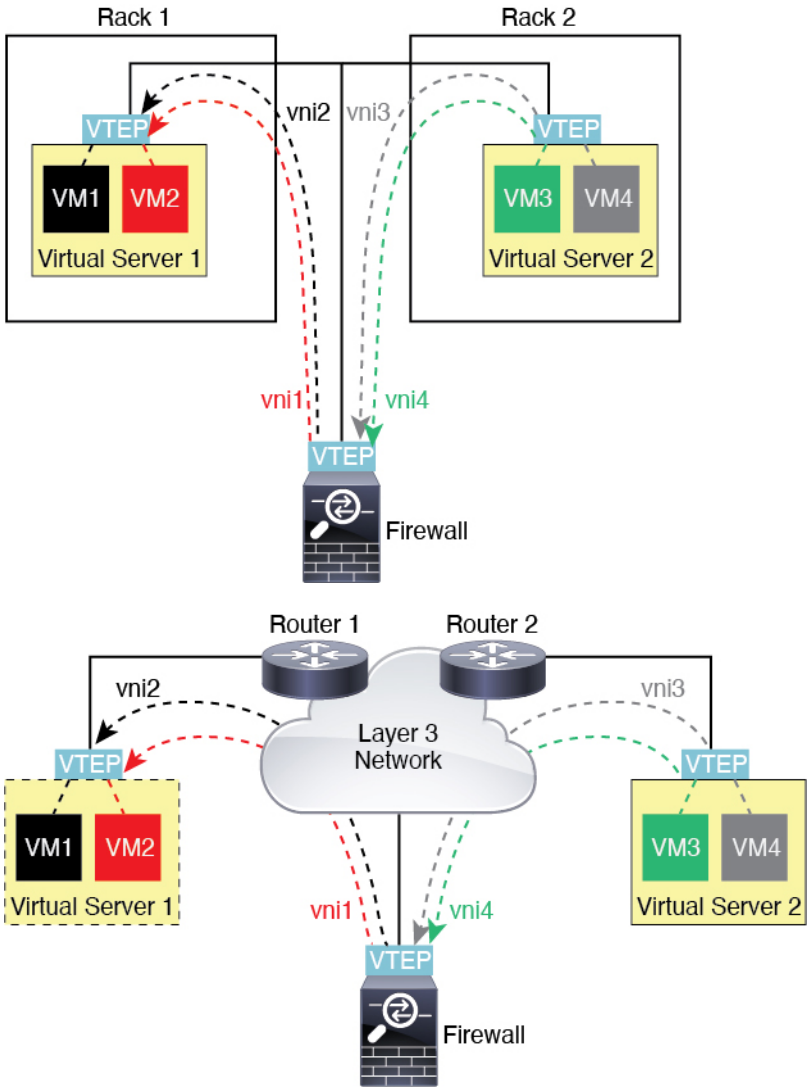
Routing Process and Packet Flow

The following steps outline the packet flow between VMs across VXLAN domains:

1. For packets from VM3 to VM1, the destination MAC address is the Firewall Threat Defense MAC address, because the Firewall Threat Defense is the default gateway.
2. The VTEP source interface on Virtual Server 2 receives packets from VM3, then encapsulates the packets with VNI 3's VXLAN tag and sends them to the Firewall Threat Defense .
3. When the Firewall Threat Defense receives the packets, it decapsulates the packets to get the inner frames.
4. The Firewall Threat Defense uses the inner frames for route lookup, then finds that the destination is on VNI 2. If it does not already have a mapping for VM1, the Firewall Threat Defense sends an encapsulated ARP broadcast on the multicast group IP on VNI 2.
5. The Firewall Threat Defense encapsulates the packets again with the VXLAN tag for VNI 2 and sends the packets to Virtual Server 1. Before encapsulation, the Firewall Threat Defense changes the inner frame destination MAC address to be the MAC of VM1.

6. When Virtual Server 1 receives the VXLAN packets, it decapsulates the packets and delivers the inner frames to VM1.

Note The Firewall Threat Defense must use dynamic VTEP peer discovery because it has multiple VTEP peers in this scenario.



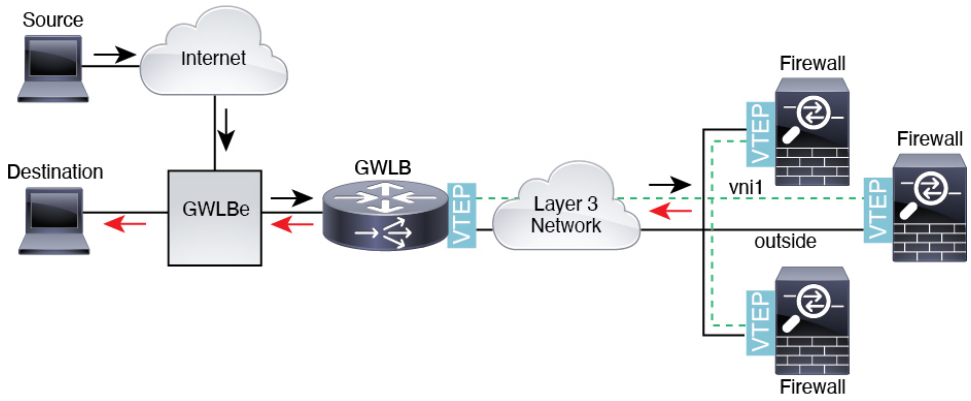
Geneve Single-Arm Proxy

In a Geneve single-arm proxy deployment, network traffic is routed through a centralized proxy device for inspection and policy enforcement.

Note This use case is the only currently supported use case for Geneve interfaces.

The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The Firewall Threat Defense Virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint). The following figure shows traffic forwarded to the Gateway Load Balancer from the Gateway Load Balancer endpoint. The Gateway Load Balancer balances traffic among multiple Firewall Threat Defense Virtuals, which inspect the traffic before either dropping it or sending it back to the Gateway Load Balancer (U-turn traffic). The Gateway Load Balancer then sends the traffic back to the Gateway Load Balancer endpoint and to the destination.

Figure 286: Geneve Single-Arm Proxy

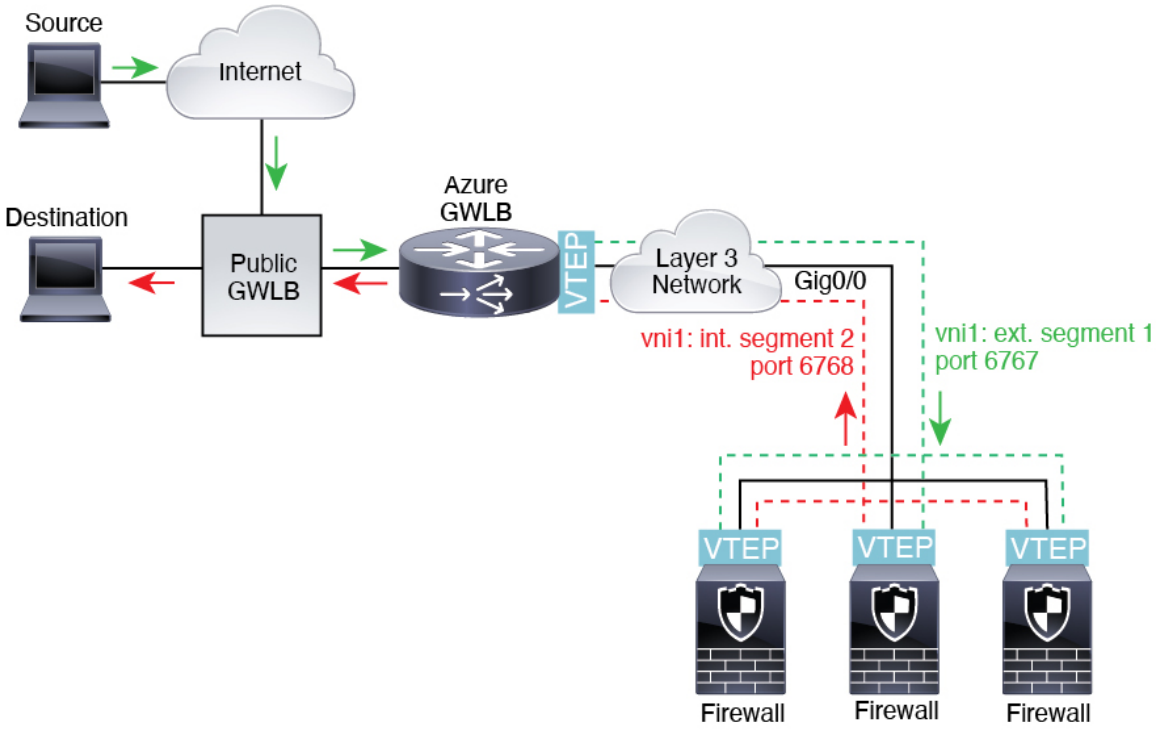


Azure Gateway Load Balancer and Paired Proxy

In an Azure service chain, Firewall Threat Defense Virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The Firewall Threat Defense Virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

The following figure shows traffic forwarded to the Azure Gateway Load Balancer from the Public Gateway Load Balancer on the external VXLAN segment. The Gateway Load Balancer balances traffic among multiple Firewall Threat Defense Virtuals, which inspect the traffic before either dropping it or sending it back to the Gateway Load Balancer on the internal VXLAN segment. The Azure Gateway Load Balancer then sends the traffic back to the Public Gateway Load Balancer and to the destination.

Figure 287: Azure Gateway Load Balancer with Paired Proxy



Requirements and prerequisites for VXLAN interfaces

This reference provides the model requirements and prerequisites for configuring VXLAN interfaces on supported platforms.

Model requirements

- VXLAN encapsulation is supported on all models.
- Geneve encapsulation is supported for these models:
  - Firewall Threat Defense Virtual in Amazon Web Services (AWS)
- VXLAN in *paired proxy mode* is supported for these models:
  - Firewall Threat Defense Virtual in Azure
- Firepower 1010 switch ports and VLAN interfaces are not supported as VTEP interfaces.

Guidelines for VXLAN interfaces

Firewall mode restrictions

Geneve interfaces are only supported in routed firewall mode.

- Paired proxy VXLAN interfaces are only supported in routed firewall mode.

IPv6 support restrictions

The VNI interface supports both IPv4 and IPv6 traffic.

- For VXLAN encapsulation, the VTEP source interface supports both IPv4 and IPv6. The Firewall Threat Defense Virtual cluster control link VTEP source interface only supports IPv4.

  For Geneve, the VTEP source interface only supports IPv4.

Clustering restrictions

Clustering does not support VXLAN in Individual Interface mode except for the cluster control link (Firewall Threat Defense Virtual only) Only Spanned EtherChannel mode supports VXLAN.

An exception is made for AWS, which can use an additional Geneve interface for use with the GWLB and for Azure, which can use an additional paired proxy VXLAN interface for use with the GWLB.

Routing restrictions

Only static routing or Policy Based Routing is supported on the VNI interface; dynamic routing protocols are not supported.

VPN restrictions

You cannot configure the VTEP source interface for VPN or use it as a VTI.

MTU requirements

If the source interface MTU is less than the required minimum, the Firewall Threat Defense automatically raises the MTU to meet encapsulation requirements.

- VXLAN encapsulation—If the source interface MTU is less than 1554 bytes for IPv4 or 1574 bytes for IPv6, then the Firewall Threat Defense automatically raises the MTU to 1554 bytes or 1574 bytes. In this case, the entire Ethernet datagram is being encapsulated, so the new packet is larger and requires a larger MTU. If the MTU used by other devices is larger, then you should set the source interface MTU to be the network MTU + 54 bytes for IPv4 or +64 bytes for IPv6. For the Firewall Threat Defense Virtual, this MTU requires a restart to enable jumbo frame reservation.
- Geneve encapsulation—If the source interface MTU is less than 1806 bytes, then the Firewall Threat Defense automatically raises the MTU to 1806 bytes. In this case, the entire Ethernet datagram is being encapsulated, so the new packet is larger and requires a larger MTU. If the MTU used by other devices is larger, then you should set the source interface MTU to be the network MTU + 306 bytes. This MTU requires a restart to enable jumbo frame reservation.

Configure VXLAN or Geneve interfaces

You can configure either VXLAN or Geneve interfaces.

Configure VXLAN interfaces

Configure VXLAN interfaces to enable virtualized network overlay functionality and network segmentation.

VXLAN provides Layer 2 overlay network capabilities over existing Layer 3 infrastructure. You can configure either VXLAN or Geneve interfaces, but not both simultaneously.

Note You can configure either VXLAN or Geneve (Firewall Threat Defense Virtual only). For Geneve interfaces, see Configure geneve interfaces, on page 683.

Note For Azure GWLB, the VXLAN interface is configured when you deploy the VM using the ARM template. You can use this section to change your configuration.

Follow these steps to configure VXLAN interfaces.

Procedure

Step 1 Configure the VTEP source interface, on page 681.

Step 2 Configure the VNI interface, on page 682.

Step 3 (Azure GWLB) Allow gateway load balancer health checks, on page 685.

Configure the VTEP source interface

This task enables you to set up VXLAN network virtualization by configuring a Network Virtualization Endpoint (NVE) on your firewall device.

You can configure one VTEP source interface per Firewall Threat Defense device. The VTEP is defined as a Network Virtualization Endpoint (NVE). VXLAN is the default encapsulation type. An exception is made for clustering on the Firewall Threat Defense Virtual in Azure, where you can use one VTEP source interface for the cluster control link and a second one for the data interface connected to the Azure GWLB.

Procedure

Step 1 If you want to specify a group of peer VTEPs, add a network object with the peer IP addresses. See Create a network object, on page 2388.

Step 2 Choose **Devices** > **Device Management**.

Step 3 Click **Edit** ( ) next to the device on which you want to configure VXLAN.

Step 4 (Optional) Specify that the source interface is NVE-only.

This setting is optional for routed mode where this setting restricts traffic to VXLAN and common management traffic only on this interface. This setting is automatically enabled for transparent firewall mode.

a) Click **Interfaces**.

b) Click **Edit** ( ) for the VTEP source interface.

c) On the **General** page, check the check box of **NVE Only**.

Step 5 Click **VTEP** if it is not already displaying.

Step 6 Check **Enable NVE**.

Step 7 Click **Add VTEP**.

a) For the **Encapsulation Type**, choose **VXLAN**.

For AWS, you can choose between **VXLAN** and **Geneve**. Other platforms have **VXLAN** chosen automatically.

b) Enter the value for the **Encapsulation port** within the specified range.

The default value is 4789.

c) Select the **VTEP Source Interface**.

Select from the list of available physical interfaces present on the device. If the source interface MTU is less than 1554 bytes for IPv4 or 1574 bytes for IPv6, then the Firewall Management Center automatically raises the MTU to 1554 bytes or 1574 bytes.

d) Select the **Neighbor Address**. The available options are:

- **None**—No neighbor address is specified.
- **Peer VTEP**—Specify a peer VTP address.
- **Peer Group**—Specify a network object with the peer IP addresses.
- **Default Multicast**—Specify a default multicast group for all associated VNI interfaces. If you do not configure the multicast group per VNI interface, then this group is used. If you configure a group at the VNI interface level, then that group overrides this setting.

Step 8 Click **OK**.

Step 9 Click **Save**.

What to do next

Configure the routed interface parameters. See Configure Routed Mode Interfaces.

Configure the VNI interface

Add a VNI interface, associate it with the VTEP source interface, and configure basic interface parameters.

For the Firewall Threat Defense Virtual in Azure, you can configure either a regular VXLAN interface, or you can configure a paired proxy mode VXLAN interface for use with the Azure GWLB. Paired proxy mode is the only supported mode with clustering.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device on which you want to configure VXLAN.

Step 3 Click **Interfaces**.

Step 4 Click **Add Interfaces**, and then choose **VNI Interface**.

a) Enter the interface **Name** and **Description**.

b) From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New**.

c) Enter a value for the **Priority** field within the specified range. By default, 0 is selected.
d) Enter a value for the **Priority** field within the specified range. By default, 0 is selected.
e) Enter a value for the **VNI ID** between 1 and 10000.

This ID is only an internal interface identifier.

Step 5 (Paired Proxy VXLAN for Azure gateway load balancer) Enable proxy paired mode and set the required parameters.

a) Check **Proxy Paired**.
b) Set the **Internal Port** between 1024 and 65535.
c) Set the **Internal Segment ID** between 1 and 16777215.
d) Set the **External Port** between 1024 and 65535.
e) Set the **External Segment ID** between 1 and 16777215.

Step 6 (Regular VXLAN) Enter a value for the **VNI Segment ID** between 1 and 16777215.

The segment ID is used for VXLAN tagging.

Step 7 Enter the **Multicast Group IP Address**.

If you do not set the multicast group for the VNI interface, the default group from the VTEP source interface configuration is used, if available. If you manually set a VTEP peer IP for the VTEP source interface, you cannot specify a multicast group for the VNI interface.

Step 8 Check **NVE Mapped to VTEP Interface**.

This option associates this interface with the VTEP source interface.

Step 9 Click **OK**.

Click **Save** to save the interface configuration.

What to do next

Configure the routed or transparent interface parameters. See Configure routed and transparent mode interfaces, on page 686.

Configure geneve interfaces

To configure Geneve interfaces for Firewall Threat Defense Virtual, perform the following steps.

Note You can configure either VXLAN or Geneve. For information about VXLAN interfaces, see Configure VXLAN interfaces, on page 680.

1. Configure the VTEP source interface, on page 684.
2. Configure the VNI, on page 684.
3. Allow gateway load balancer health checks, on page 685.

Configure the VTEP source interface

Configure the VTEP source interface to enable network virtualization functionality on the device.

You can configure one VTEP source interface per Firewall Threat Defense Virtual device. The VTEP is defined as a Network Virtualization Endpoint (NVE).

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device on which you want to configure Geneve.

Step 3 Click **VTEP**.

Step 4 Check **Enable NVE**.

Step 5 Click **Add VTEP**.

a) For the **Encapsulation Type**, choose **Geneve**.

b) Enter the value for the **Encapsulation port** within the specified range.

We do not recommend changing the Geneve port; AWS requires a port of 6081.

c) Select the **VTEP Source Interface**.

You can select from the list of available physical interfaces present on the device. If the source interface MTU is less than 1806 bytes, then the Firewall Management Center automatically raises the MTU to 1806 bytes.

d) Click **OK**.

Step 6 Click **Save**.

Step 7 Configure the routed interface parameters. See Configure Routed Mode Interfaces.

Configure the VNI

This task enables you to add a VNI interface and configure its basic parameters for Geneve functionality on your device.

Add a VNI, associate it with (VTEP) source interface, and configure basic interface parameters.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Edit** ( ) next to the device on which you want to configure Geneve.

Step 3 Click **Interfaces**.

Step 4 Click **Add Interfaces**, and then choose **VNI Interface**.

a) In the **Name** and **Description** fields, provide relevant information.

b) In the **VNI ID** field, enter a value between 1 and 10000.

Note This ID is only an internal interface identifier.

Step 5 Check the **Enable Proxy** check box.

Note When the AWS proxy is enabled on the VNI interface of your device, configuring NAT is not allowed.

This option enables single-arm proxy, and allows traffic to exit the same interface it entered (U-turn traffic). If you edit the interface later , you cannot disable single-arm proxy. To disable single-arm proxy, delete the existing interface and create a new VNI interface.

This option is only available for a Geneve VTEP.

Step 6 Select **NVE Mapped to VTEP Interface**.

This option associates this interface with the VTEP source interface.

Step 7 Click **OK**.

Step 8 Click **Save**.

What to do next

Configure the routed interface parameters. See Configure Routed Mode Interfaces.

Allow gateway load balancer health checks

The AWS or Azure gateway load balancer (GWLB) requires appliances to answer a health check properly. The GWLB will only send traffic to appliances that are considered healthy.

Configure one of these methods to enable proper health check responses.

Procedure

Step 1 Configure SSH. See Configure Secure Shell

Allow SSH from the GWLB IP address. The GWLB will attempt to establish a connection to the Firewall Threat Defense Virtual, and the Firewall Threat Defense Virtual's prompt to log in is taken as proof of health. An SSH login attempt will time out after 1 minute. You will need to configure a longer health check interval on the GWLB to accommodate this timeout.

Step 2 Configure HTTP(S) Redirection Using Static Interface NAT with Port Translation.

You can configure the Firewall Threat Defense Virtual to redirect health checks to a metadata HTTP(S) server. For HTTP(S) health checks, the HTTP(S) server must reply to the GWLB with a status code in the range 200 to 399. Because the Firewall Threat Defense Virtual has limits on the number of simultaneous management connections, you may choose to offload the health check to an external server.

Static interface NAT with port translation lets you redirect a connection to a port (such as port 80) to a different IP address. For example, translate an HTTP packet from the GWLB with a destination of the Firewall Threat Defense Virtual outside interface so that it appears to be from the Firewall Threat Defense Virtual outside interface with a destination of the HTTP server. The Firewall Threat Defense Virtual then forwards the packet to the mapped destination address. The HTTP server responds to the Firewall Threat Defense Virtual outside interface, and then the Firewall Threat Defense Virtual forwards the response back to the GWLB. You need an access rule that allows traffic from the GWLB to the HTTP server.

a) Permit HTTP(S) traffic on the outside interface from the GWLB network in an access rule. See Access Control Rules, on page 1609.
b) For HTTP(S), translate the source GWLB IP address to the Firewall Threat Defense Virtual outside interface IP address; then translate the destination of the outside interface IP address to the HTTP(S) server IP address. See Configure static manual NAT, on page 1232.

Configure routed and transparent mode interfaces

This section includes tasks to complete the regular interface configuration for all models in routed or transparent firewall mode.

Routed and transparent mode interfaces

Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this traffic according to your security policy.

Interface types by firewall mode

The types of firewall interfaces you can configure depends on the firewall mode set for the device: routed or transparent mode. See Transparent or Routed Firewall Mode, on page 71 for more information.

- Routed mode interfaces (routed firewall mode only)—Each interface that you want to route between is on a different subnet.
- Bridge group interfaces (routed and transparent firewall mode)—You can group together multiple interfaces on a network, and the Firewall Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. In routed mode, the Firewall Threat Defense device routes between BVIs and regular routed interfaces. In transparent mode, each bridge group is separate and cannot communicate with each other.

Dual IP stack (IPv4 and IPv6)

A dual IP stack is a network configuration that enables both IPv6 and IPv4 addresses on the same interface on Firewall Threat Defense device. Make sure you configure a default route for both IPv4 and IPv6.

31-bit subnet masks

A 31-bit subnet mask includes only two addresses for point-to-point connections.

31-bit subnet mask implementation

For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. Normally, the first and last address in a 2-address subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4.

31-bit subnet mask use cases

The failover link between two Firewall Threat Defenses only requires two addresses. Any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog.

Note: 31-bit subnet and clustering compatibility

You can use a 31-bit subnet mask for cluster interfaces, excluding the management interface and the cluster control link.

31-bit subnet and failover

A Firewall Threat Defense using a 31-bit subnet for its interface IP address can't configure a standby IP address due to insufficient addresses.

Interface monitoring limitations

When using a 31-bit subnet for the Firewall Threat Defense interface IP address, you cannot configure a standby IP address for the interface because there are not enough addresses. Normally, an interface for failover should have a standby IP address so the active unit can perform interface tests to ensure standby interface health. Without a standby IP address, the Firewall Threat Defense cannot perform any network tests; only the link state can be tracked.

For the failover and optional separate state link, which are point-to-point connections, you can also use a 31-bit subnet.

31-bit subnet and management

If you have a directly-connected management station, you can use a point-to-point connection for SSH or HTTP on the Firewall Threat Defense, or for SNMP or Syslog on the management station.

Recommendation: 31-bit subnet unsupported features

The 31-bit subnet does not support certain network features that require multiple host addresses.

- BVI interfaces for bridge groups—The bridge group requires at least 3 host addresses: the BVI, and two hosts connected to two bridge group member interfaces. you must use a /29 subnet or smaller.
- Multicast Routing

Guidelines and limitations for routed and transparent mode interfaces

Context mode

- PPPoE is not supported in multiple context mode.

- For multiple context mode in transparent mode, each context must use different interfaces; you cannot share an interface across contexts.
- For multiple context mode in transparent mode, each context typically uses a different subnet. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

High availability, Clustering, and Multi-Instance

Do not configure failover links with the procedures in this chapter. See the High availability chapter for more information.

- For cluster interfaces, see the clustering chapter for requirements.
- For multi-instance mode, shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode).
- When you use High availability, you must set the IP address and standby address for data interfaces manually; DHCP and PPPoE are not supported. Set the standby IP addresses on the **Devices** > **Device Management** > **High Availability** tab in the **Monitored Interfaces** area. See the High availability chapter for more information.

IPv6

IPv6 is supported on all interfaces.

- You can only configure IPv6 addresses manually in transparent mode.
- The Firewall Threat Defense device does not support IPv6 anycast addresses.
- DHCPv6 and prefix delegation options are not supported with transparent mode, clustering, or High availability.

Model guidelines

For the Firewall Threat Defense Virtual on VMware with bridged ixgbevf interfaces, bridge groups are not supported.

- For the Firepower 2100 series, bridge groups are not supported in routed mode.

VLAN IDs for the ASASM

- If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the **show interface** command for more information about interface states.

Transparent mode and bridge group guidelines

- You can create up to 250 bridge groups, with 64 interfaces per bridge group.
- Each directly-connected network must be on the same subnet.
- The Firewall Threat Defense device does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

- An IP address for the BVI is required for each bridge group for to-the-device and from-the-device management traffic, as well as for data traffic to pass through the Firewall Threat Defense device. For IPv4 traffic, specify an IPv4 address. For IPv6 traffic, specify an IPv6 address.
- You can only configure IPv6 addresses manually.
- The BVI IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).
- Management interfaces are not supported as bridge group members.
- For multi-instance mode, shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode).
- For the Firewall Threat Defense Virtual on VMware with bridged ixgbevf interfaces, transparent mode is not supported, and bridge groups are not supported in routed mode.
- For the Firepower 2100 series, bridge groups are not supported in routed mode.
- For the / 1010/ , you cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.
- For the Firepower 4100/9300, data-sharing interfaces are not supported as bridge group members.
- In transparent mode, you must use at least 1 bridge group; data interfaces must belong to a bridge group.
- In transparent mode, do not specify the BVI IP address as the default gateway for connected devices; devices need to specify the router on the other side of the Firewall Threat Defense as the default gateway.
- In transparent mode, the *default* route, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a regular static route that identifies the network from which you expect management traffic.
- Transparent mode is not supported on threat defense virtual instances deployed on Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure.
- In routed mode, to route between bridge groups and other routed interfaces, you must name the BVI.
- In routed mode, Firewall Threat Defense-defined EtherChannel interfaces are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firewall Threat Defense when using bridge group members. If there are two neighbors on either side of the Firewall Threat Defense running BFD, then the Firewall Threat Defense will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

Additional guidelines and requirements

The Firewall Threat Defense supports only one 802.1Q header in a packet and does not support multiple headers (known as Q-in-Q support) for firewall interfaces.**Note:** For inline sets and passive interfaces, the FTD supports Q-in-Q up to two 802.1Q headers in a packet, with the exception of the Firepower 4100/9300, which only supports one 802.1Q header.

- Interface problems, such as frequent up/down status changes, can prevent the floating connection timer from applying correctly to the connections going through the interface. If you have problems with an

interface's status, consider clearing all connections after the status becomes stable to clear invalid connections.

Configure routed mode interfaces

Before you begin

- Firepower 4100/9300
  1. Configure a physical interface, on page 259
  2. (Optional) Configure any special interfaces.
     - Add an EtherChannel (port channel), on page 261
     - Add a VLAN subinterface for container instances, on page 263 in FXOS
     - Configure a loopback interface, on page 662
     - Add a subinterface, on page 669 in Firewall Management Center
     - Configure VXLAN interfaces, on page 680

- (Optional) **All other models:**
  - Configure an EtherChannel, on page 619
  - Configure a loopback interface, on page 662
  - Add a subinterface, on page 669
  - Configure VXLAN interfaces, on page 680
  - Firewall Threat Defense Virtual on AWS: Configure geneve interfaces, on page 683
  - Firepower 1010 : Configure a VLAN interface, on page 653

This procedure describes how to set the name, security zone, and IPv4 address.

Note Not all fields are supported for all interface types.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 In the **Name** field, enter a name up to 48 characters in length.

You cannot start the name with the phrase "cluster". It is reserved for internal use.

Step 4 Enable the interface by checking the **Enabled** check box.

a) (Optional) Set this interface to **Management Only** to limit traffic to management traffic; through-the-box traffic is not allowed.

b) (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

c) In the **Mode** drop-down list, choose **None** .

Regular firewall interfaces have the mode set to None. The other modes are for IPS-only interface types.

d) From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New** .

The routed interface is a Routed-type interface, and can only belong to Routed-type zones.

e) See Configure the MTU, on page 717 for information about the **MTU** .

f) In the **Priority** field, enter a number ranging from 0–65535.

This value is used in the policy based routing configuration. The priority is used to determine how you want to route the traffic across multiple egress interfaces. For more information, see Configure policy-based routing policy, on page 1166.

Step 5 Click the **IPv4** tab. To set the IP address, use one of the following options from the **IP Type** drop-down list.

High Availability, clustering , and loopback interfaces only support static IP address configuration; DHCP and PPPoE are not supported.

- **Use Static IP** —Enter the IP address and subnet mask. For point-to-point connections, you can specify a 31-bit subnet mask (255.255.255.254 or /31). In this case, no IP addresses are reserved for the network or broadcast addresses. You cannot set the standby IP address in this case. For High Availability, you can only use a static IP address. Set the standby IP address on the **Devices** > **Device Management** page, click **High Availability** in the **Monitored Interfaces** area. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
- **Use DHCP** —Configure the following optional parameters:
  - **Obtain default route using DHCP** —Obtains the default route from the DHCP server.
  - **DHCP route metric** —Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.
- **Use PPPoE** —If the interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, configure the following parameters:
  - **VPDN Group Name** —Specify a group name of your choice to represent this connection.
  - **PPPoE User Name** —Specify the username provided by your ISP.
  - **PPPoE Password/Confirm Password** —Specify and confirm the password provided by your ISP.
  - **PPP Authentication** —Choose **PAP** , **CHAP** , or **MSCHAP** .

    PAP passes a cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

- **PPPoE route metric** —Assign an administrative distance to the learned route. Valid values are from 1 to 255. By default, the administrative distance for the learned routes is 1.
- **Enable Route Settings** —To manually configure the PPPoE IP address, check this box and then enter the **IP Address** .

  If you select the **Enable Route Settings** check box and leave the **IP Address** blank, the **ip address pppoe setroute** command is applied as shown in this example:

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- **Store Username and Password in Flash** —Stores the username and password in flash memory.

  The Firewall Threat Defense device stores the username and password in a special location of NVRAM.

Step 6 (Optional) Configure these fields, if you require them.

a) (Optional) See Configure IPv6 addressing, on page 699 to configure IPv6 addressing on the **IPv6** tab.

b) (Optional) See Configure the MAC address, on page 718 to manually configure the MAC address on the **Advanced** tab.

c) Enable Firewall Management Center manager access on a data interface on the **Manager Access** page.

You can enable manager access from a data interface when you first setup the Firewall Threat Defense . If you want to enable or disable manager access after you added the Firewall Threat Defense to the Firewall Management Center , see:

- Enable manager access: Change the manager access interface from management to data, on page 779



Note You cannot enable manager access unless you first initiate the manager interface migration from Management to a data interface. After you initiate the migration, you can enable manager access on the **Manager Access** page and save the configuration successfully.

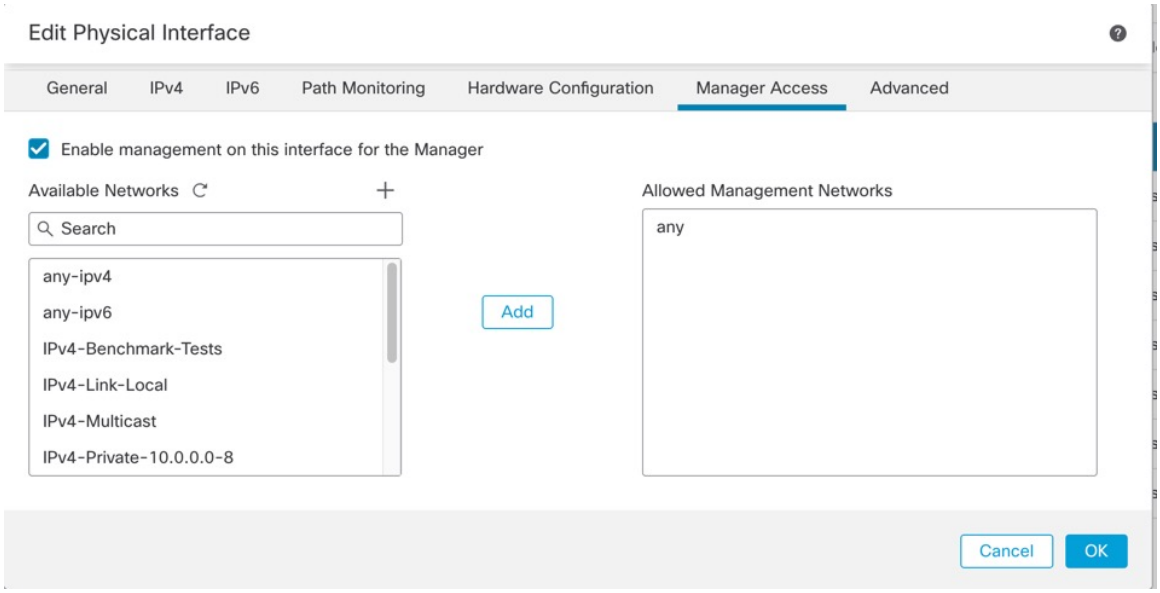
- Disable manager access: Change the manager access interface from data to management, on page 783

If you want to change the manager access interface from one data interface to another data interface, you must disable manager access on the original data interface, but do not disable the interface itself yet; the original data interface must be used to perform the deployment. If you want to use the same IP address on the new manager access interface, you can delete or change the IP configuration on the original interface; this change should not affect the deployment. If you use a different IP address for the new interface, then also change the device IP address shown in the Firewall Management Center ; see Update the Hostname or IP Address in the Firewall Management Center, on page 772 . Be sure to also update related configuration to use the new interface such as static routes, DDNS, and DNS settings.

Manager access from a data interface has the following limitations:

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel, nor can you create a subinterface on the manager access interface. You can also use the Firewall Management Center to enable manager access on a single secondary interface for redundancy.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the Firewall Threat Defense and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the Firewall Management Center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command. For Firewall Threat Defense Virtual on Amazon Web Services, a console port is not available, so you should maintain your SSH access to the Management interface: add a static route for Management before you continue with your configuration. Alternatively, be sure to finish all CLI configuration (including the **configure manager add** command) before you configure the data interface for manager access and you are disconnected.
- You cannot use separate management and event-only interfaces.
- Clustering is not supported. You must use the Management interface in this case.

Figure 288: Manager Access



- Check **Enable management on this interface for the manager** to use this data interface for management instead of the dedicated Management interface.

- (Optional) In the **Allowed Management Networks** box, add the networks from which you want to allow manager access. By default, any networks are allowed.

Step 7 (Optional) Set the duplex and speed by clicking **Hardware Configuration** > **Speed**.

- **Duplex**—Choose **Full** or **Half**. SFP interfaces only support **Full** duplex.
- **Speed**—Choose a speed (varies depending on the model).For SFPs, choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always full, autonegotiation is enabled, and FEC is set to auto. For dual-speed transceivers, the lower speed is used. This option is useful if you later change the network module to a different model, and want the speed to update automatically. Some switches and transceivers don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.



Note You cannot modify the speed of a high availability or a cluster control link interface.

- **Auto-negotiation**—Set the interface to negotiate the link status and flow control.

  Except for the 1100 and 2100, autonegotiation is set separately from the speed. Some switches don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.

- **Forward Error Correction Mode**—For 25Gbps and higher interfaces, enable Forward Error Correction (FEC).

  For an EtherChannel member interface, you must configure FEC before you add it to the EtherChannel. If you remove the interface from the EtherChannel, after rebooting, you may need to reconfigure the FEC for the interface.

  Some switches don't support auto mode for FEC, especially for larger interfaces. Be sure to manually configure the setting, depending on the switch support. We don't recommend disabling FEC; if you do so, the EtherChannel may not come up properly.

  The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 43: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

Note From Version 7.4.2, Firewall Threat Defense supports the SFP 10G_25G_CSR_S module. To avoid link-down issues after a reboot, Forward Error Correction (FEC) must be enabled on these interfaces.

Step 8 Click **OK** .

Step 9 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Bridge group interfaces

A bridge group is a group of interfaces that the Secure Firewall Threat Defense device bridges instead of routes.

Bridge group support

Bridge groups are supported in both transparent and routed firewall mode.

For more information about bridge groups, see Bridge groups, on page 73.

To configure bridge groups and associated interfaces, perform these steps.

Configure general bridge group member interface parameters

This task configures the name and security zone for each bridge group member interface to enable bridge group functionality.

The same bridge group can include different types of interfaces: physical interfaces, VLAN subinterfaces, Firepower 1010 VLAN interfaces, EtherChannels, and redundant interfaces. The Management interface is not supported. In routed mode, EtherChannels are not supported. For the Firepower 4100/9300, data-sharing type interfaces are not supported.

Before you begin

- Firepower 4100/9300
  1. Configure a physical interface, on page 259
  2. (Optional) Configure any special interfaces.
     - Add an EtherChannel (port channel), on page 261
     - Add a VLAN subinterface for container instances, on page 263 in FXOS

- Add a subinterface, on page 669 in Firewall Management Center

- (Optional) **All other models:**
  - Configure an EtherChannel, on page 619
  - Add a subinterface, on page 669
  - Firepower 1010: Configure a VLAN interface, on page 653

Follow these steps to configure general bridge group member interface parameters:

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Configure these fields:

a) In the **Name** field, enter a name up to 48 characters in length.

You cannot start the name with the phrase "cluster". It is reserved for internal use.

b) Enable the interface by checking the **Enabled** check box.

c) (Optional) Set this interface to **Management Only** to limit traffic to management traffic; through-the-box traffic is not allowed.

d) (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

e) In the **Mode** drop-down list, choose **None**.

Regular firewall interfaces have the mode set to None. The other modes are for IPS-only interface types. After you assign this interface to a bridge group, the mode will show as **Switched**.

f) From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New**.

The bridge group member interface is a Switched-type interface, and can only belong to Switched-type zones. Do not configure any IP address settings for this interface. You will set the IP address for the Bridge Virtual Interface (BVI) only. Note that the BVI does not belong to a zone, and you cannot apply access control policies to the BVI.

Step 4 Refer to Configure the MTU, on page 717 for information about **MTU**.

Step 5 (Optional) Set the duplex and speed by clicking **Hardware Configuration** > **Speed** .

- **Duplex** —Choose **Full** or **Half** . SFP interfaces only support **Full** duplex.
- **Speed** —Choose a speed (varies depending on the model). For SFPs, choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always full, autonegotiation is enabled, and FEC is set to auto. For dual-speed transceivers, the lower speed is used. This option is useful if you later change the network module to a different model, and want the speed to update automatically. Some switches and transceivers don't support autonegotiation, especially for higher speed

interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.

Note You cannot modify the speed of a high availability or a cluster control link interface.

- **Auto-negotiation** —Set the interface to negotiate the link status and flow control.

  Except for the 1100 and 2100 , autonegotiation is set separately from the speed. Some switches don't support autonegotiation, especially for higher speed interfaces. In this case, set the interface on the Firewall Threat Defense to a manual speed and also disable **Auto-negotiation** so the link can come up.

- **Forward Error Correction Mode** —For 25Gbps and higher interfaces, enable Forward Error Correction (FEC).

  For an EtherChannel member interface, configure FEC before adding it to the EtherChannel. If you remove the interface from EtherChannel and then reboot, reconfigure the FEC for the interface.

  Some switches don't support auto mode for FEC, especially for larger interfaces. Be sure to manually configure the setting, depending on the switch support. We don't recommend disabling FEC because the EtherChannel may not function correctly.

  The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 44: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC *x* M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

Note From Version 7.4.2, Firewall Threat Defense supports the SFP 10G_25G_CSR_S module. To avoid link-down issues after a reboot, Forward Error Correction (FEC) must be enabled on these interfaces.

Step 6 (Optional) Refer to Configure IPv6 addressing, on page 699 to configure IPv6 addressing on the **IPv6** tab.

Step 7 (Optional) Refer to Configure the MAC address, on page 718 to manually configure the MAC address on the **Advanced** tab.

Step 8 Click **OK**.

Step 9 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure the bridge virtual interface (BVI)

Configure a Bridge Virtual Interface (BVI) to provide IP addressing for each bridge group, which enables traffic routing and management functionality for the bridge group members.

Each bridge group requires a BVI for which you configure an IP address. The Firewall Threat Defense uses this IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the connected network. For IPv4 traffic, the BVI IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

For routed mode, if you provide a name for the BVI, then the BVI participates in routing. Without a name, the bridge group remains isolated as in transparent firewall mode.

Before you begin

You cannot add the BVI to a security zone; therefore, you cannot apply Access Control policies to the BVI. You must apply your policy to the bridge group member interfaces based on their zones.

Follow these steps to configure the Bridge Virtual Interface (BVI):

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Choose **Add Interfaces** > **Bridge Group Interface**.

a) (Routed Mode) In the **Name** field, enter a name up to 48 characters in length.

You must name the BVI if you want to route traffic outside the bridge group members, for example, to the outside interface or to members of other bridge groups. The name is not case-sensitive.

Step 3 In the **Bridge Group ID** field, enter the bridge group ID between 1 and 250.

Step 4 In the **Description** field, enter a description for this bridge group.

Step 5 On the **Interfaces** tab, click an interface and then click **Add** to move it to the **Selected Interfaces** area. Repeat for all interfaces that you want to make members of the bridge group.

Step 6 Click the **IPv4** tab.

a) (Routed Mode) To set the IP address, use one of the following options from the **IP Type** drop-down list.

High Availability and clustering interfaces only support static IP address configuration; DHCP is not supported.

- **Use Static IP**—Enter the IP address and subnet mask. For High Availability, you can only use a static IP address. Set the standby IP address on the **Devices** > **Device Management**, click the **High Availability** tab in the **Monitored Interfaces** area. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
- **Use DHCP**—Configure the following optional parameters:
  - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
  - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

b) (Transparent Mode) In the **IP Address** field, enter the IPv4 address and subnet mask.

Do not assign a host address (/32 or 255.255.255.255) to the BVI. Also, do not use other subnets that contain fewer than 3 host addresses (one each for the upstream router, downstream router, and transparent firewall) such as a /30 subnet (255.255.255.252). The Firewall Threat Defense device drops all ARP packets to or from the first and last addresses in a subnet. For example, if you use a /30 subnet and assign a reserved address from that subnet to the upstream router, then the Firewall Threat Defense device drops the ARP request from the downstream router to the upstream router.

For High Availability, set the standby IP address on the **Devices** > **Device Management** page, click the **High Availability** tab in the **Monitored Interfaces** area. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 7 (Optional) Refer to Configure IPv6 addressing, on page 699 to configure IPv6 addressing.

Step 8 (Optional) Refer to Add a static ARP entry, on page 718 and Add a static MAC address and disable MAC learning for a bridge group, on page 720 (for transparent mode only) to configure the **ARP** and **MAC** settings.

Step 9 Click **OK**.

Click **Save**.

What to do next

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure IPv6 addressing

This section describes how to configure IPv6 addressing in routed and transparent mode.

About IPv6

This section includes information about IPv6.

IPv6 addressing

IPv6 addressing provides 128 bits of network addressing, which provides more than enough globally unique IP addresses. It supports both public global addresses and private link-local addresses, and

IPv6 address types

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network. For a bridge group, this address needs to be configured for the BVI, and not per member interface. You can also configure a global IPv6 address for the management interface in transparent mode.
- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Neighbor Discovery functions such as address resolution. In a bridge group, only member interfaces have link-local addresses; the BVI does not have a link-local address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. For bridge group member interfaces, when you configure the global address on the BVI, the Firewall Threat Defense device automatically generates link-local addresses for member interfaces. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Modified EUI-64 interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The Firewall Threat Defense device can enforce this requirement for hosts attached to the local link.

Address verification process

When this feature is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and this system log message is generated:

```
325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link.

IPv6 prefix delegation client configuration

The Firewall Threat Defense can act as a DHPCv6 Prefix Delegation client so that the client interface, for example the outside interface connected to a cable modem, can receive one or more IPv6 prefixes that the Firewall Threat Defense can then subnet and assign to its inside interfaces.

IPv6 prefix delegation

IPv6 prefix delegation enables the Firewall Threat Defense to function as a Dynamic Host Control Protocol for IPv6 (DHCPv6) prefix delegation client and receive one or more IPv6 prefixes. This feature allows the Firewall Threat Defense to subnet and assign these prefixes to its inside interfaces. It enable the hosts connected to inside interfaces to use Stateless Address Auto Configuration (SLAAC) to obtain global IPv6 addresses.

Client and server behavior

The client interface, such as the outside interface connected to a cable modem, receives IPv6 prefixes that the Firewall Threat Defense can then subnet and assign to its inside interfaces. The inside Firewall Threat Defense interfaces do not in turn act as Prefix Delegation servers; the Firewall Threat Defense can only provide global IP addresses to SLAAC clients.

If a router is connected to the Firewall Threat Defense, it can act as a SLAAC client to obtain its IP address. However, if you want to use a subnet of the delegated prefix for the networks behind the router, you must manually configure those addresses on the router's inside interfaces.

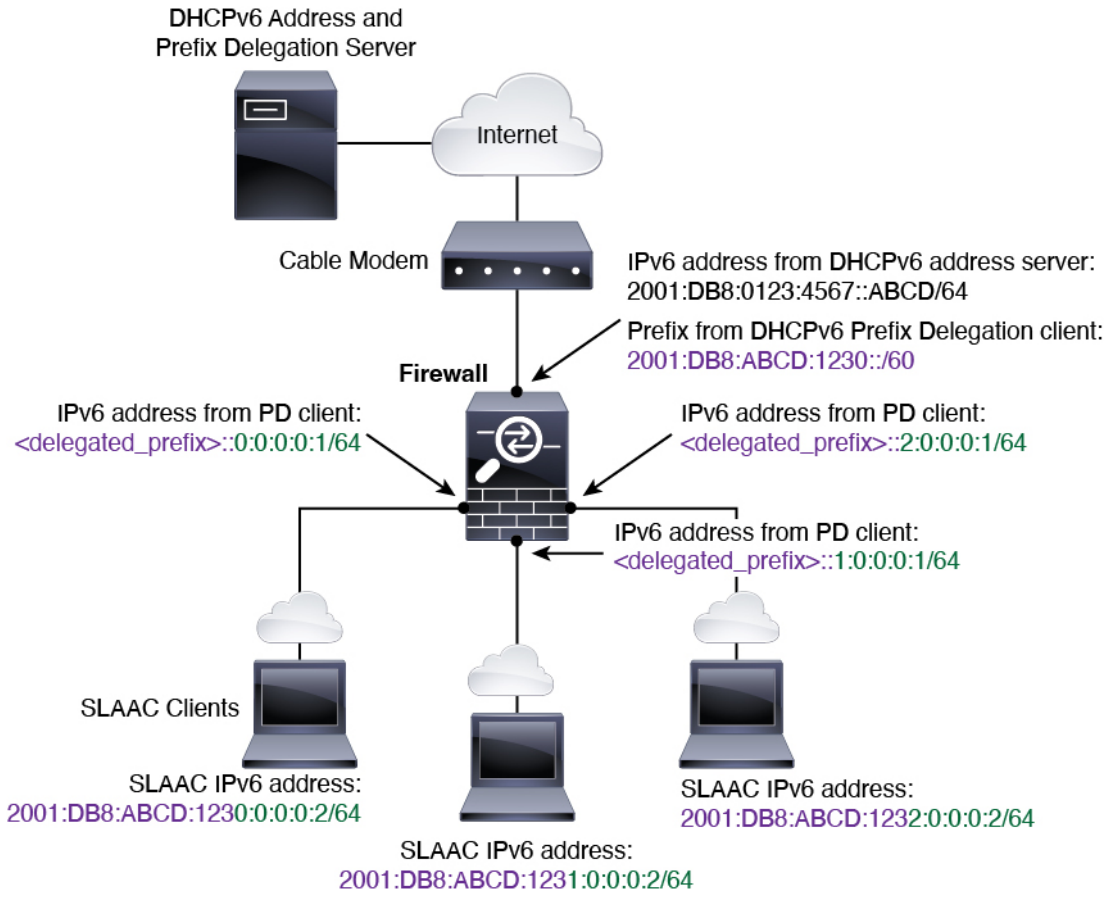
The Firewall Threat Defense includes a light DHCPv6 server. This server provides information, such as the DNS server and domain name, to SLAAC clients when they send Information Request (IR) packets to the Firewall Threat Defense. The Firewall Threat Defense only accepts IR packets, and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages. In other words, the addresses are based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

IPv6 prefix delegation /64 subnet example

Here is an IPv6 prefix delegation /64 subnet example that demonstrates how a device subnets delegated prefixes into /64 networks and assigns global IPv6 addresses to interfaces.

IPv6 prefix delegation /64 subnet configuration

This example shows the Firewall Threat Defense receiving an IP address on the outside interface using the DHCPv6 address client. It also gets a delegated prefix using the DHCPv6 Prefix Delegation client. The Firewall Threat Defense subnets the delegated prefix into /64 networks and assigns global IPv6 addresses to its inside interfaces dynamically using the delegated prefix plus a manually configured subnet (::0, ::1, or ::2) and IPv6 address (0:0:0:1) per interface. SLAAC clients connected to those inside interfaces obtain IPv6 addresses on each /64 subnet.

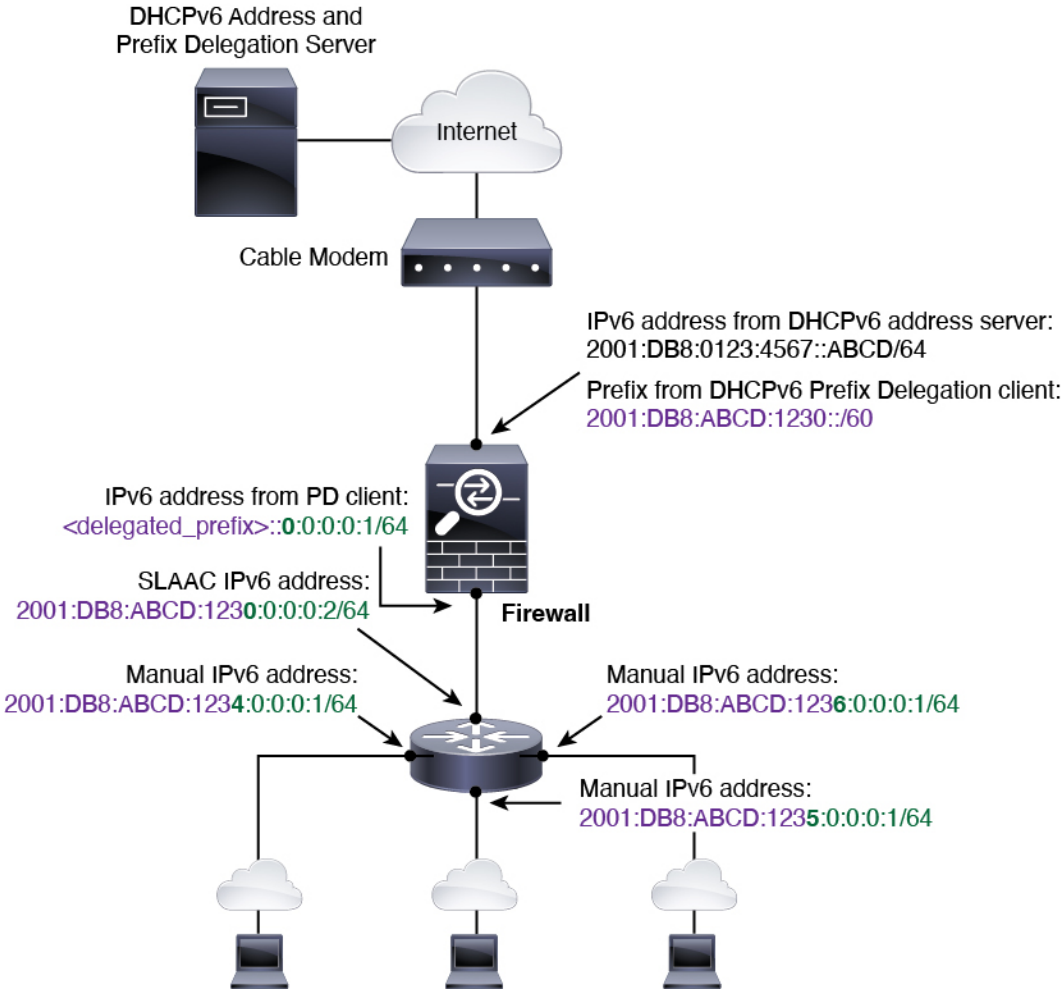


IPv6 prefix delegation /62 subnet examples

IPv6 prefix delegation /62 subnet enables subnetting of prefixes into 4 /62 subnets for downstream router delegation. It allows manual configuration of /64 subnets on router interfaces when dynamic prefix assignment is not available.

IPv6 /62 subnet delegation configuration

This example shows the Firewall Threat Defense subnetting the prefix into 4 /62 subnets: 2001:DB8:ABCD:123**0**::/62, 2001:DB8:ABCD:123**4**::/62, 2001:DB8:ABCD:123**8**::/62, and 2001:DB8:ABCD:123**C**::/62. The Firewall Threat Defense uses one of 4 available /64 subnets on 2001:DB8:ABCD:1230::/62 for its inside network (::0). You can then manually use additional /62 subnets for downstream routers. The router shown uses 3 of 4 available /64 subnets on 2001:DB8:ABCD:1234::/62 for its inside interfaces (::4, ::5, and ::6). In this case, the inside router interfaces cannot dynamically obtain the delegated prefix, so you need to view the delegated prefix on the Firewall Threat Defense, and then use that prefix for your router configuration. Usually, ISPs delegate the same prefix to a given client when the lease expires, but if the Firewall Threat Defense receives a new prefix, you will have to modify the router configuration to use the new prefix. The DHCP unique identifier (DUID) is persistent across reboots.



Enable the IPv6 prefix delegation client

Enable the DHCPv6 Prefix Delegation client to obtain one or more IPv6 prefixes that can be subnetted and assigned to inside networks.

Enable the DHCPv6 Prefix Delegation client on one or more interfaces. The Firewall Threat Defense obtains one or more IPv6 prefixes that it can subnet and assign to inside networks. Typically, the interface on which you enable the prefix delegation client obtains its IP address using the DHCPv6 address client; only other Firewall Threat Defense interfaces use addresses derived from the delegated prefix.

This feature is supported only in routed mode.

This feature is not supported in clustering or High Availability.

Before you begin

When you use Prefix Delegation, you must set the Firewall Threat Defense IPv6 neighbor discovery router advertisement interval to be much lower than the preferred lifetime of the prefix assigned by the DHCPv6 Server to prevent IPv6 traffic interruption. For example, if the DHCPv6 server sets the preferred Prefix Delegation lifetime to 300 seconds, you should set the Firewall Threat Defense RA interval to be 150 seconds. To set the preferred lifetime, use the **show ipv6 general-prefix** command. To set the Firewall Threat Defense RA interval, see Configure IPv6 neighbor discovery, on page 709. The default is 200 seconds.

Procedure

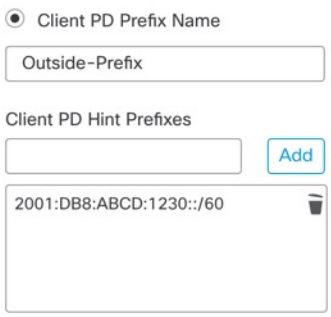
Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Click the **IPv6** page, and then click **DHCP**.

Step 4 Click **Client PD Prefix Name** and enter a name for this prefix.

Figure 289: Enable the prefix delegation client



The name can be up to 200 characters.

Step 5 (Optional) Enter the prefix and prefix length in the **Client PD Hint Prefixes** field to provide one or more hints to the DHCP server about the delegated prefix you want to receive, then click **Add**.

Typically you want to request a particular prefix length, such as ::/60, or if you have received a particular prefix before and want to ensure you get it again when the lease expires, you can enter the whole prefix as the hint. If you enter multiple hints (different prefixes or lengths), then it is up to the DHCP server which hint to honor, or whether to honor the hint at all.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure a global IPv6 address

Before you begin

For IPv6 neighbor discovery for bridge groups, you must explicitly allow Neighbor Solicitation (ICMPv6 type 135) and Neighbor Advertisement (ICMPv6 type 136) packets through the Firewall Threat Defense bridge group member interfaces using a bidirectional access rule.

To configure a global IPv6 address for any routed mode interface and for the transparent or routed mode BVI, perform the following steps.

Note Configuring the global address automatically configures the link-local address, so you do not need to configure it separately. For bridge groups, configuring the global address on the BVI automatically configures link-local addresses on all member interfaces.

For subinterfaces defined on the Firewall Threat Defense , we recommend that you also set the MAC address manually, because they use the same burned-in MAC address of the parent interface. IPv6 link-local addresses are generated based on the MAC address, so assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense . See Configure the MAC address, on page 718 .

Firewall Threat Defense Feature History:

- 7.3—DHCPv6 Address client
- 7.3—DHCPv6 Prefix Delegation client
- 7.3—DHCPv6 stateless server

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** ( ) for the interface you want to edit.

Step 3 Click the **IPv6** page.

For routed mode, the **Basic** page is selected by default. For transparent mode, the **Address** page is selected by default.

Step 4 On the **Basic** page, check **Enable IPv6** .

Use this option if you want to only configure the link-local addresses. Otherwise, configuring an IPv6 address enables IPv6 processing automatically.

Step 5 Configure the global IPv6 address using one of the following methods.

For failover and clustering, and for loopback interfaces, you must set the IP address manually. For clustering, manually configuring the link-local address is also not supported.

- (Routed interface) Stateless autoconfiguration—Check the **Autoconfiguration** check box.

  Enabling stateless autoconfiguration on the interface configures IPv6 addresses based upon prefixes received in Router Advertisement messages. A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.

  Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the Firewall Threat Defense device does send Router Advertisement messages in this case. Click the **Settings** tab and click the **IPv6** tab and then uncheck the **Enable RA** check box to suppress messages.

- Manual configuration—To manually configure a global IPv6 address:

a. Click the **Address** page, and click (+) **Add Address** .

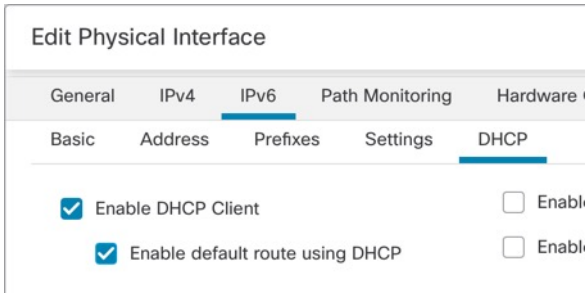
   The **Add Address** dialog box appears.

b. In the **Address** field, enter either a full global IPv6 address, including the interface ID, or enter the IPv6 prefix, along with the IPv6 prefix length. (Routed Mode) If you only enter the prefix, then be sure to check the **Enforce EUI 64** check box to generate the interface ID using the Modified EUI-64 format. For example, 2001:0DB8::BA98:0:3210/48 (full address) or 2001:0DB8::/48 (prefix, with EUI 64 checked).

   For High Availability (if you did not set **Enforce EUI 64**), set the standby IP address on the **Devices** > **Device Management** page, click **High Availability** in the **Monitored Interfaces** area. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

- (Routed interface) Obtain an address using DHCPv6—To use DHCPv6:

Figure 290: Enable the DHCPv6 Client



a. Click the **DHCP** page.

b. Check the check box of **Enable DHCP Client** .

c. (Optional) Check the check box of **Enable default route using DHCP** to obtain a default route from Router Advertisements.

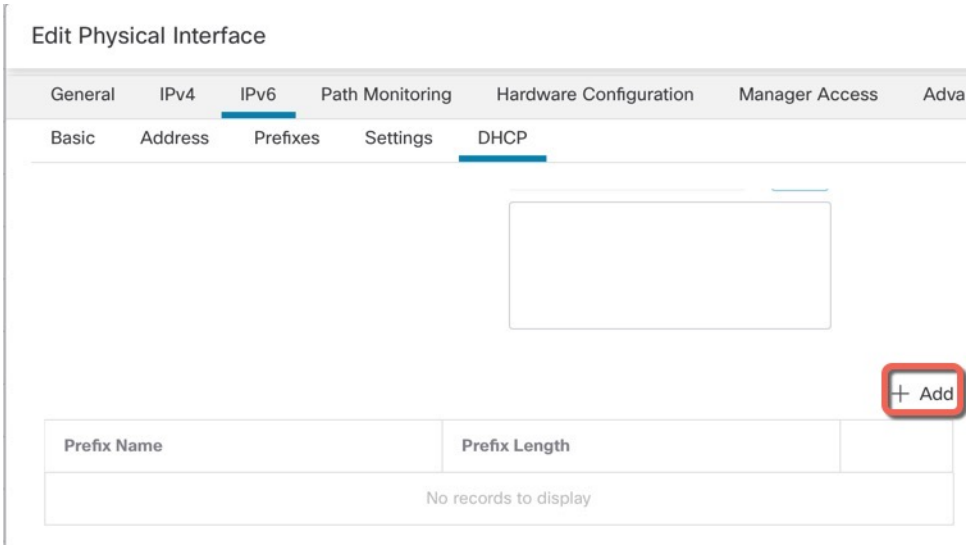
- (Routed interface) Use a delegated prefix—To assign an IPv6 address using the delegated prefix:

  This feature requires the Firewall Threat Defense to have the DHCPv6 Prefix Delegation client enabled *on a different interface* . See Enable the IPv6 prefix delegation client, on page 703 .

a. Click the **DHCP** page.

b. Click (+) .

Figure 291: Use a Delegated Prefix

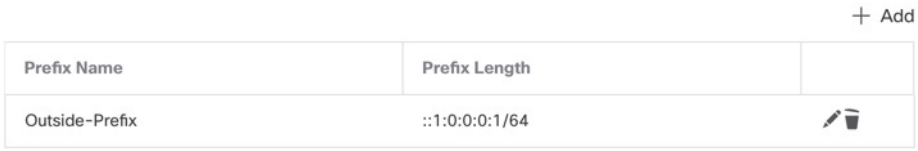


c. Enter the IPv6 address and **Prefix Length** .

Typically, the delegated prefix will be /60 or smaller so you can subnet to multiple /64 networks. /64 is the supported subnet length if you want to support SLAAC for connected clients. You should specify an address that completes the /60 subnet, for example ::1:0:0:0:1. Enter :: before the address in case the prefix is smaller than /60. For example, if the delegated prefix is 2001:DB8:1234:5670::/60, then the global IP address assigned to this interface is 2001:DB8:1234:5671::1/64. The prefix that is advertised in router advertisements is 2001:DB8:1234:5671::/64. In this example, if the prefix is smaller than /60, the remaining bits of the prefix will be 0's as indicated by the leading ::. For example, if the prefix is 2001:DB8:1234::/48, then the IPv6 address will be 2001:DB8:1234::1:0:0:0:1/64.

d. Click **OK** .

Figure 292: Prefix Delegation Table



e. Optionally enable the DHCPv6 stateless server on this interface (see Enable the DHCPv6 stateless server, on page 836). If you do so, we recommend that you also check the **Enable DHCP for non-address config** option.

Step 6 For Routed interfaces, you can optionally set these values on the **Basic** page:

- To enforce the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link, check the **Enforce EUI-64** check box.
- To manually set the link-local address, enter an address in the **Link-Local address** field.

A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. If you do not want to configure a global address, and only need to configure a link-local address, you have the option of manually defining the link-local address. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

Clustering does not support manual link-local addresses.

Step 7 For Routed interfaces, you can optionally set the following values on the **DHCP** page:

- Check the **Enable DHCP for address config** check box to set the Managed Address Config flag in the IPv6 router advertisement packet.

  This flag in IPv6 router advertisements informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.

- Check the **Enable DHCP for non-address config** check box to set the Other Address Config flag in the IPv6 router advertisement packet.

  This flag in IPv6 router advertisements informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address. Use this option when using the DHCPv6 stateless server with DHCPv6 prefix delegation.

Step 8 For Routed interfaces, see Configure IPv6 neighbor discovery, on page 709 to configure settings on the **Prefixes** and **Settings** pages. For BVI interfaces, see the following parameters on the **Settings** page:

- **DAD attempts** —The maximum number of DAD attempts , between 1 and 600. Set the value to 0 to disable duplicate address detection (DAD) processing. This setting configures the number of consecutive neighbor solicitation messages that are sent on an interface while DAD is performed on IPv6 addresses . 1 attempt is the default.
- **NS Interval** —The interval between IPv6 neighbor solicitation retransmissions on an interface , between 1000 and 3600000 ms . The default value is 1000 ms.
- **Reachable Time** —The amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred , between 0 and 3600000 ms . The default value is 0 ms. When 0 is used for the value, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value. The neighbor reachable time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Step 9 Click **OK** .

Click **Save**.

What to do next

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure IPv6 neighbor discovery

Before you begin

Supported in Routed mode only. For IPv6 neighbor settings supported in transparent mode, see Configure a global IPv6 address, on page 704 .

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the readability of a neighbor, and keep track of neighboring routers.

Nodes (hosts) use neighbor discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use neighbor discovery to find neighboring routers that are willing to forward packets on their behalf. In addition, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** ( ) for the interface you want to edit.

Step 3 Click **IPv6** , and then **Prefixes**.

To configure the IPv6 router advertisements with IPv6 prefixes, perform these steps:

a) Click ( ) **Add Prefix** .
b) In the **Address** field, enter the IPv6 address with the prefix length or check the **Default** check box to use the default prefix.
c) (Optional) Uncheck the **Advertisement** check box to indicate that the IPv6 prefix is not advertised. For the **Default** prefix, this setting only applies to on-link prefixes. Off-link prefixes will still be advertised unless you uncheck **Advertisement** for a specific off-link prefix.
d) Check the **Off Link** check box to indicate that the specified prefix is assigned to the link. Nodes sending traffic to addresses that contain the specified prefix consider the destination to be locally reachable on the link. This prefix should not be used for on-link determination.
e) To use the specified prefix for autoconfiguration, check the **Autoconfiguration** check box.
f) For the **Prefix Lifetime** , click **Duration** or **Expiration Date** .

- **Duration** —Enter a **Preferred Lifetime** for the prefix in seconds. This setting is the amount of time that the specified IPv6 prefix is advertised as being valid. The maximum value represents infinity. Valid values are from 0 to 4294967295. The default is 2592000 (30 days). Enter a **Valid Lifetime** for the prefix in seconds. This setting is the amount of time that the specified IPv6 prefix is advertised as being preferred. The maximum value represents infinity. Valid values are from 0 to 4294967295. The default setting is 604800 (seven days). Alternatively, check the **Infinite** check box to set an unlimited duration.
- **Expiration Date** —Choose a **Valid** and **Preferred** date and time.

g) Click **OK** .

Step 4 Click **Settings**.

a) (Optional) Set the maximum number of **DAD attempts** , between 1 and 600. 1 attempt is the default. Set the value to 0 to disable duplicate address detection (DAD) processing.

This setting configures the number of consecutive neighbor solicitation messages that are sent on an interface while DAD is performed on IPv6 addresses.

During the stateless autoconfiguration process, Duplicate Address Detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces.

When a duplicate address is identified, the state of the address is set to DUPLICATE, the address is not used, and the following error message is generated:

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used.

b) (Optional) Configure the interval between IPv6 neighbor solicitation retransmissions in the **NS Interval** field, between 1000 and 3600000 ms.

The default value is 1000 ms.

Neighbor solicitation messages (ICMPv6 Type 135) are sent on the local link by nodes attempting to discover the link-layer addresses of other nodes on the local link. After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICPMv6 Type 136) on the local link.

After the source node receives the neighbor advertisement, the source node and destination node can communicate. Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verifying the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link.

Step 5 (Optional) Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred in the **Reachable Time** field, between 0 and 3600000 ms.

The default value is 0 ms. When 0 is used for the value, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

The neighbor reachable time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Step 6 (Optional) To suppress the router advertisement transmissions, uncheck the **Enable RA** check box. If you enable router advertisement transmissions, you can set the RA lifetime and interval.

Router advertisement messages (ICMPv6 Type 134) are automatically sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You may want to disable these messages on any interface for which you do not want the Firewall Threat Defense to supply the IPv6 prefix (for example, the outside interface).

- **RA Lifetime** —Configure the router lifetime value in IPv6 router advertisements, between 0 and 9000 seconds.

The default is 1800 seconds.

- **RA Interval** —Configure the interval between IPv6 router advertisement transmissions, between 3 and 1800 seconds.

  The default is 200 seconds.

  To prevent synchronization with other IPv6 nodes, the firewall randomly adjusts the value that you set (jitter).

Step 7 Click **OK**.

Click **Save**.

What to do next

Go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Advanced interface settings

This section describes how to configure MAC addresses for regular firewall mode interfaces, how to set the maximum transmission unit (MTU), and how to set other advanced parameters.

About advanced interface configuration

This section describes advanced interface settings.

MAC addresses

Media Access Control (MAC) address is a unique physical address of a network device.

You can manually assign MAC addresses to override the default. For container instances, the FXOS chassis automatically generates unique MAC addresses for all interfaces.

Note You might want to assign unique MAC addresses to subinterfaces defined on the Firewall Threat Defense, because they use the same burned-in MAC address of the parent interface. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense device.

Note For container instances, even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

Default MAC addresses

This reference provides information about default MAC addresses used in network devices and their configurations.

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- VLAN interfaces (Firepower 1010)—Routed firewall mode: All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See Configure the MAC address, on page 718.

  Transparent firewall mode: Each VLAN interface has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See Configure the MAC address, on page 718.
- EtherChannels—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.
- EtherChannels (ASA Models)—The port-channel interface uses the lowest-numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can configure a MAC address for the port-channel interface. We recommend configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.
- Subinterfaces (Firewall Threat Defense-defined)—All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense.

For container instances:

- MAC addresses for all interfaces are taken from a MAC address pool. For subinterfaces, if you decide to manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification. See Automatic MAC Addresses for Container Instance Interfaces, on page 246.

MTU

Maximum Transmission Unit (MTU) specifies the maximum frame *payload* size that the Firewall Threat Defense can transmit on a given Ethernet interface. The MTU value *excludes* Ethernet headers, VLAN tags, or other overhead. For example, if you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when VLAN tagging is used. Do not set the MTU value higher to accommodate these headers.

VXLAN and geneve encapsulation requirements

For Geneve, the entire Ethernet datagram is being encapsulated, so the new IP packet is larger and requires a larger MTU. Set the Firewall Threat Defense VTEP source interface MTU to the network MTU plus 306 bytes.

Path MTU discovery

Path MTU Discovery enables all devices in a network path between two hosts to coordinate the MTU so they can standardize on the lowest MTU in the path.

Path MTU discovery support

The Firewall Threat Defense supports Path MTU Discovery (as defined in RFC 1191).

Default MTU

The default MTU on the Firewall Threat Defense device is 1500 bytes. This value does not include the 18-22 bytes for the Ethernet header, VLAN tagging, or other overhead.

MTU and fragmentation

IPv4 packets that are larger than the specified MTU are fragmented into multiple frames.

Packet handling details

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For TCP packets, the endpoints typically use their MTU to determine the TCP maximum segment size (MTU - 40, for example). If additional TCP headers are added along the way, for example for site-to-site VPN tunnels, then the TCP MSS might need to be adjusted down by the tunneling entity. See TCP MSS, on page 714.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.



Note The Firewall Threat Defense can receive frames larger than the configured MTU as long as there is room in memory.

Full reassembly for inspected fragmented packets

The FTD performs virtual reassembly by default. However, when features such as DNS or voice media inspection are active, the firewall performs full reassembly before forwarding. This ensures packets are processed correctly by inspection engines.

For example, SIP packets subject to inspection require full reassembly. If SIP inspection is disabled, the system maintains virtual reassembly. To avoid issues, we recommend reducing SIP message size or using TCP or TLS for large messages rather than sending large SIP INVITE packets over UDP.

The firewall merges fragments in memory. If the egress interface MTU is smaller than the reassembled packet, the device will refragment the data to fit. To verify behavior, use packet captures on the egress interface and adjust MTU settings as needed.

MTU and jumbo frames configuration

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network.

- Matching MTUs on the traffic path—We recommend that you set the MTU on all Firewall Threat Defense interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames—You can set the MTU 9000 bytes or higher when you enable jumbo frames. The maximum depends on the model.

TCP MSS

The TCP maximum segment size (MSS) is the size of the TCP payload *before* any TCP and IP headers are added. TCP MSS values are exchanged between client and server during the three-way handshake when establishing connections. UDP packets are not affected.

TCP MSS configuration and behavior

You can set the TCP MSS on the Firewall Threat Defense device for through traffic using the Sysopt_Basic object in FlexConfig. By default, the maximum TCP MSS is set to 1380 bytes. This setting is useful if the Firewall Threat Defense device must increase the packet size for IPsec VPN encapsulation. However, for non-IPsec endpoints, you should disable the maximum TCP MSS on the Firewall Threat Defense device.

If you set a maximum TCP MSS and either endpoint of a connection requests a TCP MSS larger than this value, the Firewall Threat Defense device overwrites the TCP MSS in the request packet with the Firewall Threat Defense device maximum. If the host or server does not request a TCP MSS, the Firewall Threat Defense device assumes the RFC 793-default value of 536 bytes for IPv4 or 1220 bytes for IPv6, but does not modify the packet.

You can also configure the minimum TCP MSS. If a host or server requests a very small TCP MSS, the Firewall Threat Defense device can increase the value. By default, the minimum TCP MSS is not enabled.

For to-the-box traffic, including for SSL VPN connections, this setting does not apply. The Firewall Threat Defense device derives the TCP MSS from MTU: MTU minus 40 for IPv4 or MTU minus 60 for IPv6.

TCP MSS adjustment scenario

For example, you leave the default MTU as 1500 bytes. A host requests an MSS of 1500 minus the TCP and IP header length, which sets the MSS to 1460. If the Firewall Threat Defense device maximum TCP MSS is 1380 (the default), then the Firewall Threat Defense device changes the MSS value in the TCP request packet to 1380. The server then sends packets with 1380-byte payloads. The Firewall Threat Defense device can add up to 120 bytes of headers to the packet, and the resulting packet fits within the MTU size of 1500 bytes.

Default TCP MSS

A default TCP MSS is a network configuration setting that sets the maximum TCP MSS on the Firewall Threat Defense device to 1380 bytes by default, accommodates IPv4 IPsec VPN connections where the headers can equal up to 120 bytes, and fits within the default MTU of 1500 bytes.

Suggested maximum TCP MSS setting

The default TCP MSS assumes the Firewall Threat Defense device acts as an IPv4 IPsec VPN endpoint and has an MTU of 1500. When the Firewall Threat Defense device acts as an IPv4 IPsec VPN endpoint, it needs to accommodate up to 120 bytes for TCP and IP headers.

If you change the MTU value, use IPv6, or do not use the Firewall Threat Defense device as an IPsec VPN endpoint, then you should change the TCP MSS setting using the Sysopt_Basic object in FlexConfig.



Note If you explicitly set an MSS, a component such as TLS/SSL decryption or server discovery might require a particular MSS.In that case, the component sets the MSS based on the interface MTU and ignores your MSS setting.

- Normal traffic—Disable the TCP MSS limit and accept the value established between connection endpoints. Because connection endpoints typically derive the TCP MSS from the MTU, non-IPsec packets usually fit this TCP MSS.
- IPv4 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 120. For example, if you use jumbo frames and set the MTU to 9000, then you need to set the TCP MSS to 8880 to take advantage of the new MTU.
- IPv6 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 140.

ARP inspection for bridge group traffic

This reference describes ARP inspection functionality for bridge group traffic in transparent firewall configurations.

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

When you enable ARP inspection, the Firewall Threat Defense device compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the Firewall Threat Defense device drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the Firewall Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated Management interface never floods packets even if this parameter is set to flood.

MAC address tables

A MAC address table associates each MAC address with its source interface for accurate packet routing.

MAC address table behavior

When you use bridge groups, the Firewall Threat Defense learns and builds a MAC address table in a way similar to a normal bridge or switch. When a device sends a packet through the bridge group, the Firewall Threat Defense adds the MAC address to its table. The table associates the MAC address with the source interface so that the Firewall Threat Defense knows to send any packets addressed to the device out the correct interface. Because traffic between bridge group members is subject to the Firewall Threat Defense security policy, if the destination MAC address of a packet is not in the table, the Firewall Threat Defense does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the packets for directly-connected devices or for remote devices.

- Packets for directly-connected devices—The Firewall Threat Defense generates an ARP request for the destination IP address so that it can learn which interface receives the ARP response.
- Packets for remote devices—The Firewall Threat Defense generates a ping to the destination IP address so that it can learn which interface receives the ping reply.

The original packet is dropped.

Default settings

This reference provides default configuration settings for ARP inspection, MAC address table entries, and interface behavior for MAC address learning.

- If you enable ARP inspection, the default setting is to flood non-matching packets.
- The default timeout value for dynamic MAC address table entries is five minutes.
- By default, each interface automatically learns the MAC addresses of entering traffic, and the Firewall Threat Defense device adds corresponding entries to the MAC address table.

Note Secure Firewall Threat Defense device generates a reset packet to reset a connection that is denied by a stateful inspection engine. Here, the destination MAC address of the packet is not determined based on the ARP table lookup but instead it is taken directly from the packets (connections) that are being denied.

Guidelines for ARP inspection and the MAC address table

Consider these configuration support limitations for ARP inspection and MAC address table management:

- ARP inspection is only supported for bridge groups.
- MAC address table configuration is only supported for bridge groups.

Configure the MTU

Customize the MTU on the interface, for example, to allow jumbo frames.

For the ISA 3000 and the Firewall Threat Defense Virtual: Changing the MTU above 1500 bytes automatically enables jumbo-frame reservation. You must restart the system before you can use jumbo frames. For the Firewall Threat Defense Virtual that supports clustering, you can enable jumbo-frame reservation in the Day0 configuration, so in that case, you do not need to restart. After you restart, you cannot disable jumbo-frame reservation. An exception is for the Firewall Threat Defense Virtual, where you can disable jumbo-frame reservation in the Day0 configuration, if supported. If you use an interface in an inline set, the MTU setting is not used. However, the jumbo-frame reservation setting *is* relevant to inline sets; jumbo frames enable the inline interfaces to receive packets up to 9000 bytes. To enable jumbo-frame reservation, you must set the MTU of *any* interface above 1500 bytes.

Jumbo frames are enabled by default on other platforms.

Caution Changing the highest MTU value on the device for a data interface restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all data interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. This caution does not apply to management-only interfaces. See Snort restart traffic behavior, on page 129 for more information.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 On the **General** tab, set the **MTU**. The minimum and maximum depends on your platform.

The default is 1500 bytes.

Step 4 Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Step 6 For the ISA 3000 and the Firewall Threat Defense Virtual, if you set the MTU above 1500 bytes, restart the system to enable jumbo-frame reservation. See Shut down or restart the device, on page 55.

Configure the MAC address

This task allows you to manually assign MAC addresses to interfaces, including active and standby MAC addresses for high availability configurations.

You might need to manually assign a MAC address. You can also set the Active and Standby MAC addresses on the **Devices** > **Device Management** window by choosing **High Availability** from the **Add** drop-down list. If you set the MAC address for an interface on both screens, the addresses on the **Interfaces** > **Advanced** tab take precedence.

Note For container instances, even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Click the **Advanced** tab.

The **Information** tab is selected.

Step 4 Set the active and standby MAC addresses.

a) In the **Active MAC Address** field, enter a MAC address in H.H.H format, where H is a 16-bit hexadecimal digit.

For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.

b) In the **Standby MAC Address** field, enter a MAC address for use with High Availability.

If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 5 Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Add a static ARP entry

Add static ARP entries to control ARP packet flow and support ARP inspection for bridge group members or routed interfaces.

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection (see Configure ARP inspection, on page 850). ARP inspection compares ARP packets with *static* ARP entries in the ARP table.

For routed interfaces, you can enter static ARP entries, but dynamic entries are usually sufficient. For routed interfaces, the ARP table is used to deliver packets to directly-connected hosts. Although senders identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry must time out before it can be updated with the new information.

For transparent mode, the Firewall Threat Defense only uses dynamic ARP entries in the ARP table for traffic to and from the Firewall Threat Defense device, such as management traffic.

Before you begin

This screen is only available for named interfaces.

Follow these steps to add a static ARP entry:

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** ( ) for the interface you want to edit.

Step 3 Click the **Advanced** tab, and then click the **ARP** tab (called **ARP and MAC** for transparent mode).

Step 4 Click ( )**Add ARP Config**.
The **Add ARP Config** dialog box appears.

Step 5 In the **IP Address** field, enter the IP address of the host.

Step 6 In the **MAC Address** field, enter the MAC address of the host; for example, 00e0.1e4e.3d8b.

Step 7 To perform proxy ARP for this address, check the **Enable Alias** check box.

If the Firewall Threat Defense device receives an ARP request for the specified IP address, then it responds with the specified MAC address.

Step 8 Click **OK**, and then click **OK** again to exit the Advanced settings.

Step 9 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Add a static MAC address and disable MAC learning for a bridge group

Add static MAC addresses to the MAC address table and optionally disable MAC address learning to guard against MAC spoofing and control traffic flow through the Firewall Threat Defense device.

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can disable MAC address learning. If you do not statically add MAC addresses to the table, no traffic can pass through the Firewall Threat Defense device. You can also add static MAC addresses to the MAC address table. One benefit to adding static entries is to guard against MAC spoofing. If a client uses the same MAC address as a static entry and sends traffic to an interface that does not match the static entry, the Firewall Threat Defense device drops the traffic and generates a system message. When you add a static ARP entry (see Add a static ARP entry, on page 718), a static MAC address entry is automatically added to the MAC address table.

Before you begin

This screen is only available for named BVIs in transparent mode.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Click the **Advanced** tab, and then click the **ARP and MAC** tab.

Step 4 (Optional) Disable MAC learning by unchecking the **Enable MAC Learning** check box.

Step 5 To add a static MAC address, click **Add MAC Config**.
The **Add MAC Config** dialog box appears.

Step 6 In the **MAC Address** field, enter the MAC address of the host; for example, 00e0.1e4e.3d8b. Click **OK**.

Step 7 Click **OK** to exit the Advanced settings.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Set security configuration parameters

This task configures security parameters on named interfaces to prevent IP spoofing attacks and control packet fragmentation behavior. You can enable anti-spoofing protection, configure full fragment reassembly, and customize fragment handling settings.

This section describes how to prevent IP spoofing, allow full fragment reassembly, and override the default fragment setting at the device level in **Platform Settings**.

Anti-spoofing

This section lets you enable Unicast Reverse Path Forwarding on an interface. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

Normally, the Firewall Threat Defense device only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the device to also look at the source address. This is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the Firewall Threat Defense device, the device routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the Firewall Threat Defense device can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the device uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the Firewall Threat Defense device drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the device drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

Fragment per packet

By default, the Firewall Threat Defense device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to let fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, if you do not have an application that fragments traffic, we recommend that you do not allow fragments through the Firewall Threat Defense device. Fragmented packets are often used as DoS attacks.

Fragment reassembly

The Firewall Threat Defense device performs the following fragment reassembly processes:

- IP fragments are collected until a fragment set is formed or until a timeout interval has elapsed.
- If a fragment set is formed, integrity checks are performed on the set. These checks include no overlapping, no tail overflow, and no chain overflow.
- IP fragments that terminate at the Firewall Threat Defense device are always fully reassembled.
- If **Full Fragment Reassembly** is disabled (the default), the fragment set is forwarded to the transport layer for further processing.
- If **Full Fragment Reassembly** is enabled, the fragment set is first coalesced into a single IP packet. The single IP packet is then forwarded to the transport layer for further processing.

Full reassembly for inspected fragmented packets

The Firewall Threat Defense performs virtual reassembly by default. However, when features such as DNS or voice media inspection are active, the firewall performs full reassembly before forwarding. This ensures packets are processed correctly by inspection engines.

For example, SIP packets subject to inspection require full reassembly. If SIP inspection is disabled, the system maintains virtual reassembly. To avoid issues, we recommend reducing SIP message size or using TCP or TLS for large messages rather than sending large SIP INVITE packets over UDP.

The firewall merges fragments in memory. If the egress interface MTU is smaller than the reassembled packet, the device will refragment the data to fit. To verify behavior, use packet captures on the egress interface and adjust MTU settings as needed.

Before you begin

This screen is only available for named interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Click the **Advanced** tab, and then click the **Security Configuration** tab.

Step 4 To enable Unicast Reverse Path Forwarding, check the **Enable Anti Spoofing** check box.

Step 5 To enable full fragment reassembly, check the **Allow Full Fragment Reassembly** check box.

Step 6 To change the number of fragments allowed per packet, check the **Override Default Fragment Setting** check box, and set the following values:

- **Size**—Set the maximum number of packets that can be in the IP reassembly database waiting for reassembly. The default is 200. Set this value to 1 to disable fragments.
- **Chain**—Set the maximum number of packets into which a full IP packet can be fragmented. The default is 24 packets.
- **Timeout**—Set the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded. The default is 5 seconds.

Step 7 Click **OK**.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

History for Regular Firewall Interfaces

Provides a comprehensive history of interface-related features, including hardware support, protocol enhancements, and configuration changes for Secure Firewall devices.

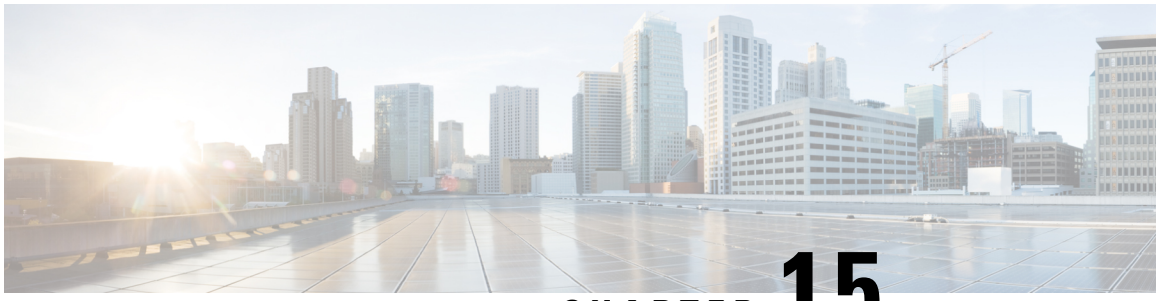
Table 45: History for Regular Firewall Interfaces

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) options to advertise a list of DNS servers and domains to IPv6 clients	10.0.0 20251121	10.0.0	You can now configure Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) options to provide DNS servers and domains to SLAAC clients using router advertisements. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **Settings** New/modified commands: **show ipv6 nd detail** , **show ipv6 nd ra dns-search-list** , **show ipv6 nd ra dns server** , **show ipv6 nd summary**
Secure Firewall 200 hardware switch support	10.0.0 20251121	10.0.0	The Secure Firewall 200 supports setting each Ethernet interface to be a switch port or a firewall interface.
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE)	7.7.0	7.7.0	See the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline** . New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **PoE** New/Modified commands: **show power inline**
For models with built-in-switches, subinterfaces can't use VLAN 1	7.6	7.6	For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade a 1010 to 7.6 or later, and you have assigned VLAN 1 to a subinterface, you must change the VLAN ID for your subinterface to a new VLAN. You will not be able to deploy the configuration using VLAN 1.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Secure Firewall supports Dual-Arm Deployment Mode on AWS with GWLB	7.6	7.6	The Secure Firewall supports the dual-arm deployment mode on AWS with GWLB. This mode enables the firewall to directly forward internet-bound traffic to the internet through the internet gateway after traffic inspection, while also performing network address translation (NAT).
Secure Firewall 1210/1220 hardware switch support	7.6	7.6	The Secure Firewall 1210/1220 supports setting each Ethernet interface to be a switch port or a firewall interface
Secure Firewall 1210CP PoE+ support on Ethernet ports 1/5-1/8	7.6	7.6	The Secure Firewall 1210CP supports Power over Ethernet+ (PoE+) on Ethernet ports 1/5-1/8.
VXLAN VTEP IPv6 support	7.4	Any	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the threat defense virtual cluster control link or for Geneve encapsulation. New/Modified screens: • **Devices** > **Device Management** > **Edit** > **VTEP** > **Add VTEP** **Devices** > **Device Management** > **Edit** > **Interfaces** > **Add Interfaces** > **VNI Interface** Requires Firewall Threat Defense version 7.4. You can specify an IPv6 address for the VXLAN VTEP interface for Secure Firewall 4200 Series devices only.
Loopback interface support for BGP and management traffic	7.4	Any	You can use a loopback interface for: AAA, BGP, DNS, HTTP, ICMP, IPsec Flow Offload, NetFlow, SNMP, SSH, and Syslog. Requires Firewall Threat Defense version 7.4.
Loopback interface support for VTI	7.3	Any	You can now add a loopback interface. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address assigned to the loopback interface. For VTI, in addition to setting a loopback interface as the source interface, support has also been added to inherit the IP address from a loopback interface instead of a statically configured IP address. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Add Interfaces** > **Add Loopback Interface**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
IPv6 DHCP	7.3	Any	The Firewall Threat Defense now supports the following features for IPv6 addressing: DHCPv6 Address client, DHCPv6 Prefix Delegation client, BGP router advertisement for delegated prefixes, and DHCPv6 stateless server. New/Modified screens: • **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **DHCP** • **Objects** > **Object Management** > **DHCP IPv6 Pool** New/Modified commands: **show bgp ipv6 unicast** , **show ipv6 dhcp** , **show ipv6 general-prefix**
Paired proxy VXLAN for the Firewall Threat Defense Virtual for the Azure Gateway Load Balancer	7.3	Any	You can configure a paired proxy mode VXLAN interface for the Firewall Threat Defense Virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). New/Modified screens: **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **VNI Interface** Supported platforms: Firewall Threat Defense Virtual in Azure
VXLAN support	7.2	Any	VXLAN encapsulation support was added. New/Modified screens: **Devices** > **Device Management** > **Device** > **VTEP** , **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **VNI Interface** , and **Devices** > **Device Management** > **Device** > **Interfaces** edit physical interface **> General** Supported platforms: All.
Geneve support for the Firewall Threat Defense Virtual	7.1	Any	Geneve encapsulation support was added for the Firewall Threat Defense Virtual to support single-arm proxy for the Amazon Web Services (AWS) Gateway Load Balancer. This feature requires Snort 3.
31-bit Subnet Mask	7.0	Any	For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. This feature is not supported for BVIs for bridge groups or with multicast routing. New/Modified screens: **Devices** > **Device Management** > **Interfaces**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Synchronization between the Firewall Threat Defense operational link state and the physical link state for the Firepower 4100/9300	6.7	Any	The Firepower 4100/9300 chassis can now synchronize the Firewall Threat Defense operational link state with the physical link state for data interfaces. **Note** This feature is not supported for clustering, container instances, or Firewall Threat Defense with a Radware vDP decorator. It is also not supported for ASA. New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled** , **show interface expand detail**
Firepower 1010 hardware switch support	6.5	Any	The Firepower 1010 supports setting each Ethernet interface to be a switch port or a firewall interface.
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	6.5	Any	The Firepower 1010 supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8 when they are configured as switch ports.
VLAN subinterfaces for use with container instances	6.3.0	Any	To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances.
Data-sharing interfaces for container instances	6.3.0	Any	To provide flexible physical interface use, you can share interfaces between multiple instances.
Integrated Routing and Bridging	6.2.0	Any	Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group.



CHAPTER 15

Inline Sets and Passive Interfaces

You can configure IPS-only passive interfaces, passive ERSPAN interfaces, and inline sets.

- IPS interfaces, on page 727
- Requirements and prerequisites for inline sets, on page 731
- Guidelines for configuring inline sets and passive interfaces, on page 733
- Configure a passive interface, on page 735
- Configure Inline Sets, on page 736
- History for inline sets and passive interfaces, on page 740

IPS interfaces

Intrusion Prevention System (IPS) interfaces include passive interfaces, passive Enhanced Remote Switch Port Analyzer (ERSPAN) interfaces, and inline sets. Interfaces in IPS-only mode bypass many firewall checks and support only IPS security policy (Snort). Implement IPS-only interfaces if you have a separate firewall protecting these interfaces and want to avoid firewall function overhead.

Note The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes.

Inline sets

An inline set acts like a bump on the wire and binds one or more interface pairs together to slot into an existing network. This function allows the Firewall Threat Defense to be installed in any network environment without requiring configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally and retransmit all traffic out of the other interface in the inline pair unless traffic is explicitly dropped. When you have multiple inline pairs in an inline set, traffic can only pass between the interfaces in the pair; it can't pass between interfaces in different pairs.

Tap mode functionality

With tap mode, the Firewall Threat Defense is deployed inline, but the network traffic flow is undisturbed. Instead, the Firewall Threat Defense makes a copy of each packet so that it can analyze the packets. Note that

rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment.

There are benefits to using tap mode with Firewall Threat Defense that are deployed inline:

- You can set up the cabling between the Firewall Threat Defense and the network as if the Firewall Threat Defense were inline and analyze the kinds of intrusion events the Firewall Threat Defense generates.
- Based on the results, you can modify your intrusion policy and add the drop rules that best protect your network without impacting its efficiency.
- When you are ready to deploy the Firewall Threat Defense inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the Firewall Threat Defense and the network.



Note Tap mode *significantly* impacts Firewall Threat Defense performance, depending on the traffic.



Note Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode or the firewall-type interfaces.

Multiple inline pairs and asynchronous routing

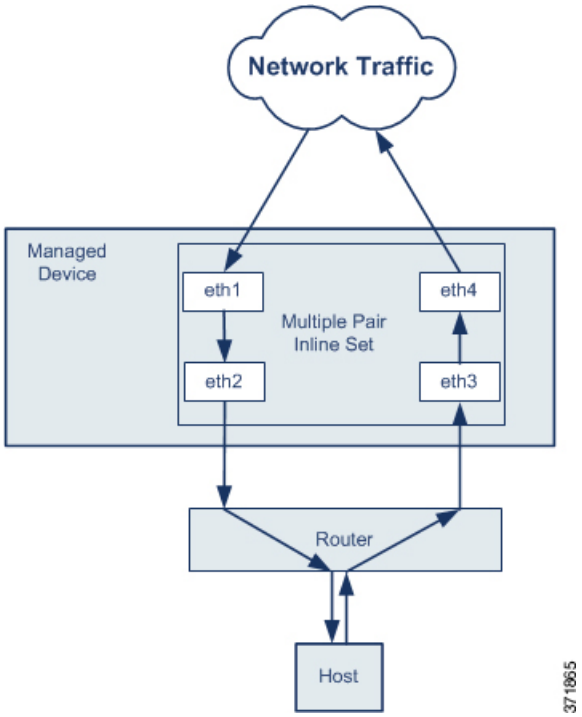
Asynchronous routing is a network configuration that routes traffic between a host on your network and external hosts through different inline pairs, depending on whether the traffic is inbound or outbound. It requires multiple inline pairs in an inline set to correctly analyze network traffic.

If you deploy asynchronous routing, but you include only one inline pair in an inline set, the device might not correctly analyze your network traffic because it might see only half of the traffic.

Multiple inline pairs configuration

Adding multiple inline pairs to the same inline set lets the system identify the inbound and outbound traffic as part of the same traffic flow. For passive interfaces only, you can also achieve this by including the interface pairs in the same security zone.

Figure 293: Asynchronous routing



Note If you assign multiple inline pairs to a single inline set, but you experience issues with duplicate traffic, you might need to reassign your inline pairs to separate inline sets or modify your security zones.

If fragments of a packet are received on different interface pairs, they are not reassembled and get dropped. Make sure all the fragments of the packet are received and sent on the same interface pair.

Passive interfaces

Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function allows the system to view network traffic without participating in the flow of data.

Passive interface functionality

The SPAN or mirror port allows for traffic to be copied from other ports on the switch. When you configure the Firewall Threat Defense in a passive deployment, the Firewall Threat Defense cannot take certain actions such as blocking or shaping traffic.

Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches and use GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the Firewall Threat Defense is in routed firewall mode.

Note Using SR-IOV interfaces as passive interfaces on NGFWv is not supported on some Intel network adapters (such as Intel X710 or 82599) using SR-IOV drivers due to a promiscuous mode restriction. In such cases, use a network adapter that supports this functionality. See Intel Ethernet Products for more information on Intel network adapters.

Hardware Bypass for inline sets

Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. It maintains network connectivity when software or hardware failures occur and is available for certain interface modules on supported models.

Supported interface modules

For information about which interface modules support this feature, see Requirements and prerequisites for inline sets, on page 731.

Hardware Bypass triggers

Hardware Bypass can be triggered in these scenarios.

- Firewall Threat Defense crash
- Firewall Threat Defense reboot
- Security Module reboot
- Chassis crash
- Chassis reboot
- Manual trigger
- Chassis power loss
- Security Module power loss

Note Hardware bypass is intended for unplanned/unexpected failure scenarios, and is not automatically triggered during planned software upgrades. Hardware bypass activates only at the end of a planned upgrade process, when the Firewall Threat Defense application reboots.

Hardware bypass switchover

When you switch from normal operation to hardware bypass, or back to normal operation, you may experience several seconds of interrupted traffic. During this time, connections may drop.

Connection interruption factors

Several factors can affect the length of the traffic interruption during hardware bypass switchover.

- Copper port auto-negotiation
- Behavior of the optical link partner such as how it handles link faults and de-bounce timing
- Spanning tree protocol convergence
- Dynamic routing protocol convergence

You may also experience dropped connections due to application identification errors when analyzing connections midstream after the returning to normal operations.

Snort Fail Open vs. Hardware Bypass

Snort Fail Open and Hardware Bypass allow traffic to flow during system failures.

Functionality differences

You can configure the Snort Fail Open option for inline sets other than those in tap mode. This option either drops traffic or allows traffic to pass without inspection when the Snort process is busy or down. Snort Fail Open is supported on all inline sets except those in tap mode, not just on interfaces that support Hardware Bypass.

The Hardware Bypass functionality allows traffic to flow during a hardware failure, including a complete power outage, and certain limited software failures. A software failure that triggers Snort Fail Open does not trigger a Hardware Bypass.

Hardware Bypass status

When the system has power, the Bypass LED indicates the Hardware Bypass status. See the Firepower chassis hardware installation guide for LED descriptions.

Requirements and prerequisites for inline sets

This reference provides the requirements and prerequisites that must be met before configuring inline sets, including user role permissions and hardware bypass support information.

User roles

- Admin
- Access Admin
- Network Admin

Hardware Bypass Support

The Firewall Threat Defense supports Hardware Bypass for interface pairs on specific network modules on the following models:

- Firepower 2130 and 2140
- Secure Firewall 3100
- Firepower 4100

- Secure Firewall 4200
- Firepower 9300

Note The ISA 3000 has a separate implementation for Hardware Bypass, which you can enable using FlexConfig only (see FlexConfig policies, on page 921). Do not use this chapter to configure ISA 3000 Hardware Bypass.

Note You can use Hardware Bypass interfaces as regular interfaces without the Hardware Bypass feature enabled.

The supported Hardware Bypass network modules for these models include:

- Firepower 2130 and 2140:
  - Firepower 6-port 1G SX FTW Network Module single-wide (FPR2K-NM-6X1SX-F)
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR2K-NM-6X10SR-F)
  - Firepower 6-port 10G LR FTW Network Module single-wide (FPR2K-NM-6X10LR-F)
- Secure Firewall 3100:
  - 6-port 1G SFP Fail-to-Wire Network Module, SX (multimode) (FPR3K-XNM-6X1SXF)
  - 6-port 10G SFP Fail-to-Wire Network Module, SR (multimode) (FPR3K-XNM-6X10SRF)
  - 6-port 10G SFP Fail-to-Wire Network Module, LR (single mode) (FPR3K-XNM-6X10LRF)
  - 6-port 25G SFP Fail-to-Wire Network Module, SR (multimode) (FPR3K-XNM-X25SRF)
  - 6-port 25G Fail-to-Wire Network Module, LR (single mode) (FPR3K-XNM-6X25LRF)
  - 8-port 1G Copper Fail-to-Wire Network Module, RJ45 (copper) (FPR3K-XNM-8X1GF)
- Secure Firewall 4200:
  - 6-port 1G SFP Fail-to-Wire Network Module, SX (multimode) (FPR4K-XNM-6X1SXF)
  - 6-port 10G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-6X10SRF)
  - 6-port 10G SFP Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X10LRF)
  - 6-port 25G SFP Fail-to-Wire Network Module, SR (multimode) (FPR4K-XNM-X25SRF)
  - 6-port 25G Fail-to-Wire Network Module, LR (single mode) (FPR4K-XNM-6X25LRF)
  - 8-port 1G Copper Fail-to-Wire Network Module, RJ45 (copper) (FPR4K-XNM-8X1GF)
- Firepower 4100:
  - Firepower 6-port 1G SX FTW Network Module single-wide (FPR4K-NM-6X1SX-F)
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR4K-NM-6X10SR-F)
  - Firepower 6-port 10G LR FTW Network Module single-wide (FPR4K-NM-6X10LR-F)

- Firepower 2-port 40G SR FTW Network Module single-wide (FPR4K-NM-2X40G-F)
- Firepower 8-port 1G Copper FTW Network Module single-wide (FPR-NM-8X1G-F)

- Firepower 9300:
  - Firepower 6-port 10G SR FTW Network Module single-wide (FPR9K-NM-6X10SR-F)
  - Firepower 6-port 10G LR FTW Network Module single-wide (FPR9K-NM-6X10LR-F)
  - Firepower 2-port 40G SR FTW Network Module single-wide (FPR9K-NM-2X40G-F)

Hardware Bypass can only use the following port pairs:

- 1 & 2
- 3 & 4
- 5 & 6
- 7 & 8

Guidelines for configuring inline sets and passive interfaces

Firewall mode restrictions

Use ERSPAN interfaces only when the device is in routed firewall mode.

Clustering restrictions

Consider clustering limitations when configuring inline sets and passive interfaces.

- Link State Propagation for an inline set is not supported with clustering.

Multi-Instance mode restrictions

Use unshared physical interfaces or EtherChannels when configuring multi-instance mode.

- Multi-instance shared interfaces are not supported. You must use an unshared interface.
- Multi-instance chassis-defined subinterfaces are not supported. You must use a physical interface or EtherChannel.

General configuration guidelines

Consider these interface and traffic inspection requirements when configuring inline sets and passive interfaces.

- Inline sets and passive interfaces support only physical interfaces and EtherChannels. You cannot use VLANs or other virtual interfaces, including multi-instance chassis-defined subinterfaces.
- Because IPS interfaces do not support regular firewall protections, traffic must pass through the same Firewall Threat Defense to ensure all traffic is inspected according to the IPS security policy (Snort).
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firewall Threat Defense when using inline sets. If there are two neighbors on either side of the Firewall Threat Defense

running BFD, then the Firewall Threat Defense will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

- For inline sets and passive interfaces, the Firewall Threat Defense supports up to two 802.1Q headers in a packet (also known as Q-in-Q support), with the exception of the Firepower 4100/9300, which only supports one 802.1Q header. **Note:** Firewall-type interfaces do not support Q-in-Q, and only support one 802.1Q header.
- Firewall Threat Defense does not support frames with Ethertype 0x8988. If a source in the Application Centric Infrastructure (ACI) fabric has Precision Time Protocol (PTP) enabled, ACI inserts Ethertype 0x8988 into data-plane frames before mirroring. Firewall Threat Defense drops frames with Ethertype 0x8988 and does not inspect them.

Hardware Bypass Guidelines

Consider Hardware Bypass limitations and clustering requirements when configuring inline sets.

- Hardware Bypass ports are supported only for inline sets.
- Hardware Bypass ports cannot be part of an EtherChannel.
- Hardware Bypass is not supported in high availability mode.
- Hardware Bypass ports are supported with intra-chassis clustering on the Firepower 9300. Ports are placed in Hardware Bypass mode when the last unit in the chassis fails. Inter-chassis clustering is not supported, because inter-chassis clustering only supports Spanned EtherChannels; Hardware Bypass ports cannot be part of an EtherChannel.
- If all modules in an intra-chassis cluster on the Firepower 9300 fail, then Hardware Bypass is triggered on the final unit, and traffic continues to pass. When units come back up, Hardware Bypass returns to standby mode. If rules matching application traffic are used, connections might be dropped and require reestablishment. Connections are dropped because state information is not retained on the cluster unit, and the unit cannot identify the traffic as belonging to an allowed application. To prevent a traffic drop, use a port-based rule instead of an application-based rule, if appropriate for your deployment.
- You can use Hardware Bypass interfaces as regular interfaces without the Hardware Bypass feature enabled.

Unsupported firewall features on IPS interfaces

These firewall features are not supported on IPS interfaces.

- DHCP server
- DHCP relay
- DHCP client
- TCP Intercept
- Routing
- NAT
- VPN
- Application inspection

- QoS
- NetFlow
- VXLAN

Configure a passive interface

Configure a passive or ERSPAN interface to enable network monitoring and traffic analysis capabilities on your security device.

This section describes how to:

- Enable the interface. By default, interfaces are disabled.
- Set the interface mode to Passive or ERSPAN. For ERSPAN interfaces, you will set the ERSPAN parameters and the IP address.
- Change the MTU. By default, the MTU is set to 1500 bytes. For more information about the MTU, see MTU, on page 712.
- Set a specific speed and duplex (if available). By default, speed and duplex are set to Auto.

Note For the Secure Firewall Threat Defense on the FXOS chassis, you configure basic interface settings on the Firepower 4100/9300. See Configure a physical interface, on page 259 for more information.

Before you begin

- If you are using EtherChannels, add them according to Configure an EtherChannel, on page 619.

Follow these steps to configure a passive interface:

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 In the **Mode** drop-down list, choose **Passive** or **ERSPAN**.

Step 4 Enable the interface by checking the **Enabled** check box.

Set these values:

a. In the **Name** field, enter a name up to 48 characters in length.

b. From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New**.

c. Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5 (Optional) On **General**, set the **MTU** between 64 and 9198 bytes; for the Secure Firewall Threat Defense Virtual and Secure Firewall Threat Defense on the FXOS chassis, the maximum is 9000 bytes.

The default is 1500 bytes.

Step 6 For ERSPAN interfaces, set the following parameters:

- **Flow ID**—Configure the ID used by the source and destination sessions to identify the ERSPAN traffic, between 1 and 1023. This ID must also be entered in the ERSPAN destination session configuration.
- **Source IP**—Configure the IP address used as the source of the ERSPAN traffic.
- **IPv4**—Set the IPv4 address and mask

Step 7 (Optional) Set the duplex and speed by clicking **Hardware Configuration**.

The exact speed and duplex options depend on your hardware.

- **Duplex**—Choose **Full**, **Half**, or **Auto**. Auto is the default.
- **Speed**—Choose **10**, **100**, **1000**, or **Auto**. Auto is the default.

Step 8 Click **OK**.

Step 9 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure Inline Sets

Enable traffic inspection by configuring multiple inline sets using physical interfaces or EtherChannels, including optional Hardware Bypass.

Inline sets allow you to designate pairs of interfaces or EtherChannels for traffic inspection, with optional Hardware Bypass. You can configure multiple inline pairs per set.

Note For the Firepower 4100/9300 , you configure basic interface settings in FXOS on the chassis. See Configure a physical interface, on page 259 for more information.

Before you begin

- If you are using EtherChannels, add them according to Configure an EtherChannel, on page 619 .
- We recommend that you set STP PortFast for STP-enabled switches that connect to the Firewall Threat Defense inline pair interfaces. This setting is especially useful for Hardware Bypass configurations and can reduce bypass times.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 For each interface in the inline pair, name the interface and enable it. Also configure necessary hardware settings, ensuring they match between interfaces in the inline pair. You can configure multiple pairs of interfaces.

a) Click **Edit** ( ) for the interface you want to edit.
b) In the **Name** field, enter a name up to 48 characters in length.
c) Enable the interface by checking the **Enabled** check box.
d) (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

e) Leave the **Mode** as **None** .

After you add this interface to an inline set, this field will show Inline for the mode.

f) Do not set the security zone yet; you must set it after you create the inline set later in this procedure.
g) (Optional) Set the duplex and speed by clicking **Hardware Configuration** .

The exact speed and duplex options depend on your hardware.

- **Duplex** —Choose **Full** , **Half** , or **Auto** . Auto is the default.
- **Speed** —Choose **10** , **100** , **1000** , or **Auto** . Auto is the default.

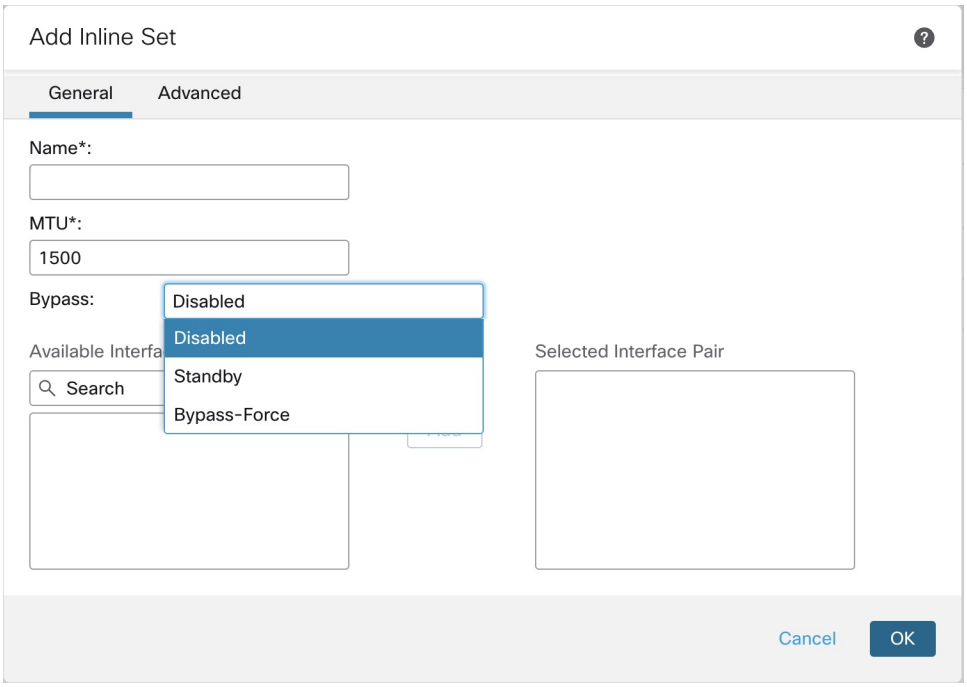
h) Click **OK** .

Do not set any other settings for this interface.

Step 3 Click **Inline Sets**.

Step 4 Click **Add Inline Set**.

Figure 294: Add Inline Set



The **Add Inline Set** dialog box appears with **General** selected.

Step 5 In the **Name** field, enter a name for the set.

Step 6 (Optional) Change the **MTU** to enable jumbo frames.

For inline sets, the MTU setting is not used. However, the jumbo frame setting is relevant to inline sets; jumbo frames enable the inline interfaces to receive packets up to 9000 bytes. To enable jumbo frames, you must set the MTU of *any* interface on the device above 1500 bytes.

Step 7 Configure Hardware Bypass.

a) For the **Bypass** mode, choose one of the following options:

- **Disabled** —Set Hardware Bypass to disabled for interfaces where Hardware Bypass is supported, or use interfaces where Hardware Bypass is not supported.
- **Standby** —Set Hardware Bypass to the standby state on supported interfaces. Only pairs of Hardware Bypass interfaces are shown. In the standby state, the interfaces remain in normal operation until there is a trigger event.
- **Bypass-Force** —Manually forces the interface pair to go into a bypass state. **Inline Sets** shows **Yes** for any interface pairs that are in Bypass-Force mode.

b) In the **Available Interfaces Pairs** area, click a pair and then click **Add** to move it to the **Selected Interface Pair** area.

All possible pairings between named and enabled interfaces with the mode set to None show in this area.

Step 8 (Optional) Click **Advanced** to set the following optional parameters:

- **Tap Mode** —Set to inline tap mode.

Note that you cannot enable this option and strict TCP enforcement on the same inline set.

Note Perform Tap mode changes during a maintenance window. Changing the mode while the device is passing traffic can cause traffic disruption.

Note Tap mode significantly impacts the Firewall Threat Defense performance, depending on the traffic.

- **Propagate Link State** —Configure link state propagation.

  Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the device senses the change and updates the link state of the other interface to match it. Note that devices require up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

Note Do not enable **Propagate Link State** when using clustering.

- **Snort Fail Open** —Enable or disable either or both of the **Busy** and **Down** options if you want new and existing traffic to pass without inspection (enabled) or drop (disabled) when the Snort process is busy or down.

  By default, traffic passes without inspection when the Snort process is down, and drops when it is busy.

  When the Snort process is:

  - Busy—It cannot process traffic fast enough because traffic buffers are full, indicating that there is more traffic than the device can handle, or because of other software resource issues.
  - Down—It is restarting because you deployed a configuration that requires it to restart. See Configurations that restart the snort process when deployed or activated, on page 131 .

  When the Snort process is down and comes back up, it inspects *new* connections. To prevent false positives and false negatives, it does not inspect existing connections on inline, routed, or transparent interfaces because initial session information might have been lost while it was down.

Note When Snort fails open, features that rely on the Snort process do not function. These include application control and deep inspection. The system performs only basic access control using simple, easily determined transport and network layer characteristics.

Note The **Strict TCP Enforcement** option is not supported.

Step 9 Set the security zone for each interface.

a) Click **Interfaces** .

b) Click **Edit** ( ) for the member interface.

c) From the **Security Zone** drop-down list, choose a security zone or add a new one by clicking **New** .

You can only set the zone after you add the interface to the inline set; adding it to an inline set configures the mode to Inline and lets you choose inline-type security zones.

d) Click **OK** .

Click **Save**.

What to do next

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

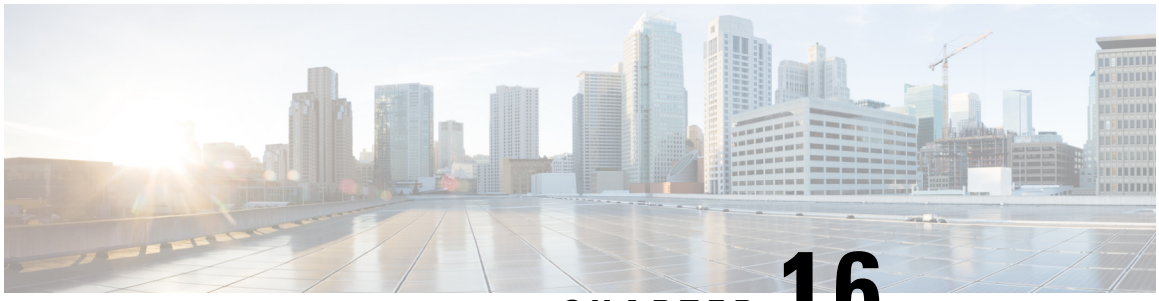
History for inline sets and passive interfaces

This reference provides the chronological history of features related to inline sets and passive interfaces, including hardware bypass support, synchronization capabilities, and EtherChannel support across various Cisco security platforms.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Hardware bypass support on the Secure Firewall 4200 for supported network modules	7.4.0	7.4.0	The Secure Firewall 4200 supports hardware bypass functionality when using the hardware bypass network modules. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Secure Firewall 4200
Hardware bypass support on the Secure Firewall 3100 for supported network modules	7.2	Any	The Secure Firewall 3100 now supports hardware bypass functionality when using the hardware bypass network modules. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Secure Firewall 3100

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Synchronization between the Firewall Threat Defense operational link state and the physical link state for the Firepower 4100/9300	6.7	Any	The Firepower 4100/9300 chassis can now synchronize the Firewall Threat Defense operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The Firewall Threat Defense application interface admin state is not considered. Without synchronization from Firewall Threat Defense, data interfaces can be in an Up state physically before the Firewall Threat Defense application has completely come online, for example, or can stay Up for a period of time after you initiate a shutdown. For inline sets, this state mismatch can result in dropped packets because external routers may start sending traffic to the Firewall Threat Defense before the Firewall Threat Defense can handle it. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for clustering, container instances, or Firewall Threat Defense with a Radware vDP decorator. It is also not supported for ASA. New/Modified Firepower Chassis Manager screens: **Logical Devices** > **Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300
Hardware bypass support on the Firepower 2130 and 2140 for supported network modules	6.3.0	Any	The Firepower 2130 and 2140 now support hardware bypass functionality when using the hardware bypass network modules. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 2130 and 2140
Support for EtherChannels in Firewall Threat Defense inline sets or passive interface	6.2.0	Any	You can now use EtherChannels in a Firewall Threat Defense inline set or passive interface.
Hardware bypass support on the Firepower 4100/9300 for supported network modules	6.1.0	Any	Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 4100/9300

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Inline set link state propagation support for the Firewall Threat Defense	6.1.0	Any	When you configure an inline set in the Firewall Threat Defense application and enable link state propagation, the Firewall Threat Defense sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. New/Modified FXOS commands: **show fault |grep link-down**, **show interface detail**



CHAPTER 16

Device Settings

After you add a device, you can edit device-related settings on the **Device** page.

1. Choose **Devices** > **Device Management**.
2. Next to the device you want to modify, click **Edit** ( ).
3. Click **Device**.

- Edit general settings, on page 743
- Edit license settings, on page 755
- View system information, on page 756
- View the inspection engine, on page 757
- Edit health settings, on page 757
- Edit management settings, on page 757
- View inventory details, on page 793
- Edit applied policies, on page 794
- Edit advanced settings, on page 796
- Edit deployment settings, on page 800
- Edit cluster health monitor settings, on page 802
- Hot swap an SSD, on page 805
- Configure SNMP for FXOS, on page 808
- Configure alarms for the ISA 3000, on page 811
- History for Device Settings, on page 823

Edit general settings

Edit general device settings to customize the device name, packet transfer options, and force deployment settings for managed devices.

The **General** section of the **Device** page displays the settings described in this table.

Figure 295: General

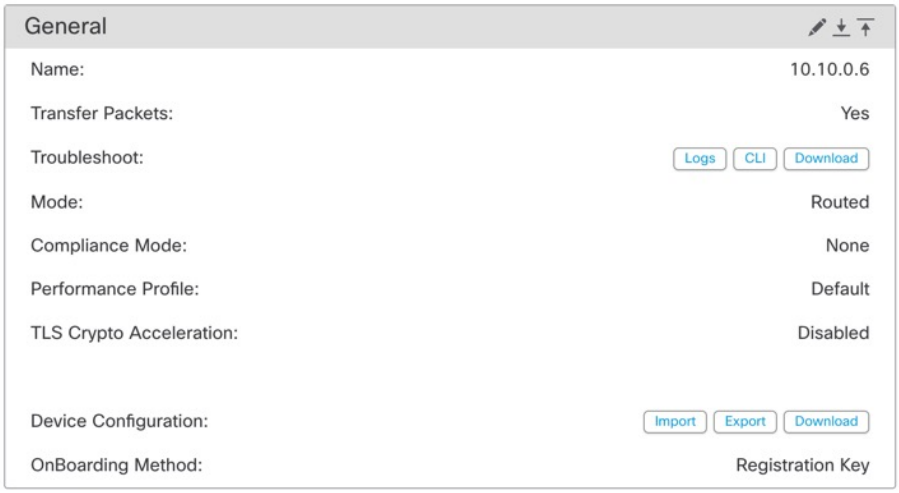


Table 46: General section table fields

Field	Description
Name	The display name of the device on the Firewall Management Center.
Transfer Packets	This displays whether or not the managed device sends packet data with the events to the Firewall Management Center.
Troubleshoot	Lets you generate and download troubleshooting files and also see CLI command output. See Generate troubleshooting files, on page 745 and View CLI output, on page 747.
Mode	The displays the mode of the management interface for the device: **routed** or **transparent**.
Compliance Mode	This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.
Performance Profile	This displays the core allocation performance profile for the device, as configured in the platform settings policy.
TLS Crypto Acceleration:	Shows whether TLS crypto acceleration is enabled or disabled.
Device Configuration	Lets you copy, export, or import a configuration. See Copy a configuration to another device, on page 749 and Export and import the device configuration, on page 751.
OnBoarding Method	Shows whether the device was registered using a registration key or using the serial number (zero-touch provisioning).

You can edit some of these settings from this section.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device you want to modify, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 In the **General** section, click **Edit** ( ).

a) Enter a **Name** for the managed device.
b) Check **Transfer Packets** to allow packet data to be stored with events on the Firewall Management Center.
c) Click **Force Deploy** to force deployment of current policies and device configuration to the device.

Note Force-deploy consumes more time than the regular deployment since it involves the complete generation of the policy rules to be deployed on the Firewall Threat Defense.

Step 5 For **Troubleshoot** actions, see Generate troubleshooting files, on page 745 and View CLI output, on page 747.

Step 6 For **Device Configuration** actions, see Copy a configuration to another device, on page 749 and Export and import the device configuration, on page 751.

Step 7 Click **Deploy**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Generate troubleshooting files

Generate troubleshooting files to collect diagnostic information for individual devices or all cluster nodes that can be used for technical support and issue resolution.

You can generate and download troubleshooting files for each device and also for all cluster nodes. For a cluster, you can download all files as a single compressed file. You can also include logs for the cluster nodes.

Alternatively, trigger file generation from the **Devices** > **Device Management**. From the **More** ( ) drop-down list, choose **Troubleshoot Files**.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device or cluster you want to view, click **Edit** ( ).

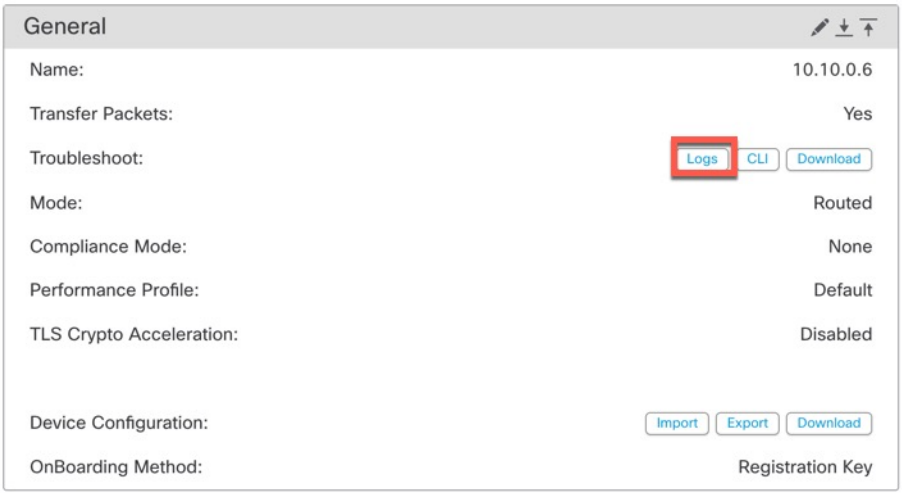
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Device** or **Cluster**.

Step 4 Generate logs for the device or for all cluster nodes.

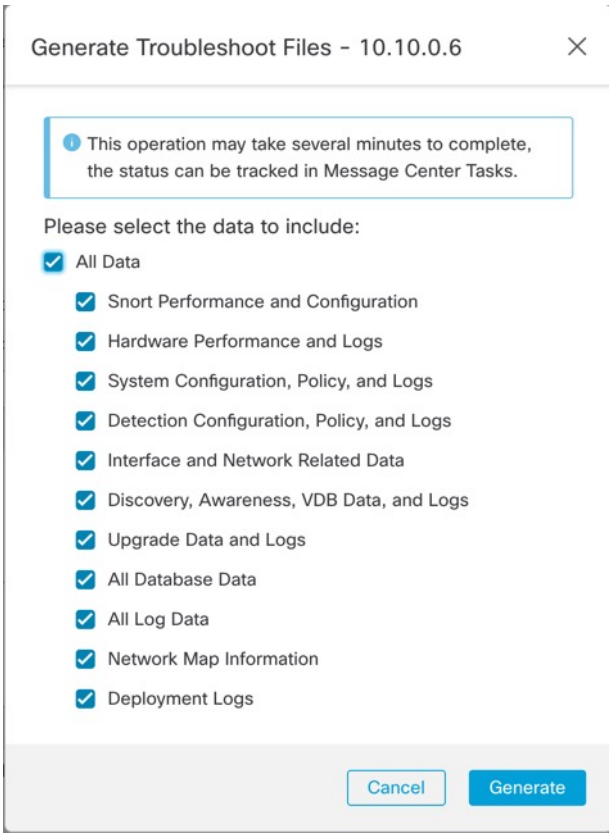
a) In the **General** area, **Troubleshoot** section, click **Logs**.

Figure 296: Logs



b) You are prompted to choose the logs you want to include. For a cluster, under **Device**, choose **All Devices** or an individual node. A cluster also has the **Cluster Logs** available.

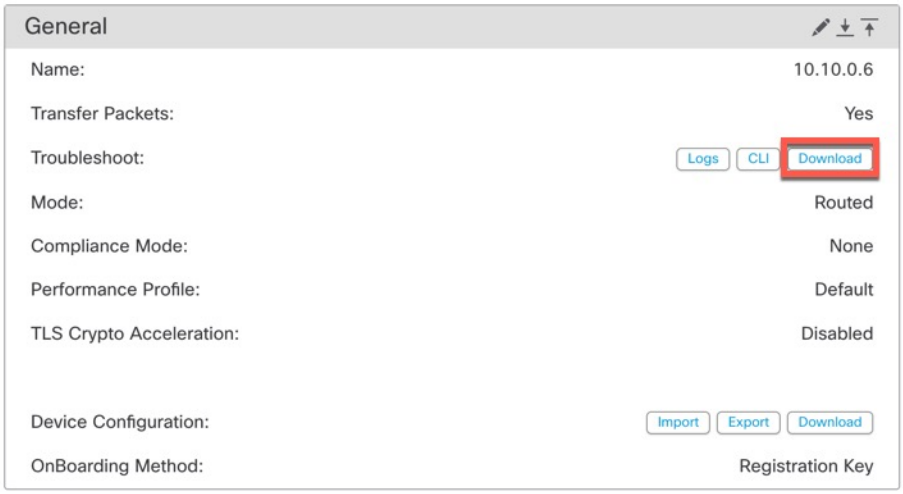
Figure 297: Generate troubleshoot files



c) Click **Generate**.

Step 5 To download the generated logs, in the **General** area, **Troubleshoot** section, click **Download**.

Figure 298: Download



The logs are downloaded to your computer.

View CLI output

This task allows you to troubleshoot devices and clusters by viewing pre-defined CLI command outputs and executing custom show commands for diagnostic purposes.

You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output.

For a device, the following commands are executed:

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

For a cluster or cluster node:

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**
- **show cluster info transport cp**

- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

Procedure

Step 1 Choose **Devices** > **Device Management**.

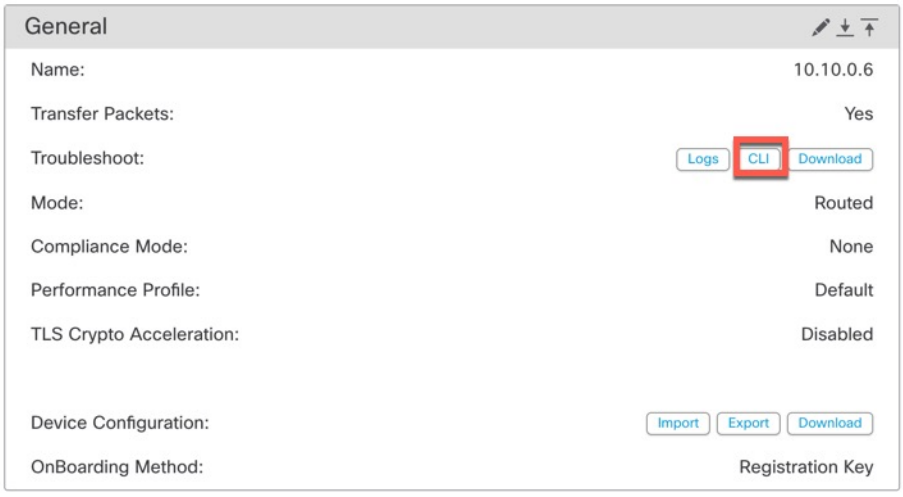
Step 2 Next to the device or cluster you want to view, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Device** or **Cluster**.

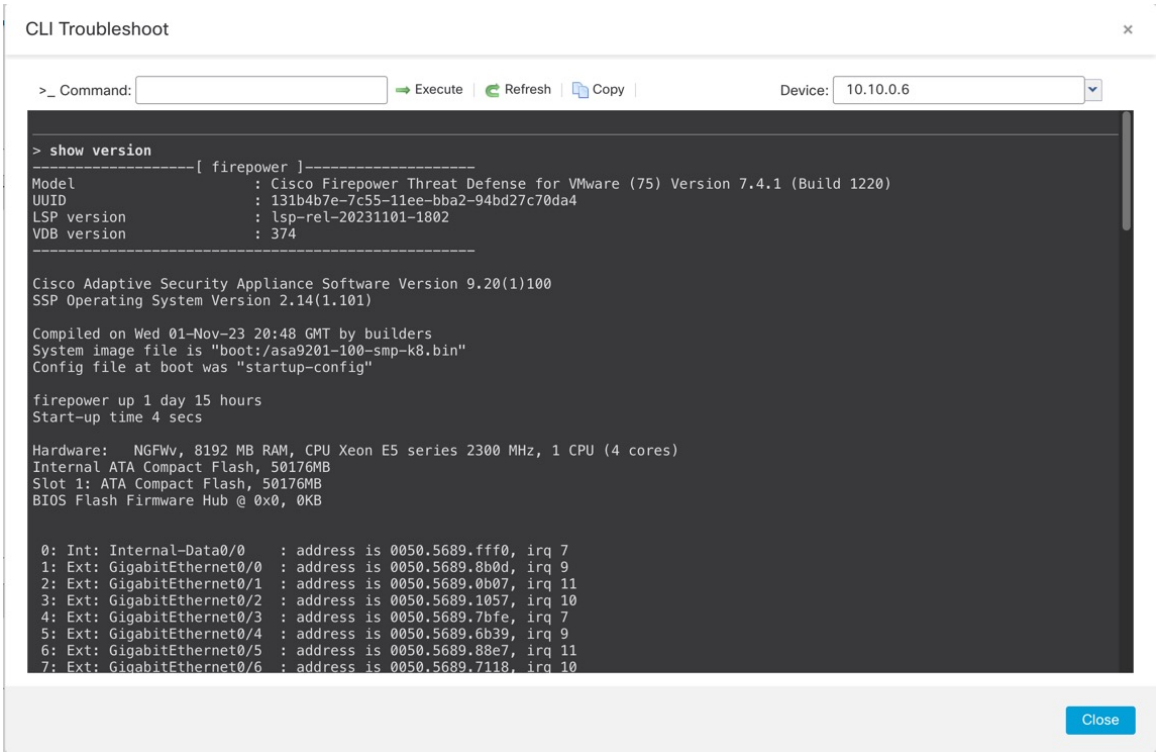
Step 4 In the **General** area, **Troubleshoot** section, click **CLI**.

Figure 299: CLI



The **CLI Troubleshoot** dialog box appears with the pre-defined CLIs executed.

Figure 300: CLI troubleshoot



Step 5 On the **CLI Troubleshoot** dialog box, you can perform these tasks.

- Enter a **show** command in the **Command** field, and click **Execute**. The new command output will be added to the window.
- Click **Refresh** to re-run the predefined CLIs.
- Click **Copy** to copy the output to your clipboard.
- For a cluster, choose a different node from the **Device** drop-down list.

Step 6 Click **Close**.

Copy a configuration to another device

Copy configurations and policies from a pre-configured device to a new device, instead of manually reconfiguring the new device.

When a new device is deployed in the network, you can copy configurations and policies from a pre-configured device, instead of manually reconfiguring the new device.

Before you begin

Confirm that:

- The source and destination devices are the same model and are running the same version of the software.

- The source is either a standalone device or a high availability pair.
- The destination device is a standalone device.
- The source and destination devices have the same number of physical interfaces.
- The source and destination devices are in the same firewall mode: routed or transparent.
- The source and destination devices are in the same security-certifications-compliance mode.
- The source and destination devices are in the same domain.
- No configuration deployment is in progress on the source or the destination devices.
- For a restored Management Center, ensure that you retain the source device in a disabled state, register the destination device, execute Copy Configuration procedure, and then finally remove the source device.

Follow these steps to copy a configuration to another device:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device you want to modify, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 In the **General** section, do one of the following:

- Click **Get Device Configuration** ( ) to copy device configuration from another device to the new device. On the **Get Device Configuration** page, select the source device in the **Select Device** drop-down list.
- Click **Push Device Configuration** ( ) to copy device configuration from the current device to the new device. On the **Push Device Configuration** page, select the destination to which configuration is to be copied in the **Target Device** drop-down list.

Step 5 (Optional) Check **Include shared policies configuration** check box to copy policies.

Shared policies such as AC policy, NAT, Platform Settings and FlexConfig policies can be shared across multiple devices.

Step 6 Click **OK**.

You can monitor the status of the copy device configuration task on **Tasks** in the Message Center.

When the copy device configuration task is initiated, it erases the configuration on the target device and copies the configuration of the source device to the destination device.

Warning When you have completed the copy device configuration task, you cannot revert the target device to its original configuration.

Export and import the device configuration

Export device-specific configuration to create a backup that can be imported for the same device in various scenarios including moving the device to a different Firewall Management Center, restoring old configurations, or reregistering a device.

You can export all device-specific configurations available on the Device pages, including:

- Interfaces
- Inline Sets
- Routing
- DHCP
- VTEP
- Associated objects

You can then import the saved configuration for the same device in these use cases:

- Moving the device to a different Firewall Management Center—First delete the device from the original Firewall Management Center, then add the device to the new Firewall Management Center. Then you can import the saved configuration.
- Moving the device between domains—When you move a device between domains, some device-specific configuration is not retained because supporting objects (such as interface groups for security zones) do not exist in the new domain. By importing the configuration after the domain move, any necessary objects are created for that domain, and the device configuration is restored.
- Restore an old configuration—If you deployed changes that negatively impacted the operation of the device, you can import a backup copy of a known working configuration to restore a previous operational state.
- Reregistering a device—If you delete a device from the Firewall Management Center, but then want to add it back, you can import the saved configuration.

Before you begin

Review these guidelines:

- You can only import the configuration to the same device (the UUID must match). You cannot import a configuration to a different device, even if it is the same model.
- Do not change the version running on the device between exporting and importing; the version must match.
- If you make inventory changes after your export (such as adding or deleting network modules or configuring or joining breakout ports), the device inventory will not match the Firewall Management Center. In this case, the device inventory will be maintained, and you will be prompted to sync the interfaces (see Sync Interface Changes with the Firewall Management Center, on page 622) and discard incompatible configuration in the Firewall Management Center when you try to deploy. You will have to repeat the inventory changes and related configuration in the Firewall Management Center.
- If you export a standalone configuration, you cannot import it to a high availability pair or vice versa.

- When moving the device to a different Firewall Management Center, the target Firewall Management Center version must be the same as the source version.
- If an object doesn't exist, it will be created. If an object exists, but the value is different, refer to this table:

Table 47: Object import action

Scenario	Import Action
Object exists with the same name and value.	Reuse existing objects.
Object exists with the same name but different value.	Network and Port objects: Create object overrides for this device. See Object overrides, on page 2342. Interface objects: Create new objects. For example, if both the type (security zone or interface group) and the interface type (routed or switched, for example) do not match, then a new object is created. All other objects: Reuse existing objects even though the values are different.
Object doesn't exist.	Create new objects.

Follow these steps to export and import the device configuration:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device you want to edit, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 Export the configuration.

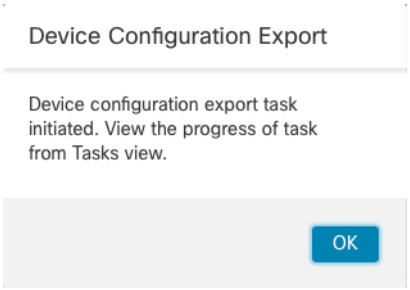
a) In the **General** area, click **Export**.

Figure 301: Export device configuration



You are prompted to acknowledge the export; click **OK**.

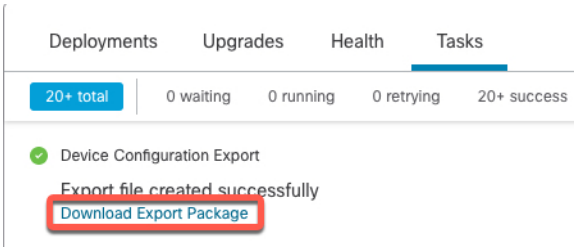
Figure 302: Acknowledge export



You can view the export progress in the **Tasks** page.

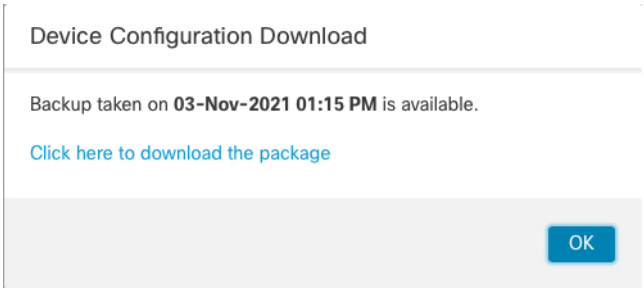
b) Click **Notifications**, and then click the **Tasks** tab. Verify if the export has completed, and then click **Download Export Package**. Alternatively, you can click the **Download** button in the **General** area.

Figure 303: Export task



You are prompted to download the package; click **Click here to download the package** to save the file locally, and then click **OK** to exit the dialog box.

Figure 304: Download package



Step 5 Import the configuration.

a) In the **General** area, click **Import**.

Figure 305: Import device configuration



You are prompted to acknowledge that the current configuration will be replaced. Click **Yes** and then navigate to the configuration package (with the suffix .sfo; note that this file is different from the Backup/Restore files).

Figure 306: Import package

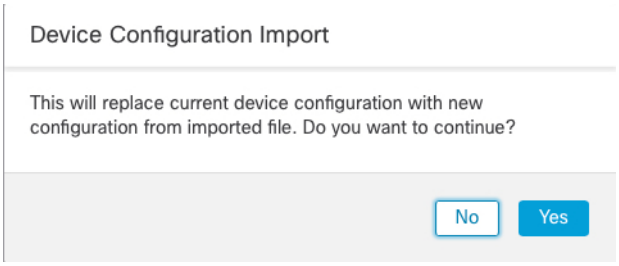
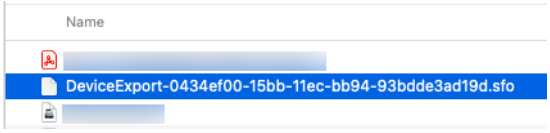
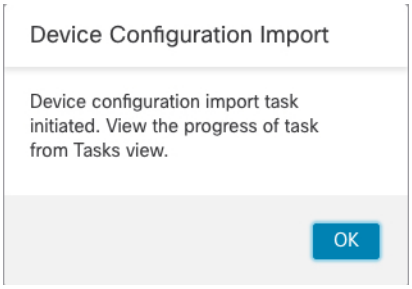


Figure 307: Navigate to package



You are prompted to acknowledge the import; click **OK**.

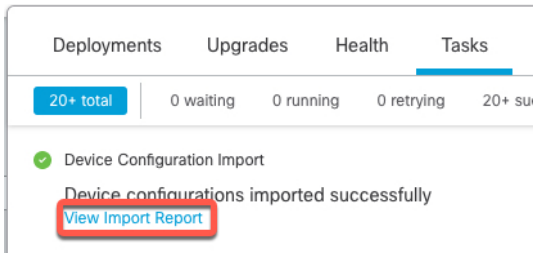
Figure 308: Acknowledge import



You can view the import progress in the **Tasks** page.

b) To view the import reports, click **Notifications**, and then click the **Tasks** tab. Click **View Import Report**.

Figure 309: View import report



The **Device Configuration Import Reports** page provides links to available reports.

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

c) Deploy configuration changes; see Deploy configuration changes, on page 135.

Edit license settings

Enable or disable specific licenses on your managed device to control which features are available for use.

The **License** section of the **Device** page displays the licenses enabled for the device.

You can enable licenses on your device if you have available licenses on your Firewall Management Center.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to enable or disable licenses, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 In the **License** section, click **Edit** ( ).

Step 5 Check or clear the check box next to the license you want to enable or disable for the managed device.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

View system information

The **System** section of the **Device** page displays a read-only table containing system information. You can also shut down or restart the device from this pane, using the icons at the top-right corner.

Figure 310: System

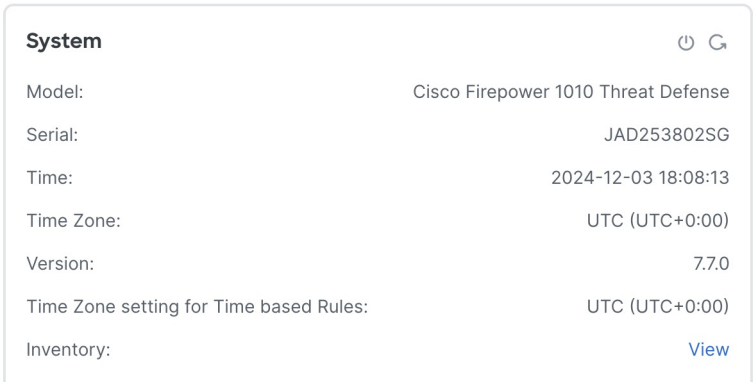


Table 48: System section table fields

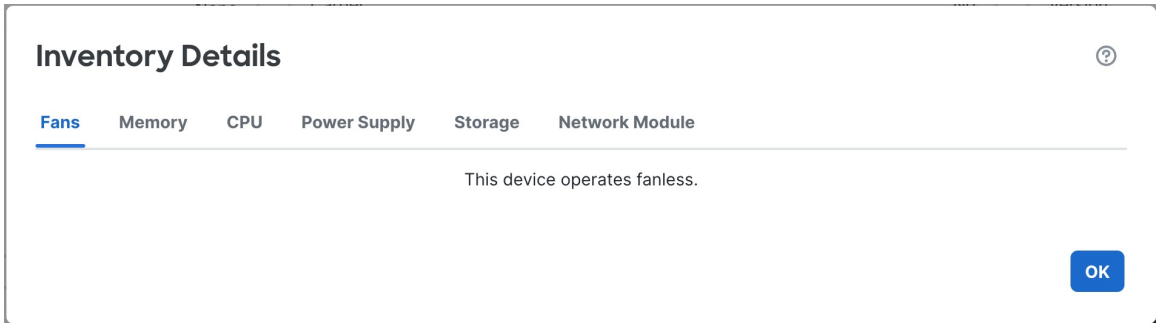
Field	Description
Shut Down Device ( )	Shuts down the device. See Shut down or restart the device, on page 55.
Restart Device ( )	Restarts the device. See Shut down or restart the device, on page 55.
Model	Model name and number.
Serial	PCB (circuit board) serial number. The firewall includes two serial numbers: the chassis serial number and the PCB serial number. The chassis serial number is shown in the Inventory section.
Time	Current system time of the device.
Time Zone	Time zone.
Version	Version of the software currently installed on the managed device.
Time Zone setting for Time based rules	Current system time of the device in the time zone specified in device platform settings.
Inventory	Inventory details. See View Device Inventory.

View device inventory

Click **View** next to **Inventory** in the **System** section to view a table of device inventory information including Fans, Memory, CPU, Power Supply, Storage, and Network Modules.

The **Inventory Details** table displays information about all the Cisco products installed in the Firewall Threat Defense devices assigned with a product identifier (PID). The PID is the product name using which the product can be ordered.

Figure 311: Inventory details



View the inspection engine

The Inspection Engine section of the **Device** page shows whether your device uses Snort 2 or Snort 3. To switch the inspection engine, see *Custom Snort 3 Intrusion Policies for Access Control*.

Note Snort3 is default for Secure Firewall 1200. It does not support Snort2.

Edit health settings

The **Health** section of the **Device** page displays the information described in this table.

Table 49: Health section table fields

Field	Description
Status	An icon that represents the current health status of the device. Clicking the icon displays the Health Monitor for the appliance.
Policy	A link to a read-only version of the health policy currently deployed at the device.
Excluded	A link to the **Health Exclude** page, where you can enable and disable health exclusion modules.

Edit management settings

These settings control how the Firewall Management Center establishes the management connection with the device.

Configure a redundant manager access data interface

This task configures a redundant manager access data interface to ensure continuous management connectivity. The secondary interface provides automatic failover capabilities when the primary management interface becomes unavailable, maintaining device management functionality.

When you use a data interface for manager access, you can configure a secondary data interface to take over management functions if the primary interface goes down. You can configure only one secondary interface. The device uses SLA monitoring to track the viability of the static routes and an ECMP zone that contains both interfaces so management traffic can use both interfaces.

High availability is not supported.

Before you begin

- The secondary interface needs to be in a separate security zone from the primary interface.
- All of requirements apply to the primary interface also apply to the secondary interface. See Using the Firewall Threat Defense data interface for management, on page 5.

Follow these steps to configure a redundant manager access data interface:

Procedure

Step 1 On the **Devices** > **Device Management** page, click **Edit** ( ) for the device.

Step 2 Enable manager access for the secondary interface.

This setting is in addition to standard interface settings such as enabling the interface, setting the name, setting the security zone, and setting a static IPv4 address.

a) Choose **Interfaces** > **Edit Physical Interface** > **Manager Access**.
b) Check **Enable management on this interface for the Manager**.
c) Click **OK**.

Both interfaces show **(Manager Access)** in the interface listing.

Figure 312: Interface listing

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

Step 3 Add the secondary address to the **Management** settings.

a) Click **Device**, and view the **Management** area.

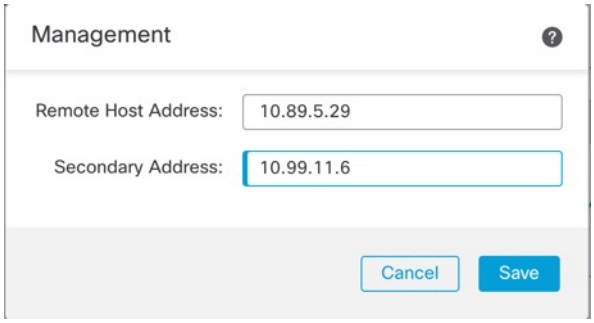
b) Click **Edit** ( ).

Figure 313: Edit management address



c) In the **Management** dialog box, modify the name or IP address in the **Secondary Address** field

Figure 314: Management IP address

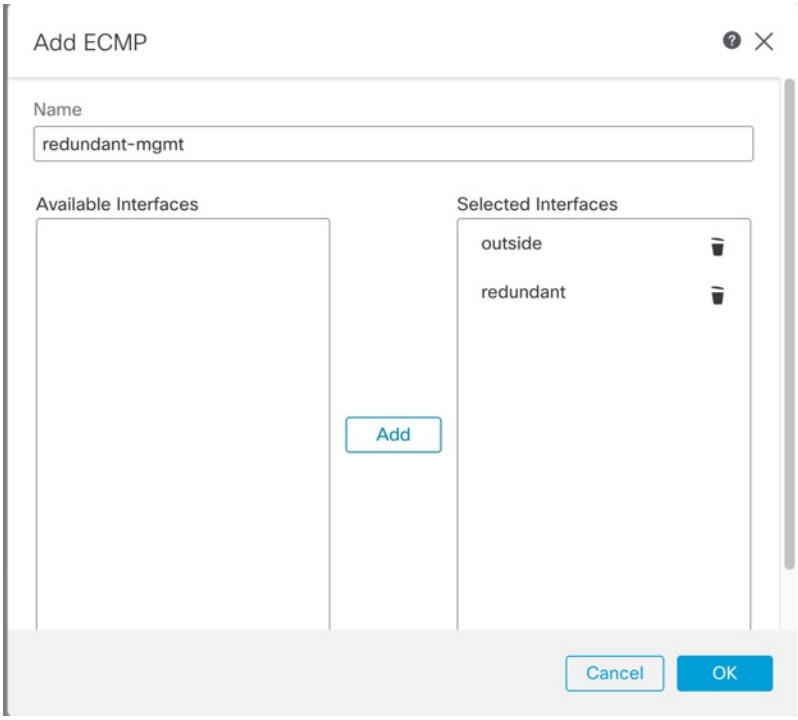


d) Click **Save**.

Step 4 Create an ECMP zone with both interfaces.

a) Click **Routing**.
b) From the virtual router drop-down, choose the virtual router in which the primary and secondary interfaces reside.
c) Click **ECMP**, and then click **Add**.
d) Enter a **Name** for the ECMP zone.
e) Select the primary and secondary interfaces under the **Available Interfaces** box, and then click **Add**.

Figure 315: Add an ECMP zone

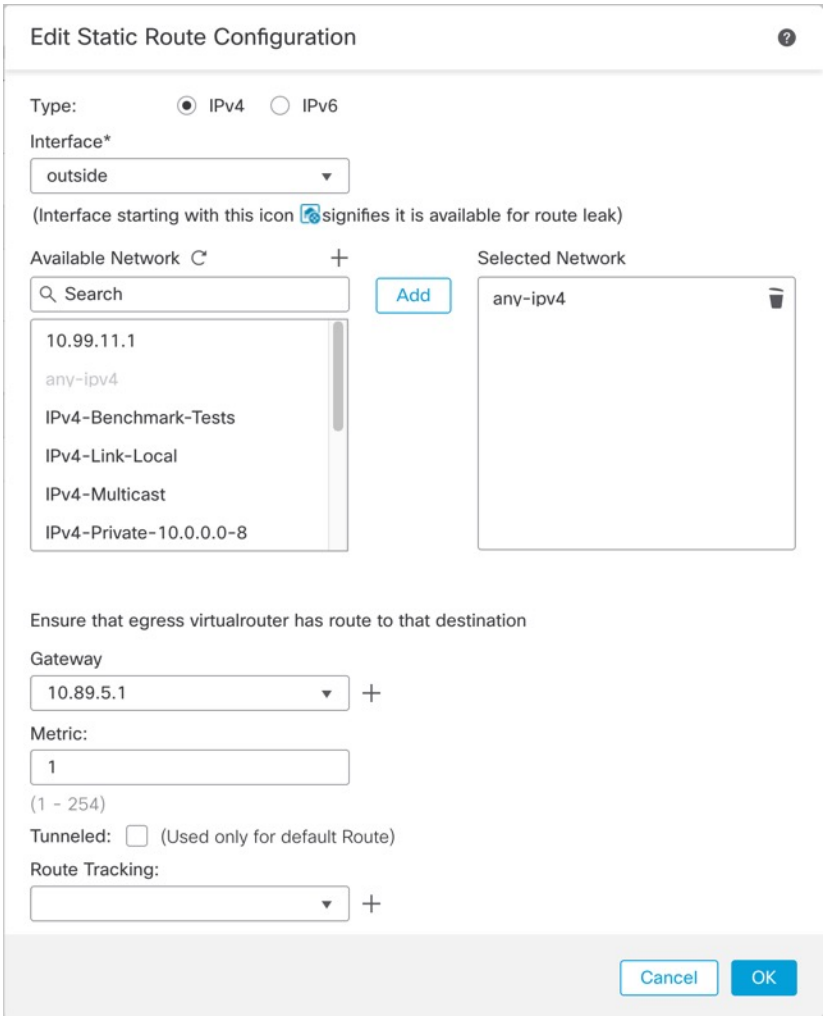


f) Click **OK**, and then **Save**.

Step 5 Add equal-cost default static routes for both interfaces and enable SLA tracking on both.

The routes should be identical except for the gateway and should both have metric 1. The primary interface should already have a default route that you can edit.

Figure 316: Add/Edit static route



a) Click **Static Route**.

b) Either click **Add Route** to add a new route, or click **Edit** ( ) for an existing route.

c) From the **Interface** drop-down, choose the interface.

d) For the destination network, select **any-ipv4** from the **Available Networks** box and click **Add**.

e) Enter the default **Gateway**.

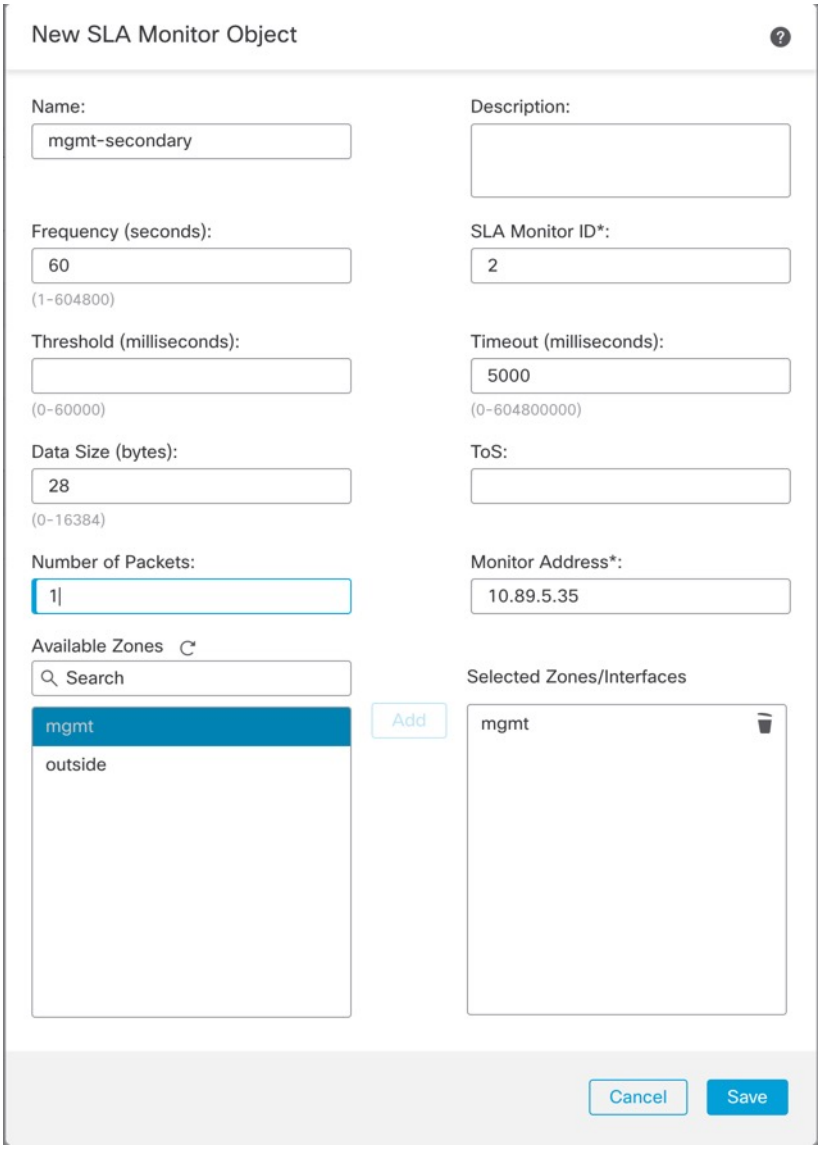
f) For **Route Tracking**, click **Add** ( ) to add a new SLA monitor object.

g) Enter the required parameters including the following:

- The **Monitor Address** as the Firewall Management Center IP address.
- The zone for the primary or secondary management interface in **Available Zones**; for example, choose the outside zone for the primary interface object, and the mgmt zone for the secondary interface object.

See Configure an SLA monitor, on page 2433 for more information.

Figure 317: Add SLA monitor



h) Click **Save**, then choose the SLA object you just created in the **Route Tracking** drop-down list.
i) Click **OK**, and then **Save**.

Repeat for the default route for the other management interface.

Step 6 Deploy configuration changes; see Deploy configuration changes, on page 135.

To deploy this feature, the Firewall Management Center enables the secondary interface for management traffic, including auto-generated policy-based routing configuration for management traffic to get to the right data interface. The Firewall Management Center also deploys a second instance of the **configure network management-data-interface** command. Note that if you edit the secondary interface at the CLI, you cannot

configure the gateway or otherwise alter the default route, because the static route for this interface can only be edited in the Firewall Management Center.

Change manager access interface settings

Changing manager interface settings on the device or on the Firewall Management Center can disrupt the management connection. Review these scenarios that change interface settings and reestablish the management connection.

Change the device IP address

Change the device IP address, and then update the address in the Firewall Management Center.

Set the device IP address

Use one of these methods to set the manager access interface IP address.

Modify Firewall Threat Defense management interface settings at the CLI

Many management interface settings are set during device initial setup; this task allows you to update them, add event-only interfaces (if supported), or configure static routes, DNS domains, and other advanced settings. Use the CLI when you need direct device access or troubleshooting. If you wish to configure network settings for a data interface used for management, use the device management center interface instead.

Note This topic applies to the dedicated management interface. You can alternatively configure a data interface for management. If you want to change network settings for that interface, you should do so within Firewall Management Center and not at the CLI. If you need to troubleshoot a disrupted management connection, and need to make changes directly on the Firewall Threat Defense , see Modify the Firewall Threat Defense data interface used for management at the CLI, on page 768 .

For information about the Firewall Threat Defense CLI, see the *Cisco Secure Firewall Threat Defense Command Reference* .

Before you begin

- You can create user accounts that can log into the CLI using the **configure user add** command ; see Add an internal user at the CLI, on page 87 . You can also configure AAA users according to Configure external authentication, on page 855 .
- Be cautious when making changes to the management interface using SSH. If you cannot re-connect because of a configuration error, access the device console port.
- In high-availability configurations, when you modify the management IP address of a registered device from the device CLI or from the Firewall Management Center , the standby Firewall Management Center does not reflect the changes even after a high-availability synchronization. To ensure that the standby Firewall Management Center is also updated, switch roles between the two Firewall Management Center s, making the secondary Firewall Management Center as the active unit. Modify the management IP address of the registered device on the **Device Management** page of the standby Firewall Management Center .

Procedure

Step 1 Connect to the device CLI, either from the console port or using SSH.

See Log into the Command-Line Interface on the device, on page 13 .

Step 2 Log in with the Admin username and password.

Step 3 (Firepower 4100/9300 /Secure Firewall 4200 only) Enable the second management interface as an event-only interface.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

You always need a management interface for management traffic. If your device has a second management interface, you can enable it for event-only traffic.

(Optional) Disable events for the main management interface using the **configure network management-interface disable-events-channel** command. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management interface even if you disable the event channel.

You cannot disable both event and management channels on an interface.

To use a separate event interface, you must enable an event-only interface on the Firewall Management Center that is dedicated exclusively to event traffic. See the *Cisco Secure Firewall Management Center Administration Guide* .

Example:

```
> configure network management-interface enable management1
Configuration updated successfully
> configure network management-interface disable-management-channel management1
Configuration updated successfully
>
```

Step 4 Configure the IP address of the management interface and/or event interface:

If you do not specify the *management_interface* argument, then you change the network settings for the default management interface. When configuring an event interface, be sure to specify the *management_interface* argument. The event interface can be on a separate network from the management interface, or on the same network. If you are connected to the interface you are configuring, you will be disconnected. You can re-connect to the new IP address.

a) Configure the IPv4 address:

- Manual configuration:

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  Note that the *gateway_ip* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *gateway_ip* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *gateway_ip* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.

Example:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
>
```

- DHCP (supported on the default management interface only):

  configure network ipv4 dhcp

b) Configure the IPv6 address:

- Stateless autoconfiguration:

  configure network ipv6 router [*management_interface*]

  Example:

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.
>
```

- Manual configuration:

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  Note that the *ipv6_gateway_ip* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *ipv6_gateway_ip* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *ipv6_gateway_ip* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.

  Example:

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.
>
```

- DHCPv6 (supported on the default management interface only):

  configure network ipv6 dhcp

c) For IPv6, enable or disable ICMPv6 Echo Replies and Destination Unreachable messages. These messages are enabled by default.

configure network ipv6 destination-unreachable { **enable** | **disable** }

configure network ipv6 echo-reply { **enable** | **disable** }

You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.

Example:

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

Step 5 Enable a DHCP server on the default management interface to provide IP addresses to connected hosts:

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

Example:

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled
>
```

You can only configure a DHCP server when you set the management interface IP address manually. This command is not supported on the Firewall Management Center Virtual . To display the status of the DHCP server, enter **show network-dhcp-server** :

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

Step 6 Add a static route for the event-only interface if the Firewall Management Center is on a remote network. Otherwise, all traffic will match the default route through the management interface.

configure network static-routes { **ipv4** | **ipv6** } **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

For the default route, do not use this command; you can only change the default route gateway IP address when you use the **configure network ipv4** or **ipv6** commands (see Step 4, on page 764).

Example:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully
> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
>
```

To display static routes, enter **show network-static-routes** (the default route is not shown):

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

Step 7 Do these settings:

a) Set the hostname:

configure network hostname *name*

Example:

```
> configure network hostname farscape1.cisco.com
```

Syslog messages do not reflect a new hostname until after a reboot.

b) Set the search domains:

configure network dns searchdomains *domain_list*

Example:

```
> configure network dns searchdomains example.com,cisco.com
```

Set the search domain(s) for the device, separated by commas. These domains are added to hostnames when you do not specify a fully-qualified domain name in a command, for example, **ping system** . The domains are used only on the management interface, or for commands that go through the management interface.

c) Set up to 3 DNS servers, separated by commas:

configure network dns servers *dns_ip_list*

Example:

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

d) Set the remote management port for communication with the Firewall Management Center :

configure network management-interface tcpport *number*

Example:

```
> configure network management-interface tcpport 8555
```

The Firewall Management Center and managed devices communicate using a two-way, TLS-1.3-encrypted communication channel, which by default is on port 8305. Do not change the management port when using multi-instance mode; only port 8305 is supported.

Note We recommend that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for *all* devices in your deployment that need to communicate with each other.

e) (Firewall Threat Defense only) Set the management or eventing interface MTU. The MTU is 1500 bytes by default.

configure network mtu [*bytes*] [*interface_id*]

- *bytes* —Sets the MTU in bytes. For the management interface, the value can be between 64 and 1500 if you enable IPv4, and 1280 to 1500 if you enable IPv6. For the eventing interface, the value can be between 64 and 9000 if you enable IPv4, and 1280 to 9000 if you enable IPv6. If you enable both IPv4 and IPv6, then the minimum is 1280. If you do not enter the *bytes* , you are prompted for a value.
- *interface_id* —Specifies the interface ID on which to set the MTU. Use the **show network** command to see available interface IDs, for example management0, management1, br1, and eth0, depending on the platform. If you do not specify an interface, then the management interface is used.

Example:

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192
Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

f) Configure an HTTP proxy. The device is configured to directly connect to the internet on ports TCP/443 (HTTPS) and TCP/80 (HTTP). You can use a proxy server, to which you can authenticate via HTTP Digest. After issuing the command, you are prompted for the HTTP proxy address and port, whether

proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

Note For proxy password on Firewall Threat Defense , you can use A-Z, a-z, and 0-9 characters only.

configure network http-proxy

Example:

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Step 8 If you change the device management IP address, then see the following tasks for Firewall Management Center connectivity. Perform these tasks depending on how you identified the Firewall Management Center during initial device setup using the **configure manager add** command (see Register with a new management center, on page 46) :

- **IP address — No action.** If you identified the Firewall Management Center using a reachable IP address, then the management connection will be reestablished automatically after several minutes. We recommend that you also change the device IP address shown in Firewall Management Center to keep the information in sync; see Update the Hostname or IP Address in the Firewall Management Center, on page 772. This action can help reestablish the connection faster. If you specified an unreachable Firewall Management Center IP address, then you must manually reestablish the connection using Update the Hostname or IP Address in the Firewall Management Center, on page 772
- **NAT ID only — Manually reestablish the connection.** If you identified the Firewall Management Center using only the NAT ID, then the connection does not automatically reestablish. In this case, change the device management IP address in Firewall Management Center according to Update the Hostname or IP Address in the Firewall Management Center, on page 772 .

Modify the Firewall Threat Defense data interface used for management at the CLI

This task allows you to specify a new data interface to replace the old interface when the management connection has been disrupted and you need to restore connectivity between the Firewall Threat Defense and the Firewall Management Center.

If the management connection is active, make changes to an existing data interface using the Firewall Management Center (see Modify the Firewall Threat Defense data interface used for management in the GUI, on page 771). For initial setup of the data management interface, see the **configure network management-data-interface** command in Complete the Firewall Threat Defense Initial Configuration Using the CLI , on page 21.

For high-availability pairs, perform all CLI steps on both units. Within the Firewall Management Center, perform steps only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

Note This topic applies to the data interface that you configured for Management, not the dedicated Management interface. If you want to change network settings for the Management interface, see Modify Firewall Threat Defense management interface settings at the CLI , on page 763.

For information about the Firewall Threat Defense CLI, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Before you begin

If you are changing the data management interface to a new interface, move the current interface cable to the new interface.

Procedure

Step 1 Connect to the device CLI.

Use the console port when executing these commands. If you are performing initial setup, then you may be disconnected from the Management interface. If you are editing the configuration due to a disrupted management connection and have SSH access to the dedicated management interface, you can use the SSH connection.

See Log into the Command-Line Interface on the device, on page 13.

a) Log in with the **admin** username and password.

Step 2 Disable the interface so you can reconfigure its settings.

configure network management-data-interface disable

Note If you only want to set a new IPv4 address on the same interface and not make any other changes, you can skip this step. Other changes require you to disable the interface first.

Example:

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

Step 3 Configure the new data interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

If you change the data management interface to a new interface on the same network, use the same settings as for the previous interface except the interface ID. In addition, for the **Do you wish to clear all the device configuration before applying ? (y/n) [n]:** option, choose **y**. This choice will clear the old data management

interface configuration, so that you can successfully reuse the IP address and interface name on the new interface.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

a) Limit data interface access to the Firewall Management Center on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

Step 4 Update the Hostname or IP Address in the Firewall Management Center, on page 772.

The connection may be reestablished automatically, but disabling and reenabling the connection in the Firewall Management Center will help the connection reestablish faster. Or you may need to update the device IP address in the Firewall Management Center according to the linked procedure.

Step 5 Check that the management connection was reestablished.

sftunnel-status-brief

See the sample output for a connection that is up, with peer channel and heartbeat information:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Step 6 In the Firewall Management Center, choose **Devices** > **Device Management**, and click **Edit** (). In the **Device** area, against the **Management** field, click **Refresh** next to **Manager Access - Configuration Details**.

The Firewall Management Center detects the interface and default route configuration changes and blocks deployment to the device. When you change the data interface settings locally on the device, you must reconcile those changes in the Firewall Management Center manually. You can view the discrepancies between the Firewall Management Center and the device on the **Configuration** tab.

Step 7 Choose **Interfaces**, and make the changes.

a) Remove the IP address and name from the old data management interface and disable manager access for this interface.

b) Configure the new data management interface with the new settings (the ones you used at the CLI) and enable manager access for it.

Step 8 Under the **Routing** tab, click **Static Route**, and change the default route from the old data management interface to the new one.

Step 9 Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.

The next time you deploy, the Firewall Management Center configuration will overwrite any remaining conflicting settings on the Firewall Threat Defense. It is your responsibility to manually fix the configuration in the Firewall Management Center before you re-deploy.

You will see expected messages of "Config was cleared" and "Manager access changed and acknowledged."

Modify the Firewall Threat Defense data interface used for management in the GUI

Configure the data interface IP address settings to change the management connection or update the interface used for manager access.

If the management connection is up but you want to change the IP address of the data interface used for manager access, follow these steps. For example, if you register a device using zero-touch provisioning, then you need to change the IP address to a static address before you can enable high availability.

You can alternatively change interface settings at the CLI, but we recommend using that method only if the management connection is down. Any changes you make at the CLI should be replicated in the GUI.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) next to the device.

Step 2 Choose **Interfaces**.

Step 3 If you want to change the interface used for manager access:

a) Remove the IP address and name from the old data management interface and disable manager access for this interface.

b) Configure the new data management interface with the new settings and enable manager access for it.

c) If you use a static IP address, you are reminded to make sure you have a default route. Click **Yes**.

d) Click **OK** to exit the interface.

e) Click **Save** on the **Interfaces** page.

Step 4 If you only want to change the IP address:

a) Change the IP address.

b) For a static IP address, you are reminded to make sure you have a default route. Click **Yes**.

c) Click **OK** to exit the interface.

d) Click **Save** on the **Interfaces** page.

Step 5 Click the **Routing** tab, click **Static Route**, and then add or change the default or static route for the manager access interface.

Step 6 Deploy configuration changes; see Deploy configuration changes, on page 135.

The Firewall Management Center will deploy the configuration changes over the current connection. After the deployment, the data interface will have a new IP address, so the management connection will need to be reestablished.

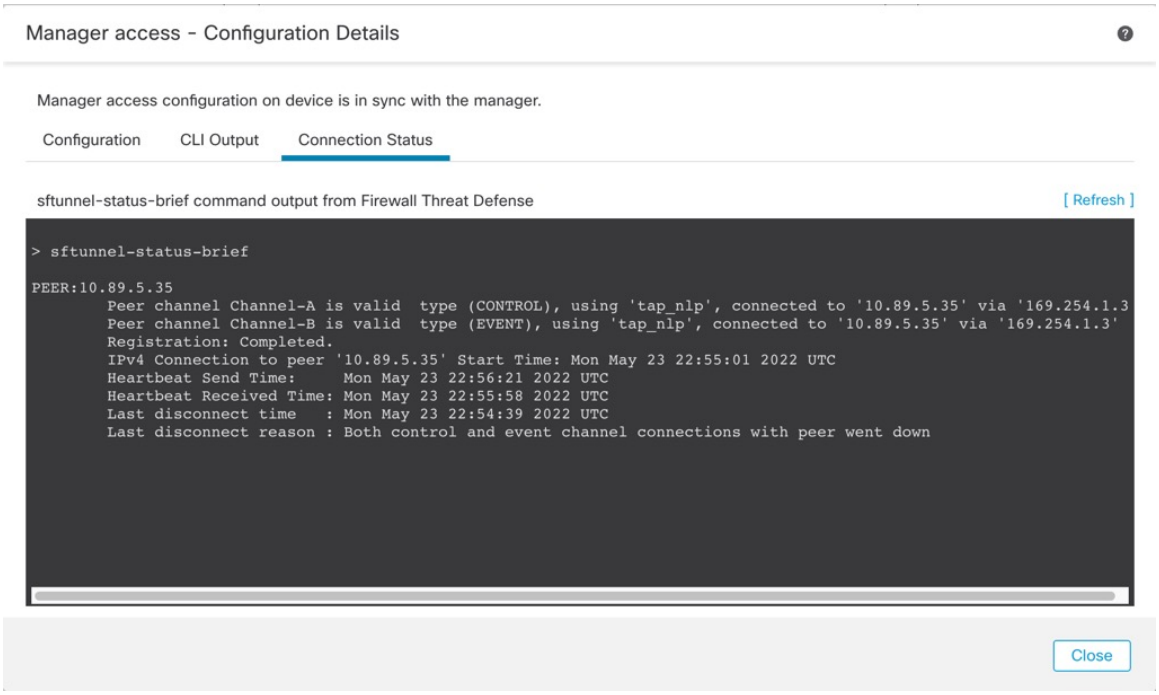
Step 7 Update the Hostname or IP Address in the Firewall Management Center, on page 772.

Step 8 Ensure the management connection is reestablished.

In the **Device** area, against the **Management** field, click **Manager Access Details: Configuration** and then click **Connection Status**.

The following status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 318: Connection status



If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 792.

Update the Hostname or IP Address in the Firewall Management Center

This task allows you to manually update the hostname or IP address on the managing Firewall Management Center when device network settings have been modified outside of the management interface.

If you edit the hostname or IP address of a device after you added it to the Firewall Management Center (using the device's CLI, for example), you need to use this procedure to manually update the hostname or IP address on the managing Firewall Management Center.

To change the device management IP address on the device, see Modify Firewall Threat Defense management interface settings at the CLI , on page 763.

If you used only the NAT ID when registering the device, then the IP shows as **NO-IP** on this page, and you do not need to update the IP address/hostname.

If you used zero-touch provisioning to register the device on the outside interface, the hostname is automatically generated along with a matching DDNS configuration. You cannot edit the hostname in this case.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to modify management options, click **Edit** ( ).

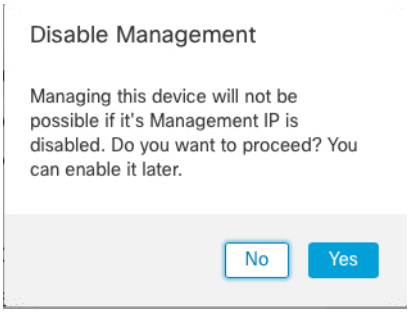
Step 3 Click **Device** and view the **Management** area.

Step 4 Disable management temporarily by clicking the slider so it is disabled **Slider disabled** ( ).

Figure 319: Disable management



You are prompted to proceed with disabling management; click **Yes**.



Disabling management blocks the connection between the Firewall Management Center and the device, but does **not** delete the device from the Firewall Management Center.

Step 5 Edit the **Remote Host Address** IP address and optional **Secondary Address** (when using a redundant data interface) or hostname by clicking **Edit** ( ).

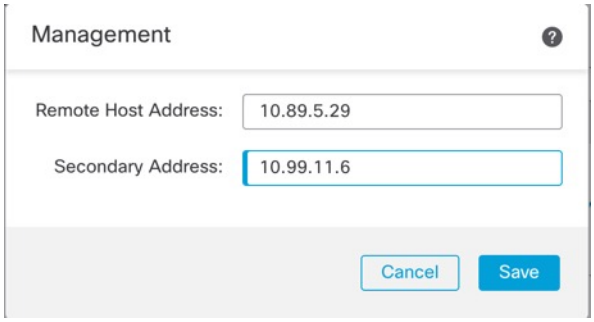
Figure 320: Edit management address



Step 6 In the **Management** dialog box, modify the name or IP address in the **Remote Host Address** field and the optional **Secondary Address** field. Click **Save**.

For information about using a secondary manager access data interface, see Configure a redundant manager access data interface, on page 758.

Figure 321: Management IP address



Step 7 Reenable management by clicking the slider so it is enabled **Slider enabled** ( ).

Figure 322: Enable management connection



Change the Firewall Management Center IP Address

This task ensures the Firewall Management Center IP address or hostname matches between the management center and device CLI, maintaining consistent configurations and network resiliency.

If you change the Firewall Management Center IP address or hostname, you should also change the value at the device CLI so the configurations match. Although in most cases, the management connection will be reestablished without changing the Firewall Management Center IP address or hostname on the device, in at

least one case, you must perform this task for the connection to be reestablished: when you added the device to the Firewall Management Center and you specified the NAT ID only. Even in other cases, we recommend keeping the Firewall Management Center IP address or hostname up to date for extra network resiliency.

Procedure

Step 1 Change the Firewall Management Center IP address.

Caution Be careful when making changes to the Firewall Management Center interface to which you are connected; if you cannot re-connect because of a configuration error, you need to access the Firewall Management Center console port to re-configure the network settings in the Linux shell. You must contact Cisco TAC to guide you in this operation.

a) Choose **System** (⚙) > **Configuration** > **Management Interfaces**.
b) In the **Interfaces** area, click **Edit** next to the interface that you want to configure.
c) Change the IP address, and click **Save**.

Step 2 At the Firewall Threat Defense CLI, view the Firewall Management Center identifier.

show managers

Example:

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

Step 3 At the Firewall Threat Defense CLI, edit the Firewall Management Center IP address or hostname.

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

If the Firewall Management Center was originally identified by **DONTRESOLVE** and a NAT ID, you can change the value to a hostname or IP address using this command. You cannot change an IP address or hostname to **DONTRESOLVE**.

The management connection will go down, and then reestablish. You can monitor the state of the connection using the **sftunnel-status** command.

Example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

Change both Firewall Management Center and Threat Defense IP addresses

You might want to change both Firewall Management Center and Firewall Threat Defense IP addresses if you need to move them to a new network.

Procedure

Step 1 Disable the management connection.

For a high-availability pair or cluster, perform these steps on all units.

a) Choose **Devices** > **Device Management**.

b) Next to the device, click **Edit** ( ).

c) Click **Device**, and view the **Management** area.

d) Disable management temporarily by clicking the slider so it is disabled ( ).

Figure 323: Disable Management



You are prompted to proceed with disabling management; click **Yes**.

Step 2 Change the device IP address in the Firewall Management Center to the new device IP address.

You will change the IP address on the device later.

For a high-availability pair or cluster, perform these steps on all units.

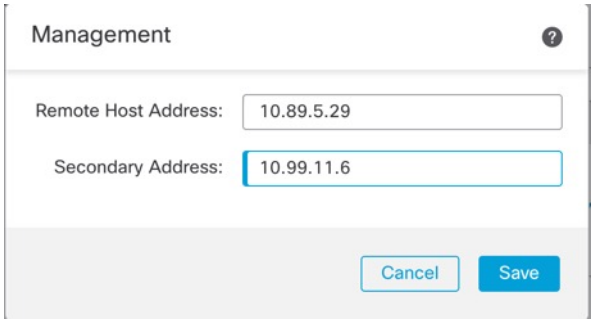
a) Edit the **Remote Host Address** IP address and optional **Secondary Address** (when using a redundant data interface) or hostname by clicking **Edit** ( ).

Figure 324: Edit Management Address



b) In the **Management** dialog box, modify the name or IP address in the **Remote Host Address** field and the optional **Secondary Address** field, and click **Save**.

Figure 325: Management IP Address



Step 3 Change the Firewall Management Center IP address.

Caution Be careful when making changes to the Firewall Management Center interface to which you are connected. If you cannot re-connect because of a configuration error, you need to access the Firewall Management Center console port to re-configure the network settings in the Linux shell. You must contact Cisco TAC to guide you in this operation.

a) Choose **System** (⚙) > **Configuration** > **Management Interfaces**.
b) In the **Interfaces** area, click **Edit** next to the interface that you want to configure.
c) Change the IP address, and click **Save**.

Step 4 Change the manager IP address on the device.

For a high-availability pair or cluster, perform these steps on all units.

a) At the Firewall Threat Defense CLI, view the Firewall Management Center identifier.

show managers

Example:

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

b) Edit the Firewall Management Center IP address or hostname.

configure manager edit *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

If the Firewall Management Center was originally identified by **DONTRESOLVE** and a NAT ID, you can change the value to a hostname or IP address using this command. You cannot change an IP address or hostname to **DONTRESOLVE**.

Example:

```
                                > configure manager edit
f7ffad78-bf16-11ec-a737-baa2f76ef602
                                hostname
```

```
10.10.5.1
```

Step 5 Change the IP address of the manager access interface at the console port.

For a high-availability pair or cluster, perform these steps on all units.

If you use the dedicated Management interface:

configure network ipv4

configure network ipv6

If you use the dedicated Management interface:

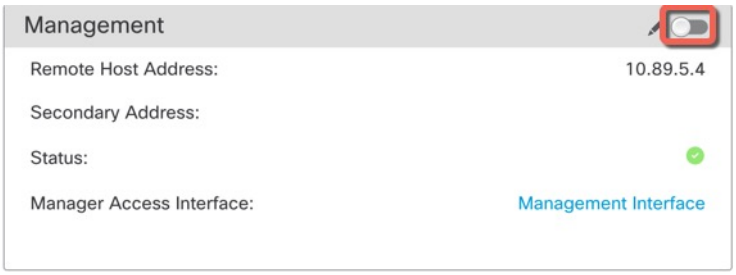
configure network management-data-interface disable

configure network management-data-interface

Step 6 Re-enable management by clicking the slider ( ).

For a high-availability pair or cluster, perform these steps on all units.

Figure 326: Enable Management Connection



Step 7 (If you use a data interface for manager access) Refresh the data interface settings in the Firewall Management Center.

For a high-availability pair, perform this step on both units.

a) Choose **Devices** > **Device Management**, and click **Manager Access - Configuration Details** , and then click **Refresh**.
b) Choose **Devices** > **Device Management**, and click the **Interfaces** tab and set the IP address to match the new address.
c) Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.

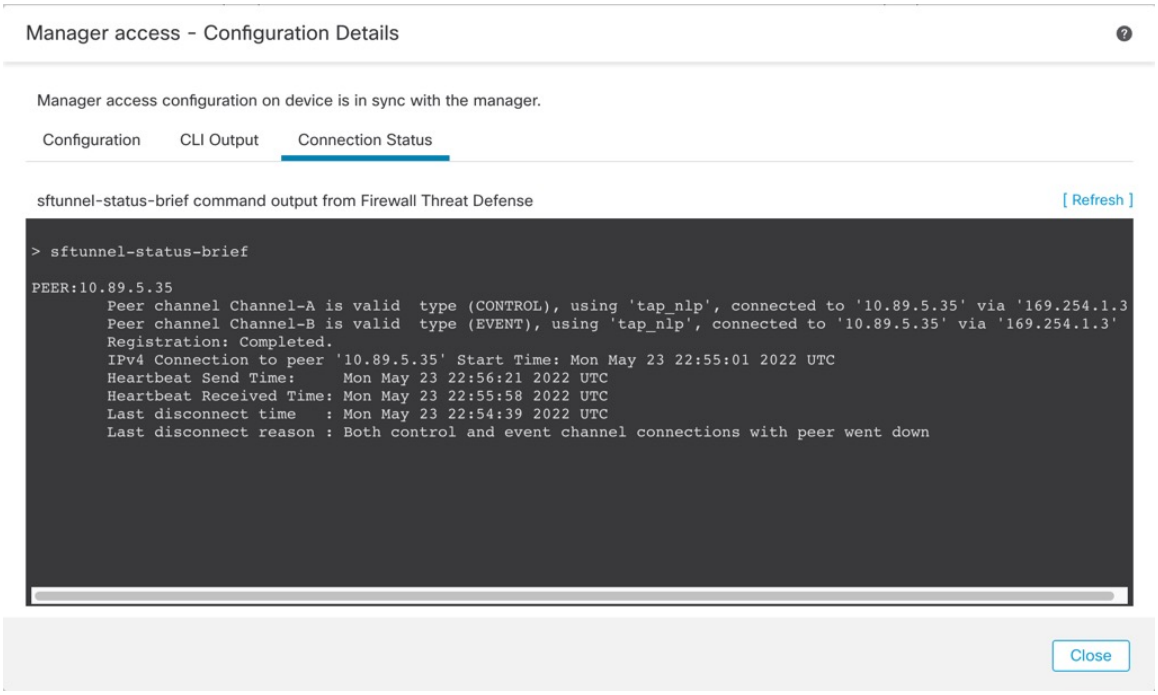
Step 8 Ensure the management connection is reestablished.

In the Firewall Management Center, check the management connection status. Navigate to the **Devices** > **Device Management**, and click **Management** section under the **Device** tab. Then, click **Manager Access - Configuration Details** to view the **Connection Status** page.

At the Firewall Threat Defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

This status indicates a successful connection for a data interface and displays the internal "tap_nlp" interface.

Figure 327: Connection Status



Step 9 (For a high-availability Firewall Management Center pair) Repeat configuration changes on the secondary Firewall Management Center.

a) Change the secondary Firewall Management Center IP address.
b) Specify the new peer addresses on both units.
c) Make the secondary unit the active unit.
d) Disable the device management connection.
e) Change the device IP address in the Firewall Management Center.
f) Re-enable the management connection.

Change the manager access interface

After you register the device, you can change the manager access interface between the Management interface and a data interface.

Change the manager access interface from management to data

You can manage the Firewall Threat Defense from either the dedicated management interface or from a data interface. If you want to change the manager access interface after you added the device to the Firewall Management Center , follow these steps to migrate from the Management interface to a data interface. To migrate the other direction, refer to Change the manager access interface from data to management, on page 783 .

When you initiate the manager access migration from management to data, the Firewall Management Center applies a block on deployment to the Firewall Threat Defense. To remove the block, enable manager access on the data interface.

Before you begin

For high-availability pairs:

- Ensure that you configure a standby IP address for data-managed interfaces before changing the manager access interface from management to data. For more information about configuring standby IP address, refer to Configure standby IP addresses and interface monitoring, on page 309.
- For high-availability pairs, unless stated otherwise, perform all steps only on the active unit. After deploying the configuration changes, the standby unit synchronizes configuration and other state information from the active unit.
-

For high-availability pairs, unless stated otherwise, perform all steps only on the active unit. After deploying the configuration changes, the standby unit synchronizes configuration and other state information from the active unit.

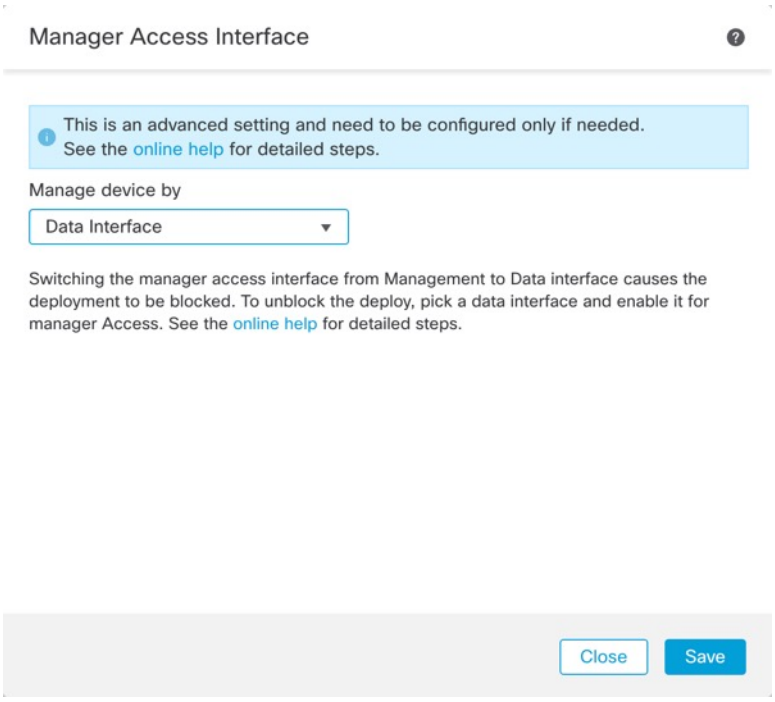
Procedure

Step 1 Initiate the interface migration.

a) On the **Devices** > **Device Management** page, click **Edit** ( ) for the device. Click **Device** , and in the **Management** area, click the **Manager Access Interface** link.

The **Manager Access Interface** field shows the current Management interface. When you click the link, choose the new interface type, **Data Interface** , in the **Manage device by** drop-down list.

Figure 328: Manager Access Interface



b) Click **OK** and then **Close** .

You must now complete the remaining steps in this procedure to enable manager access on the data interface. The **Management** area now shows **Manager Access Interface: Data Interface** , and **Manager Access Details: Configuration** .

Figure 329: Manager Access



If you click **Configuration** , the **Manager Access - Configuration Details** dialog box opens. The **Manager Access Mode** shows a Deploy pending state.

Step 2 Enable manager access on the data interface (s) . Click **Interfaces** , click **Edit** ( ) for the interface, and then click **Manager Access** .

Check **Enable management access** and click **OK** . By default, all networks are allowed, but you can limit access as long as the Firewall Management Center address is allowed.

If the manager access interface uses a static IP address, you are reminded to configure routing for it.

Click **Save** on the **Interfaces** page. See Configure routed mode interfaces, on page 690 for more information about interface settings. You can enable manager access on one routed data interface , plus an optional secondary interface . Make sure these interfaces are fully configured with a name and IP address and that they are enabled.

If you use a secondary interface for redundancy, see Configure a redundant manager access data interface, on page 758 for additional required configuration.

Step 3 (Optional) If you use DHCP for the interface, enable the web type DDNS method on the DDNS page. Navigate to **Devices** > **Device Management** , and then click **DDNS** under the **DHCP** tab.

See Configure Dynamic DNS, on page 838 . DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.

Step 4 Make sure the Firewall Threat Defense can route to the Firewall Management Center through the data interface. Add a static route if necessary on the Static Route page. Navigate to **Devices** > **Device Management** and then click **Static Route** under the **Routing** tab.

See Add a static route, on page 977 .

Step 5 (Optional) Configure DNS in a Platform Settings policy: choose **Devices** > **Platform Settings** , and click **DNS** . Apply the policy to this device.

See Configure DNS server settings, on page 852 . DNS is required if you use DDNS. You may also use DNS for FQDNs in your security policies.

Step 6 (Optional) Enable SSH for the data interface in a Platform Settings policy, and apply it to this device at **Devices** > **Device Management** page. Click **Edit** ( ) for the device and then click **SSH Access** .

See Configure Secure Shell (SSH) access, on page 867 . SSH is not enabled by default on the data interfaces, so if you want to manage the Firewall Threat Defense using SSH, you need to explicitly allow it.

Step 7 Deploy configuration changes; see Deploy configuration changes, on page 135.

You will see a validation error to confirm that you are changing the manager access interface. Check **Ignore warnings** and deploy again.

The Firewall Management Center will deploy the configuration changes over the current Management interface. After the deployment, the data interface is now ready for use, but the original management connection to Management is still active.

Step 8 After deployment, perform these actions.

a) At the Firewall Threat Defense CLI (preferably from the console port), set the Management interface to use a static IP address and set the gateway to use the data interfaces. For high availability, perform this step on both units.

```
configure network
{
ipv4
 |
ipv6
}
manual
ip_address netmask
data-interfaces
```

- *ip_address netmask* —Although you do not plan to use the Management interface, you must set a static IP address, for example, a private address so that you can set the gateway to **data-interfaces** (see the next bullet). You cannot use DHCP because the default route, which must be **data-interfaces** , might be overwritten with one received from the DHCP server.
- **data-interfaces** —This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.

We recommend that you use the console port instead of an SSH connection because when you change the Management interface network settings, your SSH session will be disconnected.

b) If necessary, re-cable the Firewall Threat Defense so it can reach the Firewall Management Center on the data interface. For high availability, perform this step on both units.

c) In the Firewall Management Center , disable the management connection, update the **Remote Host Address** IP address and optional **Secondary Address** for the Firewall Threat Defense in the **Devices** > **Device Management** page in the **Management** area under the **Device** tab, and reenable the connection.

Refer to Update the Hostname or IP Address in the Firewall Management Center, on page 772 . If you used the Firewall Threat Defense hostname or just the NAT ID when you added the Firewall Threat Defense to the Firewall Management Center , you don't have to update the value. To restart the connection, you must disable and re-enable the management connection.

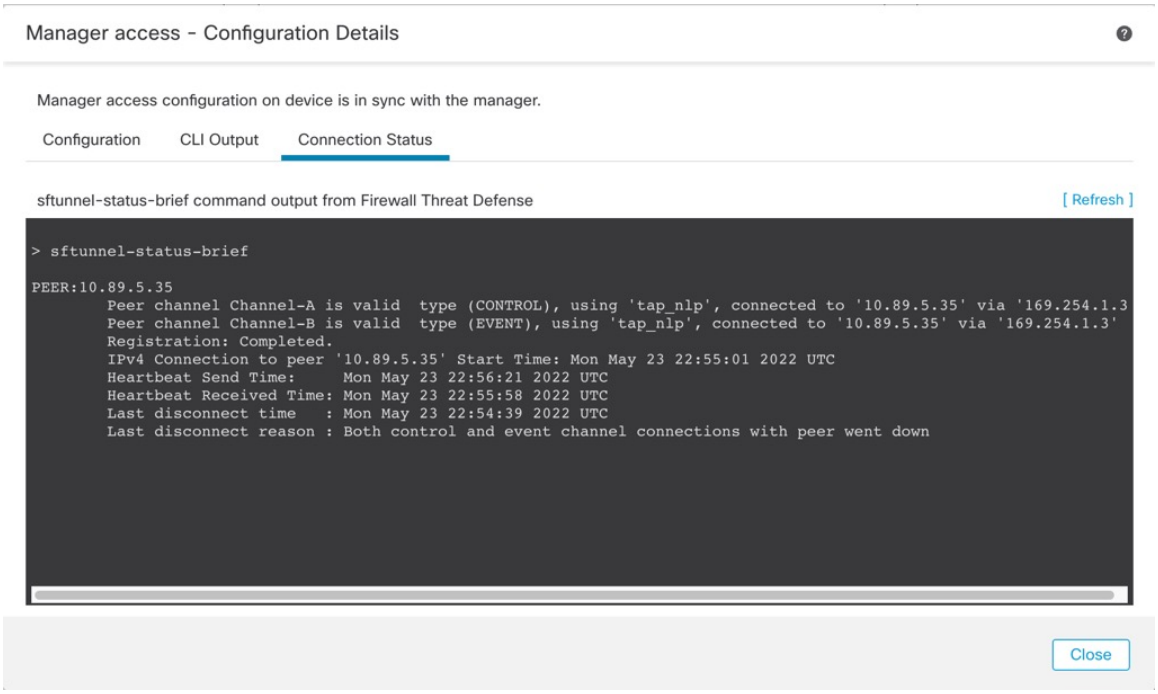
Step 9 Ensure the management connection is reestablished.

In the **Devices** > **Device Management** page, click **Manager Access Details: Configuration** and then click **Connection Status** .

Alternatively, you can check at the Firewall Threat Defense CLI. Enter the **sftunnel-status-brief** command to view the management connection status.

This status indicates a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 330: Connection Status



If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 792 .

Change the manager access interface from data to management

This task enables you to migrate manager access from a data interface to the dedicated management interface, allowing you to manage the Firewall Threat Defense through the Management interface instead of a data interface.

You can manage the Firewall Threat Defense from either the dedicated management interface or from a data interface. If you want to change the manager access interface after you added the device to the Firewall Management Center, follow these steps to migrate from a data interface to the management interface. To migrate the other direction, see Change the manager access interface from management to data, on page 779.

Initiating the manager access migration from data to management causes the Firewall Management Center to apply a block on deployment to the Firewall Threat Defense. You must disable manager access on the data interface to remove the block.

Before you begin

For high-availability pairs, unless stated otherwise, perform all steps only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

Follow these steps to disable manager access on a data interface, and also configure other required settings.

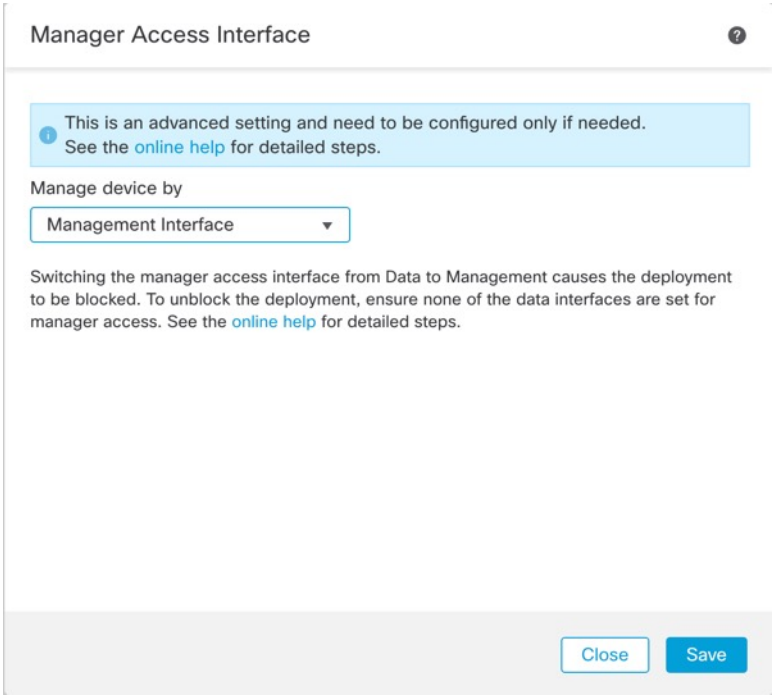
Procedure

Step 1 Initiate the interface migration.

a) On the **Devices** > **Device Management** page, click **Edit** (✎) for the device. Click **Device**, and in the **Management** area, click the link for **Manager Access Interface**.

The **Manager Access Interface** field shows the current management interface as data. When you click the link, choose the new interface type, **Management Interface**, in the **Manage device by** drop-down list.

Figure 331: Manager access interface



b) Click **Save**.

Click **OK** and then **Close**.

You must now complete the remaining steps in this procedure to enable manager access on the Management interface. The **Management** area now shows the **Manager Access Interface: Management Interface**.

Figure 332: Manager access



Step 2 Disable manager access on the data interface(s). Click **Interfaces**, click **Edit** (✎) for the interface, and then click **Manager Access**.

Uncheck **Enable management access** and click **OK**. Click **Save** on the **Interfaces** page. This step removes the block on deployment.

Step 3 If you have not already done so, configure DNS settings for the data interface in a Platform Setting policy, and apply it to this device at **Devices** > **Device Management** page. Click **Edit** (✎) for the device and then click **DNS**.

See Configure DNS server settings, on page 852. The Firewall Management Center deployment that disables manager access on the data interface will remove any local DNS configuration. If that DNS server is used in any security policy, such as an FQDN in an Access Rule, then you must re-apply the DNS configuration using the Firewall Management Center.

Step 4 Deploy configuration changes; see Deploy configuration changes, on page 135.

The Firewall Management Center will deploy the configuration changes over the current data interface.

Step 5 If necessary, re-cable the Firewall Threat Defense so it can reach the Firewall Management Center on the Management interface. For High Availability, perform this step on both units.

Step 6 At the Firewall Threat Defense CLI, configure the Management interface IP address and gateway using a static IP address or DHCP. For high availability, perform this step on both units.

When you originally configured the data interface for manager access, the Management gateway was set to data-interfaces, which forwarded management traffic over the backplane so it could be routed through the manager access data interface. You now need to set an IP address for the gateway on the management network.

Static IP address:

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **DHCP**

Step 7 In the Firewall Management Center, disable the management connection, update the **Remote Host Address** IP address and optional **Secondary Address** for the Firewall Threat Defense in the **Devices** > **Device Management**, **Management** section under **Device** tab, and reenable the connection.

See Update the Hostname or IP Address in the Firewall Management Center, on page 772. If you used the Firewall Threat Defense hostname or just the NAT ID when you added the Firewall Threat Defense to the Firewall Management Center, you do not need to update the value; however, you need to disable and reenable the management connection to restart the connection.

Step 8 Ensure the management connection is reestablished.

In the Firewall Management Center, check the management connection status on the **Devices** > **Device Management**, **Management** section under **Device** tab, **Status** field or view notifications in the Firewall Management Center.

At the Firewall Threat Defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 792.

View manager access details for data interface management

If you use a data interface for Firewall Management Center management instead of the dedicated management interface, you must be careful about changing the interface and network settings for the device in the Firewall Management Center to prevent disruption of the connection. When you change data interface settings locally on the device, you must reconcile them manually in the Firewall Management Center.

Use the **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** dialog box to resolve any discrepancies between the Firewall Management Center and the Firewall Threat Defense local configuration.

Typically, you configure the manager access data interface as part of initial Firewall Threat Defense setup before you add the Firewall Threat Defense to the Firewall Management Center. When you add the Firewall Threat Defense to the Firewall Management Center, the Firewall Management Center discovers and maintains the interface configuration, which includes interface name and IP address, static route to the gateway, DNS servers, and DDNS server. The DNS server configuration is maintained locally if discovered during registration, but it is not added to the Platform Settings policy in Firewall Management Center.

After you add the Firewall Threat Defense to the Firewall Management Center, if you change the data interface settings on the Firewall Threat Defense locally using the **configure network management-data-interface** command, the Firewall Management Center detects the configuration changes and blocks deployment to the Firewall Threat Defense. The Firewall Management Center detects the configuration changes using one of these methods:

- Deploy to the Firewall Threat Defense. Before the Firewall Management Center deploys, it will detect the configuration differences and stop the deployment.
- The **Sync** button in the **Interfaces** page.
- The **Refresh** button on the **Manager Access - Configuration Details** dialog box.

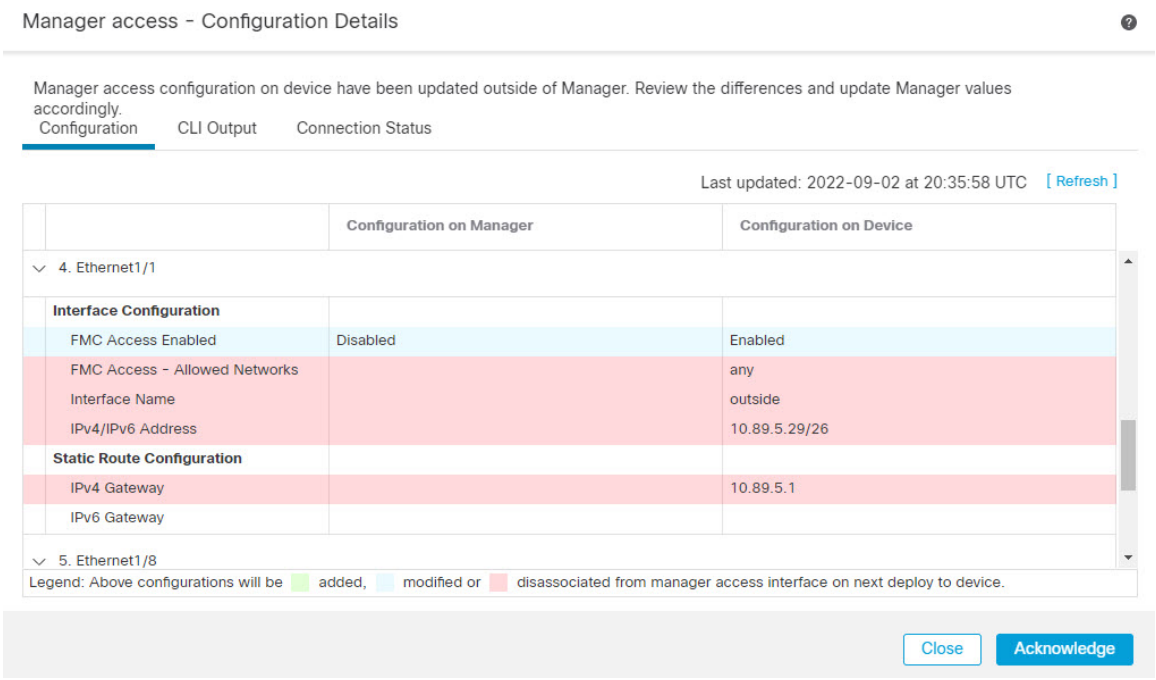
To remove the block, you must go to the **Manager Access - Configuration Details** dialog box and click **Acknowledge**. The next time you deploy, the Firewall Management Center configuration will overwrite any remaining conflicting settings on the Firewall Threat Defense. It is your responsibility to manually fix the configuration in the Firewall Management Center before you re-deploy.

Configuration

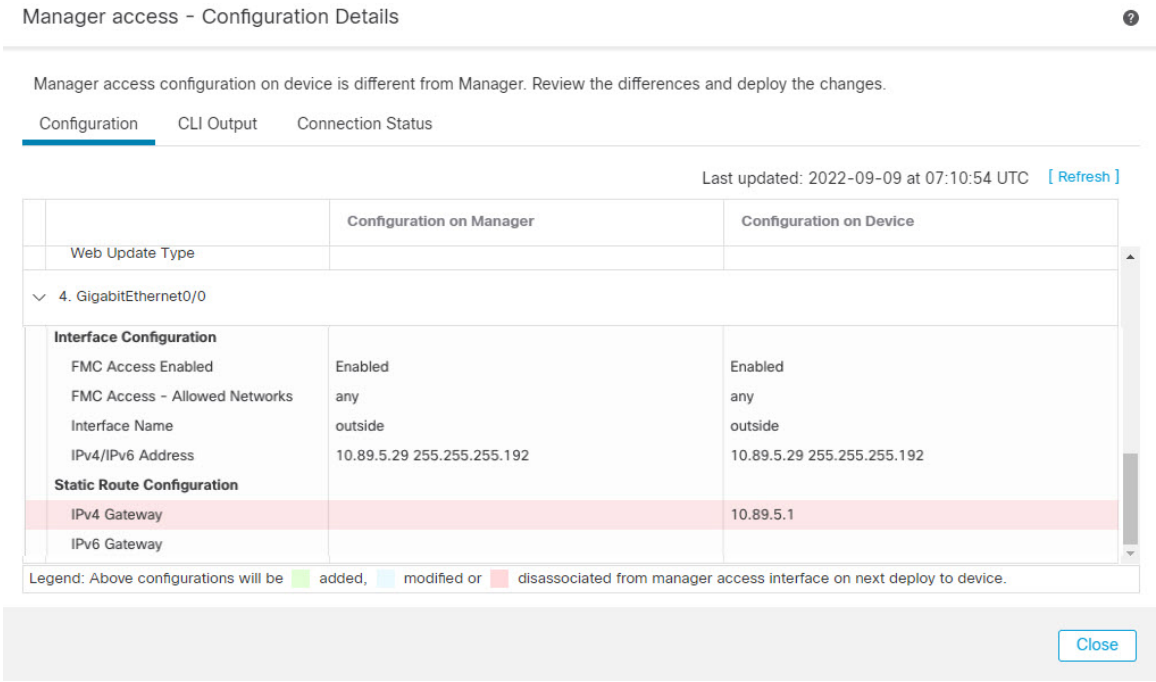
View the configuration comparison of the manager access data interface on the Firewall Management Center and the Firewall Threat Defense.

This example shows the configuration details of the Firewall Threat Defense where the **configure network management-data-interface** command was entered on the Firewall Threat Defense. Pink highlights indicate

that, if you **Acknowledge** the differences but do not match the configuration in the Firewall Management Center, then the Firewall Threat Defense configuration will be removed. Blue highlights mark configurations that will be modified on the Firewall Threat Defense. Green highlights mark configurations that will be added to the Firewall Threat Defense.



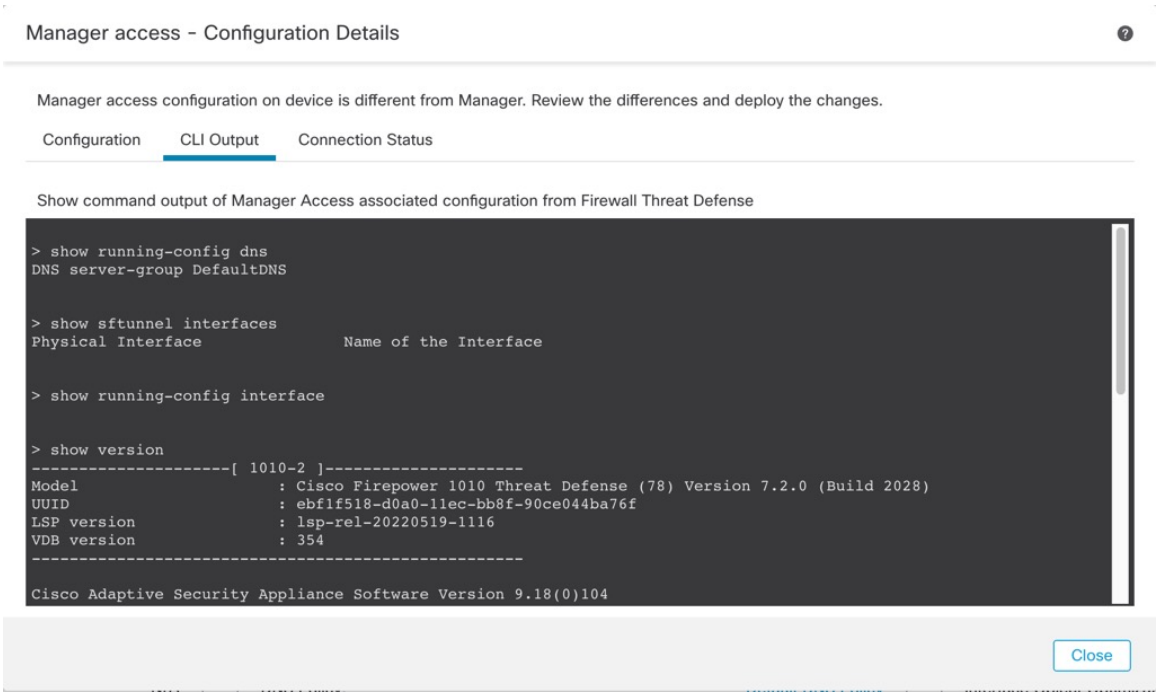
This example shows the page after configuring the interface in the Firewall Management Center. The interface settings match, and the pink highlight was removed.

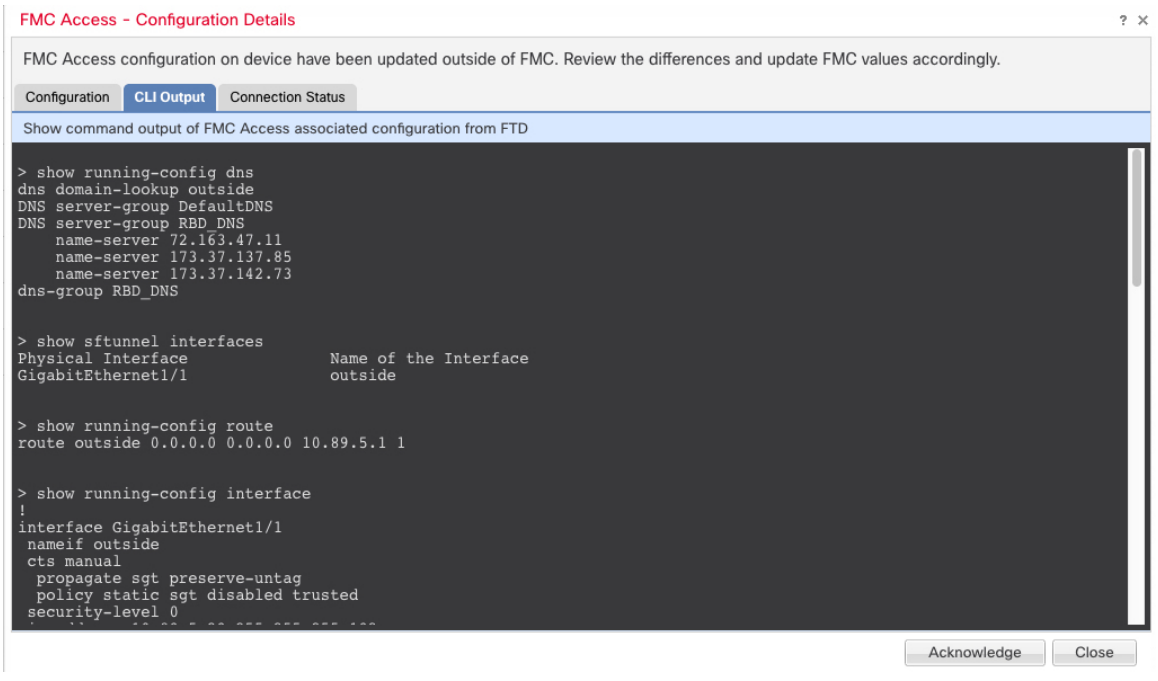


CLI output

View the CLI configuration of the manager access data interface, which is useful if you are familiar with the underlying CLI.

Figure 333: CLI output

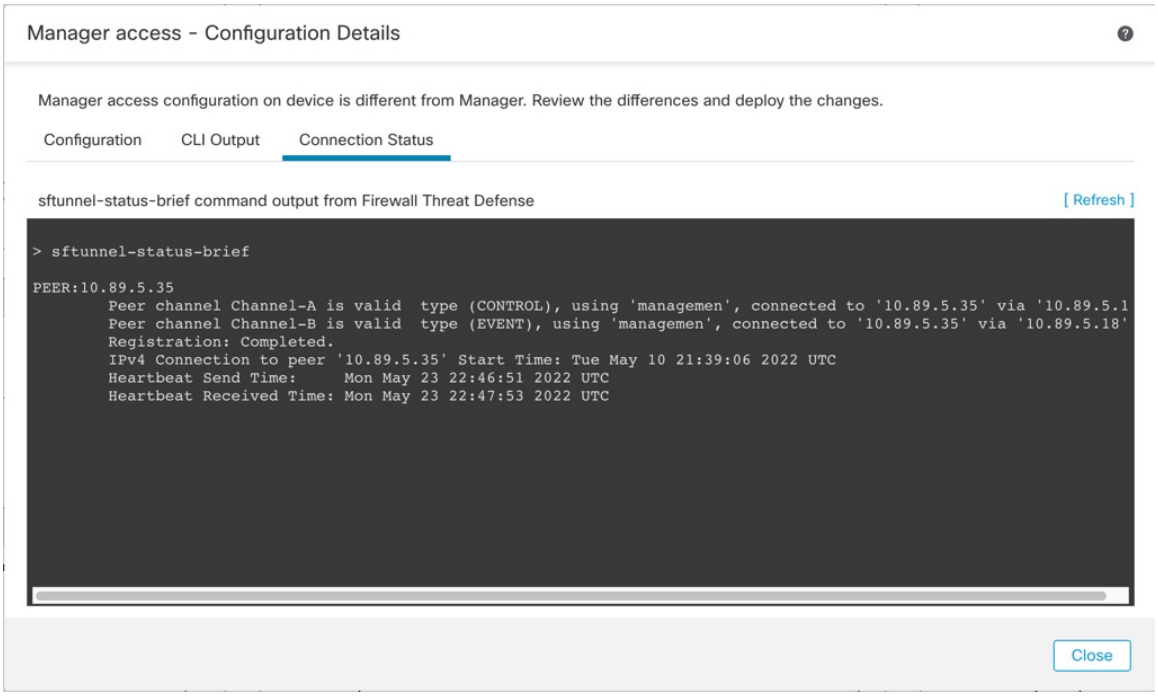




Connection status

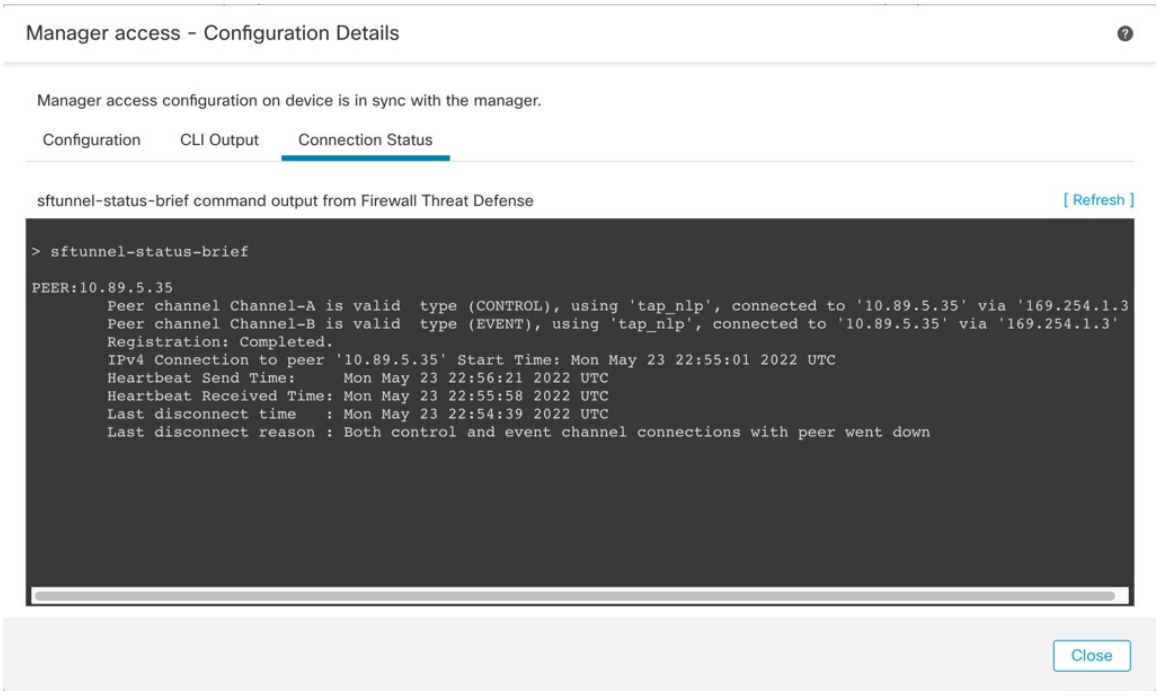
View the management connection status. In this example, the management connection still uses the Management "management0" interface.

Figure 334: Connection status



This status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 335: Connection status



This sample output shows a connection that is down. No peer channel "connected to" information or heartbeat information appears:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

This sample output shows a connection that is up, with peer channel and heartbeat information displayed:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Troubleshoot the management connection

This reference provides information to help diagnose and resolve management connection issues.

Manually Roll Back the configuration if the Firewall Management Center loses Connectivity

Use this task to restore management connectivity when a configuration change deployed from the Firewall Management Center affects network connectivity and you need to roll back to the last-deployed configuration.

If you use a data interface on the Firewall Threat Defense for manager access and deploy a configuration change from the Firewall Management Center that affects network connectivity, you can roll back the configuration on the Firewall Threat Defense to the last-deployed configuration to restore management connectivity. Afterward, update the configuration settings in Firewall Management Center to maintain network connectivity, and re-deploy. You can use the rollback feature even if you do not lose connectivity; it is not limited to this troubleshooting situation.

Alternatively, you can enable auto rollback of the configuration if you lose connectivity after a deployment; see Edit deployment settings, on page 800.

See these guidelines:

- Only the previous deployment is available locally on the Firewall Threat Defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability but not supported for clustering deployments.
- The rollback only affects configurations that you can set in the Firewall Management Center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the Firewall Threat Defense CLI. If you change data interface settings after the last Firewall Management Center deployment using the **configure network management-data-interface** command and then you use the rollback command, those settings are not be preserved. They roll back to the last-deployed Firewall Management Center settings.
- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Procedure

Step 1 At the Firewall Threat Defense CLI, roll back to the previous configuration.

configure policy rollback

After the rollback, the Firewall Threat Defense notifies the Firewall Management Center about the successful completion. The deployment screen In the Firewall Management Center displays a banner indicating that the configuration was rolled back.



Note If the rollback fails and the Firewall Management Center management is restored, refer to https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html for common deployment problems. In some cases, the rollback may fail after the Firewall Management Center management access is restored. Resolve any Firewall Management Center configuration issues and redeploy from the Firewall Management Center.

Example:

For the Firewall Threat Defense that uses a data interface for manager access:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Step 2 Check that the management connection was reestablished.

In Firewall Management Center, check the management connection status on the Connection Status page. Navigate to **Devices** > **Device Management** and then navigate to **Management** area under the **Devices** tab. Then in the **Manager Access - Configuration Details** screen, click **Connection Status**.

At the Firewall Threat Defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 792.

Troubleshoot Management Connectivity on a Data Interface

This topic helps you troubleshoot the loss of management connectivity when using a data interface for manager access instead of the dedicated Management interface.

If you use a data interface for manager access instead of the dedicated Management interface, exercise caution when changing the interface and network settings for the Firewall Threat Defense in the Firewall Management Center to avoid disrupting the connection. If you change the management interface type after adding the Firewall Threat Defense to the Firewall Management Center (switching between data and Management interfaces), misconfiguration of interfaces and network settings can result in loss of management connectivity.

Use the following methods to troubleshoot management connectivity:

- View management connection status: Check the status in the **Devices** > **Device Management** page or use **sftunnel-status-brief** at the CLI.
- View network information: Use **show network** to verify Management and manager access data interface settings.
- Check registration: Use **show managers** to confirm registration completion.
- Ping the manager: Use **ping** or **ping system** to test connectivity.
- Capture packets: Use **capture** on the `nlp_int_tap` interface to trace management traffic.
- Check interface status: Use **show interface detail** for the `nlp_int_tap` interface.

- Check routing and NAT: Use **show route** and **show nat** to verify routing and internal NAT rules.
- Check DDNS: Use **debug ddns** and related commands to verify DDNS updates.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went
down
```

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
Gateway                 : data-interfaces
...
```

Note At the Firewall Threat Defense CLI, check that the Firewall Management Center registration was completed. Note that this command will not show the *current* status of the management connection.

Refer to https://cisco.com/go/fmc-reg-error for Firewall Management Center log file information.

View inventory details

The **Inventory Details** section of the **Device** page shows chassis details such as the CPU and memory.

Figure 336: Inventory details



This section shows the chassis serial number. The firewall includes two serial numbers: the chassis serial number and the PCB (circuit board) serial number. The PCB serial number is shown in the System section. The Firewall Threat Defense Virtual does not have a chassis serial number.

Note For physical Firewall Threat Defense devices, the Memory field in **Inventory Details** shows only the data plane memory, not the total system memory.

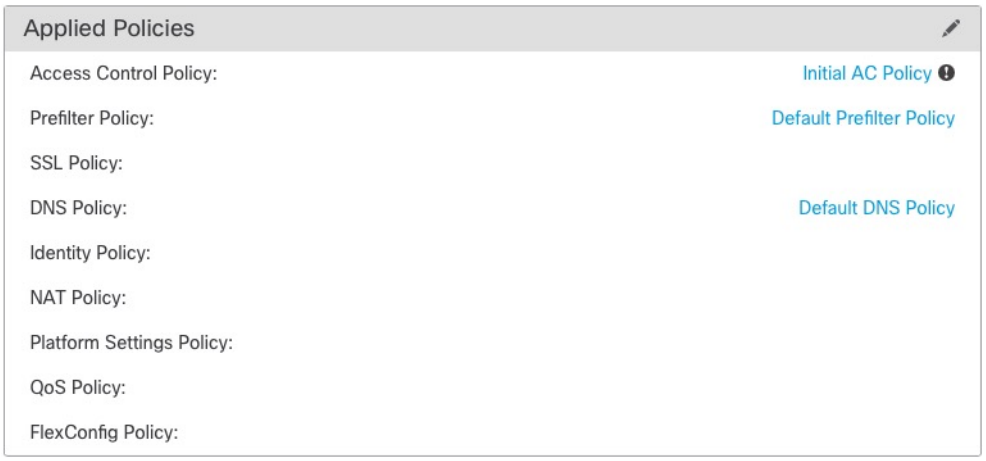
To update information, click **Refresh** ( ).

Edit applied policies

This task allows you to assign or modify policies for an individual firewall device, including access control policies and other security policies that govern device behavior.

The **Applied Policies** section of the **Device** page displays the following policies applied to your firewall:

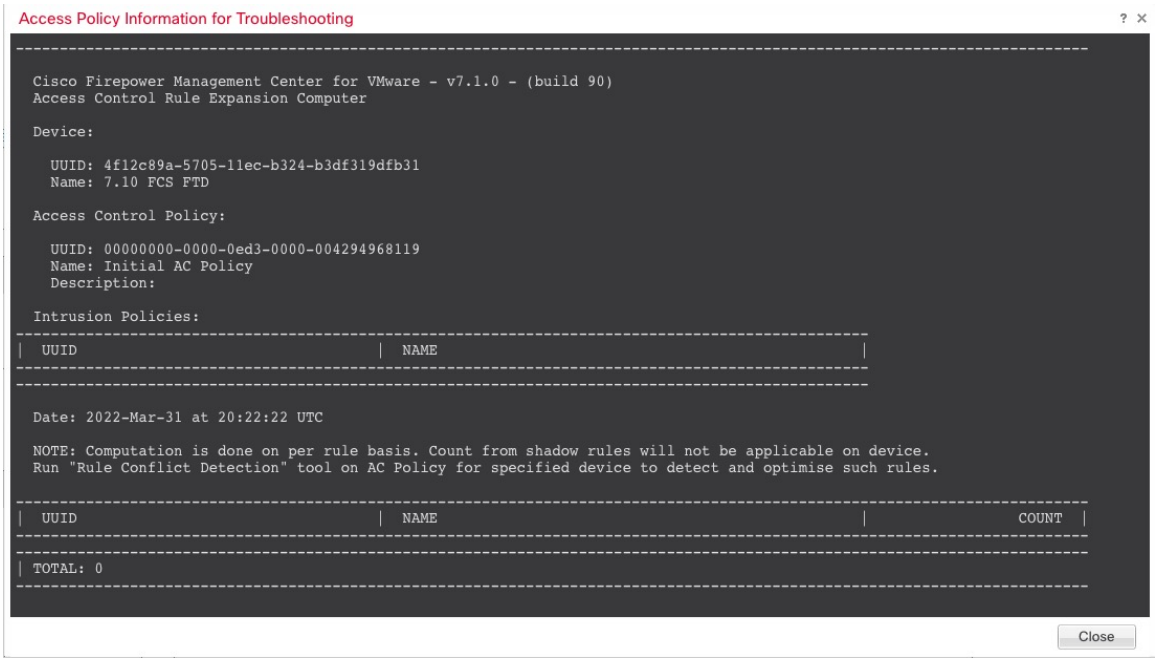
Figure 337: Applied policies



For policies with links, you can click the link to view the policy.

For the Access Control Policy, view the **Access Policy Information for Troubleshooting** dialog box by clicking the **Exclamation** ( ) icon. This dialog box shows how access rules are expanded into access control entries (ACEs).

Figure 338: Access policy information for troubleshooting



Procedure

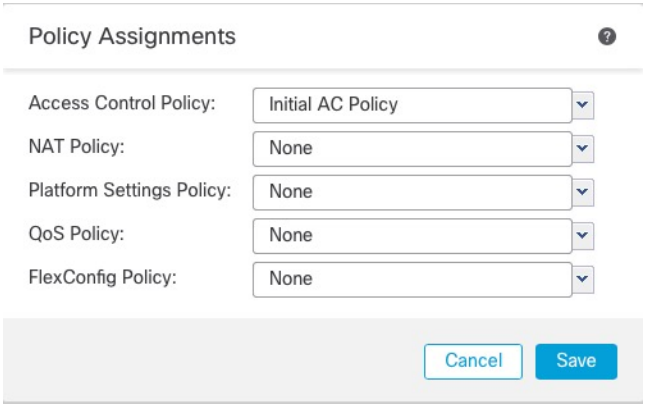
Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to assign policies, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 In the **Applied Policies** section, click **Edit** ( ).

Figure 339: Policy assignments



Step 5 For each policy type, choose a policy from the drop-down menu. Only existing policies are listed.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Edit advanced settings

The **Advanced Settings** section of the **Device** page displays a table of advanced configuration settings, as described below. You can edit any of these settings.

Table 50: Advanced settings table fields

Field	Description
Application Bypass	The state of Automatic Application Bypass on the device.
Bypass Threshold	The Automatic Application Bypass threshold, in milliseconds.
Object Group Search	The state of object group search on the device. While operating, the FTD device expands access control rules into multiple access control list entries based on the contents of any network or interface objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network or interface objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in Firepower Management Center. It impacts only how the device interprets and processes them while matching connections to access control rules. **Note** By default, the **Object Group Search** is enabled when you add threat defense for the first time in the management center.
Interface Object Optimization	The state of interface object optimization on the device. During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. If you select this option, also select the **Object Group Search** option to reduce memory usage on the device.

These topics explain how to edit the advanced device settings.

Note For information about the Transfer Packets setting, see Edit general settings, on page 743.

Configure automatic application bypass

Automatic Application Bypass (AAB) enables packet processing to continue when Snort detection becomes unavailable or exceeds processing time limits. This feature ensures network traffic flow continuity while providing diagnostic information for troubleshooting detection engine failures.

Automatic Application Bypass (AAB) allows packets to bypass detection if Snort is down or, for a Classic device, if a packet takes too long to process. AAB causes Snort to restart within ten minutes of the failure, and generates troubleshooting data that can be analyzed to investigate the cause of the Snort failure.

Caution AAB activation partially restarts the Snort process, which temporarily interrupts the inspection of a few packets.Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Note the following behavior:

Firewall Threat Defense Behavior: If Snort is down, then AAB is triggered after the specified timer duration. If Snort is up, then AAB is never triggered, even if packet processing exceeds the configured timer.

Classic Device Behavior: AAB limits the time allowed to process packets through an interface. You balance packet processing delays with your network's tolerance for packet latency.

The feature functions with any deployment; however, it is most valuable in inline deployments.

Typically, you use Rule Latency Thresholding in the intrusion policy to fast-path packets after the latency threshold value is exceeded. Rule Latency Thresholding does not shut down the engine or generate troubleshooting data.

If detection is bypassed, the device generates a health monitoring alert.

By default the AAB is disabled; to enable AAB follow these steps:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to edit advanced device settings, click **Edit** ( ).

Step 3 Click **Device**, then click **Edit** ( ) in the **Advanced Settings** section.

Step 4 Check **Automatic Application Bypass**.

Step 5 Enter a **Bypass Threshold** from 250 ms to 60,000 ms. The default setting is 3000 milliseconds (ms).

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure object group search

This task enables object group search on a Firewall Threat Defense device to reduce memory requirements for access control policies that include network or interface objects.

While operating, the Firewall Threat Defense device expands access control rules into multiple access control list entries based on the contents of any network or interface objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network or interface objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in Firewall Management Center. It impacts only how the device interprets and processes them while matching connections to access control rules.

Enabling object group search reduces memory requirements for access control policies that include network or interface objects. However, it is important to note that object group search might also decrease rule lookup performance and thus increase CPU utilization. You should balance the CPU impact against the reduced memory requirements for your specific access control policy. In most cases, enabling object group search provides a net operational improvement.

By default, the object group search is enabled for the threat defense devices that are added for the first time in the Firewall Management Center. In the case of upgraded devices, if the device is configured with disabled object group search, then you need to manually enable it. You can enable it on one device at a time; you cannot enable it globally. We recommend that you enable it on a device to which you deploy access rules that use network or interface objects.



Note

- If you enable object group search and then configure and operate the device for a while, be aware that subsequently disabling the feature might lead to undesirable results.
- When you disable object group search, your existing access control rules will be expanded in the device's running configuration. If the expansion requires more memory than is available on the device, your device can be left in an inconsistent state and you might see a performance impact.
- If your device is operating normally, do not disable the object group search after you have enabled it.

Before you begin

- Model support—Firewall Threat Defense
- We recommend that you also enable transactional commit on each device. From the device CLI, enter the **asp rule-engine transactional-commit access-group** command.
- Changing this setting can be disruptive to system operation while the device recompiles the ACLs. We recommend that you change this setting during a maintenance window.
- You can use FlexConfig to configure the **object-group-search threshold** command to enable a threshold to help prevent performance degradation. When operating with a threshold, for each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. Configure your rules to prevent an excessive number of matches.

Follow these steps to configure object group search:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the Firewall Threat Defense device where you want to configure the rule, click the **Edit** ( ).

Step 3 Click the **Device** tab, then click the **Edit** ( ) in the **Advanced Settings** section.

Step 4 Check **Object Group Search**.

Step 5 To have object group search work on interface objects in addition to network objects, check **Interface Object Optimization**.

If you do not select **Interface Object Optimization**, the system deploys separate rules for each source/interface pair, rather that use the security zones and interface groups used in the rules. This means the interface groups are not available for object group search processing.

Step 6 Click **Save**.

Configure interface object optimization

Interface object optimization enables the system to deploy a single rule per access control/prefilter rule instead of generating separate rules for each source/destination interface pair, simplifying device configuration and improving deployment performance.

During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source and destination interface pair. Enabling interface object optimization deploys a single rule per access control or prefilter rule. This approach simplifies device configuration and can improve deployment performance. If you select this option, also select the **Object Group Search** option to reduce evice memory usage.

Interface object optimization is disabled by default. You can enable it on one device at a time; you cannot enable it globally.

Note If you disable interface object optimization, the system deploys existing access control rules without using interface objects. This process might take longer. If object group search is enabled, its benefits do not apply to interface objects, and the device's running configuration might show expanded access control rules. If this expansion requires more memory than is available, the device can become inconsistent, which may affect performance

Before you begin

Model support—Firewall Threat Defense

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the Firewall Threat Defense device where you want to configure the rule, click the **Edit** ( ).

Step 3 Under the **Device** tab, click **Edit** ( ) in the **Advanced Settings** section.

Step 4 Check **Interface Object Optimization**.

Step 5 Click **Save**.

Edit deployment settings

Configure the deployment settings to enable auto rollback of the deployment if the management connection fails as a result of the deployment. For example, if you use data for management center access and then you misconfigure the data interface.

The **Deployment Settings** section of the **Device** page displays information for managing automatic rollback configuration. As an alternative, you can manually roll back the configuration using the **configure policy rollback** command (see Manually Roll Back the configuration if the Firewall Management Center loses Connectivity, on page 791).

Figure 340: Deployment settings



Table 51: Deployment settings

Field	Description
Auto Rollback Deployment if Connectivity Fails	Enabled or Disabled. You can enable auto rollback if the management connection fails as a result of the deployment; specifically if you use data for management center access, and then you misconfigure the data interface.
Connectivity Monitor Interval (in Minutes)	Shows the amount of time to wait before rolling back the configuration.

Consider the following guidelines:

- Only the previous deployment is available locally on the Firewall Threat Defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability but not supported for clustering deployments.
- The rollback only affects configurations that you can set in the Firewall Management Center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the Firewall Threat Defense CLI. If you change data interface settings after the last Firewall Management Center deployment using the **configure network management-data-interface** command and then you use the rollback command, those settings are not be preserved. They roll back to the last-deployed Firewall Management Center settings.

- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Procedure

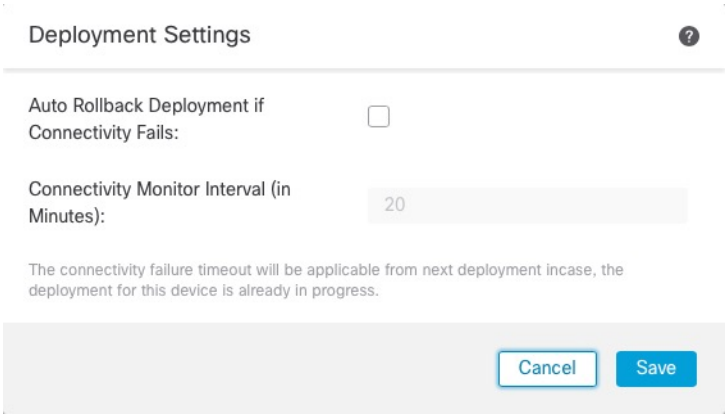
Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to assign policies, click **Edit** ( ).

Step 3 Click **Device**.

Step 4 In the **Deployment Settings** section, click **Edit** ( ).

Figure 341: Deployment settings



Step 5 Check **Auto Rollback Deployment if Connectivity Fails** to enable auto rollback.

Step 6 Set the **Connectivity Monitor Interval (in minutes)** to configure the wait time before rolling back the configuration. The default is 20 minutes.

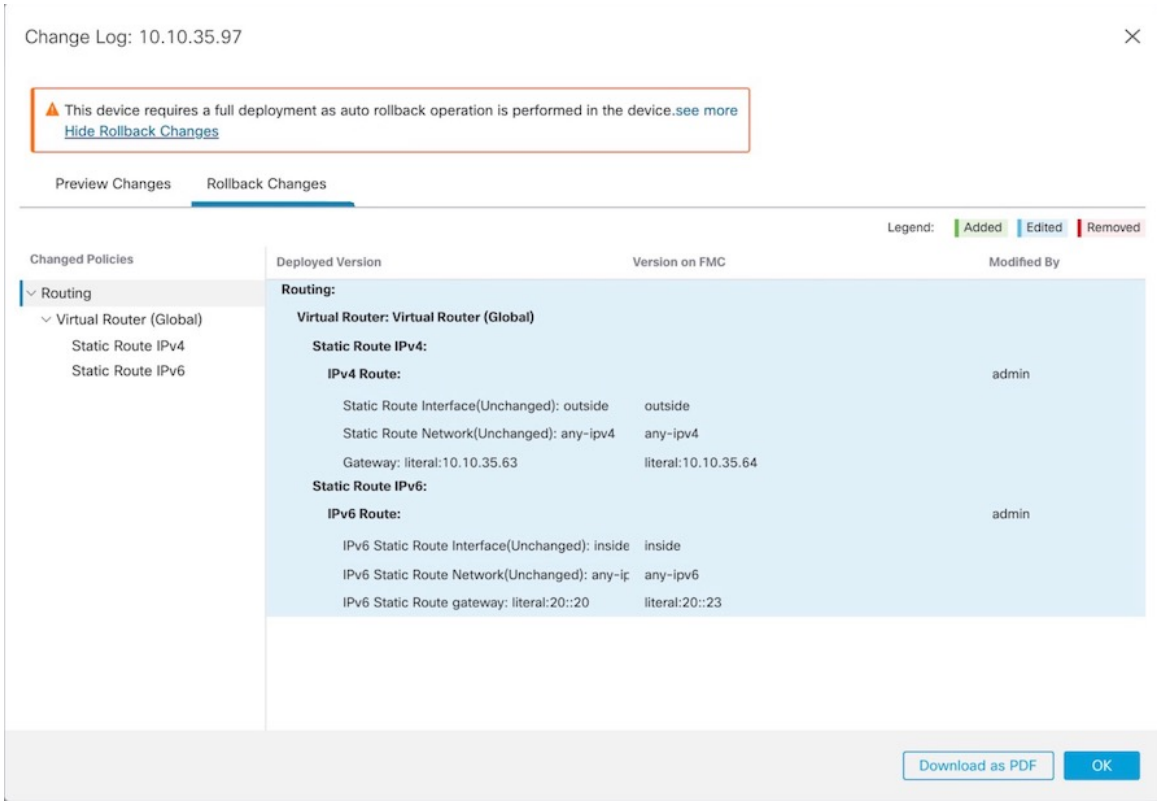
Step 7 If a rollback occurs, consider these next steps.

- If the auto rollback was successful, you see a success message instructing you to do a full deployment.
- Go to **Deploy** > **Advanced Deploy** page and click the **Preview** ( ) icon to view the parts of the configuration that were rolled back (see Deploy configuration changes, on page 135).

  To view the changes, click **Show Rollback Changes**.

  To hide the changes, click **Hide Rollback Changes**.

Figure 342: Rollback changes



- In the Deployment History Preview, you can view the rollback changes. See View deployment history, on page 141.

Step 8 Verify that the management connection was reestablished.

a. In Firewall Management Center, check the management connection status on the connection status page.

b. Navigate to **Devices** > **Device Management** and then in **Management** area under the **Devices** tab, click **Connection Status** to view the **Connection Status** page.

c. At the Firewall Threat Defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 792.

Edit cluster health monitor settings

This task allows you to modify cluster health monitor settings to control how cluster nodes monitor system health and automatically rejoin the cluster after failures.

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings for monitoring cluster node health. You can monitor any port-channel ID, any single physical interface ID, and the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link. It is always monitored.

When a topology change occurs (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature. Also, disable interface monitoring for any interfaces that are disabled. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Procedure

Step 1 Choose **Devices** > **Device Management**.

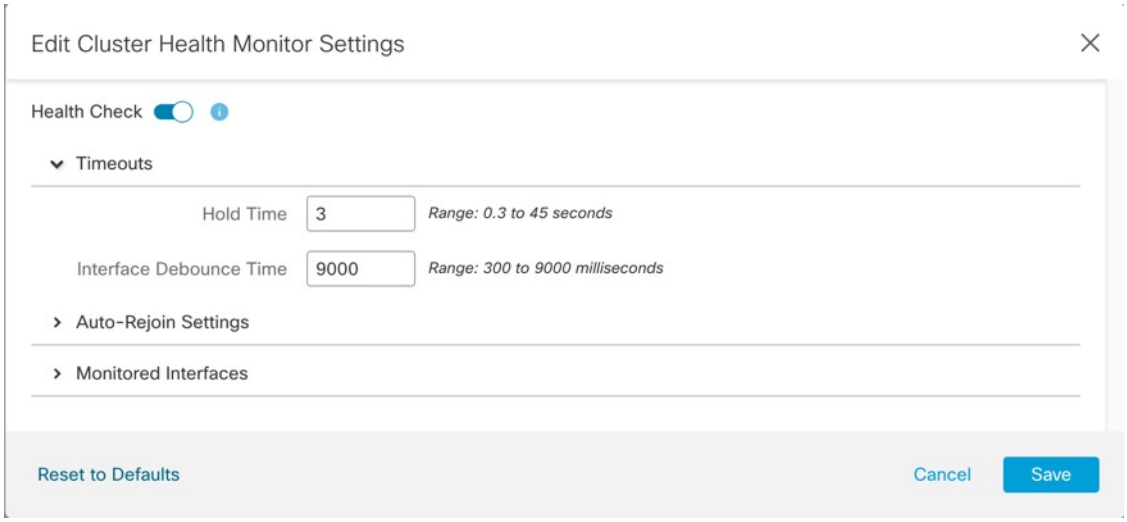
Step 2 Next to the cluster you want to modify, click **Edit** ( ).

Step 3 Click **Cluster**.

Step 4 In the **Cluster Health Monitor Settings** section, click **Edit** ( ).

Step 5 Disable the system health check by clicking the **Health Check** slider.

Figure 343: Disable the system health check



When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

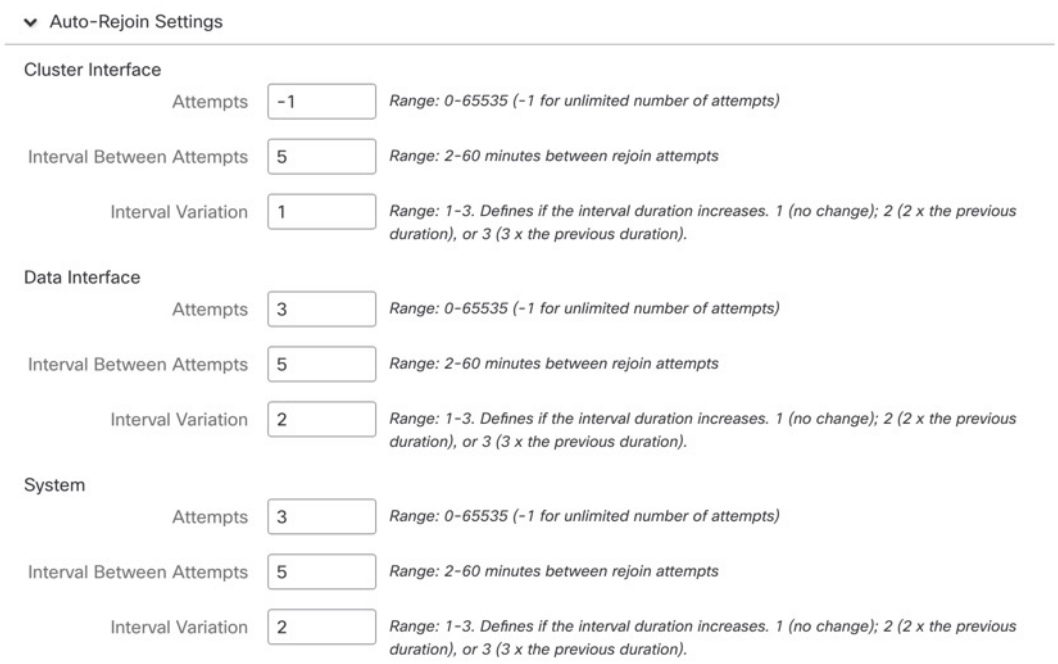
Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between 0.3 and 45 seconds. The default is 3 seconds.

- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the specified number of milliseconds before marking the interface as failed and removing the node from the cluster. If an EtherChannel transitions from a down state to an up state, such as after the switch reloads or enables an EtherChannel, a longer debounce time can prevent the interface from appearing failed on a cluster node if another cluster node bundles the ports more quickly.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 344: Configure Auto-Rejoin settings

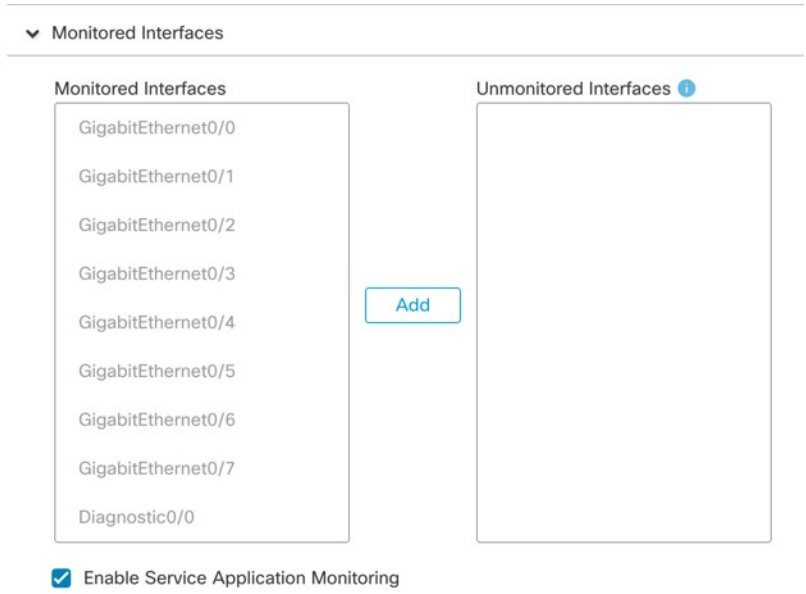


Set values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8 Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 345: Configure monitored interfaces



The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The time required to remove a member from the cluster depends on the type of interface and whether the node is established or is joining the cluster. By default, health check is enabled for all interfaces and the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC or VNet) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save**.

Deploy configuration changes; see Deploy configuration changes, on page 135.

Hot swap an SSD

Hot swapping SSDs allows you to maintain system operation while replacing faulty drives, removing drives, or adding drives to form a RAID configuration.

If you have two SSDs, they form a RAID when you boot up. You can perform the following tasks at the Firewall Threat Defense CLI while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.

- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.

  When you use only one SSD in Secure Firewall devices, the **Drive State** will show as **degraded**.



Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Procedure

Step 1 Remove one of the SSDs.

a) Remove the SSD from the RAID.

configure RAID remove-secure local-disk {**1** | **2**}

The **remove-secure** keyword removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD. If you only want to remove the SSD from the RAID and want to keep the data intact, you can use the **remove** keyword.

Example:

```
> configure raid remove-secure local-disk 2
```

b) Monitor the RAID status until the SSD no longer shows in the inventory.

show RAID

After the SSD is removed from the RAID, the **Operability** and **Drive State** will show as **degraded**. The second drive will no longer be listed as a member disk.

Example:

```
> show raid
Virtual Drive
ID:                     1
Size (MB):              858306
Operability:            operable
Presence:               equipped
Lifecycle:              available
Drive State:            optimal
Type:                   raid
Level:                  raid1
Max Disks:              2
Meta Version:           1.0
Array State:            active
Sync Action:            idle
Sync Completed:         unknown
Degraded:               0
Sync Speed:             none

RAID member Disk:
Device Name:            nvme0n1
Disk State:             in-sync
Disk Slot:              1
Read Errors:            0
```

```
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Physically remove the SSD from the chassis.

Step 2 Add an SSD.

a) Physically add the SSD to the empty slot.

b) Add the SSD to the RAID.

configure RAID add local-disk {**1** | **2**}

It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up. Use the **show RAID** command to show the status.

If you install an SSD that was previously used on another system, and is still locked, enter the following command:

configure RAID add local-disk {**1** | **2**} *psid*

The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.

Configure SNMP for FXOS

You can configure the Simple Network Management Protocol (SNMP) for the underlying FXOS operating system that controls low-level chassis functions. For SNMP for the Firewall Threat Defense, see Configure SNMP for a security device, on page 870.

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the chassis that maintains the data for the chassis and reports the data, as needed, to the SNMP manager. The chassis includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in the Firewall Management Center.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

The chassis supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMPv3 uses username and password for security.

Enable SNMP for FXOS

Enable SNMP and configure settings.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **SNMP**.

Step 3 Complete the following fields:

Name	Description
Admin State check box	Whether SNMP is enabled or disabled. Enable this service only if your system includes integration with an SNMP server.
Port field	The port on which the Firepower chassis communicates with the SNMP host. You cannot change the default port.

Name	Description
Community field	The default SNMPv1 or v2 community name or SNMP v3 username and password that the Firepower chassis includes on any trap messages it sends to the SNMP host. Enter a valid community string for SNMPv1 and SNMPv2: • Alphanumeric string between 1 and 32 characters and special characters ! (exclamation), - (hyphen), ~ (tilde), && (double ampersand), [ ] (square brackets), ^ (carat), ' (single quote), " (double quotes), and < > (angle brackets). • Do not use @ (at sign), \ (backslash), ? (question mark) or an empty space. • The string can also be in ASCII characters ranging 0x21 to 0x7E inclusive, excluding HTML interjection vectors, namely single quote ('), double quotes ("), and angle brackets (< >). Enter a valid username and password for SNMPv3: • Username can be alphanumeric string and can include @ (at sign), \ (backslash), . (period), _ (underscore), and - (hyphen). • The password restrictions are same as the community string restrictions. Note that if the **Community** field is already set, the text to the right of the empty field reads **Set: Yes**. If the **Community** field is not yet populated with a value, the text to the right of the empty field reads **Set: No**.
System Admin Name field	The contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 4 Click **Save**.

What to do next

Create SNMP traps and users.

Create an SNMP Trap for FXOS

Create traps for SNMP.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **SNMP**.

Step 3 In the **SNMP Traps Configuration** area, click **Add**.

Step 4 In the **SNMP Trap Configuration** dialog box, complete the following fields:

Name	Description
Host Name field	The hostname or IP address of the SNMP host to which the Firepower chassis should send the trap.
Community field	The SNMP v1 or v2 community name or the SNMP v3 username the Firepower chassis includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which the Firepower chassis communicates with the SNMP host for the trap. Enter an integer between 1 and 65535.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3**
Type field	If you select **V2** or **V3** for the version, the type of trap to send. This can be one of the following: • **Traps** • **Informs**
Privilege field	If you select **V3** for the version, the privilege associated with the trap. This can be one of the following: • **Auth**—Authentication but no encryption • **Noauth**—No authentication or encryption • **Priv**—Authentication and encryption

Step 5 Click **OK** to close the **SNMP Trap Configuration** dialog box.

Step 6 Click **Save**.

Create an SNMP user for FXOS

Create SNMP users.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **SNMP**.

Step 3 In the **SNMP Users Configuration** area, click **Add**.

Step 4 In the **SNMP User Configuration** dialog box, complete the following fields:

Name	Description
Username field	The username assigned to the SNMP user. Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).
Auth Algorithm Type field	The authorization type: **SHA**.
Use AES-128 checkbox	If checked, this user uses AES-128 encryption. **Note** SNMPv3 does not support DES. If you leave the AES-128 box unchecked, no privacy encryption will be done and any configured privacy password will have no effect.
Authentication Password field	The password for the user.
Confirm field	The password again for confirmation purposes.
Encryption Password field	The privacy password for the user.
Confirm field	The privacy password again for confirmation purposes.

Step 5 Click **OK** to close the **SNMP User Configuration** dialog box.

Step 6 Click **Save**.

Configure alarms for the ISA 3000

You can configure the alarm system on a Cisco ISA 3000 device to alert you when undesirable conditions occur.

About alarms

You can configure the ISA 3000 to issue alarms for a variety of conditions. If any conditions do not match the configured settings, the system triggers an alarm, which is reported by way of LEDs, syslog messages, SNMP traps, and through external devices connected to the alarm output interface. By default, triggered alarms issue syslog messages only.

You can configure the alarm system to monitor the following:

- Power supply.
- Primary and secondary temperature sensors.
- Alarm input interfaces.

The ISA 3000 has internal sensors plus two alarm input interfaces and one alarm output interface. You can connect external sensors, such as door sensors, to the alarm inputs. You can connect external alarm devices, such as buzzers or lights, to the alarm output interface.

The alarm output interface is a relay mechanism. Depending on the alarm conditions, the relay is either energized or de-energized. When it is energized, any device connected to the interface is activated. A de-energized relay results in the inactive state of any connected devices. The relay remains in an energized state as long as alarms are triggered.

For information about connecting external sensors and the alarm relay, Refer to Alarms for the Cisco ISA 3000 chapter in Cisco ASA Series General Operations CLI Configuration Guide. see Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide.

Alarm input interfaces

You can connect the alarm input interfaces (or contacts) to external sensors, such as one that detects if a door is open.

Each alarm input interface has a corresponding LED. These LEDs convey the alarm status of each alarm input. You can configure the trigger and severity for each alarm input. In addition to the LED, you can configure the contact to trigger the output relay (to activate an external alarm), to send syslog messages, and to send SNMP traps.

The following table explains the statuses of the LEDs in response to alarm conditions for the alarm inputs. It also explains the behavior for the output relay, syslog messages, and SNMP traps, if you enable these responses to the alarm input.

Alarm Status	LED	Output Relay	Syslog	SNMP Trap
Alarm not configured	Off	—	—	—
No alarms triggered	Solid green	—	—	—
Alarm activated	Minor alarm—solid red Major alarm—flashing red	Relay energized	Syslog generated	SNMP trap sent
Alarm end	Solid green	Relay de-energized	Syslog generated	—

Alarm output interface

You can connect an external alarm, such as a buzzer or light, to the alarm output interface.

The alarm output interface functions as a relay and also has a corresponding LED, which conveys the alarm status of an external sensor connected to the input interface, and internal sensors such as the dual power supply and temperature sensors. You configure which alarms should activate the output relay, if any.

The following table explains the statuses of the LEDs and output relay in response to alarm conditions. It also explains the behavior for syslog messages, and SNMP traps, if you enable these responses to the alarm.

Alarm Status	LED	Output Relay	Syslog	SNMP Trap
Alarm not configured	Off	—	—	—
No alarms triggered	Solid green	—	—	—
Alarm activated	Solid red	Relay energized	Syslog generated	SNMP trap sent
Alarm end	Solid green	Relay de-energized	Syslog generated	—

Syslog alarms

By default, the system sends syslog messages when any alarm is triggered. You can disable syslog messaging if you do not want the messages.

For syslog alarms to work, you must also enable diagnostic logging. Choose **Devices** > **Platform Settings**, add or edit a Threat Defense platform settings policy that is assigned to the device, and configure destinations and settings on the **Syslog** page. For example, you can configure a syslog server, console logging, or internal buffer logging.

Without enabling a destination for diagnostic logging, the alarm system has nowhere to send syslog messages.

SNMP Alarms

You can optionally configure the alarms to send SNMP traps to your SNMP server. For SNMP trap alarms to work, you must also configure SNMP settings.

Choose **Devices** > **Platform Settings**, add or edit a Threat Defense platform settings policy that is assigned to the device, and enable SNMP and configure settings on the **SNMP** page.

Defaults for alarms

The following table specifies the defaults for alarm input interfaces (contacts), redundant power supply, and temperature.

	Alarm	Trigger	Severity	SNMP Trap	Output Relay	Syslog Message
Alarm Contact 1	Enabled	Closed State	Minor	Disabled	Disabled	Enabled
Alarm Contact 2	Enabled	Closed State	Minor	Disabled	Disabled	Enabled

	Alarm	Trigger	Severity	SNMP Trap	Output Relay	Syslog Message
Redundant Power Supply (when enabled)	Enabled	—	—	Disabled	Disabled	Enabled
Temperature	Enabled for the primary temperature alarm (default values of 92°C and -40°C for the high and low thresholds respectively) Disabled for the secondary alarm.	—	—	Enabled for primary temperature alarm	Enabled for primary temperature alarm	Enabled for primary temperature alarm

Prerequisites for alarms

Model support

Firewall Threat Defense on the ISA 3000.

Configure alarms for the ISA 3000

You use FlexConfig to configure alarms for the ISA 3000. The following topics explain how to configure the different types of alarms.

Configure alarm input contacts

If you connect the alarm input contacts (interfaces) to external sensors, you can configure the contacts to issue alarms based on the input from the sensor. In fact, the contacts are enabled by default to send syslog messages if the contact is closed, that is, if the electrical current stops flowing through the contact. You need to configure the contact only if the defaults do not meet your requirements.

The alarm contacts are numbered 1 and 2, so you need to understand how you have wired the physical pins to configure the correct settings. You configure the contacts separately.

Procedure

Step 1 Create the FlexConfig object to configure the alarm input contacts.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Configure_Alarm_Contacts.

- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the alarm contacts. The following steps explain the commands.

c) Configure a description for the alarm contact.

alarm contact {**1** | **2**} **description** *string*

For example, to set the description of contact 1 to "Door Open," enter the following:

```
alarm contact 1 description Door Open
```

d) Configure the severity for the alarm contact.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

Instead of configuring one contact, you can specify **any** to change the severity for all contacts. The severity controls the behavior of the LED associated with the contact.

- **major**—The LED blinks red.
- **minor**—The LED is solid red. This is the default.
- **none**—The LED is off.

For example, to set the severity of contact 1 to Major, enter the following:

```
alarm contact 1 severity major
```

e) Configure the trigger for the alarm contact.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

Instead of configuring one contact, you can specify **any** to change the trigger for all contacts. The trigger determines the electrical condition that signals an alert.

- **open**—The normal condition for the contact is closed, that is, the electrical current is running through the contact. An alert is triggered if the contact becomes open, that is, the electrical current stops flowing.
- **closed**—The normal condition for the contact is open, that is, the electrical current does not run through the contact. An alert is triggered if the contact becomes closed, that is, the electrical current starts running through the contact. This is the default.

For example, you connect a door sensor to alarm input contact 1, and its normal state has no electrical current flowing through the alarm contact (it is open). If the door is opened, the contact is closed and electrical current flows through the alarm contact. You would set the alarm trigger to closed so that the alarm goes off when the electrical current starts flowing.

```
alarm contact 1 trigger closed
```

f) Configure the actions to take when the alarm contact is triggered.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message. This option is enabled by default.
- **notifies**—Send an SNMP trap.

For example, to enable all actions for the alarm input contact 1, enter the following:

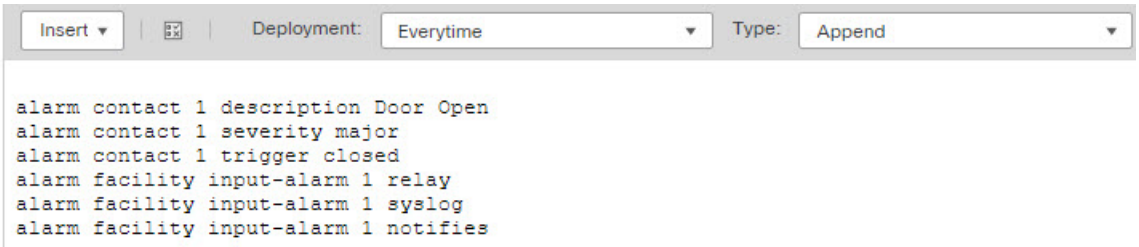
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

g) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

The object body should look similar to the following:



h) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

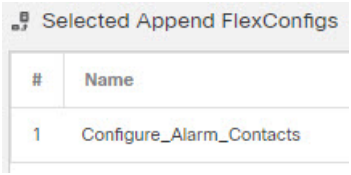
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the alarm contact FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the alarm contact commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration, on page 954.

Configure power supply alarms

The ISA 3000 has two power supplies. By default, the system operates in single-power mode. However, you can configure the system to operate in dual mode, where the second power supply automatically provides power if the primary power supply fails. When you enable dual-mode, the power supply alarm is automatically enabled to send syslog alerts, but you can disable the alert altogether, or also enable SNMP traps or the alarm hardware relay.

The following procedure explains how to enable dual mode, and how to configure the power supply alarms.

Procedure

Step 1 Create the FlexConfig object to configure the power supply alarm.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Power_Supply_Alarms.

- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the power supply alarms. The following steps explain the commands.

c) Enable dual power supply mode.

power-supply dual

For example:

```
power-supply dual
```

d) Configure the actions to take when the power supply alarm is triggered.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message. This option is enabled by default.
- **notifies**—Send an SNMP trap.
- **disable**—Disable the power supply alarm. Any other actions configured for the power supply alarm are inoperable.

For example, to enable all actions for the power supply alarm, enter the following:

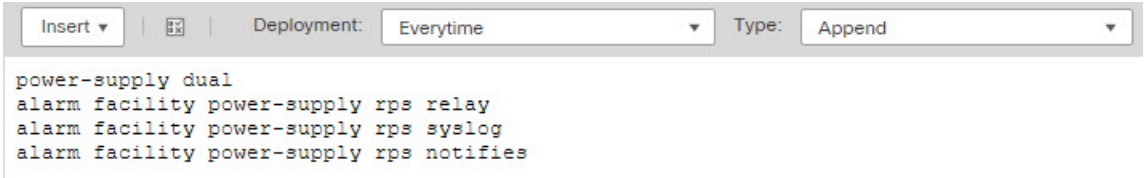
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

e) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

The object body should look similar to the following:



f) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

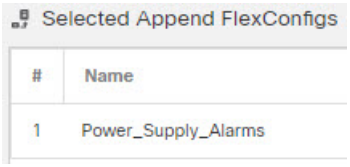
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the power supply alarm FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the power supply alarm commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration, on page 954.

Configure temperature alarms

You can configure alarms based on the temperature of the CPU card in the device.

You can set a primary and secondary temperature range. If the temperature drops below the low threshold, or exceeds the high threshold, the alarm is triggered.

The primary temperature alarm is enabled by default for all alarm actions: output relay, syslog, and SNMP. The default settings for the primary temperature range is -40°C to 92°C.

The secondary temperature alarm is disabled by default. You can set the secondary temperature within the range -35°C to 85°C.

Because the secondary temperature range is more restrictive than the primary range, if you set either the secondary low or high temperature, that setting disables the corresponding primary setting, even if you configure non-default values for the primary setting. You cannot enable two separate high and two separate low temperature alarms.

Thus, in practice, you should configure the primary only, or the secondary only, setting for high and low.

Procedure

Step 1 Create the FlexConfig object to configure the temperature alarms.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Configure_Temperature_Alarms.
- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the temperature alarms. The following steps explain the commands.

c) Configure the acceptable temperature range.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

The temperature is in Celsius. The allowed range for the primary alarm is -40 to 92, which is also the default range. The allowed range for the secondary alarm is -35 to 85. The low value must be lower than the high value.

For example, to set a more restrictive temperature range of -20 to 80, which falls within the allowed range for the secondary alarm, configure the secondary alarm as follows:

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

d) Configure the actions to take when the temperature alarm is triggered.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message.

- **notifies**—Send an SNMP trap.

For example, to enable all actions for the secondary temperature alarm, enter the following:

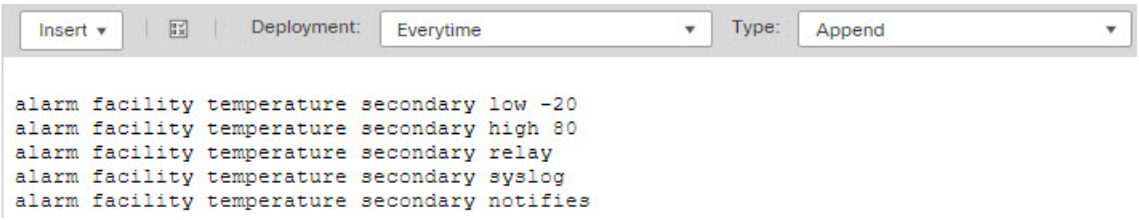
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

e) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

The object body should look similar to the following:



f) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

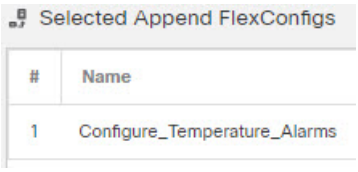
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the temperature alarms FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the

preview. Note that you will also see commands generated from other changes you have made to managed features. For the temperature alarms commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration, on page 954.

Turn off the external alarm

If you are using an external alarm that is attached to the alarm output, and the alarm is triggered, you can turn off the external alarm from the device CLI using the **clear facility-alarm output** command. This command de-energizes the output pin and also turns off the output LED.

Monitoring alarms

The following topics explain how to monitor and manage alarms.

Monitoring alarm status

You can use the following commands in the CLI to monitor alarms.

- **show alarm settings**

  Shows the current configuration for each possible alarm.

- **show environment alarm-contact**

  Shows information about the physical status of the input alarm contacts.

- **show facility-alarm relay**

  Shows information about the alarms that have triggered the output relay.

- **show facility-alarm status** [**info** | **major** | **minor**]

  Shows information on all alarms that have been triggered. You can limit the view by filtering on **major** or **minor** status. The **info** keyword provides the same output as using no keyword.

Monitoring syslog messages for alarms

Depending on the type of alarms you configure, you might see the following syslog messages.

Dual Power Supply Alarms

- %FTD-1-735005: Power Supply Unit Redundancy OK
- %FTD-1-735006: Power Supply Unit Redundancy Lost

Temperature Alarms

In these alarms, *Celsius* is replaced by the temperature detected on the device, in Celsius.

- %FTD-6-806001: Primary alarm CPU temperature is High *Celsius*
- %FTD-6-806002: Primary alarm for CPU high temperature is cleared
- %FTD-6-806003: Primary alarm CPU temperature is Low *Celsius*
- %FTD-6-806004: Primary alarm for CPU Low temperature is cleared
- %FTD-6-806005: Secondary alarm CPU temperature is High *Celsius*
- %FTD-6-806006: Secondary alarm for CPU high temperature is cleared
- %FTD-6-806007: Secondary alarm CPU temperature is Low *Celsius*
- %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared

Alarm Input Contact Alarms

In these alarms, *description* is the description for the contact that you configured.

- %FTD-6-806009: Alarm asserted for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806010: Alarm cleared for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806011: Alarm asserted for ALARM_IN_2 *alarm_2_description*
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*

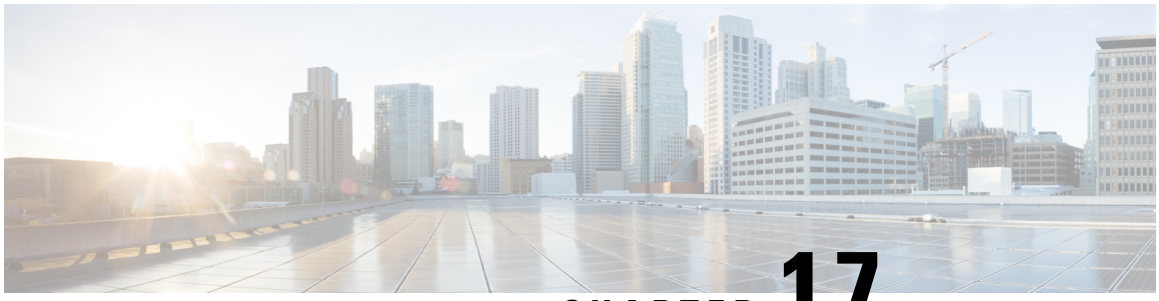
History for Device Settings

Provides a comprehensive reference of feature introductions, command modifications, and interface updates related to device settings and management.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**
Cluster health monitor settings.	7.3.0	Any	You can now edit cluster health monitor settings. New/modified screens: **Devices** > **Device Management** > **Cluster** > **Cluster Health Monitor Settings** **Note** If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.
Redundant manager access data interface.	7.3.0	7.3.0	When you use a data interface for manager access, you can configure a secondary data interface to take over management functions if the primary interface goes down. The device uses SLA monitoring to track the viability of the static routes and an ECMP zone that contains both interfaces so management traffic can use both interfaces. New/modified screens: • **Devices** > **Device Management** > **Device** > **Management** • **Devices** > **Device Management** > **Device** > **Interfaces** > **Manager Access**
Policy rollback support for high availability devices.	7.2.0	7.2.0	The **configure policy rollback** command is supported for high availability devices.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Auto rollback of a deployment that causes a loss of management connectivity.	7.2.0	7.2.0	You can now enable auto rollback of the configuration if a deployment causes the management connection between the management center and the threat defense to go down. Previously, you could only manually rollback a configuration using the **configure policy rollback** command. New/modified screens: • **Devices** > **Device Management** > **Device** > **Deployment Settings** • **Deploy** > **Advanced Deploy** > **Preview** • **Deploy** > **Deployment History** > **Preview**
Object group search is enabled by default for access control rules.	7.2.0	7.2.0	The **Object Group Search** setting is enabled by default for managed devices starting with Version 7.2.0. This option is in the **Advanced Settings** section when editing device settings on the Device Management page.
Import and export device configurations.	7.1.0	7.1.0	You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases: • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. New/modified screens: **Devices** > **Device Management** > **Device** > **General**
Update the FMC IP address on FTD.	6.7.0	6.7.0	If you change the FMC IP address, you can now use the FTD CLI to update the device. New/modified commands: **configure manager edit**
Alarms for the Cisco ISA 3000 series.	6.7	Any	Configuring alarms for the Cisco ISA 3000 series was validated using FlexConfig. You should be able to configure the alarms in older releases that support FlexConfig, except for the dual power supply alarms. Supported platforms: Secure Firewall Threat Defense



CHAPTER 17

DHCP and DDNS

The following topics explain DHCP and DDNS services and how to configure them on Threat Defense devices.

- About DHCP and DDNS services, on page 827
- Requirements and prerequisites for DHCP and DDNS, on page 829
- Guidelines for DHCP and DDNS services, on page 829
- Configure the DHCPv4 server, on page 831
- DHCPv6 stateless server configuration, on page 833
- Configure the DHCP relay agent, on page 837
- Configure Dynamic DNS, on page 838
- History for DHCP and DDNS, on page 844

About DHCP and DDNS services

This topic describes the DHCP server, DHCP relay agent, and DDNS update.

DHCPv4 servers

A DHCPv4 server provides network configuration parameters, such as IP addresses, to DHCP clients.

- delivers configuration parameters directly to DHCP clients attached to Firewall Threat Defense device interfaces, and
- uses UDP port communication for client-server messaging.

DHCPv4 server communication details

The DHCP communication uses specific network protocols and port assignments:

- IPv4 DHCP client: Uses broadcast rather than multicast address to reach the server and listens for messages on UDP port 68
- DHCP server: Listens for messages on UDP port 67

DHCP options

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters are carried in tagged items that are stored in the Options field of the DHCP message and the data are also called options. Vendor information is also stored in Options, and all of the vendor information extensions can be used as DHCP options.

Common DHCP options

Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers.
- DHCP option 66 gives the IP address or the hostname of a single TFTP server.
- DHCP option 3 sets the default route.

A single request might include both options 150 and 66. In this case, the DHCP server provides values for both options in the response if they are already configured on the Firewall Threat Defense.

You can use advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients. DHCP option 15 is used for the DNS domain suffix. You can also use the DHCP automatic configuration setting to obtain these values or define them manually. When you use more than one method to define this information, it is passed to DHCP clients in the following sequence:

1. Manually configured settings.
2. Advanced DHCP options settings.
3. DHCP automatic configuration settings.

Domain name configuration precedence

You can manually define the domain name that you want the DHCP clients to receive and then enable DHCP automatic configuration. Although DHCP automatic configuration discovers the domain together with the DNS and WINS servers, the manually defined domain name is passed to DHCP clients with the discovered DNS and WINS server names, because the domain name discovered by the DHCP automatic configuration process is superseded by the manually defined domain name.

DHCPv6 stateless server

A DHCPv6 stateless server is a DHCP IPv6 configuration that

- provides information such as DNS server or domain name when clients send Information Request (IR) packets,
- accepts IR packets but does not assign addresses to clients, and
- works in conjunction with StateLess Address Auto Configuration (SLAAC) and Prefix Delegation features.

DHCPv6 stateless server operation

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (Enable the IPv6 prefix delegation client, on page 703), you can configure the Firewall Threat Defense to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the Firewall Threat Defense by defining a DHCP IPv6 Pool and assigning it to the DHCPv6 server. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

DHCP relay agents

A DHCP relay agent forwards DHCP requests received on an interface to one or more DHCP servers.

DHCP relay agent operation

DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firewall Threat Defense device because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the Firewall Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server on another device.

Requirements and prerequisites for DHCP and DDNS

This reference provides the model support and user role requirements necessary for configuring DHCP and DDNS functionality.

Model support

Firewall Threat Defense

User roles

- Admin
- Access Admin
- Network Admin

Guidelines for DHCP and DDNS services

Context mode restrictions

DHCPv6 stateless server is not supported in multiple context mode.

Firewall mode restrictions

Consider these firewall mode limitations when configuring DHCP and DDNS services:

- DHCP Relay is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.
- DHCP Server is supported in transparent firewall mode on a bridge group member interface. In routed mode, the DHCP server is supported on the BVI interface, not the bridge group member interface. The BVI must have a name for the DHCP server to operate.
- DDNS is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.
- DHCPv6 stateless server is not supported in transparent firewall mode or in routed mode on the BVI or bridge group member interface.

Clustering limitations

DHCPv6 stateless server is not supported with clustering.

IPv6 support

DHCPv4 server guidelines

Follow these guidelines when configuring DHCPv4 server:

- The maximum available DHCP pool is 256 addresses.
- You can configure a DHCP server on any interface with a name and IP address, such as a physical interface, a subinterface, or a BVI in routed mode.
- Do not select an interface that uses DHCP or PPPoE to obtain it's address as a DHCP server interface.
- You can configure only one DHCP server on each interface. Each interface can have its own pool of addresses to use. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers, are configured globally and used by the DHCP server on all interfaces.
- You cannot configure an interface as a DHCP client if that interface also has DHCP server enabled; you must use a static IP address.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- The Firewall Threat Defense does not support DHCP clients behind DHCP relay servers; the client must be directly connected to the Firewall Threat Defense.
- The DHCP server does not support BOOTP requests.

DHCPv6 server guidelines

Consider these guidelines when configuring DHCPv6 server:

- The DHCPv6 Stateless server cannot be configured on an interface where the DHCPv6 address, Prefix Delegation client, or DHCPv6 relay is configured.

DHCP relay guidelines

Follow these guidelines when configuring DHCP relay:

- You can configure a maximum of 10 DHCPv4 relay servers per virtual router, global (VRF) and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers per virtual router. Interface-specific servers for IPv6 are not supported.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- Do not select an interface that uses DHCP or PPPoE to obtain it's address as a DHCP relay interface.
- DHCP relay services are not available in transparent firewall mode or in routed mode on the BVI or bridge group member interface. You can, however, allow DHCP traffic through using an access rule. To allow DHCP requests and replies through the Firewall Threat Defense, you need to configure two access rules, one that allows DCHP requests from the inside interface to the outside (UDP destination port 67), and one that allows the replies from the server in the other direction (UDP destination port 68).
- For IPv4, clients must be directly-connected to the Firewall Threat Defense and cannot send requests through another relay agent or a router. For IPv6, the Firewall Threat Defense supports packets from another relay server.
- The DHCP clients must be on different interfaces from the DHCP servers to which the Firewall Threat Defense relays requests.
- You cannot enable DHCP Relay on an interface in a traffic zone.

DDNS service configuration

The firewall's DDNS supports only DynDNS service. Hence, ensure that the DDNS is configured with update URL in the following syntax:

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

Configure the DHCPv4 server

Configure a DHCPv4 server to automatically assign IP addresses, DNS servers, domain names, and other network configuration parameters to DHCP clients on your network.

The DHCPv4 server provides dynamic IP address allocation and network configuration to clients. You can configure global server settings, interface-specific pools, and advanced DHCP options to customize the service for your network requirements.

Before you begin

Follow these steps to configure the DHCPv4 server:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **DHCP** > **DHCP Server**.

Step 3 Configure these DHCP server options:

- **Ping Timeout**—The amount of time in milliseconds that Firewall Threat Defense device waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.

  To avoid address conflicts, the Firewall Threat Defense device sends two ICMP ping packets to an address before assigning that address to a DHCP client.

- **Lease Length**—The amount of time in seconds that the client may use its allocated IP address before the lease expires. Valid values range from 300 to 1048575 seconds. The default value is 3600 seconds (1 hour).

- (Routed mode) **Auto-configuration**—Enables DHCP auto configuration on the Firewall Threat Defense device. Auto-configuration enables the DHCP server to provide the DHCP clients with the DNS server, domain name, and WINS server information obtained from a DHCP client running on the specified interface. Otherwise, you can disable auto configuration and add the values yourself in Step 4.

- (Routed mode) **Interface**—Specifies the interface to be used for auto configuration. For a device with virtual routing capability, this interface can only be a global virtual router interface.

Step 4 To override auto-configured settings, do the following:

- Enter the domain name of the interface. For example, your device may be in the Your_Company domain.
- From the drop-down list, choose the DNS servers (primary and secondary) configured for the interface. To add a new DNS server, see Create a network object, on page 2388.
- From the drop-down list, choose the WINS servers (primary and secondary) configured for the interface. To add a new WINS server, see Create a network object, on page 2388.

Step 5 Select **Server**, click **Add**, and configure the following options:

- **Interface**—Choose the interface from the drop-down list. In transparent mode, specify a named bridge group member interface. In routed mode, specify a named routed interface or a named BVI; do not specify the bridge group member interface. Note that each bridge group member interface for the BVI must also be named for the DHCP server to operate.
- **Address Pool**—The range of IP addresses from lowest to highest that is used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enables the DHCP server on the selected interface.

Step 6 Click **OK** to save the DHCP server configuration.

Step 7 (Optional) Select **Advanced**, click **Add**, and specify the type of information you want the option to return to the DHCP client:

- **Option Code**—The Firewall Threat Defense device supports the DHCP options listed in RFC 2132, RFC 2562, and RFC 5510 to send information. All DHCP options (1 through 255) are supported except for 1, 12, 50–54, 58–59, 61, 67, and 82. See DHCPv4 servers, on page 827for more information on DHCP option codes.

Note The Firewall Threat Defense device does not verify that the option type and value that you provide match the expected type and value for the option code, as defined in RFC 2132. For more information about option codes and their associated types and expected values, see RFC 2132.

- **Type**—DHCP option type. Available options include **IP**, **ASCII**, and **HEX**. If you chose IP, you must add IP addresses in the IP Address fields. If you chose ASCII, you must add the ASCII value in the ASCII field. If you chose HEX, you must add the HEX value in the HEX field.
- **IP Address 1** and **IP Address 2**—The IP address(es) to be returned with this option code. To add a new IP address, see Create a network object, on page 2388.
- **ASCII**—The ASCII value that is returned to the DHCP client. The string cannot include spaces.
- **HEX**—The HEX value that is returned to the DHCP client. The string must have an even number of digits and no spaces. You do not need to use a 0x prefix.

Step 8 Click **OK** to save the option code configuration.

Step 9 Click **Save** on the DHCP page to save your changes.

a) To view DHCP bindings, use **show dhcpd binding**.

Example:

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

DHCPv6 stateless server configuration

The DHCPv6 stateless server configuration enables the Firewall Threat Defense to provide network information such as the DNS server or domain name to clients using StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature. When clients send Information Request (IR) packets to Firewall Threat Defense, they receive this information.

Create a DHCP IPv6 pool

Create a DHCP IPv6 pool to define the parameters sent in IR messages from the DHCPv6 server to clients.

Create a DHCP IPv6 pool for use with the DHCPv6 server. The DHCPv6 server provides information such as the DNS server or domain name when they clients send Information Request (IR) packets to the Firewall Threat Defense. The DHCP IPv6 pool defines the parameters to sent in IR messages.

This feature is only supported in routed mode. This feature is not supported in clustering or High Availability.

Procedure

Step 1 Choose **Objects** > **Object Management** > **DHCP IPv6 Pool**.

Step 2 Click **Add** ( ).

Step 3 Configure the **DNS Server** and **Domain Name**.

You can either manually define the values and click **Add**, or you can check **Import** to use one or more parameters that the Firewall Threat Defense obtained from the DHCPv6 server on the Prefix Delegation client interface. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and also use **Import**.

Figure 346: Manually define values

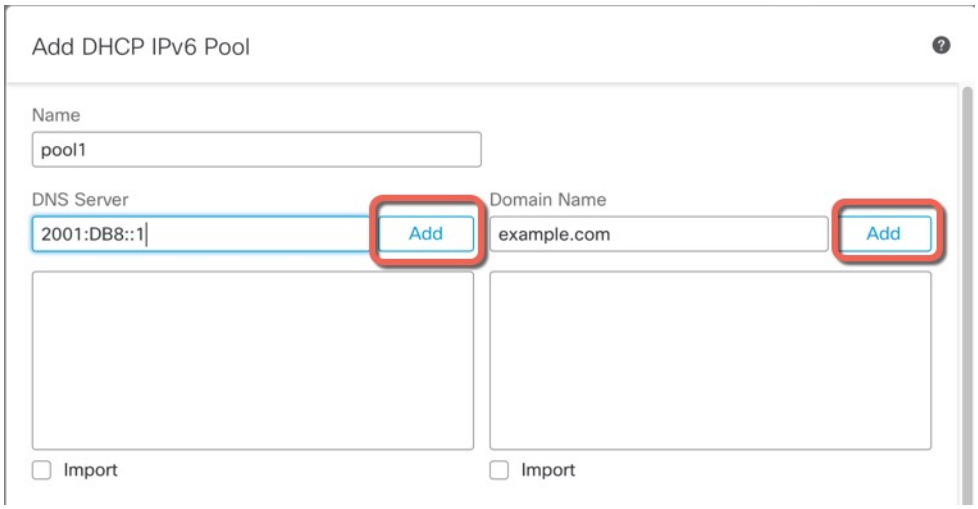
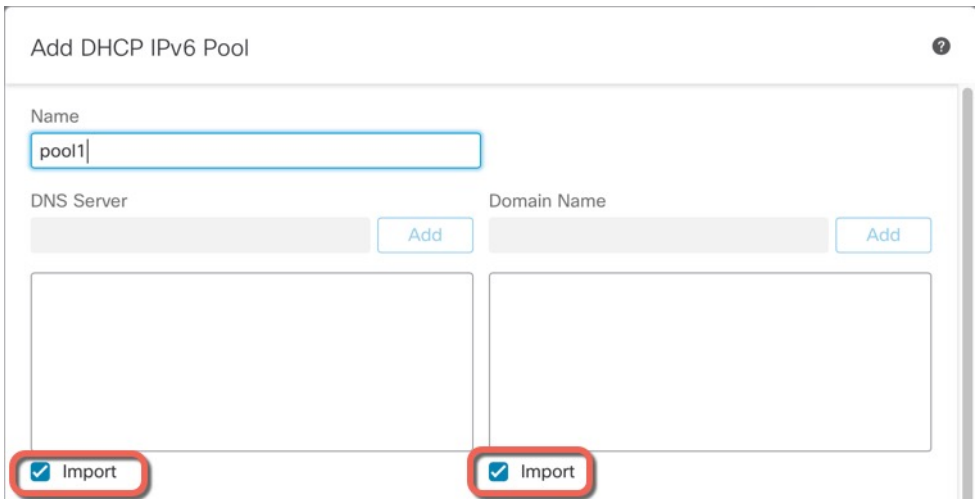


Figure 347: Import values



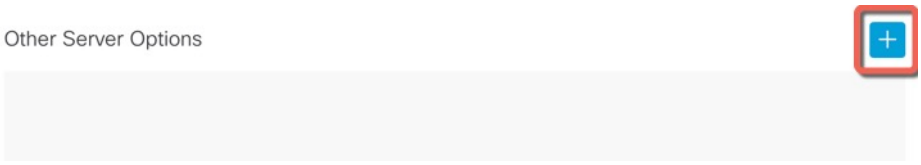
Step 4 Define **Other Server Options**.

You can define the domain name and IP address for these servers:

- NIS
- NISP
- SIP
- SNTP

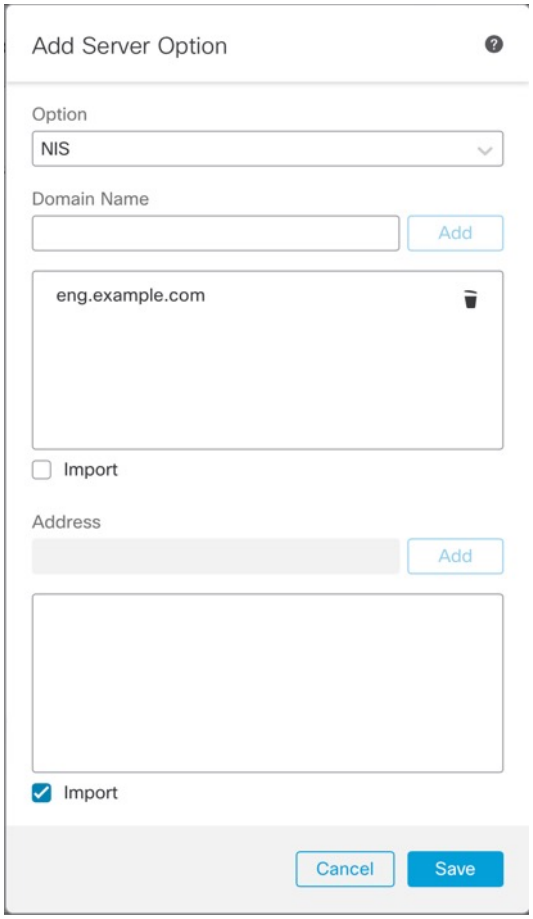
a) Click **Add** ( ).

Figure 348: Other server options



b) Choose the server type under **Option**, and either manually define the **Domain Name** and **Address**, or check **Import**.

Figure 349: Define server domain name and address



Import uses one or more parameters that the Firewall Threat Defense obtained from the DHCPv6 server on the Prefix Delegation client interface. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and also use **Import**.

c) Click **Save**.

d) Repeat for each server type.

Step 5 Click **Save**.

Step 6 Use this pool with the DHCPv6 server. See Enable the DHCPv6 stateless server, on page 836.

Enable the DHCPv6 stateless server

This task enables the DHCPv6 stateless server to provide configuration information to IPv6 autoconfiguration clients without assigning addresses. The server responds to Information Request (IR) packets with DNS server addresses, domain names, and other configuration parameters.

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (Enable the IPv6 prefix delegation client, on page 703), you can configure the Firewall Threat Defense to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the Firewall Threat Defense. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

This feature is only supported in routed mode. This feature is not supported in clustering or High Availability.

Before you begin

Add a DHCP IPv6 Pool object. See Create a DHCP IPv6 pool, on page 833. This object defines the server parameters included in the IR messages.

Follow these steps to enable the DHCPv6 stateless server:

Procedure

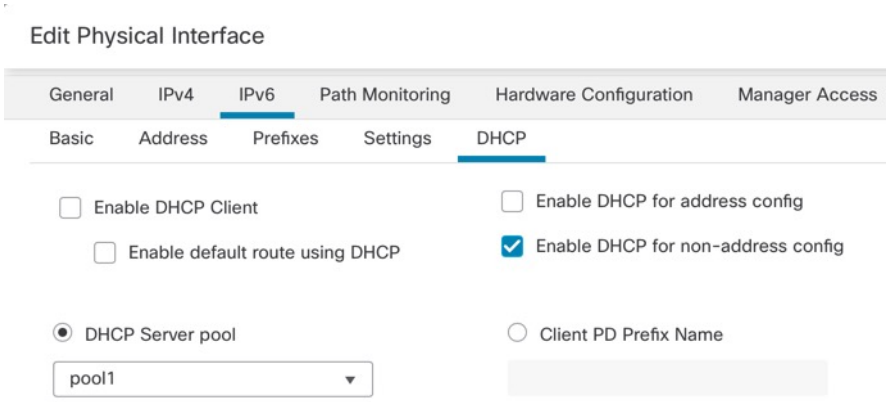
Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Click the **IPv6** page, and then click **DHCP**.

Step 4 Click **DHCP Server Pool**, and choose the object you created earlier.

Figure 350: Enable the DHCPv6 server



Step 5 Check **Enable DHCP for non-address config** to inform SLAAC clients about the DHCPv6 server.

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure the DHCP relay agent

Configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers when DHCP clients and servers are on different network segments.

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firewall Threat Defense device because it does not forward broadcast traffic.

You can remedy this situation by configuring the interface of the Firewall Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

Note DHCP Relay is not supported in transparent firewall mode.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **DHCP** > **DHCP Relay**.

Step 3 In the **IPv4 Relay Timeout** and **IPv6 Relay Timeout** fields, enter the amount of time in seconds that the Firewall Threat Defense device waits to time out the DHCP relay agent. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.

The timeout is for address negotiation through the local DHCP Relay agent.

Step 4 (Optional) Check **Trust All Information** to set all client interfaces as trusted.

You can configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the Firewall Threat Defense DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the Firewall Threat Defense will drop that packet by default. You can preserve Option 82 and forward the packet by identifying an interface as a trusted interface.

Step 5 On **DHCP Relay Agent**, click **Add**, and configure these options:

- **Interface**—The interface connected to the DHCP clients.
- **Enable IPv4 Relay**—Enables IPv4 DHCP Relay for this interface.
- **Set Route**—(For IPv4) Changes the default gateway address in the DHCP message from the server to that of the Firewall Threat Defense device interface that is closest to the DHCP client, which relayed the original DHCP request. This action allows the client to set its default route to point to the Firewall Threat Defense device even if the DHCP server specifies a different router. If there is no default router option in the packet, the Firewall Threat Defense device adds one containing the interface address.
- **Enable IPv6 Relay**—Enables IPv6 DHCP Relay for this interface.

Step 6 Click **OK** to save the DHCP relay agent changes.

Step 7 On **DHCP Servers**, click **Add**, and configure these options:

Add the IPv4 and IPv6 server addresses as separate entries, even if they belong to the same server.

- **Server**—The IP address of the DHCP server. Chose an IP address from the drop-down list. To add a new one, see Create a network object, on page 2388
- **Interface**—The interface to which the specified DHCP server is attached. The DHCP Relay agent and the DHCP server cannot be configured on the same interface.

Step 8 Click **OK** to save the DHCP server changes.

Step 9 Click **Save** on the DHCP page to save your changes.

Configure Dynamic DNS

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS) provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates these RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The Firewall Threat Defense supports these DDNS update methods:

- Standard DDNS—The standard DDNS update method is defined by RFC 2136.

  With this method, the Firewall Threat Defense and the DHCP server use DNS requests to update the DNS RRs. The Firewall Threat Defense or DHCP server sends a DNS request to its local DNS server for information about the hostname and, based on the response, determines the main DNS server that owns the RRs. The Firewall Threat Defense or DHCP server then sends an update request directly to the main DNS server. See these typical scenarios.

  - The Firewall Threat Defense updates the A RR, and the DHCP server updates the PTR RR.

    Typically, the Firewall Threat Defense "owns" the A RR, while the DHCP server "owns" the PTR RR, so both entities need to request updates separately. When the IP address or hostname changes, the Firewall Threat Defense sends a DHCP request (including the FQDN option) to the DHCP server to inform it that it needs to request a PTR RR update.

  - The DHCP server updates both the A and PTR RR.

    Use this scenario if the Firewall Threat Defense does not have the authority to update the A RR. When the IP address or hostname changes, the Firewall Threat Defense sends a DHCP request (including the FQDN option) to the DHCP server to inform it that it needs to request an A and PTR RR update.

  You can configure different ownership depending on your security needs and the requirements of the main DNS server. For example, for a static address, the Firewall Threat Defense should own the updates for both records.

- Web—The Web update method uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

  With this method when the IP address or hostname changes, the Firewall Threat Defense sends an HTTP request directly to a DNS provider with which you have an account.

Note For devices that were registered using zero-touch provisioning from the outside interface, DDNS is enabled automatically using the "fmcOnly" method, which is similar to the Web method. This method is only available for zero-touch provisioning devices. You can edit some options for this method using this screen, or delete the method and configure a different one. For more information about zero-touch provisioning, see Add a Device Using the Serial Number (Zero-Touch Provisioning) , on page 36.

The **DDNS** page also supports setting DHCP server settings relating to DDNS.

Note DDNS is not supported on the BVI or bridge group member interfaces.

Before you begin

- Configure a DNS server group on **Objects** > **Object Management** > **DNS Server Group**, and then enable the group for the interface on **Devices** > **Platform Settings**, create or edit a Threat Defense policy and click **DNS**. See Configure DNS server settings, on page 852.
- Configure the device hostname. You can configure the hostname when you perform the Firewall Threat Defense initial setup, or by using the **configure network hostname** command. If you do not specify the hostname per interface, then the device hostname is used.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **DHCP** > **DDNS**.

Step 3 Standard DDNS method: Configure a DDNS update method to enable DNS requests from the Firewall Threat Defense.

You do not need to configure a DDNS update method if the DHCP server will perform all requests.

a) On **DDNS Update Methods**, click **Add**.
b) Set the **Method Name**.
c) Click **DDNS**.
d) (Optional) Configure the **Update Interval** between DNS requests. By default when all values are set to 0, update requests are sent whenever the IP address or hostname changes. To send requests regularly, set the **Days** (0-364), **Hours**, **Minutes**, and **Seconds**.
e) Set the **Update Records** you want the Firewall Threat Defense to update.

This setting only affects the records you want to update directly from the Firewall Threat Defense; to determine the records you want the DHCP server to update, configure the DHCP client settings per interface or globally. See, Step 5, on page 841.

- **Not Defined**—Disables DNS updates from the Firewall Threat Defense.
- **Both A and PTR Records**—Sets the Firewall Threat Defense to update both A and PTR RRs. Use this option for static or PPPoE IP addressing.
- **A Records**—Sets the Firewall Threat Defense to update the A RR only. Use this option if you want the DHCP server to update the PTR RR.

f) Click **OK**.
g) Assign this method to the interface in Step 5, on page 841.

Step 4 Web method: Configure a DDNS update method to enable HTTP update requests from the Firewall Threat Defense.

a) On **DDNS Update Methods**, click **Add**.
b) Set the **Method Name**.
c) Click **Web**.
d) Set the **Web Update Type** to update IPv4, IPv6, or both types of addresses.
e) Set the **Web URL**. Specify the update URL. Check with your DNS provider for the URL required.

Use this syntax:

https://*username***:***password***@***provider-domain/path***?hostname=<h>&myip=<a>**

Example:

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) (Optional) Configure the **Update Interval** between DNS requests. By default when all values are set to 0, update requests are sent whenever the IP address or hostname changes. To send requests regularly, set the **Days** (0-364), **Hours**, **Minutes**, and **Seconds**.

g) Click **OK**.

h) Assign this method to the interface in Step 5, on page 841.

i) The web type method for DDNS also requires you to identify the DDNS server root CA to validate the DDNS server certificate for the HTTPS connection. See, Step 9, on page 842.

Step 5 Configure interface settings for DDNS, including setting the update method, DHCP client settings, and the hostname for this interface.

a) On **DDNS Interface Settings**, click **Add**.

b) Choose the **Interface** from the drop-down list.

c) Choose the **Method Name** that you created on the **DDNS Update Methods** page.

(Standard DDNS method) You do not need to assign a method if you want the DHCP server to perform all updates.

d) Set the **Host Name** for this interface.

If you do not set the hostname, the device hostname is used. If you do not specify an FQDN, then the default domain from the DNS server group is appended (for static or PPPoE IP addressing) or the domain name from the DHCP server is appended (for DHCP IP addressing).

e) Standard DDNS method: Configure the **DHCP Client requests DHCP server to update requests** to determine which records you want the DHCP server to update.

The Firewall Threat Defense sends DHCP client requests to the DHCP server. Note that the DHCP server must also be configured to support DDNS. The server can be configured to honor the client requests, or it can override the client (in which case, it will reply to the client so the client does not also try to perform updates that the server is performing).

For static or PPPoE IP addressing, these settings are ignored.

Note You can also set these values globally for all interfaces on the **DDNS** page. The per-interface settings take precedence over the global settings.

- **Not Selected**—Disables DDNS requests to the DHCP server. Even if the client does not request DDNS updates, the DHCP server can be configured to send updates anyway.
- **No Update**—Requests the DHCP server not to perform updates. This setting works in conjunction with a DDNS update method with **Both A and PTR Records** enabled.
- **Only PTR**—Requests that the DHCP server perform the PTR RR update. This setting works in conjunction with a DDNS update method with **A Records** enabled. Use this setting to enable DHCP option 81.
- **Both A and PTR Records**—Requests that the DHCP server perform both A and PTR RR updates. This setting does not require a DDNS update method to be associated with the interface.

f) Click **OK**.

Note The **Dynamic DNS Update** settings relate to DHCP server settings when you enable a DHCP server on the Firewall Threat Defense. See, Step 6, on page 842 for more information.

Step 6 If you enable the DHCP server on an Firewall Threat Defense, you can configure DHCP server settings for DDNS.

To enable the DHCP server, see Configure the DHCPv4 server, on page 831). You can configure the server behavior when DHCP clients use the standard DDNS update method. If the server performs any updates, then if the client lease expires (and is not renewed), the server will request that the DNS server remove the RRs for which it was responsible.

a) You can configure server settings globally or per interface. For global settings, refer to the main **DDNS** page. For per-interface settings, refer to the **DDNS Interface Settings** page. Interface settings take precedence over global settings.

b) Configure which DNS RRs you want the DHCP server to update under **Dynamic DNS Update**.

- **Not Selected**—DDNS updates are disabled, even if the client requests them.
- **Only PTR**—Enables DDNS updates. If you enable the **Override DHCP Client Requests** setting, then the server will only update the PTR RR. Otherwise, the server will update RRs that the client requests. If the client does not send an update request with the FQDN option, the server will request an update for both A and PTR RRs using the hostname discovered in DHCP option 12.
- **Both A and PTR Records**—Enables DDNS updates. If you enable the **Override DHCP Client Requests** setting, then the server will update both the A and PTR RRs. Otherwise, the server will update RRs that the client requests. If the client does not send an update request with the FQDN option, the server will request an update for both A and PTR RRs using the hostname discovered in DHCP option 12.

c) To override the update actions requested by the DHCP client, check **Override DHCP Client Requests**.

The server will reply to the client that the request was overridden, so the client does not also try to perform updates that the server is performing.

Step 7 (Optional) Configure general DHCP client settings. These settings are not related to DDNS, but are related to how the DHCP client behaves.

a) On the **DDNS** page, check **Enable DHCP Client Broadcast** to request that the DHCP server broadcast the DHCP reply (DHCP option 1).

b) To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally generated string, on **DDNS** > **DHCP Client ID Interface**, choose the interface from the **Available Interfaces** list, and then click **Add** to move it to the **Selected Interfaces** list.

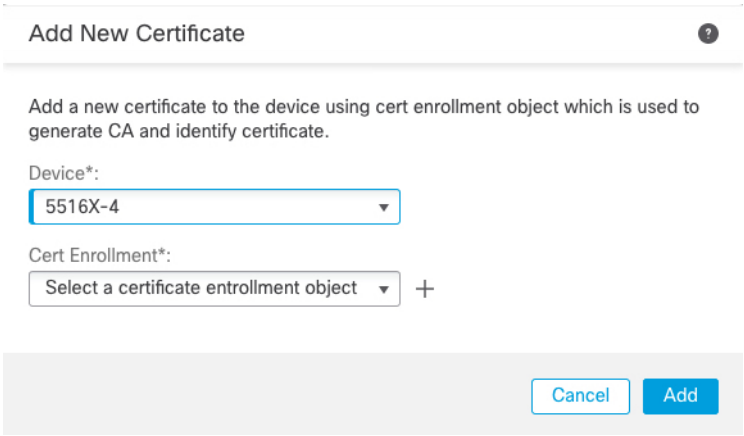
Some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. This setting does not directly relate to DDNS, but is a general DHCP client setting.

Step 8 Click **Save** on the Device page to save your changes.

Step 9 The Web method for DDNS also requires you to identify the DDNS server root CA to validate the DDNS server certificate for the HTTPS connection.

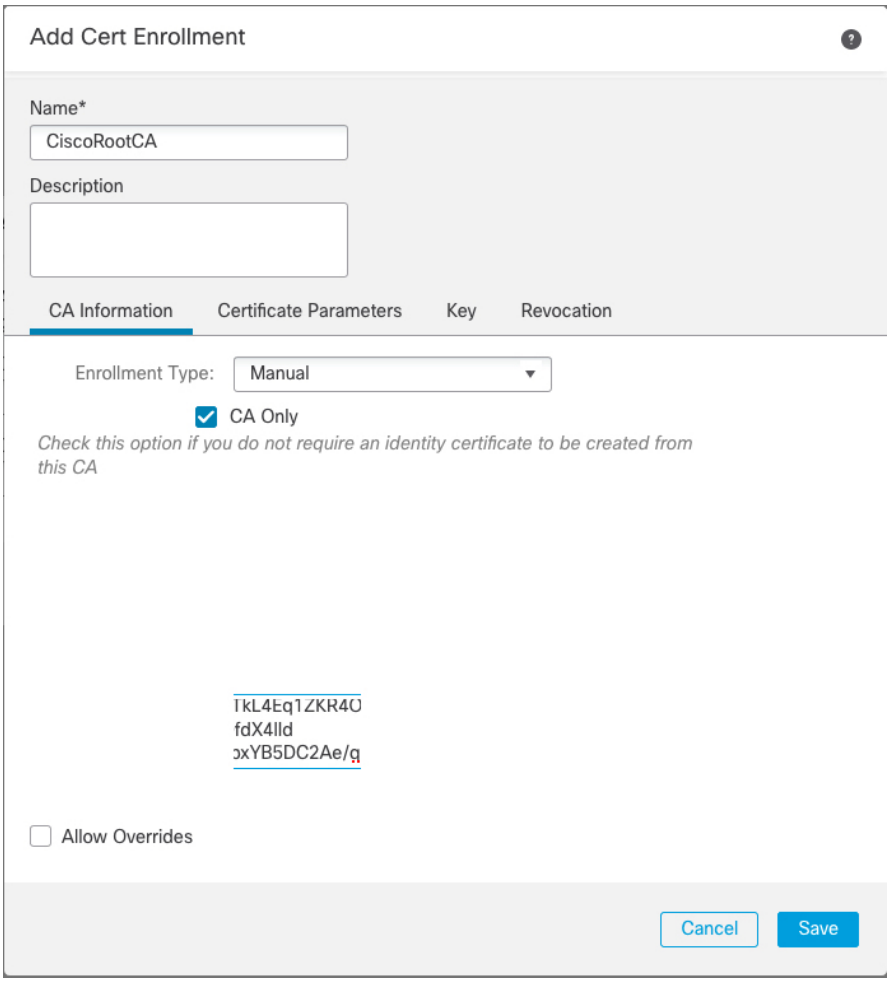
This example shows how to add a DDNS server's CA as a trustpoint.

a) Obtain the DDNS server CA certificate. This procedure shows a manual import using PEM format, but you can also use PKCS12.
b) In Firewall Management Center, choose **Devices** > **Certificates**, and click **Add**.
c) Select a **Device**, and click **Add** (+).



The **Add Cert Enrollment** dialog box appears.

d) Enter these fields, and click **Save**:



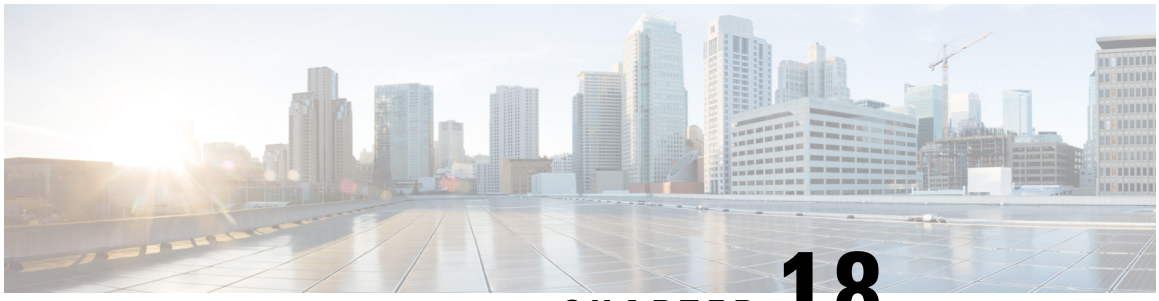
- Enter a **Name**.
- Choose **Enrollment Type** > **Manual**.
- Click **CA Only**.
- Paste in the CA text from step 9.a, on page 843.

e) Click **Save**.

History for DHCP and DDNS

This reference provides the release history for DHCP and DDNS features, including version requirements and implementation details for Secure Firewall Management Center and Threat Defense devices.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Configure DHCP relay trusted interfaces from the Firewall Management Center web interface.	7.2.6/7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the Firewall Management Center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the Firewall Threat Defense DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then Firewall Threat Defense will drop that packet by default. You can preserve Option 82 and forward the packet by identifying an interface as a trusted interface. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **DHCP** > **DHCP Relay**
DHCPv6 Stateless Server	7.3.0	7.3.0	The Firewall Threat Defense now supports a light DHCPv6 stateless server when using the DHCPv6 Prefix Delegation client. The Firewall Threat Defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to the Firewall Threat Defense. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. New/modified screens: • **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **DHCP** • **Objects** > **Object Management** > **DHCP IPv6 Pool** New/modified commands: **show ipv6 DHCP**



CHAPTER 18

Platform Settings

Platform settings for Firewall Threat Defense devices configure a range of unrelated features whose values you might want to share among several devices. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

Note In 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices (7.3 and earlier, and some upgraded 7.4 devices).

- Platform settings policies, on page 848
- List requirements and prerequisites for platform settings policies, on page 848
- Manage platform settings policies, on page 849
- Chassis platform settings, on page 850
- Configure ARP inspection, on page 850
- Configure a banner, on page 852
- Configure DNS server settings, on page 852
- Configure external authentication, on page 855
- Configure fragment settings, on page 861
- Configure HTTP access, on page 862
- Configure ICMP access, on page 864
- Configure NetFlow, on page 865
- Configure Secure Shell (SSH) access, on page 867
- Configure an SMTP server, on page 869
- Configure SNMP for a security device, on page 870
- Configure SSL settings, on page 884
- Syslog, on page 888
- Configure timeouts, on page 906
- Synchronize time on FTD devices, on page 908
- Configure a time zone for a device, on page 911
- Configure UCAPL/CC compliance, on page 911
- Configure a performance profile, on page 912
- History for platform settings, on page 913

Platform settings policies

A platform settings policy is a shared set of features or parameters that

- define aspects of managed devices that are likely to be similar to other managed devices in a deployment, such as time settings and external authentication,
- enable configuration of multiple managed devices at once, providing consistency and streamlining management efforts, and
- apply changes to all managed devices where the policy is used, requiring creation and application of shared policies even for device-specific settings.

Platform settings policy reference information

Use platform settings policies to enforce security requirements, such as displaying a login banner message, and to manage device configurations efficiently.

- You can set a “No Unauthorized Use” message for appliance logins using platform settings policies.
- You can apply multiple platform settings policies to a single Firewall Management Center to accommodate different mail relay hosts or access lists.

Platform settings policy example

Your organization’s security policies may require that appliances display a “No Unauthorized Use” message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

Multiple platform settings policy example

If your organization has different mail relay hosts that you use for different circumstances or if you want to test different access lists, you can create several platform settings policies and switch between them, rather than editing a single policy.

List requirements and prerequisites for platform settings policies

You must meet specific requirements and prerequisites before you configure Platform Settings Policies, including supported domains and user roles.

Supported domains

Any

User roles

Admin

Access Admin

Network Admin

Manage platform settings policies

Manage platform settings policies to control device configurations and assignments within your environment. This task allows you to create, edit, or delete policies for supported device types.

Use the **Platform Settings** page (**Devices** > **Platform Settings**) to manage platform settings policies. This page indicates the type of device for each policy. The **Status** column shows the device targets for the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 For an existing policy, you can **Copy** ( ), **Edit** ( ), or **Delete** ( ) the policy.

Caution You should not delete a policy that is the last-deployed policy on any of its target devices, even if it is out of date. Before you delete the policy completely, it is a good practice to deploy a different policy to those targets.

Step 3 To create a new policy, click **New Policy**.

a) Choose a device type from the drop-down list:

- **Firepower Settings** to create a shared policy for managed Classic devices.
- **Threat Defense Settings** to create a shared policy for managed Firewall Threat Defense devices.
- **Chassis Platform Settings** to create a shared policy for managed Firewall Threat Defense chassis in multi-instance mode.

b) Enter a **Name** for the new policy and optionally, a **Description**.

c) Optionally, choose the **Available Devices** or **Available Chassis** where you want to apply the policy and click **Add** (or drag and drop) to add the selected devices. You can enter a search string in the **Search** field to narrow the list of devices.

d) Click **Save**.

- When you have selected a device and if the device is already applied with a policy, the **Confirm PFS Overwrite** dialog appears. To override the applied policy, click **OK**. The selected device is applied with the new policy.
- The system creates the policy and opens it for editing.

Step 4 To change the target devices for a policy, click **Edit** ( ) next to the platform settings policy that you want to edit.

a) Click **Policy Assignment**.

b) To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** or **Available Chassis** list and click **Add**. You can also drag and drop.

c) To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** or **Selected Chassis** list.
d) Click **OK**.

After completing these steps, platform settings policies are created, edited, or deleted as needed, and device assignments are updated accordingly.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Chassis platform settings

Chassis platform settings reference information

Chassis platform settings apply to multiple-instance mode chassis. For more information, see Chassis platform settings, on page 199.

Configure ARP inspection

Configure ARP inspection to ensure that only valid ARP packets are accepted on your network, reducing the risk of ARP spoofing and related attacks.

- Apply ARP inspection policies to specific interfaces and security zones.
- Add static ARP entries for enhanced control and security.

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

When you enable ARP inspection, the Firewall Threat Defense device compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the Firewall Threat Defense device drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the Firewall Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated Management interface never floods packets even if this parameter is set to flood.

Use this task when you need to protect your network from ARP spoofing by validating ARP packets and controlling ARP traffic on selected interfaces and zones.

Use ARP inspection in environments where network security is a priority and static ARP entries are needed.

Before you begin

Make sure you have device access and permission to edit platform settings and ARP inspection policies.

- Have the list of interfaces and security zones where ARP inspection will be applied.
- Prepare the static ARP entries that you intend to add.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **ARP Inspection**.

Step 3 Add entries to the ARP inspection table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the desired options.

- **Inspect Enabled**—To perform ARP inspection on the selected interfaces and zones.
- **Flood Enabled**—Floods ARP requests that do not match static ARP entries to all interfaces except the originating or dedicated management interface. By default, this behavior is enabled.

  If you choose not to flood ARP requests, only requests that match static ARP entries are allowed.
- **Security Zones**—Add the zones that contain the interfaces on which to perform the selected actions. The zones must be switched zones. For interfaces not in a zone, type the interface name into the field in the Selected Security Zone list and click **Add**. The device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Add static ARP entries according to Add a static ARP entry, on page 718.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ARP inspection is enabled on the selected interfaces and security zones. Only valid ARP packets are accepted, and static ARP entries are enforced. The policy is active after deployment.

Configure a banner

Configure a banner to display messages to users when they connect to the device command line interface (CLI). This helps inform users and discourage unauthorized access.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Banner**.

Step 3 Configure the banner.

These are some tips and requirements for banners.

- Use only ASCII characters. You can add line returns (press Enter), but do not use tabs.
- You can dynamically add the hostname or domain name of the device by including the variables **$(hostname)** or **$(domain)**.
- Although banners do not have an absolute length restriction, Telnet or SSH sessions close if the system does not have enough memory to process banner messages.
- Create a banner that discourages unauthorized access by avoiding the words "welcome" or "please," which may seem inviting. The sample banner provided discourages intruders.

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The system displays the banner to users when they connect to the device CLI. The changes occur after you deploy the policy.

Configure DNS server settings

Configure DNS server settings to enable hostname resolution for data traffic on managed devices. This task allows you to set up DNS server groups, trusted DNS services, and interface-specific DNS lookups. These configurations support features such as access control rules, NAT, and application detection.

- Set up DNS server groups for resolving FQDNs used in data traffic.
- Configure trusted DNS servers for DNS snooping and application-based PBR.
- Enable DNS lookups on specific interfaces to control routing behavior.

The Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. Data DNS settings apply to services that use FQDNs, such as access control rules and remote access VPN. Special management traffic uses separate DNS settings configured via CLI commands. This procedure applies only to data DNS servers. For management DNS settings, see the CLI **configure network dns servers** and **configure network dns searchdomains** commands.

Managed devices use routing lookups to determine the correct interface for DNS server communications. The system selects the routing table based on the interfaces enabled for DNS. Multiple DNS server groups can be configured to resolve different DNS domains, allowing internal and external DNS resolution as needed.

Trusted DNS servers

You can configure trusted DNS services for DNS snooping. DNS snooping is used to map the application domains to IPs in order to detect the application on the first packet. You can also include the already configured servers in DNS group, DHCP pool, DHCP relay and DHCP client as trusted DNS servers.

For application-based PBR, configure trusted DNS servers. Ensure DNS traffic passes through Firewall Threat Defense in clear text format (because encrypted DNS is not supported) for domain resolution and application detection.

Before you begin

- Ensure you have created one or more DNS server groups. For more information, see Create a DNS server group object, on page 2366.
- Ensure you have created interface objects to connect to the DNS servers.
- Ensure that the managed device has appropriate static or dynamic routes to access the DNS servers.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Threat Defense policy.

Step 2 Click **DNS**, and then click the **DNS Settings** tab.

Step 3 Check **Enable DNS name resolution by device**.

Step 4 Configure the DNS server groups.

a) Do any of these actions in the DNS server group list:

- To add a group, click **Add**. You cannot add another group once there are 30 filter domains configured within the existing list of server groups.
- To edit a group, click **Edit** ( ) next to the group.
- To remove a group, click **Delete** ( ) next to the group. When you remove a group, you do not delete the DNS server group object. You remove it only from this list.

b) When adding or editing a group, configure the following settings, then click **OK**:

- **Select DNS Group**—Select an existing DNS server group object, or click **+** to create a new one.
- **Make as default**—Select this option to make this group the default group. Any DNS resolution request that does not match the filters for other groups will be resolved using the servers in this group.

- **Filter Domains**—For non-default groups only, enter a list of domain names separated by commas, such as example.com,example.net. Do not include spaces.

  The group is used only for DNS resolutions for these domains. You can enter up to 30 separate domains across all groups in this DNS platform settings policy. Each domain name can contain up to 127 characters.

  Note that these filter domains are not related to the default domain name for the group. The filter list can be different from the default domain.

Step 5 (Optional) Enter the **Expiry Entry Timer** and **Poll Timer** values in minutes.

These options apply to FQDNs specified in network objects only and do not apply to FQDNs used in other features.

- **Expire Entry Timer** specifies the minimum time-to-live (TTL) value for the DNS entry, in minutes. If the expiration timer is longer than the entry's TTL, the TTL is increased to the expire entry time value. If the TTL is longer than the expiration timer, the expire entry time value is ignored. Upon expiration, the entry is removed from the DNS lookup table. When you remove an entry, the device recompiles the table. Frequent removals can increase the processing load on the device. Some DNS entries can have very short TTL (as short as three seconds); use this setting to virtually extend the TTL. The default is 1 minute. The range is 1 to 65535 minutes.

  For systems running 7.0 or earlier, the expiration time is actually added to the TTL; it does not specify a minimum value.

- **Poll Timer** specifies the time limit after which the device queries the DNS server to resolve the FQDN defined in a network object. An FQDN is resolved periodically when either the poll timer has expired or the TTL of the resolved IP entry has expired, whichever occurs first.

Step 6 Enable DNS lookups on all interfaces or on specific interfaces. These choices also affect which routing tables are used.

Enabling DNS lookups on an interface is not the same as specifying the source interface for lookups. The Firewall Threat Defense always uses a route lookup to determine the source interface. Management-only interfaces other than the dedicated Management interface cannot be used.

- No interfaces selected—This setting enables DNS lookups on all interfaces. The Firewall Threat Defense checks the data routing table only.
- Specific interfaces selected but not the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on the specified interfaces. The Firewall Threat Defense checks the data routing table only.
- Specific interfaces selected plus the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on the specified interfaces and the Management interface. The Firewall Threat Defense checks the data routing table, and if no route is found, falls back to the management-only routing table.
- Only the **Enable DNS Lookup via diagnostic/management interface also** option—Enables DNS lookups on Management. The Firewall Threat Defense checks only the management-only routing table.

Step 7 Configure Trusted DNS servers.

a) Click the **Trusted DNS Servers** tab.

b) By default, the existing DNS servers that are configured in DHCP pool, DHCP relay, DHCP client, or DNS server group are included as trusted DNS servers. If you want to exclude any of them, uncheck the appropriate check boxes.
c) To add trusted DNS servers, under **Specify DNS Servers**, click **Edit**.
d) In the **Select DNS Servers** dialog box, either choose a host object as the trusted DNS server or directly specify the IP address of the trusted DNS server:

1. To choose existing host objects, under **Available Host Objects**, select the required host object and click **Add** to include it to **Selected DNS Servers**. For information on adding the host objects, see Create a network object, on page 2388.
2. To directly provide the IP address (IPv4 or IPv6) of the trusted DNS server, enter the address in the given text field, and click **Add** to include it to **Selected DNS Servers**.
3. Click **Save**. The added DNS servers are displayed in the **Trusted DNS Servers** page.

Note You can configure a maximum of 12 DNS servers per policy.

To search for a DNS server that was added, using either the host name or the IP address, use the search field under **Specify DNS Servers**.

Step 8 Click **Save**.

What to do next

To use FQDN objects for access control rules, create an FQDN network object which can then be assigned to an access control rule. For instructions, see Create a network object, on page 2388.

Configure external authentication

Configure external authentication to allow management users to be authenticated using an LDAP or RADIUS server, as specified in an external authentication object. Centralized user management also enhances security for device access.

Note You must have administrator privileges to perform this task.

When you enable external authentication for management users, the Firewall Threat Defense verifies the user credentials with an LDAP or RADIUS server as specified in an external authentication object.

Sharing External Authentication Objects

External authentication objects can be used by the Firewall Management Center and Firewall Threat Defense devices. You can share the same object between the Firewall Management Center and devices. Alternatively, create separate objects. Note that the Firewall Threat Defense supports defining users on the RADIUS server, while the Firewall Management Center requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the Firewall Threat Defense, but if you want to

define users on the RADIUS server, you must create separate objects for the Firewall Threat Defense and the Firewall Management Center.

Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1 to 30 seconds for LDAP, and 1 to 300 seconds for RADIUS). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Assigning External Authentication Objects to Devices

For the Firewall Management Center, enable the external authentication objects directly on **System** (⚙) > **Users** > **External Authentication**; this setting only affects Firewall Management Center usage, and it does not need to be enabled for managed device usage. For Firewall Threat Defense devices, you must enable the external authentication object in the platform settings that you deploy to the devices, and you can only activate one external authentication object per policy. An LDAP object with CAC authentication enabled cannot also be used for CLI access. Be sure that both the Firewall Threat Defense and the Firewall Management Center can reach the LDAP server, even if you are not sharing the object. The Firewall Management Center is essential to retrieving the user list and downloading it to the device.

Firewall Device Supported Fields

Only a subset of fields in the external authentication object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for the Firewall Management Center, those fields will be used. This procedure only covers the supported fields for the Firewall Threat Defense. For other fields, see *Configure External Authentication for the Firewall Management Center* in the *Cisco Secure Firewall Management Center Administration Guide*.

Usernames

Usernames must be Linux-valid usernames and be lowercase only, using alphanumeric characters plus period (.) or hyphen (-). Special characters such as at sign (@) and slash (/) are not supported. You cannot add these default internal users for external authentication—**root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, ntp, lldpd, bind, dhcp, qemu, rpcuser, rpc, sshd, radiusd, messagebus, admin, mysql, www, sfrna, snorty, sfsnort, sfremediation, nobody, samdme, extuser, p2puser, rloginUser**. You can only add external users (as part of the External Authentication object) in the Firewall Management Center; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the Firewall Management Center.

If you previously configured the same username for an internal user using the **configure user add** command, the Firewall Threat Defense first checks the password against the internal user, and if that fails, it checks the AAA server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported. For users defined on the RADIUS server, be sure to set the privilege level to be the same as any internal users; otherwise you cannot log in using the external user password.

Privilege Level

LDAP users always receive Config privileges. You can define RADIUS users as either config or basic users.

Before you begin

- SSH access is enabled by default on the management interface. To enable SSH access on data interfaces, see Configure Secure Shell (SSH) access, on page 867.
- Inform RADIUS users of the following behavior to set their expectations appropriately:

- The first time an external user logs in, Firewall Threat Defense creates the required structures but cannot simultaneously create the user session. The user simply needs to authenticate again to start the session. The user will see a message similar to this: "New external username identified. Please log in again to start a session."
- If the user's Service-Type attribute is not defined or incorrectly configured in the RADIUS server and you use the RADIUS-defined users for authentication, the user will see a message similar to this: "Your username is not defined with a service type that is valid for this system. You are not authorized to access the system?".

  In some cases, the SSH clients close the CLI window on an unsuccessful SSH connection, even before displaying the failure message. Hence, ensure that the user's Service-Type attribute is correctly defined in the RADIUS server.
- Similarly, if the user's Service-Type authorization was changed since the last login, the user will need to re-authenticate. The user will see a message similar to this: "Your authorization privilege has changed. Please log in again to start a session."

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **External Authentication**, and then click the **Manage External Authentication Server** link.

You can also open the External Authentication screen by clicking **System** > **Users** > **External Authentication**.

Step 3 Click **Add External Authentication Object**.

Step 4 Configure an LDAP Authentication Object.

Step 5 Configure a RADIUS Authentication Object.

Step 6 Return to **System** (⚙) > **Users** > **External Authentication**.

Step 7 Click **Refresh** (↻) to view any newly-added objects.

For LDAP when you specify SSL or TLS encryption, you must upload a certificate for the connection; otherwise, the server will not be listed on this window.

Step 8 Click **Slider enabled** (⬭) next to the External Authentication object you want to use. You can only enable one object.

Step 9 Click **Save**; deploy configuration changes (see Deploy configuration changes, on page 135).

After completing this task, external authentication is enabled for management users. The system verifies user credentials with the configured LDAP or RADIUS server and grants access based on the authentication object and user privileges.

Configure an LDAP External Authentication Object

Configure external authentication to allow management users to be authenticated using an LDAP server.

Note You must have administrator privileges to perform this task.

Procedure

Step 1 In the **External Authentication Object** page, select **LDAP** from the **Authentication Method** drop-down list and enter appropriate values in these fields:

a) Enter a **Name**.

b) (Optional) Enter **Description**.

Step 2 Choose a **Server Type** from the drop-down list.

Step 3 For the **Primary Server** enter these values:

a) Enter a **Host Name/IP Address**.

Note If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

b) Change the **Port** from the default.

Step 4 Enter the **Backup Server** parameters.

Step 5 Enter **LDAP-Specific Parameters**.

- **Base DN**—Enter the base distinguished name for the LDAP directory you want to access. For example, to authenticate names in the Security organization at the Example company, enter `ou=security,dc=example,dc=com`. Alternatively click **Fetch DNs**, and choose the appropriate base distinguished name from the drop-down list.
- (Optional) **Base Filter**—For example, if the user objects in a directory tree have a `physicalDeliveryOfficeName` attribute and users in the New York office have an attribute value of `NewYork` for that attribute, to retrieve only users in the New York office, enter `(physicalDeliveryOfficeName=NewYork)`.
- **User Name**—Enter a distinguished name for a user who has sufficient credentials to browse the LDAP server. For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute, and the object for the administrator in the Security division at our example company has a `uid` value of `NetworkAdmin`, you might enter `uid=NetworkAdmin,ou=security,dc=example,dc=com`.
- **Password** and **Confirm Password**—Enter and confirm the password for the user.
- (Optional) **Show Advanced Options**—Configure the following advanced options.
  - **Encryption**—Click **None**, **TLS**, or **SSL**.

Note If you change the encryption method after specifying a port, you reset the port to the default value for that method. For **None** or **TLS**, the port resets to the default value of 389. If you choose SSL encryption, the port resets to 636.

- **SSL Certificate Upload Path**—For SSL or TLS encryption, you must choose a certificate by clicking **Choose File**.
- (Not Used) **User Name Template**—Not used by the Firewall Threat Defense.
- **Timeout**—Enter the number of seconds before rolling over to the backup connection between 1 and 30. The default is 30.

Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Step 6 (Optional) Set the **CLI Access Attribute** if you want to use a shell access attribute other than the user distinguished type. For example, on a Microsoft Active Directory Server, use the `sAMAccountName` shell access attribute to retrieve shell access users by typing `sAMAccountName` in the **CLI Access Attribute** field.

Step 7 Set the **CLI Access Filter**.

Choose one of these methods:

- To use the same filter you specified when configuring authentication settings, choose **Same as Base Filter**.
- To retrieve administrative user entries based on attribute value, enter the attribute name, a comparison operator, and the attribute value you want to use as a filter, enclosed in parentheses. For example, if all network administrators have a `manager` attribute which has an attribute value of `shell`, you can set a base filter of `(manager=shell)`.

The names on the LDAP server must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Step 8 Click **Save**.

Step 9 For LDAP, if you later add or delete users on the LDAP server, you must refresh the user list and redeploy the Platform Settings.

a) Choose **System** ( ) > **Users** > **External Authentication**.

b) Click **Refresh** ( ) next to the LDAP server.

If the user list changed, you will see a message advising you to deploy configuration changes for your device. The Firepower Theat Defense Platform Settings will also show that it is "Out-of-Date on *x* targeted devices."

c) Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure a RADIUS Authentication Object

Configure external authentication to allow management users to be authenticated using a RADIUS server



Note You must have administrator privileges to perform this task.

Procedure

Step 1 In the **External Authentication Object** page, select **RADIUS** from the **Authentication Method** drop-down list and enter appropriate values in these fields:

a) Check the **Enabled Message Authenticator** check box to require the Message-Authenticator attribute in all RADIUS responses, ensuring that every response from the RADIUS server is securely verified by the Firewall Threat Defense.

This feature is enabled by default for new RADIUS servers. We recommend you enable it for existing servers after the upgrade. Disabling message authenticators may expose your firewalls to potential attacks. Ensure that your RADIUS server has the Message-Authenticator configuration.

b) Define users on the RADIUS server using the Service-Type attribute.

This is the list of supported values for the Service-Type attribute:

- Administrator (6)—Provides Config access authorization to the CLI. These users can use all commands in the CLI.
- NAS Prompt (7) or any level other than 6—Provides Basic access authorization to the CLI. These users can use read-only commands, such as **show** commands, for monitoring and troubleshooting purposes.

The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Alternatively, you can predefine users in the external authentication object (see Step Configure external authentication, on page 855). To use the same RADIUS server for the Firewall Threat Defense and Firewall Management Center while using the Service-Type attribute method for the Firewall Threat Defense, create two external authentication objects that identify the same RADIUS server: one object includes the

predefined **CLI Access Filter** users (for use with the Firewall Management Center), and the other object leaves the **CLI Access Filter** empty (for use with Firewall Threat Defenses).

c) Enter a **Name** and optional **Description**.

Step 2 For the **Primary Server**, enter a **Host Name/IP Address**.

Note If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

Step 3 (Optional) Change the **Port** from the default.

Step 4 Enter a **RADIUS Secret Key**.

Step 5 (Optional) Enter the **Backup Server** parameters.

Step 6 Enter **RADIUS-Specific Parameters**.

- **Timeout (Seconds)**—Enter the number of seconds before rolling over to the backup connection. The default is 30.
- **Retries**—Enter the number of times the primary server connection should be tried before rolling over to the backup connection. The default is 3.

Step 7 (Optional) Enter a comma-separated list of usernames in the **Administrator CLI Access User List** field. For example, enter `jchrichton, aerynsun, rygel`.

You may want to use the **CLI Access Filter** method for Firewall Threat Defense so you can use the same external authentication object with Firewall Threat Defense and other platform types. Note that if you want to use RADIUS-defined users, you must leave the **CLI Access Filter** empty.

Make sure that these usernames match usernames on the RADIUS server. The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Note If you want to only define users on the RADIUS server, you must leave this section empty.

Step 8 Click **Save**.

Configure fragment settings

Configure fragment settings to manage the handling of fragmented IP packets on your Firewall Threat Defense device. These settings help prevent Denial of Service (DoS) attacks and ensure applications that require packet fragmentation operate properly.

- Set limits for the number of fragments per packet and for fragments awaiting reassembly.
- Set the timeout for fragment reassembly.
- Allow fragments only if your network applications require them.

By default, the Firewall Threat Defense device allows up to 24 fragments per IP packet. It also allows up to 200 fragments awaiting reassembly. Applications such as NFS over UDP may require fragmented packets, but attackers often use fragmented packets in Denial of Service (DoS) attacks.

These settings establish the defaults for devices assigned this policy. You can override these settings for specific interfaces on a device by selecting **Override Default Fragment Setting** in the interface configuration. When you edit an interface, you can find the option on **Advanced** > **Security Configuration**. Select **Devices** > **Device Management**, edit a Firewall Threat Defense device, and select **Interfaces** to edit interface properties.

- Allow fragments only if required by your network applications.
- Override the default settings for specific interfaces when your configuration requires it.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Fragment Settings**.

Step 3 Configure the available options. To use the default settings, click **Reset to Defaults**.

- **Size (Block)**—The maximum number of packet fragments from all connections collectively that can be waiting for reassembly. The default value is 200 fragments. (One fragment equals one packet segment.)
- **Chain (Fragment)**—The maximum number of packets into which a full IP packet can be fragmented. The default is 24 packets. Set this option to one to disallow fragments.
- **Timeout (Sec)**—The maximum number of seconds to wait for an entire fragmented packet to arrive. The default is five seconds. If all fragments are not received within this time, all fragments are discarded.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Deploy the policy to activate the new fragment settings on assigned devices. Monitor device performance and change fragment settings as needed.

Configure HTTP access

You can enable the HTTPS server to provide a health check mechanism for a cloud load balancer, for example, for the Firewall Threat Defense Virtual on AWS using an Application Load Balancer.

Use HTTPS with the Firewall Threat Defense only as described for health checks and management. You cannot configure the Firewall Threat Defense through a web interface in this management mode.

Configure HTTP access only on data interfaces, including interfaces you set as management-only. Use only data interfaces for HTTP access, not the dedicated Management interface. The Management interface is separate from the other interfaces on the device. Use the Management interface only to set up and register your device to the Firewall Management Center. It has a separate IP address and static routing.

Configure HTTPS access as described in this section. An access rule for the host IP address is not required.

Use HTTPS only on a reachable interface. If your HTTPS host is on the outside interface, initiate the management connection directly to it.

Before you begin

- Configure HTTPS and AnyConnect VPN module of Cisco Secure Client on separate TCP ports if both features are required on the same interface. For example, assign a different port to HTTPS, such as port 4443.
- Create network objects to define the hosts or networks that are allowed for HTTPS connections. You can add these objects as part of this procedure. If you plan to use object groups for IP addresses, ensure the groups exist in the rules. Select **Objects** > **Object Management** to configure objects.

Note Use the **any-ipv4** or **any-ipv6** network object group instead of the system-provided **any** object.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **HTTP Access**.

Step 3 Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4 (Optional) Change the HTTP port. The default is 443.

Step 5 Identify the interfaces and IP addresses that allow HTTP connections.

Allow HTTP connections only from specific interfaces and client IP addresses by configuring this table. You may use network addresses instead of individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make HTTP connections. Choose an object from the drop-down menu, or click + to add a new network object.
- **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow HTTP connections. For interfaces not in a zone, type the interface name into the field under the selected **Selected Zones/Interfaces** list. Then click **Add**. The device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After you complete this task, the device enables HTTP access on the specified interfaces and IP addresses. Use secure connections for health checks or management.

Configure ICMP access

By default, you can send ICMP packets to any interface using either IPv4 or IPv6, with these exceptions:

- The Firewall Threat Defense does not respond to ICMP echo requests directed to a broadcast address.
- The Firewall Threat Defense only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

To protect the device from attacks, you can use ICMP rules to limit ICMP access to interfaces to particular hosts, networks, or ICMP types. ICMP rules function like access rules, where the rules are ordered, and the first rule that matches a packet defines the action.

If you configure any ICMP rule for an interface, an implicit deny ICMP rule is added to the end of the ICMP rule list, changing the default behavior. Thus, if you want to simply deny a few message types, you must include a permit any rule at the end of the ICMP rule list to allow the remaining message types.

We recommend that you always grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. Additionally ICMP packets in IPv6 are used in the IPv6 neighbor discovery process.

Before you begin

Make sure the required objects exist before you configure rules. Select **Objects** > **Object Management** to configure objects. Create network objects or groups to specify the hosts or networks, and port objects to specify the ICMP message types you want to control.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **ICMP Access**.

Step 3 Configure ICMP rules.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **Action**—Whether to permit (allow) or deny (drop) matching traffic.
- **ICMP Service**—The port object that identifies the ICMP message type.
- **Network**—The network object or groupthat identifies the hosts or networks whose access you are controlling.
- **Available Zones/Interfaces**—Add the zones that contain the interfaces that you are protecting. If an interface is not in a zone, type the interface name into the field beneath the **Selected**

Zones/Interfaces list, and click **Add**. A device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 4 (Optional.) Set rate limits on ICMPv4 Unreachable messages.

- **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
- **Burst Size**—Sets the burst rate, between 1 and 10. The system sends this number of replies, but subsequent replies are not sent until the rate limit is reached.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ICMP access rules take effect after you deploy the policy to the assigned devices. Your configuration permits or denies ICMP traffic for the hosts or networks you specified.

Configure NetFlow

Configure NetFlow to enable the collection and export of IP network traffic information from your device interfaces. This allows you to analyze traffic patterns, bandwidth usage, and identify sources and causes of network congestion.

The NetFlow feature enables you to collect IP network traffic information as it enters or exits an interface. The collected traffic information is sent as records to a NetFlow Collector server or NetFlow Analyzer. You can analyze the data from NetFlow and determine information such as source and destination of traffic, class of service, traffic pattern, bandwidth usage, type of traffic, traffic volume, and the causes of congestion.

With the native NetFlow configuration support, the traffic information collection that was enabled through syslogs flow exports has to be disabled.

NetFlow provides the option to configure the flow exporter and collectors along with flow event types that must be monitored.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **NetFlow**.

Step 3 Enable the **Enable Flow Export** toggle to enable NetFlow data export.

Step 4 Configure the general NetFlow parameters that control the frequency of events pushed to the collector.

a) **Active Refresh Interval**—For active connections, specify the time interval (in minutes) between flow-update events.

b) **Delay Flow Create**—Specify the delay (in seconds) before sending a flow-create event. If you do not enter any value, there is no delay and the flow-create event is exported as soon as the flow is created.

c) **Template Timeout Rate**—Specify the time interval (in minutes) at which the template records are sent to the collectors.

Step 5 Click **Add Collector** to configure the collector. See Add a collector in NetFlow, on page 866.

Step 6 Click **Add Traffic Class** to configure the traffic class. See Add a traffic class to NetFlow, on page 867.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, NetFlow will be enabled and configured on your device. Traffic data will be exported to the configured collector, allowing you to analyze network traffic patterns and usage.

Add a collector in NetFlow

Use this task when you need to export NetFlow data from Cisco Threat Defense devices to a collector for traffic analysis and monitoring.

This configuration is applicable to Cisco Threat Defense policies with NetFlow enabled.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Choose **NetFlow**.

Step 3 Enable the **Enable Flow Export** toggle to enable NetFlow data export.

Step 4 Click **Add Collector** to configure the collector. You can configure a maximum of five collectors.

Step 5 From the **Host** dropdown list, choose the collector host IP address (IPv4 only) of the NetFlow event collector or server to which the NetFlow packets must be sent. Alternatively, you can click the (+) icon to create a new network host.

Step 6 In the **Port** field, enter the UDP port on the collector to which the NetFlow packets must be sent.

Step 7 From **Available Interfaces or Interface Groups**, choose the interface or interface group through which the collector must be reached. You can choose multiple interfaces or interface groups. The Interface Group object can contain only one interface for a given device. A collector can be reached only through one interface. The object can include a virtual-router-aware interface. Loopback interface is not supported in NetFlow.

You can click the (+) icon to create a new interface group.

Step 8 Click **Add** to add the interfaces you chose. Alternatively, you can also enter the interface name and click **Add** to add the interface.

Step 9 Click **OK**.

Add a traffic class to NetFlow

Use this task when you need to monitor, filter, and export specific types of network traffic using NetFlow on a Threat Defense device. Adding a traffic class helps you focus on relevant traffic for security or operational analysis.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **NetFlow**.

Step 3 Click the **Enable Flow Export** toggle to export NetFlow data.

Step 4 Click **Add Traffic Class** to configure the traffic class.

Step 5 In the **Name** field, enter the name of the traffic class that must match the NetFlow events.

Step 6 In the **Type** field, choose the traffic class to filter the type of traffic you want to capture:

- **Default**—The traffic class that is matched if none of the traffic classes matches the traffic.
- **Access List**—The specific traffic class that must match the traffic captured for the NetFlow events.

Step 7 If you select **Access List** as the **Type**, then select the access list object from the **Access List Object** drop-down list.

Note You can also click the (+) icon to create a new extended access list object. See Configure an extended ACL object, on page 2351.

Step 8 In **Event Types**, check the checkboxes for the different NetFlow events that you want to capture and send to the collectors.

Step 9 Click **OK**.

Configure Secure Shell (SSH) access

If you enabled Firewall Management Center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the Firewall Threat Defense.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

Data vs. Management SSH

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. SSH for data interfaces shares the internal and external user lists with SSH for the Management interface. Other settings are configured separately. For data interfaces, enable SSH and access lists using this screen. SSH traffic for data interfaces uses the regular routing configuration. Routing for the Management interface configured during setup or at the CLI is not used.

For the Management interface, to configure an SSH access list, see the **configure SSH-access-list** command in the *Cisco Secure Firewall Threat Defense Command Reference*. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

Interface Access

You can SSH only to a reachable interface(including an interface in a user-defined virtual router); for example, if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. When you enable SSH in a user-defined virtual router, and you want VPN users to access SSH, be sure to terminate the VPN on the same virtual router. If the VPN is terminated on another virtual router, then you must configure route leaks between the virtual routers.

Ciphers and Key Exchange

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256

SSH Stack

The Firewall Threat Defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Maximum Attempts

After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command; see Add an internal user at the CLI, on page 87. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings. See Configure external authentication, on page 855.
- You need network objects that define the hosts or networks permitted to make SSH connections to the device. You can add objects during the procedure. If you want to use object groups to identify a group of IP addresses, make sure the required groups already exist in the rules. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SSH Access**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
- **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. You can also add loopback interfaces and virtual-router-aware interfaces. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure an SMTP server

Configure an SMTP server to enable email alerts in Syslog. Ensure the source email address configured for Syslog is a valid account on the SMTP servers.

Before you begin

Ensure that the network objects for the primary and secondary SMTP server addresses exist. Define the objects using **Objects** > **Object Management**. You can also create these objects when you edit the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **SMTP Server**.

Step 3 Select the network objects that identify the **Primary Server IP Address** and optionally, the **Secondary Server IP Address**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, email alerts can be sent through Syslog using the specified SMTP servers.

Configure SNMP for a security device

Configure SNMP monitoring to allow network management stations to monitor the health and status of Cisco security devices. This task enables centralized visibility and management of devices using SNMP.

- Enable SNMP so that SNMP management stations can monitor devices.
- SNMP versions 1, 2c, and 3, including traps and read access, are supported. SNMP write access is not supported.

Simple Network Management Protocol (SNMP) defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers, and security appliances. You can use the SNMP page to configure a firewall device for monitoring by SNMP management stations.

SNMPv3 supports read-only users and encryption with DES(deprecated), 3DES, AES256, AES192, and AES128.

The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption and that were created using a version earlier than 6.5, you can continue to use those users for Firewall Threat Defense devices running versions 6.6 or earlier. However, you cannot edit those users and retain DES encryption or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defense devices running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defense devices will fail.

Note

- You can configure SNMP only on Routed and Diagnostic interfaces.
- To create an alert to an external SNMP server, access **Policies** > **Actions** > **Alerts**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SNMP**.

Step 3 Enable SNMP, and configure basic options.

- **Enable SNMP Servers**—Whether to provide SNMP information to the configured SNMP hosts. You can deselect this option to disable SNMP monitoring while retaining the configuration information.
- **Read Community String**, **Confirm**—Enter the password used by a SNMP management station when sending requests to the Firewall Threat Defense device. The SNMP community string (also known as password) is a shared secret among the SNMP management stations and the network nodes. The security

device uses this password to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces and special characters are not permitted.

- **System Administrator Name**—Enter the name of the device administrator or other contact person. This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Location**—Enter the location of this security device (for example, Building 42, Sector 54). This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Port**—Enter the UDP port on which incoming requests will be accepted. The default is 161.

Step 4 (SNMPv3 only.) Add SNMPv3 users, on page 877.

Step 5 Add SNMP hosts, on page 880.

Step 6 Configure SNMP traps, on page 882.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

SNMP protocol

SNMP protocol is an application-layer protocol that

- facilitates the exchange of management information between network devices, and
- is part of the TCP/IP protocol suite.

SNMP protocol support and access

Firewall Threat Defense provides support for network monitoring using SNMP Versions 1, 2c, and 3, and supports the use of all three versions simultaneously. The SNMP agent runs on the Firewall Threat Defense interface. You can monitor network devices using management systems (NMSs) such as OpenView network management system. Firewall Threat Defense supports SNMP read-only access with a GET request. SNMP does not support write access or the SNMP SET request, so you cannot make changes with SNMP.

You can configure the Firewall Threat Defense to send traps, which are messages sent to the management station when certain events occur. These messages are called event notifications. You can also use the NMS to browse Management Information Bases (MIBs) on the security devices. MIBs are collections of definitions, and the Firewall Threat Defense maintains a database of values for each definition. To browse a MIB, issue a series of GET-NEXT or GET-BULK requests from the NMS to the MIB tree to get values.

The SNMP agent sends a notification to your management station when a specified event occurs, such as a network link going up or down. The notification includes an SNMP OID, which identifies the source device. The agent also replies when your management station requests information.

List SNMP terminology

This reference lists and defines the terms that are commonly used when working with SNMP.

Table 52: SNMP terminology

Term	Description
Agent	The SNMP server running on the Secure Firewall Threat Defense. The SNMP agent has these features: • responds to requests for information and actions from the network management station. • ontrols access to its Management Information Base, the collection of objects that the SNMP manager can view or change. • does not allow SET operations.
Browsing	Monitoring the health of a device from the network management station by polling required information from the SNMP agent on the device. This activity may include issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the network management station to determine values.
Management Information Bases (MIBs)	Standardized data structures for collecting information about packets, connections, buffers, failovers, and other items. MIBs are defined by the product, protocols, and hardware standards used by most network devices. SNMP network management stations can browse MIBs and request specific data or events be sent as they occur.
Network management stations (NMSs)	The PCs or workstations SET up to monitor SNMP events and manage devices.
Object identifier (OID)	The system that identifies a device to its NMS and indicates to users the source of information monitored and displayed.
Trap	Predefined events that generate a message from the SNMP agent to the NMS. Events include alarm conditions such as link-up, link-down, cold-start, warm-start, authentication events, or syslog messages. **coldStart**—The coldStart trap occurs when the SNMP agent starts after the SNMP configuration. This trap also occurs when the agent starts after a system reboot. **Note** For cluster and HA nodes, after a reload, if the interface reboot time exceeds 5 minutes (preset threshold), the trap is dropped. When the cluster and HA nodes have rebooted successfully, all other traps are sent as expected. The **SNMP-server enable traps SNMP coldstart** command is used to enable and disable transmission of these traps.

Describe MIBs and traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and described in various RFCs. Traps report significant events, such as errors or failures, on a network device. SNMP traps can be defined in standard or enterprise-specific MIBs. The IETF also creates standard traps, documented in various RFCs. SNMP traps are compiled into ASA software.

If needed, you can also download RFCs, standard MIBs, and standard traps from these locations:

http://www.IETF.org/

Browse the SNMP Object Navigator to look up Cisco MIBs, traps, and OIDs from this location:

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

In addition, download Cisco OIDs by FTP from this location:

ftp://FTP.cisco.com/pub/mibs/oid/oid.tar.gz

List of supported tables and objects in MIBs

This reference lists the supported tables and objects for the specified MIBs, including details for each MIB such as counters, OIDs, and descriptions.

Remote Access VPN polling

Table 53: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
Active Sessions	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	The number of currently active sessions.
Users	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	The number of users who have active sessions.
Peak Sessions	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	The number of peak RA sessions since system up.

Site-to-site VPN tunnel polling

Table 54: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
LAN to LAN Sessions	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	The number of currently active LAN to LAN sessions.
Peak LAN to LAN Sessions	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	The number of peak concurrent LAN to LAN sessions since the system is up.

Connection polling

Table 55: CISCO-FIREWALL-MIB

Counter	OID	Description
Active Connections	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	The number of connections currently in use by the entire firewall.

Counter	OID	Description
Peak Connections	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	The highest number of connections in use at any one time since system startup.
Connections Per Second	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	The current connections per second rate on the firewall.
Peak Connections Per Second	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	The highest number of connections per second on the firewall since system startup.

NAT translation polling

Table 56: CISCO-NAT-EXT-MIB

Counter	OID	Description
Active Translations	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	The total number of address translation entries that are currently available in the NAT device. This indicates the aggregate of the translation entries created from both the static and dynamic address translation mechanisms.
Peak Active Translations	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	The maximum number of address translation entries that are active at any one time since system startup. This value indicates the high watermark of address translation entries active at any one time since system startup. This object includes the translation entries created from both the static and dynamic address translation mechanisms.

Routing table entries polling

Table 57: IP-FORWARD-MIB

Counter	OID	Description
Active Translations	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	The total number of current inetCidrRouteTable entries that are valid.

Interface duplex status polling

Table 58: CISCO-IF-EXTENSION-MIB

Counter	OID	Description
Duplex Status	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	This object specifies the configured duplex status for the given interface.
Detected Duplex Status	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	This object specifies the detected duplex status for the given interface.

Snort 3 intrusion EVENT rate polling

Table 59: CISCO-UNIFIED-FIREWALL-MIB

Counter	OID	Description
Snort 3 Intrusion event Rate	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The rate at which intrusion events were recorded by Snort on this firewall, averaged over the last 300 seconds.

BGP peer-flap trap notification

Table 60: BGP4-MIB

Counter	OID	Description
BGP Peer-flap	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The BGPBackwardTransition event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

CPU utilization polling

Table 61: CISCO-PROCESS-MIB

Counter	OID	Description
CPU Total Utilization	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	Total system CPU utilization for the last one minute.
Individual CPU Core Utilization	Associated parameters and values of cpmCPUTotal1minRev 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	Individual CPU core utilization values for the last one minute, where 'n' represents the number of cores. Examples: • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - Aggregate system CPU utilization % (This value is the same as the system CPU usage from .3.6.1.4.1.9.9.109.1.1.1.1.7.1 in single context mode). • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort average CPU utilization % (total aggregate value of all snort instances) • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - System PROCESS average % (average of "Sysproc" cores)

Note The SNMP OIDs 1.3.6.1.2.1.25.3.3 and 1.3.6.1.2.1.25.3.4 pertaining to CPU monitoring (hrProcessorTable and hrNetworkTable) were removed on ASA FirePOWER. You can view and MONITOR the CPU health details of the device only through its device manager.

In ENTITY-MIB, two new vendor OIDs were added for the dual EPM 2X100G and 4X200G cards of Secure Firewall 4200 for slot 2 and slot 3—cevFPRNM4X200Gng and cevFPRNM2X100Gng.

Add SNMPv3 users

Add SNMPv3 users to provide secure, authenticated, and encrypted SNMP management access to your device. This task ensures that only authorized users can access SNMPv3 features using specified authentication and encryption algorithms.

You create users for SNMPv3 only. These steps are not applicable for SNMPv1 or SNMPv2c.



Note SNMPv3 only supports read-only users.

SNMP users have a specified username, an authentication password, an encryption password, and authentication and encryption algorithms to use.



Note If you add a new cluster unit or replace a High Availability unit when using SNMPv3 with clustering or High Availability, SNMPv3 users are not replicated to the new unit. Remove the users, add them again, and redeploy your configuration to replicate users to the new unit.

For a successful SNMPv3 user authentication, the authentication key size should be equal to or larger than the encryption key size. For example, a user authentication using SHA-1 with AES256 fails, whereas authentication using SHA256 with AES256 succeeds.

The authentication algorithm options are MD5 (deprecated, pre-6.5 only), SHA, SHA224, SHA256, and SHA384.



Note The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTD devices running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those threat defenses will fail.

The encryption algorithm options are DES (deprecated, pre-6.5 only), 3DES, AES256, AES192, and AES128.



Note The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for threat defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those threat defenses will fail.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Choose **SNMP** > **Users** tab.

Step 3 Click **Add** and completed the following:

a) Select the security level for the user from the **Security Level** drop-down list.

- **Auth**—Authentication but No Privacy, which means that messages are authenticated.
- **No Auth**—No Authentication and No Privacy, which means that no security is applied to messages.
- **Priv**—Authentication and Privacy, which means that messages are authenticated and encrypted.

b) Enter the name of the SNMP user in the **Username** field. Usernames must be 32 characters or fewer.

c) From the **Encryption Password Type** drop-down list, choose one of these options:

- **Clear text**—The Firewall Threat Defense device encrypts the password when you deploy the policy. In High Availability or cluster deployments, choose this option so that each unit localizes the SNMPv3 key with its own SNMP engineID.
- **Encrypted**—The Firewall Threat Defense device directly deploys the precomputed localized key in hexadecimal format.



Note Do not choose **Encrypted** for SNMPv3 users in High Availability or cluster deployments. An encrypted SNMPv3 password is a localized key that is generated from a specific SNMP engineID. Each High Availability or cluster unit has a unique SNMP engineID. If you deploy a localized key generated for one unit to its peer, SNMPv3 polling to the peer fails with an authentication error.

Choose **Clear text** so that each unit localizes the key during deployment.

d) In the **Auth Algorithm Type** drop-down list, select the type of authentication you want to use: SHA, SHA224, SHA256, or SHA384.



Note The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTD devices running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those Firewall Threat Defenses will fail.

e) In the **Authentication Password** field, enter the password to use for authentication. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values.

Note The length of the password will depend on the authentication algorithm selected. For all passwords, the length must be 256 characters or less.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

f) In the **Encryption Type** drop-down list, select the type of encryption you want to use: AES128, AES192, AES256, 3DES.

Note To use AES or 3DES encryption, you must have the appropriate license installed on the device.

Note The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for Firewall Threat Defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defenses will fail.

g) Enter the password to use for encryption in the **Encryption Password** field. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values. For encrypted passwords, the length of the password depends on the encryption type selected. The password sizes are as follows. Each xx is one octal.:

- AES 128 requires 16 octals
- AES 192 requires 24 octals
- AES 256 requires 32 octals
- 3DES requires 32 octals
- DES can be any size

Note For all passwords, the length must be 256 characters or fewer.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

Step 4 Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing these steps, SNMPv3 users are added with the specified authentication and encryption settings. The device is now configured for secure SNMPv3 management access.

Add SNMP hosts

Define SNMP hosts and their communication parameters to enable SNMP management stations to access and monitor the device. This task allows you to specify which hosts are permitted and how they communicate with the device.

Use Host to add or edit entries in the SNMP Hosts table on the SNMP page. These entries represent SNMP management stations allowed to access the Firewall Threat Defense device.

You can add up to 8192 hosts. Only 128 of this number can be for traps.



Note In 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices (7.3 and earlier, and some upgraded 7.4 FTDs).

Before you begin

Ensure that the network objects that define the SNMP management stations exist. Select **Device** > **Object Management** to configure network objects.



Note The supported network objects include IPv6 hosts, IPv4 hosts, IPv4 range and IPv4 subnet addresses.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Choose **SNMP** > **Hosts** tab.

Step 3 Click **Add** and completed the following:

a) In the **IP Address** field, either enter a valid IPv6 or IPv4 host or select the network object that defines the SNMP management station's host address.

The IP address can be an IPv6 host, IPv4 host, IPv4 range or IPv4 subnet.

b) Select the appropriate SNMP version from the **SNMP version** drop-down list.

c) (SNMPv3 only.) Select the username of the SNMP user that you configured from the **User Name** drop-down list.



Note You can associate up to 23 SNMP users per SNMP host.

d) (SNMPv1, 2c only.) In the **Read Community String** field, enter the community string that you have already configured, for read access to the device. Re-enter the string to confirm it.

Note This string is required, only if the string used with this SNMP station is different from the one already defined in the **Enable SNMP Server** section.

e) Select the type of communication between the device and the SNMP management station. You can select both types. Choose from:

- **Poll**—The management station periodically requests information from the device.
- **Trap**—The device sends trap events to the management station as they occur.

Note When the SNMP host IP address is either an IPv4 range or an IPv4 subnet, you can configure either **Poll** or **Trap**, not both.

f) In the **Port** field, enter a UDP port number for the SNMP host. The default value is 162. The valid range is 1 to 65535.

g) Select the interface type for communication between the device and the SNMP management station under the **Reachable By** options. You can select either the Management interface of the device or an available security zone/named interface. Choose from:

- **Device Management Interface**—Communication between the device and the SNMP management station occurs over the Management interface.
  - When you choose this interface for SNMPv3 polling, all configured SNMPv3 users are allowed to poll and are not restricted to the user chosen in 3.c, on page 880. Here, SNMPv1 and SNMPv2c are not allowed from an SNMPv3 host.
  - When you choose this interface for SNMPv1 and SNMPv2c polling, the polling is not restricted at all to the version selected in 3.b, on page 880.
- **Security Zones or Named Interface**—Communication between the device and the SNMP management station occurs over a security zone or interface.
  - Search for zones in the **Available Zones** field.
  - Add the zones that contain the interfaces through which the device communicates with the management station to the **Selected Zone/Interface** field. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. You can also choose a loopback interface and virtual-router-aware interfaces. The host will be configured on a device only if the device includes the selected interfaces or zones.

Note VTI tunnel interfaces are not supported for SNMP.

Step 4 Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure SNMP traps

Use SNMP traps to configure event notifications for Firewall Threat Defense. Traps are unsolicited notifications sent from the device to the management station for certain events, such as linkup, linkdown, and syslog event generation. Each SNMP trap includes an object ID (OID) for your device.

Some traps are not applicable to certain hardware models. These traps will be ignored if you apply the policy to one of these models. For example, not all models have field-replaceable units, so the **Field Replaceable Unit Insert/Delete** trap will not be configured on those models.

SNMP traps are defined in standard MIBs or in enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The Firewall Threat Defense software includes SNMP traps.

If needed, you can download RFCs, standard MIBs, and standard traps from http://www.IETF.org/.

Browse the complete list of CISCO MIBs, traps, and OIDs using the SNMP Object Navigator on the Cisco website: SNMP Object Navigator.

In addition, download CISCO OIDs by FTP: ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **SNMP** > **SNMP Traps** to configure SNMP traps (event notifications) for the Firewall Threat Defense device.

Step 3 Select the appropriate Enable Traps options. You can select either or both options.

a) Check **Enable All SNMP Traps** to select all traps in the subsequent four sections.

b) Check **Enable All Syslog Traps** to enable transmission of trap-related syslog messages.

Note SNMP traps are of higher priority than other notification messages because they are expected to be near real-time. When you enable all SNMP or syslog traps, it is possible for the SNMP process to consume excess resources in the agent and in the network, causing the system to hang. If you notice system delays, unfinished requests, or timeouts, you can selectively enable SNMP and syslog traps. You can also limit the rate at which syslog messages are generated by severity level or message ID. For example, all syslog message IDs that begin with the digits 212 are associated with the SNMP class; see Configure syslog rate limits, on page 902.

Step 4 The event-notification traps in the **Standard** section are enabled by default for an existing policy:

- **Authentication** – Unauthorized SNMP access. This authentication failure occurs for packets with an incorrect community string.
- **Link Up** – One of the device's communication links has become available (it has "come up"), as indicated in the notification.

- **Link Down** – One of the device's communication links has failed, as indicated in the notification.
- **Cold Start** – The device is reinitializing itself such that its configuration or the protocol entity implementation may be altered.
- **Warm Start** – The device is reinitializing itself such that its configuration and the protocol entity implementation is unaltered.

Step 5 Select the desired event-notification traps in the **Entity MIB** section:

- **Field Replaceable Unit Insert** – A Field Replaceable Unit (FRU) has been inserted, as indicated. (FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc.)
- **Field Replaceable Unit Delete** – A Field Replaceable Unit (FRU) has been removed, as indicated in the notification
- **Configuration Change** – There has been a hardware change, as indicated in the notification

Step 6 Select the desired event-notification traps in the **Resource** section:

- **Connection Limit Reached** – This trap indicates that a connection attempt was rejected because the configured connections limit has been reached.

Step 7 Select the desired event-notification traps in the **Other** section:

- **NAT Packet Discard** – This notification is generated when IP packets are discarded by the NAT function. Available Network Address Translation addresses or ports have fallen below configured threshold.
- **CPU Rising Threshold** – This notification is generated when rising CPU utilization exceeds a predefined threshold for a configured period of time. Check this option to enable CPU rising threshold notifications:
  - **Percentage** – The default value is 70% for the high threshold notification; the range is 10 to 94%. The critical threshold is 95%.
  - **Period** – The default monitoring period is 1 minute; the range is 1 to 60 minutes.
- **Memory Rising Threshold** – This notification is generated when rising memory utilization exceeds a predefined threshold, thus reducing available memory. Check this option to enable memory rising threshold notifications:
  - **Percentage** – The default value is 70% for the high threshold notification; the range is 50 to 95%.
- **Failover** – This notification is generated when there is a change in the failover state as reported by the CISCO-UNIFIED-FIREWALL-MIB.
- **Cluster** – This notification is generated when there is a change in the cluster health as reported by the CISCO-UNIFIED-FIREWALL-MIB.
- **Peer Flap** – This notification is generated when there is BGP route flapping, a situation in which BGP systems send an excessive number of update messages to advertise network reachability information.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, SNMP traps are configured on the Firewall Threat Defense device, and event notifications will be sent to the management station for the selected events. This enables proactive monitoring and timely response to device events.

Configure SSL settings

This task enables you to configure SSL settings for remote access VPN sessions, allowing you to specify protocol versions, security levels, and available algorithms to ensure secure communication.

You must have administrator privileges and be in a leaf domain to perform this task.

Make sure that you are running a fully licensed version of the Secure Firewall Management Center. The SSL Settings are disabled if you are running Secure Firewall Management Center in evaluation mode. SSL Settings are also disabled if the licensed Secure Firewall Management Center version does not meet the export-compliance criteria. If you are using Remote Access VPN with SSL, your Smart Account must have the strong-crypto features enabled. For more information, see *License Types and Restrictions* in the *Cisco Secure Firewall Management Center Administration Guide*.

Before you begin

Ensure you have administrator privileges and are in a leaf domain. Verify that you are running a fully licensed version of the management center with strong-crypto features enabled if using Remote Access VPN with SSL.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a Firewall Threat Defense policy.

Step 2 Select **SSL**.

Step 3 Add entries to the **Add SSL Configuration** table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the required security configurations from the drop-down list.

- **Protocol Version**—Specifies the TLS protocols to be used while establishing remote access VPN sessions.
- **Security Level**—Indicates the kind of security positioning you would like to set up for the SSL.

Step 4 Select the **Available Algorithms** based on the protocol version that you select and click **Add** to include them for the selected protocol. For more information, see Configure SSL settings, on page 885.

The algorithms are listed based on the protocol version that you select. Each security protocol identifies a unique algorithm for setting up the security level.

Step 5 Click **OK** to save the changes.

What to do next

Select **Deploy** > **Deployment** and click **Deploy** to deploy the policy to the assigned devices.

Configure SSL settings

The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. The SSL Settings window lets you configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL.

Note Though you configure Firewall Management Center and Firewall Threat Defense to operate in a security certifications (UCAPL, CC, or FIPS) compliance mode, the Firewall Management Center allows configuration of unsupported ciphers. For example, in a FIPS enabled mode, management center allows configuring DH Group 5 which is not FIPS-compliant. However, VPN tunnel does not negotiate due to the non-compliant cipher usage.

Configure the SSL Settings at this location:

Devices > **Platform Settings**, and then click **SSL**.

Fields

Minimum SSL Version as Server—Specify the minimum SSL/TLS protocol version that the Firewall Threat Defense device uses when acting as a server. For example, when it functions as a Remote Access VPN Gateway.

TLS Version—Select one of these TLS versions from the drop-down list:

TLS V1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
TLSV1.3	Accepts SSLv2 client hellos and negotiates TLSv1.3 (or greater).

Note TLS 1.3 in remote access VPN requires Cisco Secure Client, Version 5.0 and above.

DTLS Version—Select the DTLS versions from the drop-down list, based on the selected TLS version. By default, DTLSv1 is configured on Firewall Threat Defense devices, you can choose the DTLS version as per your requirement.

Note Ensure that the TLS protocol version is higher than or equal to the DTLS protocol version selected. TLS protocol versions support these DTLS versions:

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1, DTLSv1.2
TLSV1.3	DTLSv1, DTLSv1.2

Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group1 - 768-bit modulus, Group2 - 1024-bit modulus, Group5 - 1536-bit modulus, Group14 - 2048-bit modulus, 224-bit prime order, and Group24 - 2048-bit modulus, 256-bit prime order. The default is Group1.

Elliptical Curve Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group19 - 256-bit EC, Group20 - 384-bit EC, and Group21 - 521-bit EC. The default value is Group19.

TLSv1.2 adds support for these ciphers:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Note
ECDSA and DHE ciphers are the highest priority.

TLSv1.3 adds support for these ciphers:

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

The SSL configuration table can be used to specify the protocol version, security level, and Cipher algorithms that you want to support on the Secure Firewall Threat Defense devices.

Protocol Version—Lists the protocol version that the Secure Firewall Threat Defense device supports and uses for SSL connections. Available protocol versions are:

- Default
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSV1.3
- DTLSv1
- DTLSv1.2

Security Level—Lists the cipher security levels that Firewall Threat Defense device supports and uses for SSL connections.

If you have Firewall Threat Defense devices with evaluation license, the security level is Low by default. With Firewall Threat Defense smart license, the default security level is High. You can choose one of these options to configure the required security level:

- **All** includes all ciphers, including NULL-SHA.
- **Low** includes all ciphers, except NULL-SHA.
- **Medium** includes all ciphers, except NULL-SHA, DES-CBC-SHA, RC4-SHA, and RC4-MD5 (this is the default).
- **FIPS** includes all FIPS-compliant ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA, TLS_CHACHA20_POLY1305_SHA256.
- **High** includes only AES-256 with SHA-2 ciphers and applies to TLS version 1.2 and the *default* version.
- **Custom** includes one or more ciphers that you specify in the Cipher algorithms/custom string box. This option provides you with full control of the cipher suite using OpenSSL cipher definition strings.

Cipher Algorithms/Custom String—Lists the cipher algorithms that the Firewall Threat Defense device supports and uses for SSL connections. For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/apps/ciphers.html

Ciphers supported by TLSv1.2 only

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384

- DHE-RSA-AES256-SHA256
- AES256-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- AES128-SHA256



Note ECDSA and DHE ciphers are the highest priority.

Ciphers not supported by TLSv1.1 or TLSv1.2

- RC4-SHA
- RC4-MD5
- DES-CBC-SHA
- NULL-SHA

Syslog

Logging information

Logging information can help you identify and isolate network or device configuration problems.

- System logging (syslog) can be enabled for Firewall Threat Defense devices.
- Some security events can be sent to a syslog server.

Syslog messages

A syslog message is a log event that

- collects messages from devices to a server running a syslog daemon
- enables aggregation of logs and alerts for centralized management, and
- provides protected long-term storage for logs, supporting troubleshooting and incident handling.

System log configuration details

Devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and either stores them in files or prints them, based on a simple configuration file.

Table 62: System logs for Secure Firewall Threat Defense

Logs related to	Details	Configure in
Device and system health, network configuration	This syslog configuration generates messages for features running on the data plane, that is, features that are defined in the CLI configuration that you can view with the **show running-config** command. This includes features such as routing, VPN, data interfaces, DHCP server, NAT, and so forth. Data plane syslog messages are numbered, and they are the same as those generated by devices running ASA software. However, Secure Firewall Threat Defense does not necessarily generate every message type that is available for ASA Software. For information on these messages, see *Cisco Secure Firewall Threat Defense syslog messages* at https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html. This configuration is explained in these topics.	**Platform settings**
Security events	This syslog configuration generates alerts for file and malware, connection, Security Intelligence, and intrusion events. For details, see *About sending syslog messages for security events* and subtopics in the *Cisco Secure Firewall Management Center Administration Guide*.	**Platform settings** and the **Logging** in an access control policy
(All devices) Policies, rules, and events	This syslog configuration generates alerts for access control rules, intrusion rules, and other advanced services as described in *Configurations supporting alert responses* in the *Cisco Secure Firewall Management Center Administration Guide*. These messages are not numbered. For information on configuring this type of syslog, see *Creating a syslog alert response* in the *Cisco Secure Firewall Management Center Administration Guide*.	**alert responses** and the **Logging** in an access control policy

You can set up multiple syslog servers and control the messages and events sent to each server. You can also configure varied destinations, such as console, email, or internal buffer.

Syslog message severity levels

The syslog message severity levels define the importance of system messages.

Table 63: Syslog message severity levels

Level Number	Severity Level	Description
0	**emergencies**	You cannot use the system.
1	**alert**	You need to take immediate action.
2	**critical**	The system has critical conditions to be addressed.
3	**error**	Error conditions.
4	**warning**	The system has warnings you should review.
5	**notification**	The system reports significant events you should monitor.
6	**informational**	Informational messages only.
7	**debugging**	The system generates only debugging messages Log at this level only temporarily, when debugging issues. This log level can generate many messages, which might affect system performance.



Note Firewall Threat Defense does not generate syslog messages with a severity level of zero (emergencies).

Syslog message filters

Syslog message filter criteria

You can direct syslog messages to an output destination according to these criteria:

- Syslog message ID number

  (This does not apply to syslog messages for security events such as connection and intrusion events.)

- Syslog message severity level
- Syslog message class (equivalent to a functional area)

  (This rule does not apply to syslog messages for security events, including connection and intrusion events.)

You can create a message list with specific criteria, which you can then specify as the output destination is set. Alternatively, you can configure the Firewall Threat Defense device to send a particular message class to each type of output destination independently of the message list.

(Message lists do not apply to syslog messages for security events such as connection and intrusion events.)

Syslog message classes and associated message ID numbers

Note This topic does not apply to messages for security events (connection, intrusion, etc.)

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages.
- Create a message list that specifies the message class.

Use the syslog message class to categorize syslog messages by type, such as features or functions of the device. For example, use the RIP class for RIP routing.

Syslog messages in the same class have the same three initial digits in their message ID numbers. For example, the syslog messages for the VPN client feature use ID numbers 611101 to 611323.

Most ISAKMP syslog messages include prepended objects that identify the tunnel. When available, these objects appear before the descriptive text of a syslog message. If the object is unknown when the syslog message is generated, the heading and value combination is omitted.

The objects are prefixed in this manner:

Group = *groupname*, Username = *user*, IP = *IP_address*

The term 'group' here refers to the tunnel-group configuration. The username is from the local database or AAA server. The IP address is the public IP address of the remote access client or Layer 2 peer.

See the message classes and the range of message ID numbers in each class in this table.

Table 64: Syslog message classes and associated message ID numbers

Class	Definition	Syslog Message ID Numbers
access-list*	Access Lists	106
application-firewall*	Application Firewall	415
auth	User Authentication	109, 113
botnet-traffic-filtering*	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
card-management*	Card Management	323
citrix	Citrix Client	723
clustering*	Clustering	747
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724

Class	Definition	Syslog Message ID Numbers
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
EAP, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
EIGRP	EIGRP Routing	336
email	E-mail Proxy	719
environment-monitoring*	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
identity-based-firewall*	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733
ikev2-toolkit*	IKEv2 Toolkit	750, 751, 752
IP	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	400, 401, 420
ipv6*	IPv6	325
licensing*	Licensing	444
MDM-proxy	MDM Proxy	802
NAC	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
NAT-and-PAT*	NAT and PAT	305
network-access-point*	Network Access Point	713
NP	Network Processor	319
NP-SSL*	NP SSL	725
OSPF	OSPF Routing	318, 409, 503, 613
password-encryption*	Password Encryption	742
phone-proxy*	Phone Proxy	337
RIP	RIP Routing	107, 312

Class	Definition	Syslog Message ID Numbers
rm	Resource Manager	321
scansafe*	ScanSafe	775
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
smart-call-home*	Smart Call Home	120
SNMP	SNMP proxy	212
SSL	SSL Stack	725
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
tag-switching	Service Tag Switching	779
threat-detection*	Threat Detection	733
transactional-rule-engine-tre*	Transactional Rule Engine	780
uc-IMS*	UC-IMS	339
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
VPN	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
VXLAN*	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and Secure Client	716

*The management center web interface provisions these classes to facilitate creation of event lists. The device console does not display these classes.

Guidelines for logging

Restrictions for IPv6 logging

- IPv6 is supported. Syslog message can be sent using TCP or UDP.
- Ensure that the interface configured for sending syslogs is enabled, IPv6 capable, and the syslog server is reachable through the designated interface.
- You cannot use IPv6 for secure logging.

Syslog server configuration guidelines

- The syslog server must run a server program called syslogd. Windows includes a syslog server as part of its operating system.
- The syslog server operates based on the syslog-ng process of the firewall system. Do not use external configuration files, such as the *scwx.conf* file from SecureWorks. Because these files are not compatible with the device, using them causes parsing errors and the syslog-ng process fails.
- You can configure up to 16 syslog servers.
- Assign only one list or class to each syslog server and location.
- Do not configure Firewall Management Center as a primary syslog server. The Firewall Management Center can log some syslogs. However, it does not have adequate storage provision to accommodate large amounts of information from connection events for every sensor, especially when multiple sensors are used and all send syslogs.
- The syslog server should be reachable through the Firewall Threat Defense device. Configure the device to deny ICMP unreachable messages on the interface through which the syslog server is reachable, and to send syslogs to the same server. Enable logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.
- To view logs generated by the Firewall Threat Defense device, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the Firewall Threat Defense device generates messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately.
- The Firewall Threat Defense syslog supports one-way TLS for secure logging. It does not support client certificate authentication, trustpoint configuration for syslog, or mutual TLS (X.509 certificate authentication).

Interfaces for syslog configuration

- Determining the egress interface for the syslog:
  - If the specified management-only interface has management-access enabled, the management center will perform route table lookups and determine the egress interface (could be data or management) based on best routing logic.
  - If you configure a management-only interface as logging host, that does not have management-access enabled, the management center will use the interface regardless of routing table entries.

Thus, for the management center to always uses a dedicated management path for syslog traffic, configure the management interface without management-access, and then specify the interface in the logging host:

```
interface <management-interface>
management-only ----->Do not include management-access
logging host <management-interface> <syslog-server-ip>
```

- When the syslog rate exceeds 50,000 messages per second, ensure that a data interface is used as egress interface rather than a management interface.
- Configure the data interface as the syslog source interface for production monitoring and auditing. Use the management interface only for temporary testing. This approach ensures optimal syslog reliability and prevents rate-limiting on the management interface.

TCP and UDP connections for syslog

- If you use TCP as the transport protocol, the system opens 4 connections to the syslog server to ensure that messages are not lost. If you collect messages from many devices and the combined connection overhead is too much for the server, use UDP instead.
- The number of UDP connections for syslog is directly related to the number of CPUs on the hardware platform and the number of syslog servers you configure. At any point in time, there can be as many UDP syslog connections as there are CPUs times the number of configured syslog servers. The global UDP connection idle timeout applies to these sessions, and the default duration is two minutes. You can adjust this setting to close sessions more quickly, but the timeout applies to all UDP connections, not just syslog. This is the intended behavior.
- When the Firewall Threat Defense device sends syslogs via TCP, the connection takes about one minute to initiate after the syslogd service restarts.
- When the TCP logging host goes down, it takes approximately six minutes to change its connection status from *Connected* to *Not connected*. Logging relies on TCP to detect the channel state; until then, logging sends the logs through the channel. During this time, when you execute the **show log**, the output would display the TCP logging host as connected. Once the TCP channel is closed, the TCP logging host state is updated to *Not connected*.

Configure syslog logging for Firewall Threat Defense devices

This task enables you to configure syslog logging for Firewall Threat Defense devices, allowing you to monitor and manage system events efficiently.

Syslog logging helps track security events and system activity on your devices. If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages.

See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896 for more information about platform settings that apply to security event syslog messages.

Before you begin

See requirements in Guidelines for logging, on page 894.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **Syslog** from the table of contents.

Step 3 Click **Logging Setup** to enable logging, specify FTP server settings, and specify Flash usage. For more information, see Configure logging and basic settings, on page 897.

Step 4 Click **Logging Destinations** to enable logging to specific destinations and to specify filtering on message severity level, event class, or on a custom event list. For more information, see Enable logging destinations, on page 898.

You must enable a logging destination to see messages at that destination.

Step 5 Click **E-mail Setup** to specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages. For more information, see Configure syslog messages to be sent to an e-mail address, on page 900.

Step 6 Click **Events List** to define a custom event list that includes an event class, a severity level, and an event ID. For more information, see Create a custom event list, on page 900.

Step 7 Click **Rate Limit** to specify the volume of messages being sent to all configured destinations and define the message severity level to which you want to assign rate limits. For more information, see Configure syslog rate limits, on page 902.

Step 8 Click **Syslog Settings** to specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination. For more information, see Configure syslog settings, on page 903.

Step 9 Click **Syslog Servers** to specify the IP address, protocol used, format, and security zone for the syslog server that is designated as a logging destination. For more information, see Configure a syslog server, on page 904.

After you complete these steps, your Firewall Threat Defense device sends system events to the specified destinations for monitoring and analysis.

Firewall Threat Defense platform settings that apply to security event syslog messages

Security events include connection, Security Intelligence, intrusion, and file and malware events. Some syslog settings configured on the **Syslog** page and its tabs apply to syslog messages for security events. However, most settings only apply to messages for events related to system health and networking. This reference lists the settings that apply to syslog messages for security events.

Settings that apply to syslog messages for security events:

- **Logging Setup** tab:
  - **Send syslogs in EMBLEM format**
- **Syslog Settings** tab:
  - **Enable Timestamp on Syslog Messages**
  - **Timestamp Format**
  - **Enable Syslog Device ID**

- **Syslog Servers** tab:
  - All options on the **Add Syslog Server** form and the list of configured servers.

Configure logging and basic settings

Enable logging and configure syslog settings so the system generates and manages logs for data plane events. This setup ensures log data is archived and available for analysis or reporting.

Perform this task when you need to generate syslog messages for data plane events and manage log storage on your device. You can manipulate saved logging data. You can also specify actions for certain syslog messages, extract data for reporting, or track statistics using scripts.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Before you begin

- Determine where logs should be stored, such as an FTP server or flash memory.
- Understand the desired logging level (critical, alerts, emergencies, errors, etc)
- Identify if logging should be enabled on standby or failover units.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Logging Setup** in your device's configuration interface.

Step 3 Enable logging and configure basic logging settings.

- **Enable Logging**—Turns on the data plane system logging.
- **Enable Logging on the Failover Standby Unit**—Turns on logging for the standby device, if available.
- **Send syslogs in EMBLEM format**—Enables EMBLEM format logging for every logging destination. If you enable EMBLEM, you must use the UDP protocol to publish syslog messages. EMBLEM is not compatible with TCP.

  The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. When EMBLEM is enabled, the syslog message prints a colon (:) after the <PRI> field, which differs from the RFC 5424 format.

Note Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in Firewall Management Center, if you want to display the PRI value in the syslog messages of the managed Firewall Threat Defense device, ensure to enable the EMBLEM format. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

- **Send debug messages as syslogs**—Redirects debug trace output to the syslog. The syslog message number is 711001 and the default logging level is set to debug. To view these messages, ensure logging is enabled at the console and configured for the debug syslog message number and level.
- **Memory Size of Internal Buffer**—Specify the size of the internal buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 52428800 bytes.

Step 4 (Optional) Configure the syslog message logging to the Firewall Management Center.

a) Enable VPN logging by checking the **Enable Logging to Secure Firewall Management Center** check box.

b) Choose the syslog severity level for the logging messages in the **Logging Level** drop-down list.

- The logging level for the VPN messages is set to **errors** by default.

  VPN troubleshooting syslogs can add excessive load on the Firewall Management Center. Hence, enable this option with caution. Also, when you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the management center by default. We recommend that you limit the logging level to **error** and above to restrict the excessive flow of syslogs to the Firewall Management Center, especially in case of RAVPN, where multiple devices are involved.

For information on the levels, see Syslog message severity levels, on page 889.

Step 5 (Optional) Save log buffer contents to an FTP server before the buffer is overwritten.

- Enable **FTP Server Buffer Wrap** and enter the necessary destination information in the following fields.
- **IP Address**—Select the host network object that contains the IP address of the FTP server.
- **User Name**—Enter the username to use when connecting to the FTP server.
- **Path**—Enter the path, relative to the FTP root, where the buffer contents should be saved.
- **Password/ Confirm**—Enter and confirm the password used to authenticate the username to the FTP server.

Step 6 (Optional) Save log buffer contents to flash memory before overwriting.

- Check the **Flash** checkbox
- Specify **Maximum flash to be used by logging (KB)** (range: 4-8044176 KB).
- Specify **Minimum free space to be preserved (KB)** (range: 0-8044176 kilobytes.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Logging is enabled and syslog messages are generated and stored based on your configuration. Log data is archived as specified and is accessible for further analysis or reporting.

Enable logging destinations

Enable logging destinations to ensure that syslog messages are received at the specified destination. This task allows you to control which messages are sent by applying message filters to each destination.

To see messages at a logging destination, enable the destination and specify a message filter.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Before you begin

Before you begin, ensure you have access to the system and the necessary permissions to configure logging destinations.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Logging Destinations**.

Step 3 Click **Add** to enable a destination and apply a logging filter, or edit an existing destination.

Step 4 In the **Logging Destinations** dialog box, select a destination and configure the filter for that destination:

a) Choose the destination to enable in the **Logging Destination** drop-down list. You can create one filter for each destination. Examples include Console, E-Mail, Internal buffer, SNMP trap, SSH Sessions, and Syslog servers.

Note Console and SSH session logging works in the diagnostic CLI only. Enter **system support diagnostic-CLI**.

b) In **Event Class**, choose the filter that will apply to all classes not listed in the table.

You can configure these filters:

- **Filter on severity** —Select the severity level. Messages at this level or higher are sent to the destination
- **Use Event List** —Select the event list that defines the filter. You create these lists on the **Event Lists** page.
- **Disable Logging** —Prevents messages from being sent to this destination.

c) To create filters for each event class, click **Add** for a new filter or edit an existing filter. Select the event class and severity level to limit messages in that class. Click **OK** to save the filter.

For an explanation of the event classes, see Syslog message classes and associated message ID numbers, on page 891.

d) Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, the selected logging destinations will receive syslog messages according to the filters you have configured.

Configure syslog messages to be sent to an e-mail address

Enable syslog messages to be delivered as e-mails to designated recipients so administrators receive important system notifications directly through e-mail.

You can set up a list of recipients for syslog messages to be sent as e-mails.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Before you begin

- Configure an SMTP server on the platform settings page
- Configure logging and basic settings, on page 897
- Setup Email as the Logging Destination

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Email Setup**.

Step 3 Specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.

Step 4 Click **Add** to enter a new e-mail address recipient of the specified syslog messages.

Step 5 Set the desired severity level for syslog messages for each recipient.

The severity filter ensures only messages of the specified level and higher are sent via e-mail. For information on the levels, see Syslog message severity levels, on page 889.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Syslog messages are sent as e-mails to the specified recipients according to the configured severity level.

Create a custom event list

Create a custom event list to control which syslog messages are sent to a logging destination. This allows you to filter messages based on event class, severity, and message identifier for more granular control.

An event list is a custom filter you can apply to a logging destination, allowing greater control over which messages are sent. Normally, you filter messages for a destination based solely on severity. Using an event list, you can fine-tune filters using event class, severity, and message ID.

Creating a custom event list is a two-step process. You create a custom list in the **Event Lists**, and then use the event list to define the logging filter for the various types of destination, in the **Logging Destinations**.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Before you begin

Ensure you have access to the system where syslog event lists can be configured.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Events List**.

Step 3 Click **Add** to create a new list or click an existing list to edit.

a) Enter a unique name for the event list in the **Name** field; avoid spaces.

b) Set criteria to filter messages by severity or event class, select the **Severity/Event Class** tab and add or edit entries.

For information on the available classes see Syslog message classes and associated message ID numbers, on page 891.

For information on the levels, see Syslog message severity levels, on page 889.

Certain event classes do not apply to devices in transparent mode. If you configure these options, the system does not use or deploy them.

c) To identify messages specifically by message ID, select the **Message ID** and add or edit the IDs.

You can enter a range of IDs using a hyphen, for example, 100000-200000. Each message ID you enter must contain six digits. For information on how the initial three digits map to features, see Syslog message classes and associated message ID numbers, on page 891.

For specific message numbers, see Cisco ASA Series Syslog Messages.

d) Click **OK** to save the event list.

Step 4 Click **Logging Destinations** and add or edit the destination that should use the custom event list filter.

See Enable logging destinations, on page 898.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The system creates the custom event list and applies it to the logging destination you select.

Configure syslog rate limits

Limit the rate at which syslog messages are generated, reducing log flooding and ensuring that important messages are not lost.

Syslog message generation can overwhelm logging systems if not managed properly. Configure rate limits for severity levels or specific message IDs to ensure efficient log management. When limits set for severity level and message ID conflict, the message ID limit takes precedence.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Rate Limit**.

Step 3 To limit message generation by severity level, click **Logging Level** > **Add**, then configure these options:

- **Logging Level**—Specify the severity level for the rate limit. For information on the levels, see Syslog message severity levels, on page 889.
- **Number of messages**—The maximum number of messages of the specified type allowed in the specified time period.
- **Interval**—The number of seconds before the rate limit counter resets.

Step 4 Click **OK**.

Step 5 To limit message generation by syslog message ID, click **Syslog Level** > **Add**, then configure these options:

- **Syslog ID**—Specify the syslog message ID to be rate limited. For specific message numbers, see Cisco ASA Series Syslog Messages.
- **Number of messages**—Enter the maximum number of messages allowed in the specified interval.
- **Interval**—Set the interval (in seconds) for the rate limit counter to reset.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Syslog message generation is limited based on configured severity levels or message IDs, preventing excessive log messages and supporting efficient log management.

Configure syslog settings

Configure syslog settings to manage how syslog messages are generated and sent to external syslog servers. You can specify the facility code, timestamp, device ID, and control message severity and suppression.

General syslog settings let you choose what information is included in syslog messages sent to syslog servers. This information includes the facility code, timestamp, device ID, severity levels, and message suppression. If you configure devices to send syslog messages about security events (such as connection and intrusion events), some settings do not apply to messages that relate to security events. See *Threat Defense Platform Settings That Apply to Security Event Syslog Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.

Before you begin

Make sure you have access to the device and the permissions needed to change syslog settings.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Syslog Settings**.

Step 3 Choose a system log facility from the **Facility** list as required by your syslog server.

Most UNIX systems use the default LOCAL4(20). Change the facility if your network devices use the same codes. In most cases, you do not need to set the facility value for security event logs.

Step 4 Select the **Enable timestamp on each syslog message** check box to include the date and time a message was generated in the syslog message.

Step 5 Select the desired **Timestamp Format**:

- **Legacy (MMM dd yyyy HH:mm:ss)**: Default format without a timezone (always UTC).
- **RFC 5424 (yyyy-MM-ddTHH:mm:ssZ)**: Uses ISO 8601 with "Z" indicating UTC.

Step 6 To add a device identifier at the start of messages, check the **Enable Syslog Device ID** check box and select the identifier type:

- **Interface**—Use the IP address of a specific interface.

Note VTI tunnel interfaces are not supported for Syslog.

- **User Defined ID**—Enter a custom text string (up to 16 characters).
- **Host Name**—Use the device's hostname.

Step 7 Use the Syslog Message table to adjust severity or suppress messages:

Change a message's severity level or disable its generation if necessary. By default, syslog entries for NetFlow are enabled and appear in the table.

a) To suppress redundant messages due to NetFlow, select **Netflow Equivalent Syslogs**.

This adds the messages to the table as suppressed messages.

Note If any of these syslog equivalents are already in the table, your existing rules are not overwritten.

b) To add a rule, click **Add**.
c) Select the message number (Syslog ID) to change, from the **Syslog ID** drop-down list.
d) Choose the new severity level from the **Logging Level** drop-down list or select **Suppressed** to disable the generation of the message. Usually, you do not change both the severity level and disable the message. However, you can modify both fields if you want.
e) Click **OK** to add the rule to the table.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure a syslog server

This task enables you to configure a syslog server for your device, allowing you to collect and monitor system-generated messages for security and operational visibility.

To configure a syslog server to handle messages generated from your system, perform this task.

If you want this syslog server to receive security events such as connection and intrusion events, see also Firewall Threat Defense platform settings that apply to security event syslog messages , on page 896.

Note In version 7.4 and later, the Management and Diagnostic interfaces are merged. If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, you must use separate Platform Settings policies for merged and unmerged devices. This requirement also applies to version 7.3 and earlier, and to some Firewall Threat Defense devices upgraded to version 7.4.

Before you begin

- See requirements in Guidelines for logging, on page 894.
- Make sure your devices can reach your syslog collector on the network.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Syslog Server**.

Step 3 Check the **Allow user traffic to pass when TCP syslog server is down (Recommended)** check box, to allow traffic if any syslog server that is using the TCP protocol is down.



Note

- This option is enabled by default. Unless required, we recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device.
- When the **Allow user traffic to pass when TCP syslog server is down** option is disabled in Firewall Management Center version 6.2.x or earlier, it remains in the Disabled state even after upgrading to version 6.3 or later. You must manually enable this option.
- If this option is disabled and more than one TCP syslog server is configured on the device, user traffic is allowed if at least one server is reachable by thethreat defense device. This option only blocks traffic when none of the configured TCP syslog servers are reachable. The device generates a syslog message that describes the root cause of denied traffic.

  ```
  %FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New connections
  are denied based on logging permit-hostdown policy
  ```

Step 4 In the **Message queue size (messages)** field, enter the queue size for storing syslog messages on the security appliance when the syslog server is busy. The minimum is 1 message. The default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).

If the number of messages exceeds the configured queue size, the excess messages are dropped, resulting in missing syslog entries. To determine the ideal queue size, you need to identify the available block memory. Use the **show blocks** command to know the current memory utilization. For more information on the command and its attributes, see *Cisco Secure Firewall ASA Series Command Reference Guide*. Contact Cisco TAC for assistance.

Step 5 Click **Add** to add a new syslog server.

a) In the **IP Address** drop-down list, select a network host object containing the IP address of the syslog server.

b) Choose the protocol, either TCP or UDP, and enter the port number used for communication between the Firewall Threat Defense device and the syslog server.

UDP is faster and uses fewer resources than TCP on the device.

The default port for UDP is 514. You must manually configure port 1470 for TCP. Valid non-default port values for either protocol are 1025 through 65535.

c) Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).

The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field.



Note Syslog messages in RFC5424 format typically displays the priority value, referred to as PRI. However, in Firewall Management Center, only when you enable logging in Cisco EMBLEM format, the PRI value in the syslog messages of the managed Firewall Threat Defense is displayed. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

d) Check the **Enable Secure Syslog** check box to encrypt the connection between the device and server using SSL or TLS over TCP.

Note You must select TCP as the protocol and its port value ranging between 1025 and 65535 to use this option. Upload the certificate required to communicate with the syslog server on the **Devices** > **Certificates** page. Then, upload the certificate from the Firewall Threat Defense device to the syslog server to complete the secure relationship and allow it to decrypt the traffic. The **Enable Secure Syslog** option is not supported on the device Management interface.

e) Select **Device Management Interface** or **Security Zones or Named Interfaces** to communicate with the syslog server.

- **Device Management Interface**: Send syslogs out of the Management interface. We recommend that you use this option when configuring syslog on Snort events.

Note The **Device Management Interface** option does not support the **Enable Secure Syslog** option.

- **Security Zones or Named Interfaces**: Select the interfaces from the list of **Available Zones** and click **Add**. You can also add virtual-router-aware interfaces.

Important The Firewall Threat Defense data plane (Lina) syslog messages cannot be sent out through the diagnostic interface. Configure other interfaces or the Management interface (Br1/Management0) to send out the data plane syslog messages.

f) Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure timeouts

Configure timeout values for console sessions and protocol connections in a Threat Defense policy to manage session durations and optimize device resource usage.

You can set the global idle timeout durations for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool.

You can also set a timeout for console sessions on the device.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Timeouts**.

Step 3 Configure the timeouts you want to change.

For any setting, select **Custom** to specify your own value or **Default** to use the system default value. In most cases, the maximum timeout is 1193 hours.

You can disable some timeouts by selecting **Disable**.

- **Console Timeout**—The idle time until a connection to the console is closed, range is 0 or 5 to 1440 minutes. The default is 0, which means the session does not time out. If you change the value, existing console sessions will continue to use the previous timeout value. The updated timeout will apply only to new connections.
- **Translation Slot (xlate)**—The idle time until a NAT translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.
- **Connection (Conn)**—The idle time until a connection slot is freed. This duration must be at least 5 minutes. The default is 1 hour.
- **Half-Closed**—The idle time until a TCP half-closed connection closes. A connection is considered half-closed if both the FIN and FIN-ACK have been seen. If only the FIN has been seen, the regular connection timeout applies. The minimum is 30 seconds. The default is 10 minutes.
- **UDP**—The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.
- **ICMP**—The idle time after which general ICMP states are closed. The default (and minimum) is 2 seconds.
- **RPC/Sun RPC**—The idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.

  In a Sun RPC-based connection, if the parent connection is deleted or times out, a new child connection might not be treated as part of the parent–child relationship. As a result, the new connection could be evaluated according to the system's policy or rules. After the parent connection times out, existing child connections remain valid only until their own timeout value is reached.
- **H.225**—The idle time until an H.225 signaling connection closes. The default is 1 hour. To close a connection immediately after all calls are cleared, a timeout of 1 second (0:0:1) is recommended.
- **H.323**—The idle time after which H.245 (TCP) and H.323 (UDP) media connections close. The default (and minimum) is 5 minutes. Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.
- **SIP**—The idle time until a SIP signaling port connection closes. This duration must be at least 5 minutes. The default is 30 minutes.

- **SIP Media**—The idle time until a SIP media port connection closes. This duration must be at least 1 minute. The default is 2 minutes. The SIP media timer is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
- **SIP Disconnect**—The idle time after which SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 0:10:0. The default is 2 minutes (0:2:0).
- **SIP Invite**—The idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 00:30:0. The default is 3 minutes (0:3:0).
- **SIP Provisional Media**—The timeout value for SIP provisional media connections, between 1 and 30 minutes. The default is 2 minutes.
- **Floating Connection**—When multiple routes exist to a network with different metrics, the system uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0. This timer does not apply to connections through virtual tunnel interfaces (VTI). If a connection through a VTI gets stuck, you must manually clear it.
- **Xlate PAT**—The idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.
- **TCP Proxy Reassembly**—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).
- **ARP Timeout**—The number of seconds between ARP table rebuilds, from 60 to 4294967. The default is 14,400 seconds (4 hours).

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The configured timeout values are applied to the Threat Defense policy. Sessions and protocol connections will now use the specified timeout durations after you deploy the policy.

Synchronize time on FTD devices

Use a Network Time Protocol (NTP) server to synchronize the clock settings on your devices. We recommend you configure all Firewall Threat Defenses managed by a Firewall Management Center to use the same NTP server as the Firewall Management Center. Depending on the platform and configuration, the Firewall Threat Defense synchronizes either directly with the configured NTP server or through Firewall Management Center. If the Firewall Threat Defense's configured NTP servers are not reachable for any reason, it synchronizes its time with the Firewall Management Center.

The device supports NTPv4.

Note If you are deploying Firewall Threat Defense on the Firepower 4100/9300 chassis, you must configure NTP on the Firepower 4100/9300 chassis so that Smart Licensing will work properly and to ensure proper timestamps on device registrations. You should use the same NTP server for the Firepower 4100/9300 chassis and the Firewall Management Center.

Before you begin

- If your organization has one or more NTP servers that your Firewall Threat Defense can reach, use the same NTP server or servers for your devices that you have configured for Time Synchronization on the **System** (⚙) > **Configuration** page on your Firewall Management Center.
- If you selected **Use the authenticated NTP server only** when configuring NTP server or servers for the Firewall Management Center, for your devices use only the NTP server or servers that are configured to authenticate with the Firewall Management Center. (The managed devices will use the same NTP servers as the Firewall Management Center, but their NTP connections will not use authentication.)
- If your device cannot reach an NTP server or your organization does not have one, use the **Via NTP FROM Management Center** option as discussed in this procedure.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Time Synchronization**.

Step 3 Configure one of these clock options:

- **Via NTP FROM Management Center**: (Default). The managed device gets time FROM the NTP servers you configured for the Firewall Management Center (except for authenticated NTP servers) and synchronizes time with those servers directly. However, if any of these are true, the managed device synchronizes time FROM the Firewall Management Center:
  - The Firewall Management Center's NTP servers are not reachable by the device.
  - The Firewall Management Center has no unauthenticated servers.

Note NTP synchronization behavior and NTP status output can differ between Firewall Threat Defense Virtual devices and Secure Firewall 3100 appliances when the devices are configured to synchronize time through Firewall Management Center.

- Firewall Threat Defense Virtual devices synchronize directly with the NTP servers configured on Firewall Management Center. If the configured NTP servers become unreachable, the device uses Firewall Management Center as the fallback NTP source.
- Secure Firewall 3100 appliances synchronize with Firewall Management Center instead of directly synchronizing with the external NTP servers configured on Firewall Management Center. In NTP status output, Firewall Management Center can appear as 127.0.0.2.
- On Secure Firewall 3100 appliances, the **ntpq -pn** command can display 127.0.0.2 as the active NTP source, indicating synchronization with Firewall Management Center rather than with external NTP servers.

Example:

```
# ntpq -pn
remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
127.0.0.2       .FMC.      16 u   10   64   377    0.123    0.045    0.010
```

When you configure Secure Firewall 3100 appliances to synchronize directly with NTP servers instead of synchronizing through Firewall Management Center, and the configured NTP servers become unreachable, the appliance falls back to its local system clock. In this case, the appliance does not use Firewall Management Center as the fallback NTP source.

Consider these platform-specific differences when interpreting show **ntp** and **ntpq -pn** output during NTP validation and troubleshooting.

- **Via NTP FROM**: If your Firewall Management Center is using NTP servers on the network, select this option and enter the fully-qualified DNS name (such as NTP.example.com), or IPv4 or IPv6 address, of the same NTP servers you specified in **System** (⚙) > **Configuration** > **Time Synchronization**. If the NTP servers are not reachable, the Firewall Management Center acts as an NTP server.

When multiple NTP servers are configured, the device uses the NTP server that is deemed appropriate based on the criteria defined in RFC. Thus, the status "Being used" for a specific NTP server indicates that the server is currently used by the device.

Step 4 Click **Save**.

After completing these steps, the Firewall Threat Defense Virtual device synchronizes its clock with the configured NTP server, Management Center, or the local system clock, depending on platform behavior and configuration.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure a time zone for a device

By default, your device uses the UTC time zone. To set a different time zone for the device, use this procedure.

The time zone you specify is used only in policies that use time-based policy application.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a Firewall Threat Defense policy.

You can also create time zone objects from the **Objects** > **Object Management** > **Time Zone** page.

Step 2 Create a new time zone object by clicking +.

Step 3 Select the time zone.

Step 4 Click **Save**.

What to do next

- Create time range objects, select applicable time ranges in access control and prefilter rules, and assign the parent policies to devices associated with the correct time zone.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure UCAPL/CC compliance

Configure Unified Capabilities Approved Products List (UCAPL) or Common Criteria (CC) compliance to ensure your Secure Firewall Threat Defense device meets security certifications and export-controlled feature requirements.

Use this task when you need to enable security certifications compliance for your device. This is required for export-controlled features and may be necessary for regulatory or organizational compliance.

For more information about this setting and how to enable it for the Firewall Management Center, see the *Cisco Secure Firewall Management Center Administration Guide*.

Caution After you enable this setting, disabling it is not possible. To return the appliance to standard mode, reimage the appliance.

Before you begin

- Secure Firewall Threat Defense devices cannot use an evaluation license; your Smart Software Manager account must be enabled for export-controlled features.
- Secure Firewall Threat Defense devices must be deployed in routed mode.
- You must have administrative privileges to perform this task.

- Security certifications compliance mode cannot be changed if the Firewall Threat Defense device is in high availability. Change the security certifications compliance mode before you create the high availability pair.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **UCAPL/CC Compliance**.

Step 3 To *permanently* enable security certifications compliance on the appliance, you have two choices:

- To enable security certifications compliance in Common Criteria mode, choose **CC** from the drop-down list.
- To enable security certifications compliance in Unified Capabilities Approved Products List (UCAPL) mode, choose **UCAPL** from the drop-down list.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing these steps, your device operates in the selected compliance mode (UCAPL or CC), and the policy is enforced once deployed.

Configure a performance profile

Configure the performance profile to control how CPU cores are allocated between the data plane and Snort processes on supported devices. This configuration optimizes device performance for VPN, improves intrusion prevention, or balances the workload.

The performance profile determines how the CPU cores on the device are assigned to two of the main system processes: the data plane (Lina) and Snort. The data plane handles VPN connections, routing, and basic layer 3/4 processing. Snort provides advanced inspection for intrusion and malware prevention, URL filtering, application filtering, and other deep packet inspection features.

If you use both basic and advanced features, keep the performance profile unchanged. The system is designed to provide a balanced assignment of cores to these processes. This assignment differs based on the hardware model.

However, if you use the device primarily for VPN, or for intrusion and other advanced inspection, you can skew the performance profile so that more cores are assigned to the more heavily used features. This change can improve system performance.

Before you begin

- These settings apply to systems running release 7.3+ only.
- Performance profile is supported on these device types:
  - Firepower 4100/9300

- Secure Firewall 3100/4200 (7.4+)
- Secure Firewall Threat Defense Virtual

- Changing the performance profile is not supported on units in a cluster or high-availability group, or those configured for multi-instance.
- The minimum number for core allocation is 2. Cores are assigned in even numbers based on the selected performance profile.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Performance Profile**.

Step 3 Select a profile:

- **Default**—This is the recommended setting and is the best option if you configure both VPN and intrusion inspection.
- **VPN Heavy with prefilter fastpath**—If you primarily use the device as a VPN endpoint or headend, and you configure rules in the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. The allocation is 90% data plane, 10% Snort.
- **VPN Heavy with inspection**—If you primarily use the device as a VPN endpoint or headend, but do not use the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. This option assumes that you leave intrusion inspection, URL filtering, and other advanced functions that use Snort, to a different device in the network. The allocation is 60% data plane, 40% Snort.
- **IPS Heavy**—If you do not configure VPN, but you do use the device for intrusion prevention, you can choose this option to assign the majority of CPU core to the Snort process. The allocation is 30% data plane, 70% Snort.

Step 4 Click **Save**.

Step 5 Deploy the policy to apply your configuration.

Step 6 After deployment completes, reboot each affected device to apply the new core assignments.

After completing these steps, the device will use the selected performance profile and allocate CPU cores according to your configuration. The new core assignments take effect after you reboot the device.

History for platform settings

This reference provides a historical overview of feature additions, changes, and removals for platform settings in Secure Firewall releases. Use this information to track platform settings support and modifications across software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Device management services supported on user-defined VRF interfaces.	7.4.1	7.4.1	Device management services configured in the Firewall Threat Defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices.
Chassis platform settings for the Secure Firewall 3100.	7.4.1	7.4.1	New platform settings for multi-instance chassis on the Secure Firewall 3100. New/modified screens: • **Devices** > **Platform Settings** > **Add** > **Chassis Platform Settings** • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **DNS** • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **SSH** • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Time Synchronization** • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Time Zones** • **Devices** > **Platform Settings** > **Edit** > **Chassis Platform Settings** > **Syslog** Supported platforms: Secure Firewall 3100
Performance profile support for the Secure Firewall 3100/4200.	7.4.0	7.4.0	The performance profile settings available in the platform settings policy now apply to Secure Firewall 3100/4200 devices.

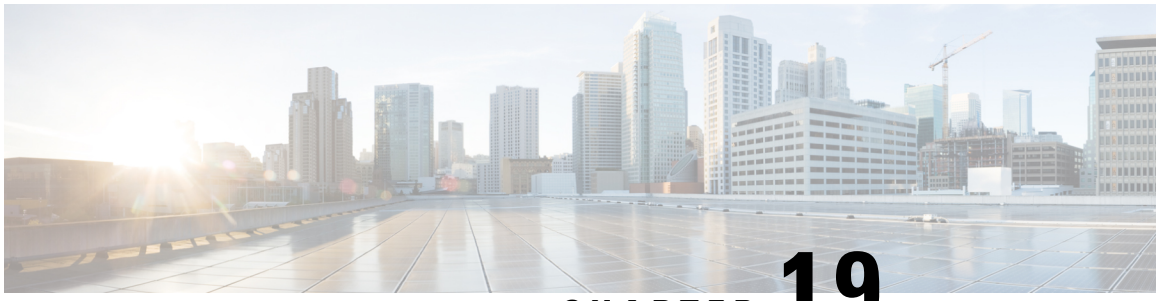
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Loopback interface support for DNS, HTTP, ICMP, NetFlow, SNMP and SSH.	7.4.0	7.4.0	You can create a loopback interface and use it for: • DNS • HTTP • ICMP • NetFlow • SNMP • SSH New/modified screens: • **Devices** > **Platform Settings** > **DNS** > **DNS Settings** **Devices** > **Platform Settings** > **HTTP Access** > **Add** **Devices** > **Platform Settings** > **ICMP Access** > **Add** • **Devices** > **Platform Settings** > **Network flow** > **Add Collector** • **Devices** > **Platform Settings** > **SNMP** > **Hosts** > **Add** • **Devices** > **Platform Settings** > **SSH Access** > **Add**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged Management and Diagnostic interfaces.	7.4.0	7.4.0	For new devices using 7.4 and later, you cannot use the legacy Diagnostic interface. Only the merged Management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the Diagnostic interface, then the interfaces will merge automatically. If you upgraded to 7.4 or later, and you have configuration for the Diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate Diagnostic interface. Note that support for the Diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for Diagnostic. • For SNMP, you can allow hosts on Management instead of Diagnostic. • For Syslog servers, you can reach them on Management instead of Diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the Diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: • **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence**
Performance profile for CPU core allocation.	7.3.0	7.3.0	You can adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance. The adjustment is based on your relative use of VPN and intrusion policies. If you use both, leave the core allocation to the default values. If you use the system primarily for VPN (without applying intrusion policies), or as an IPS (with no VPN configuration), you can skew the core allocation to the data plane (for VPN) or Snort (for intrusion inspection). We added the **Performance Profile** page to the platform settings policy.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
TLS 1.3 in Remote Access VPN.	7.3.0	7.3.0	You can now use TLS 1.3 to encrypt remote access VPN connections. Use threat defense platform settings to specify that the device must use TLS 1.3 protocol when acting as a remote access VPN server. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0 and above. New/modified screens: **Devices** > **Platform Settings** > **New Policy** > **Add/Edit Threat Defense Settings** > **SSL** > **TLS version**
Multiple DNS server groups for resolving DNS requests.	7.2.0	7.2.0	You can configure multiple DNS groups for the resolution of DNS requests from client systems. You can use these DNS server groups to resolve requests for different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. We changed the **Platform Settings** > **DNS** page.
Network object support for HTTP, ICMP, and SSH platform settings.	7.1.0	7.1.0	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Support to specify trusted DNS servers.	7.1.0	7.1.0	The option to specify DNS servers that you can trust for address resolution while using direct internet access was introduced. We added a tab for configuring the trusted DNS servers when configuring direct internet access: **Devices** > **Platform Settings** > **DNS** > **Trusted DNS Servers**.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Platform settings using the MD5 authentication algorithm or DES encryption for SNMPv3 users can not be deployed to Firewall Threat Defense devices running Versions 7.0+.	7.0.0	7.0.0	The MD5 authentication algorithm and DES encryption for SNMPv3 users on Firewall Threat Defense were deprecated in Version 6.5. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using Version 6.4 or earlier, you can continue to use those users for Firewall Threat Defense devices running Version 6.7 or earlier. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy with SNMP v3 users using the MD5 authentication algorithm or DES encryption to those Firewall Threat Defenses will fail. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts**
Specify SHA224 or SHA384 for SNMPv3 users' authorization algorithm.	7.0.0	7.0.0	You can now select SHA224 or SHA384 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
Specify time zone for device.	6.6.0	6.6.0	Specify a local time zone for a managed device, for use in time-based policy application. New/modified screens: **Devices** > **Platform Settings** > **Time Zone**
Specify the Management interface for SNMP communication.	6.6.0	6.6.0	You can now select the Management interface for communication between the device and the SNMP management station. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts**
Specify SHA256 for SNMPv3 users' authorization algorithm.	6.6.0	6.6.0	You can now select SHA256 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
DES encryption and the MD5 authentication algorithm for SNMPv3 users on Firewall Threat Defense have been deprecated.	6.5.0	Any	We recommend that you not use the MD5 authentication algorithm or DES encryption for SNMPv3 users on Firewall Threat Defense devices, as these options have been deprecated. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using a Version 6.4 or earlier, you can continue to use those users. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
Allow user traffic to pass when TCP syslog server is down.	6.3.0	6.3.0	We recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device. The **Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)** option in the Platform Settings is Enabled by default.
Limit number of SSH login failures.	6.3.0	6.3.0	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
External authentication added for SSH.	6.2.3	6.2.3	You can now configure external authentication for SSH access to the Firewall Threat Defense using LDAP or RADIUS. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**
Support for UC/APPL compliance mode.	6.2.1	6.2.1	You can enable security certifications compliance in CC mode or UCAPL mode. Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. For more information on hardening procedures, refer to the guidelines for this product provided by the certifying entity. New/modified screens: **Devices** > **Platform Settings** > **UC/APPL Compliance**
SSL settings for remote access VPN.	6.2.1	6.2.1	The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. You can configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL. New/modified screens: **Devices** > **Platform Settings** > **SSL**
External authentication for SSH and HTML removed.	6.1.0	6.1.0	Due to changes to support converged management access, only local users are supported for SSH and HTML to data interfaces. Also, you can no longer SSH to the logical Diagnostic interface; instead you can SSH to the logical Management interface (which shares the same physical port). Previously, only external authentication was supported for SSH and HTML access to Diagnostic and data interfaces, while only local users were supported to the Management interface. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**
Firepower Threat Defense support.	6.0.1	6.0.1	This feature was introduced. New/modified screens: **Devices** > **Platform Settings**



CHAPTER 19

FlexConfig policies

These topics describe how to configure and deploy FlexConfig policies.

- FlexConfig policy overview, on page 921
- Requirements and prerequisites for FlexConfig policies, on page 942
- Guidelines and limitations for FlexConfig, on page 943
- Customize device configuration with FlexConfig policies, on page 943
- Examples for FlexConfig, on page 958
- Migrate FlexConfig policies, on page 964
- History for FlexConfig, on page 966

FlexConfig policy overview

A FlexConfig policy is a container of an ordered list of FlexConfig objects that

- includes a series of Apache Velocity scripting language commands, ASA software configuration commands, and variables that you define
- contains FlexConfig objects that are essentially programs that generate a sequence of ASA commands that will then be deployed to the assigned devices, and
- configures the related feature on the Firewall Threat Defense device.

FlexConfig policy usage and limitations

Firewall Threat Defense uses ASA configuration commands to implement some features, but not all features. There is no unique set of Firewall Threat Defense configuration commands. Instead, the point of FlexConfig is to allow you to configure features that are not yet directly supported through Firewall Management Center policies and settings.

Caution We recommend using FlexConfig policies only if you are an advanced user with a strong ASA background and at your own risk. You may configure any commands that are not prohibited. Enabling features through FlexConfig policies may cause unintended results with other configured features.

Contact the Cisco Technical Assistance Center for support concerning FlexConfig policies that you have configured. The Cisco Technical Assistance Center does not design or write custom configurations on any customer's behalf. Cisco expresses no guarantees for correct operation or interoperability with other features. FlexConfig features may become deprecated at any time. For fully guaranteed feature support, you must wait for the Firewall Management Center support. When in doubt, do not use FlexConfig policies.

Recommended usage for FlexConfig policies

Use FlexConfig policies in two main scenarios to ensure proper firewall configuration and functionality.

- You are converting from ASA to Firewall Threat Defense, and there are compatible features you are using (and need to continue using) that Firewall Management Center does not directly support. In this case, use the **show running-config** command on the ASA to see the configuration for the feature and create your FlexConfig objects to implement it. Experiment with the object's deployment settings (once/every time and append/prepend) to get the right setting. Verify by comparing **show running-config** output on the two devices.
- You are using Firewall Threat Defense but there is a setting or feature that you need to configure, e.g. the Cisco Technical Assistance Center tells you that a particular setting should resolve a specific problem you are encountering. For complicated features, use a lab device to test the FlexConfig and verify that you are getting the expected behavior.

The system includes a set of predefined FlexConfig objects that represent tested configurations. If the feature you need is not represented by these objects, first determine if you can configure an equivalent feature in standard policies. For example, the access control policy includes intrusion detection and prevention, HTTP and other types of protocol inspection, URL filtering, application filtering, and access control. The ASA implements these functions using separate features. Many features are not configured using CLI commands, so not every policy appears in the output of the **show running-config** command.

Note At all times, keep in mind that there is not a one-to-one overlap between ASA and Firewall Threat Defense. Do not attempt to completely recreate an ASA configuration on a Firewall Threat Defense device. You must carefully test any feature that you configure using FlexConfig.

CLI commands in FlexConfig objects

A managed device uses ASA configuration commands to configure some features. Although not all ASA features are compatible with the device, some features can work on the managed device but you cannot configure them through Firewall Management Center policies. You can use FlexConfig objects to specify the CLI required to configure these features.

ASA documentation resources

When using FlexConfig to manually configure a feature, you are responsible for knowing and implementing the commands according to the proper syntax. FlexConfig policies do not validate CLI command syntax. For more information about proper syntax and configuring CLI commands, use the ASA documentation as a reference:

- ASA CLI configuration guides explain how to configure a feature. Find the guides at https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- ASA command references provide additional information sorted by command name. Find the references at https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

Determine the ASA software version and current CLI configuration

Determine the ASA software version and examine the current CLI-based configuration to identify which ASA CLI configuration guides to use for instructions on configuring a feature.

Because the system uses ASA software commands to configure some features, you need to determine the current ASA version used in software running on the Firewall Threat Defense device. This version number indicates which ASA CLI configuration guides to use for instructions on configuring a feature. You also should examine the current CLI-based configuration and compare it to the ASA configuration you want to implement.

Keep in mind that any ASA configuration will be very different from a Firewall Threat Defense configuration. Many Firewall Threat Defense policies are configured outside of the CLI, so you cannot see the configuration by looking at the commands. Do not try to create a one-to-one correspondence between an ASA and Firewall Threat Defense configuration.

To view this information, make an SSH connection to the device's management interface and issue the following commands:

- **show version system** and look for the Cisco Adaptive Security Appliance Software Version number. (If you issue the command through the Secure Firewall Management Center CLI tool, omit the **system** keyword.)
- **show running-config** to view the current CLI configuration.
- **show running-config all** to include all the default commands in the current CLI configuration.

You can also issue these commands from within Firewall Management Center using this procedure.

Procedure

Step 1 Choose **System** (⚙) > **Health** > **Monitor**.

Step 2 Click the name of the device targeted by the FlexConfig policy.

You might need to click the open/close arrow in the **Count** column in the Status table to see any devices.

Step 3 Click **View System and Troubleshoot Details**.

Step 4 Click **Advanced Troubleshooting**.

Step 5 Click **Threat Defense CLI**.

Step 6 Choose the **Device**, then choose **show** as the command, and type **version** or one of the other commands as the parameter.

Step 7 Click **Execute**.

For version, search the output for the Cisco Adaptive Security Appliance Software Version number.

You can select the output and press Ctrl+C, then paste it into a text file for later analysis.

Prohibited CLI commands

The purpose of FlexConfig is to configure features that are available on ASA devices that you cannot configure on Firewall Threat Defense devices using Firewall Management Center.

Thus, you are prevented from configuring ASA features that have equivalents in Firewall Management Center. The following table lists some of these prohibited command areas.

In addition, some **clear** commands are prohibited because they overlap with managed policies, and can delete part of the configuration for a managed policy.

The FlexConfig object editor prevents you from including prohibited commands in the object.

Prohibited CLI Command	Description
AAA	Configuration blocked.
AAA-Server	Configuration blocked.
Access-list	Advanced ACL, Extended ACL, and Standard ACL are blocked. Ethertype ACL is allowed. You can use standard and extended ACL objects defined in the object manager inside the template as variables.
ARP Inspection	Configuration blocked.
As-path Object	Configuration blocked.
Banner	Configuration blocked.
BGP	Configuration blocked.
Clock	Configuration blocked.
Community-list Object	Configuration blocked.
Copy	Configuration blocked.
Delete	Configuration blocked.
DHCP	Configuration blocked.
Enable Password	Configuration blocked.
Erase	Configuration blocked.

Prohibited CLI Command	Description
Fragment Setting	Blocked, except for **fragment reassembly**.
Fsck	Configuration blocked.
HTTP	Configuration blocked.
ICMP	Configuration blocked.
Interface	Only **nameif**, **mode**, **shutdown**, **ip address** and **mac-address** commands are blocked.
Multicast Routing	Configuration blocked.
NAT	Configuration blocked.
Network Object/Object-group	Network object creation in the FlexConfig object is blocked, but you can use network objects and groups defined in the object manager inside the template as variables.
NTP	Configuration blocked.
OSPF/OSPFv3	Configuration blocked.
pager	Configuration blocked.
Password Encryption	Configuration blocked.
Policy-list Object	Configuration blocked.
Prefix-list Object	Configuration blocked.
Reload	You cannot schedule reloads. The system does not use the **reload** command to restart the system, it uses the **reboot** command.
RIP	Configuration blocked.
Route-Map Object	Route-map object creation in the FlexConfig object is blocked, but you can use route map objects defined in the object manager inside the template as variables.
Service Object/Object-group	Service object creation in the FlexConfig object is blocked, but you can use port objects defined in the object manager inside the template as variables.
SNMP	Configuration blocked.
SSH	Configuration blocked.
Static Route	Configuration blocked.
Syslog	Configuration blocked.
Time Synchronization	Configuration blocked.

Prohibited CLI Command	Description
Timeout	Configuration blocked.
VPN	Configuration blocked.

Template scripts

You can use scripting language to control processing within a FlexConfig object. Scripting language instructions are a subset of commands supported in the Apache Velocity 1.3.1 template engine. The Apache Velocity engine is a Java-based scripting language that supports looping, if/else statements, and variables.

To learn how to use the scripting language, see the *Velocity Developer Guide* at http://velocity.apache.org/engine/devel/developer-guide.html.

FlexConfig variables

You can use variables in a FlexConfig object in cases where part of a command or processing instruction depends on runtime information rather than static information. During deployment, the variables are replaced with strings obtained from other device configurations, depending on the type of variable.

FlexConfig variable types

Variables are replaced with strings based on the type of variable.

- Policy object variables are replaced with strings obtained from objects defined in Firewall Management Center.
- System variables are replaced with information obtained from the device itself or from policies configured for it.
- Processing variables are loaded with the contents of policy object or system variables as during script execution. For example, in a loop, you iteratively load one value from a policy object or system variable into a processing variable, then use the processing variable to form a command string or perform another action. These processing variables do not show up in the Variables list within a FlexConfig object. Also, you do not add them using the **Insert** menu in the FlexConfig object editor.
- Secret key variables are replaced with the single string defined for the variable within the FlexConfig object.

Variables start with the $ character, except for secret keys, which start with the @ character. For example, $ifname is a policy object variable in this command, whereas @keyname is a secret key.

```
interface $ifname
key @keyname
```

Note The first time you insert a policy object or system variable, you must do so through the **Insert** menu in the FlexConfig object editor. This action adds the variable to the **Variables** list at the bottom of the FlexConfig object editor. You must type in the variable string on subsequent uses, even when using system variables. If you are adding a processing variable, which does not have an object or system variable assignment, do not use the **Insert** menu. If you are adding a secret key, always use the **Insert** menu. Secret key variables do not show up in the Variables list.

Whether a variable is resolved as a single string, a list of strings, or a table of values depends on the type of policy object or system variable you assign to the variable. (Secret keys always resolve to a single string.) You must understand what will be returned in order to process the variables correctly.

Variable processing

At runtime, a variable can resolve to any of these: a single string; a list of strings of the same type; a list of strings of different types; or a table of named values. Variables that resolve to multiple values can have a determinate or indeterminate length. To process the values correctly, you must understand what will be returned.

The main possibilities include these scenarios.

Single value variables

If a variable always resolves to a single string, use the variable directly without modification in the FlexConfig script.

For example, the predefined text variable tcpMssBytes always resolves to a single value (which must be numeric). The **Sysopt_basic** FlexConfig then uses an if/then/else structure to set the maximum segment size based on the value of another single-value text variable, *tcpMssMinimum*.

Implementation methods

The implementation of single value variables depends on the variable type:

- **Standard text variables**: Use the variable directly in the FlexConfig script. For example, the predefined text variable tcpMssBytes always resolves to a single numeric value.
- **Secret key variables**: Always use the **Insert** menu to add the variable, even for second and subsequent uses. These variables do not show up in the Variables list within the FlexConfig object.
- **Policy object variables for network objects**: Equate to a single IP address specification (host address, network address, or address range). You must know what type of address to expect because ASA commands require specific address types.

Note Policy object variables for network objects also equate to a single IP address specification, either a host address, network address, or address range. However, in this case, you must know what type of address to expect, because the ASA commands require specific address types. For example, if a command requires a host address, using a network object variable that points to an object that contains a network address will result in an error during deployment.

TCP MSS configuration using single value variables

The **Sysopt_basic** FlexConfig uses an if/then/else structure to set the maximum segment size based on the value of another single-value text variable, tcpMssMinimum:

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

In this example, you would use the **Insert** menu in the FlexConfig object editor to add the first use of $tcpMssBytes, but you would type in the variable directly on the #else line.

Multiple value variables with same type values

Several policy object and system variables resolve to multiple values of the same type. For example, an object variable that points to a network object group resolves to a list of the IP addresses within the group. Similarly, the system variable $SYS_FW_INTERFACE_NAME_LIST resolves to a list of interface names.

You can also create text objects for multiple values of the same type. For example, the predefined text object enableInspectProtocolList can contain more than one protocol name.

Processing characteristics

Multiple value variables that resolve to a list of items of the same type are frequently of indeterminate length. For example, you cannot know beforehand how many interfaces on a device are named, as users can configure or unconfigure interfaces at any time.

You would typically use a loop to process multiple value variables of the same type. For example, the predefined FlexConfig **Default_Inspection_Protocol_Enable** uses a #foreach loop to go through the enableInspectProtocolList object and process each value.

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

In this example, the script assigns each value in turn to the $protocol variable, which is then used in an ASA **inspect** command to enable the inspection engine for that protocol. In this case, you simply type in $protocol as a variable NAME. You do not use the **Insert** menu to add it, because you are not assigning an object or system value to the variable. However, you must use the **Insert** menu to add $enableInspectProtocolList.

The system loops through the code between #foreach and #end until there are no values remaining in $enableInspectProtocolList.

Multiple value variables with different types

You can create multiple value text objects and have each value serve a different purpose. For example, the predefined **netflow_Destination** text object should include three values in this order: interface name, destination IP address, and UDP port number.

Objects defined in this way should have a determinate number of values to make them easier to process.

Processing multiple value variables

Use the get method to process these objects. Type **.get(*n*)** at the end of the object name, replacing *n* with an index into the object. Start counting at 0, even though the text object lists its values starting at 1.

NetFlow destination configuration example

The predefined **netflow_Destination** text object should have 3 values, in order, interface name, destination IP address, and UDP port number.

The Netflow_Add_Destination object uses this line to add the 3 values from netflow_Destination to the ASA **flow-export** command:

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

In this example, you would use the **Insert** menu in the FlexConfig object editor to add the first use of $netflow_Destination, and then add **.get(0)**. But you would type in the variable directly for the **$netflow_Destination.get(1)** and **$netflow_Destination.get(2)** specifications.

Multiple value variables that resolve to a table of values

Some system variables return a table of values. These variables include the string MAP in their names. For example, $SYS_FTD_ROUTED_INTF_MAP_LIST is one such variable. The routed interface map returns data in a table of values. Line breaks have been added for clarity.

Variable structure and processing

These variables return data that includes a table of named values for each item. For example, the ROUTED interface MAP returns data that looks like this (line returns added for clarity):

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]
```

In the above example, information is returned for 4 interfaces. Each interface includes a table of named values. For example, intf_hardwarare_id is the name of the interface hardware name property, and returns strings such as GigabitEthernet0/0.

This type of variable is typically of indeterminate length, so you need to use looping to process the values. You also need to add the property name to the variable name to indicate which value to retrieve.

IS-IS interface configuration

For example, IS-IS configuration requires that you add the ASA **ISIS** command to an interface that has a logical name in interface configuration mode. However, you enter that mode using the interface's hardware name. Thus, you need to identify which interfaces have logical names, then configure just those interfaces using their hardware names. The ISIS_Interface_Configuration predefined FlexConfig does this using an if/then structure nested in a loop. In this code, you can see that the #foreach scripting command loads each interface MAP into the $INTF variable, then the #if statement keys off the intf_logical_name value in the MAP ($INTF.intf_logical_name), and if the value is in the LIST defined in the isisIntfList predefined text variable, enters the interface command using the intf_hardwarare_id value ($INTF.intf_hardwarare_id). You would need to edit the isisIntfList variable to add the names of the interfaces on which to configure IS-IS.

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

Evaluate device variable results

To evaluate what a variable will return by creating a simple FlexConfig object that processes variables and shows their resolved values in a configuration preview.

This method allows you to test and analyze variable resolution without deploying potentially invalid configuration commands to devices.

Procedure

Step 1 Create a simple FlexConfig object that processes an annotated list of variables.

Example:

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST
```

```
Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

Step 2 Assign the FlexConfig object to a FlexConfig policy.

Step 3 Assign the policy to a device.

Step 4 Save the policy.

Step 5 Preview the configuration for that device.

The preview shows the resolved values.

Step 6 Select the preview text, copy it, then paste the output into a text file for analysis.

Example:

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, management]
```



Note Do not deploy this FlexConfig to the device, however, because it will not contain any valid configuration commands. You would get deployment errors. After obtaining the preview, delete the FlexConfig object from the FlexConfig policy and save the policy.

You can analyze the resolved variable values in the text file to understand what each variable returns for the device.

FlexConfig policy object variables

A policy object variable is associated with a specific policy object configured in the Object Manager. When you insert a policy object variable in a FlexConfig object, you give the variable a name and select the object associated with it.

Policy object variable types

Although you can give the variable the exact same name as the associated object, the variable itself is not the same thing as the associated object. You must use the **Insert** > **Insert Policy Object** > ***Object Type*** menu in the FlexConfig object editor to add the variable for the first time to the script in the FlexConfig to establish the association with the object. Simply typing in the name of the object preceded by a $ sign does not create a policy object variable.

You can create variables to point to these types of objects. Ensure that you create the right type of object for each variable. To create objects, go to the **Objects** > **Object Management** page.

- **Text Objects**—For text strings, which can include IP addresses, numbers, and other free-form text such as interface or zone names. Select **FlexConfig** > **Text Object** from the table of contents, then click **Add Text Object**. You can configure these objects to contain a single value or multiple values. These objects are highly flexible and built specifically for use within FlexConfig objects. For detailed information, see Configure FlexConfig text objects, on page 950.
- **Network**—For IP addresses. You can use network objects or groups. Select **Network** from the table of contents, then select **Add Network** > **Add Object** or **Add Group**. If you use a group object, the variable returns a list of each IP address specification within the group. Addresses can be host, network, or address ranges, depending on the object contents. See Networks, on page 2386.
- **Security Zones**—For interfaces within a security zone or interface group. Select **Interface** from the table of contents, then select **Add** > **Security Zone** or **Interface Group**. A security zone variable returns a list of the interfaces within that zone or group for the device being configured. See Interfaces, on page 2383.
- **Standard ACL Object**—For standard access control lists. A standard ACL variable returns the name of the standard ACL object. Select **Access List** > **Standard** from the table of contents, then click **Add Standard Access List Object**. See Access lists, on page 2351.
- **Extended ACL Object**—For extended access control lists. An extended ACL variable returns the name of the extended ACL object. Select **Access List** > **Extended** from the table of contents, then click **Add Extended Access List Object**. See Access lists, on page 2351.

- **Route Map**—For route map objects. A route map variable returns the name of the route map object. Select **Route Map** from the table of contents, then click **Add Route Map**. See Configure a route map, on page 2415.

FlexConfig system variables

System variables are replaced with information obtained from the device itself or from policies configured for it. To add a variable for the first time in the FlexConfig script and establish its association with the system variable, use the **Insert** > **Insert System Variable** > ***Variable NAME*** menu in the FlexConfig object editor. Typing the system variable name with a preceding $ sign does not create a system variable in the context of the FlexConfig object.

Before using a variable, check the typical value it returns. Refer to Evaluate device variable results, on page 930.

Table 65: System variables

NAME	Description
SYS_FW_OS_MODE	The operating system MODE of the device. Possible values are ROUTED or TRANSPARENT.
SYS_FW_OS_MULTIPLICITY	Whether the device is running in SINGLE or multiple context MODE. Possible values are SINGLE, MULTI, or NOT_APPLICABLE.
SYS_FW_MANAGEMENT_IP	The MANAGEMENT IP address of the device
SYS_FW_HOST_NAME	The device hostname
SYS_FTD_INTF_POLICY_MAP	A MAP with INTERFACE NAME as key and POLICY-MAP as value. This variable returns nothing if there are no INTERFACE-based service policies defined on the device.
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	The LIST of protocols for which inspection is ENABLED.
SYS_FTD_ROUTED_INTF_MAP_LIST	A LIST of ROUTED INTERFACE maps on the device. Each MAP includes a set of named values related to ROUTED INTERFACE configuration.
SYS_FTD_SWITCHED_INTF_MAP_LIST	A LIST of SWITCHED INTERFACE maps on the device. Each MAP includes a set of named values related to SWITCHED INTERFACE configuration.
SYS_FTD_INLINE_INTF_MAP_LIST	A LIST of INLINE INTERFACE maps on the device. Each MAP includes a set of named values related to INLINE set INTERFACE configuration.
SYS_FTD_PASSIVE_INTF_MAP_LIST	A LIST of PASSIVE INTERFACE maps on the device. Each MAP includes a set of named values related to PASSIVE INTERFACE configuration.
SYS_FTD_INTF_BVI_MAP_LIST	A LIST of Bridge Virtual INTERFACE maps on the device. Each MAP includes a set of named values related to BVI configuration.

NAME	Description
SYS_FW_INTERFACE_HARDWARE_ID_LIST	A LIST of the HARDWARE names for interfaces on the device, such as GigabitEthernet0/0.
SYS_FW_INTERFACE_NAME_LIST	A LIST of logical names for interfaces on the device, such as inside.
SYS_FW_INLINE_INTERFACE_NAME_LIST	A LIST of logical names for interfaces configured as PASSIVE or ERSPAN PASSIVE.
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	A LIST of logical names for interfaces that are NOT part of INLINE sets, such as all ROUTED interfaces.

Predefined FlexConfig objects

The predefined FlexConfig objects provide tested configurations for select features. Use these objects if you need to configure these features, which otherwise cannot be configured using the management center. Note that some objects might become obsolete as features are added to the GUI.

This table lists the available objects. Make note of the associated text objects. You must edit these text objects to customize the behavior of the predefined FlexConfig object. The text objects make it possible for you to customize the configuration using the IP addresses and other attributes required by your network and device.

If you need to modify a predefined FlexConfig object, copy the object, make changes to the copy, and save it with a new name. You cannot directly edit a predefined FlexConfig object.

Although you might be able to configure other ASA-based features using FlexConfig, the configuration of those features has not been tested. If an ASA feature overlaps with something that you can configure in Firewall Management Center policies, do not attempt to configure it through FlexConfig.

For example, Snort inspection includes the HTTP protocol, so do not enable ASA-style HTTP inspection. You cannot add **http** to the enableInspectProtocolList object; this restriction prevents you from misconfiguring your device. Instead, configure the access control policy to perform application or URL filtering, as needed, to implement your HTTP inspection requirements.

Table 66: Predefined FlexConfig objects

FlexConfig Object Name	Description	Associated Text Objects
Default_Inspection_Protocol_Disable	Disables protocols in the global_policy default policy map.	disableInspectProtocolList
Default_Inspection_Protocol_Enable	Enables protocols in the global_policy default policy map.	enableInspectProtocolList
Inspect_IPv6_Configure	Configures IPv6 inspection in the global_policy policy map, logging and dropping traffic based on IPv6 header contents.	IPv6RoutingHeaderDropLogList, IPv6RoutingHeaderLogList, IPv6RoutingHeaderDropList.
Inspect_IPv6_UnConfigure	Clears and disables IPv6 inspection.	—

FlexConfig Object Name	Description	Associated Text Objects
ISIS_Configure	Configures global parameters for IS-IS routing.	isIsNet, isIsAddressFamily, isISType
ISIS_Interface_Configuration	Interface level IS-IS configuration.	isIsAddressFamily, IsIsIntfList Also uses the system variable SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	Clears the IS-IS router configuration on the device.	—
ISIS_Unconfigure_All	Clears the IS-IS router configuration from the device, including the router assignment from the device interface.	—
NGFW_TCP_NORMALIZATION	Modifies the default TCP normalization configuration.	—
Policy_Based_Routing	To use this example configuration, copy it, modify the interface name, and use the r-map-object text object to identify a route map object in the object manager.	—
Policy_Based_Routing_Clear	Clears Policy Based Routing configurations from the device.	—
Sysopt_AAA_radius	Ignores the authentication key in RADIUS accounting responses.	—
Sysopt_AAA_radius_negate	Negates the Sysopt_AAA_radius configuration.	—
Sysopt_basic	Configures sysopt wait time , maximum segment size for TCP packets, and detailed traffic statistics.	tcpMssMinimum, tcpMssBytes
Sysopt_basic_negate	Clears sysopt_basic detailed traffic statistics, wait time, and TCP maximum segment size.	—
Sysopt_clear_all	Clears all sysopt configurations from the device.	—
Sysopt_noproxyarp	Configures noproxy-arp CLIs.	Uses system variable SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	Clears Sysopt_noproxyarp configurations.	Uses system variable SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	Configures syopt preserve VPN flow.	—
Sysopt_Preserve_Vpn_Flow_negate	Clears the Sysopt_Preserve_Vpn_Flow configuration.	—

FlexConfig Object Name	Description	Associated Text Objects
Sysopt_Reclassify_Vpn	Configures sysopt reclassify vpn.	—
Sysopt_Reclassify_Vpn_Negate	Negates sysopt reclassify vpn.	—
Threat_Detection_Clear	Clear the threat detection TCP Intercept configuration.	—
Threat_Detection_Configure	Configure threat detection statistics for attacks intercepted by TCP Intercept.	threat_detection_statistics
Wccp_Configure	This template provides an example for configuring WCCP.	isServiceIdentifier, serviceIdentifier, wccpPassword
Wccp_Configure_Clear	Clears WCCP configurations.	—

Deprecated FlexConfig objects

This table lists objects that configure features you can now configure natively in the GUI. Discontinue using these objects at the earliest convenience.

Table 67: Deprecated predefined FlexConfig objects

Deprecated Version	FlexConfig Object	Description	Now Configure In
7.3	DHCPv6_Prefix_Delegation_Configure	Configure one outside (Prefix Delegation client) and one inside interface (recipient of delegated prefix) for IPv6 prefix delegation. To use this template, copy it and modify the variables. Associated text objects: pdoutside, pdinside Also uses the system variable SYS_FTD_ROUTED_INTF_MAP_LIST	Interface IPv6 Settings.
7.3	DHCPv6_Prefix_Delegation_UnConfigure	Removes the DHCPv6 prefix delegation configuration.	Interface IPv6 Settings.
6.3	Default_DNS_Configure	Configure the Default DNS group, which defines the DNS servers that can be used when resolving fully-qualified domain names on the data interfaces. Associated text objects: defaultDNSNameServerList, defaultDNSParameters	Platform settings.

Deprecated Version	FlexConfig Object	Description	Now Configure In
6.3	DNS_Configure	Configure DNS servers in a non-default DNS server group. Copy the object to change the name of the group.	**DNS Server Group** in the object manager.
6.3	DNS_UnConfigure	Removes the DNS server configuration performed by Default_DNS_Configure and DNS_Configure. Copy the object to change the DNS server group names if you altered DNS_Configure.	**DNS Server Group** in the object manager.
7.2	Eigrp_Configure	Configures EIGRP routing next-hop, auto-summary, router-id, eigrp-stub. Associated text objects: eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary	For all EIGRP objects, see EIGRP, on page 1095. The system does allow you to deploy post-upgrade, but also warns you to redo your EIGRP configurations. To help you with this process, we provide a command-line migration tool.
7.2	Eigrp_Interface_Configure	Configures EIGRP interface authentication mode, authentication key, hello interval, hold time, split horizon. Associated text objects: eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon Also uses the system variable SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	Clears EIGRP configuration for an autonomous system from the device.	
7.2	Eigrp_Unconfigure_all	Clears all EIGRP configurations.	
7.4	Netflow_Add_Destination	Creates and configures a Netflow export destination. Associated text objects: Netflow_Destinations, netflow_Event_Types	Platform settings.
7.4	Netflow_Clear_Parameters	Restores Netflow export global default settings.	Platform settings.

Deprecated Version	FlexConfig Object	Description	Now Configure In
7.4	Netflow_Delete_Destination	Deletes a Netflow export destination. Associated text objects: Netflow_Destinations, netflow_Event_Types	Platform settings.
7.4	Netflow_Set_Parameters	Sets global parameters for Netflow export. Associated text objects: netflow_Parameters	Platform settings.
6.3	TCP_Embryonic_Conn_Limit	Configures embryonic connection limits to protect against SYN Flood Denial of Service (DoS) attacks. Associated text objects: tcp_conn_misc, tcp_conn_limit	Service policy.
6.3	TCP_Embryonic_Conn_Timeout	Configures embryonic connection timeouts to protect against SYN Flood Denial of Service (DoS) attacks. Associated text objects: tcp_conn_misc, tcp_conn_timeout	Service policy.
7.2	VxLAN_Clear_Nve	Removes the NVE 1 configured when VxLAN_Configure_Port_And_Nve is used from the device.	For all VxLAN objects, see Configure VXLAN Interfaces, on page 671. If you configured VXLAN interfaces with FlexConfig in a previous version, they continue to work. In fact, FlexConfig takes precedence in this case—if you redo your VXLAN configurations in the web interface, remove the FlexConfig settings.
7.2	VxLAN_Clear_Nve_Only	Clears the NVE configured on the interface when deployed.	
7.2	VxLAN_Configure_Port_And_Nve	Configures VLAN port and NVE 1. Associated text objects: vxlan_Port_And_Nve	

Deprecated Version	FlexConfig Object	Description	Now Configure In
7.2	VxLAN_Make_Nve_Only	Sets an interface for NVE only. Associated text objects: vxlan_Nve_Only Also uses system variables SYS_FTD_ROUTED_MAP_LIST and SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	Creates a VNI interface. After deploying this you have to unregister and re-register the device to properly discover the VNI interface. Associated text objects: vxlan_Vni	

Predefined text objects

There are several predefined text objects. These objects are associated with variables used in the predefined FlexConfig objects. In most cases, you must edit these objects to add values if you use the associated FlexConfig object, or you will see errors during deployment. Although some of these objects contain default values, others are empty.

For information on editing text objects, refer to Configure FlexConfig text objects, on page 950.

Name	Description	Associated FlexConfig Object
defaultDNSNameServerList (Deprecated.)	The DNS server IP address to configure in the Default DNS group. Starting with version 6.3, configure DNS for the data interfaces in the Threat Defense Platform Settings policy.	Default_DNS_Configure
defaultDNSParameters (Deprecated.)	The parameters to control DNS behavior for the default DNS server group. The object contains separate entries, in order, for retries, timeout, expire-entry-timer, poll-timer, domain-name. Starting with version 6.3, configure DNS for the data interfaces in the Threat Defense Platform Settings policy.	Default_DNS_Configure
disableInspectProtocolList	Disables protocols in the default policy map (global_policy).	Disable_Default_Inspection_Protocol
dnsNameServerList	The DNS server IP address to configure in a user-defined DNS group.	DNS_Configure

Name	Description	Associated FlexConfig Object
dnsParameters	The parameters to control DNS behavior for a non-default DNS server group. The object contains separate entries, in order, for retries, timeout, domain-name, name-server-interface.	DNS_Configure
enableInspectProtocolList	Enables protocols in the default policy map (global_policy). You are prevented from adding protocols whose inspection conflicts with Snort inspection.	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	The list of IPv6 routing header types that you want to disallow. IPv6 inspection drops packets that contain these headers without logging the drop.	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	The list of IPv6 routing header types that you want to disallow and log. IPv6 inspection drops packets that contain these headers and sends a syslog message about the drop.	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	The list of IPv6 routing header types that you want to allow but log. IPv6 inspection allows packets that contain these headers, but sends a syslog message about the existence of the header.	Inspect_IPv6_Configure
isIsAddressFamily	The IPv4 or IPv6 address family.	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	List of logical interface names.	ISIS_Interface_Configuration
isIsISType	IS Type (level-1, level-2-only or level-1-2).	ISIS_Configure
isIsNet	Network entity.	ISIS_Configure
isServiceIdentifier	When false, uses the standard **web-cache** service identifier.	Wccp_Configure
netflow_Destination	Defines a single NetFlow export destination's interface, destination, and UDP port number.	Netflow_Add_Destination
netflow_Event_Types	Defines the types of events to be exported for a destination as any subset of: **all**, **flow-create**, **flow-defined**, **flow-teardown**, **flow-update**.	Netflow_Add_Destination

Name	Description	Associated FlexConfig Object
netflow_Parameters	Provides the NetFlow export global settings: active refresh interval (number of minutes between flow update events), delay (flow create delay in seconds; default 0 = command will not appear), and template time-out rate in minutes.	Netflow_Set_Parameters
PrefixDelegationInside	Configures the inside interface for DHCPv6 prefix delegation. The object includes multiple entries, in order, interface name, IPv6 suffix with prefix length, and prefix pool name.	None, but could be used with a copy of DHCPv6_Prefix_Delegation_Configure.
PrefixDelegationOutside	Configure the outside DHCPv6 prefix delegation client. The object includes multiple entries, in order, interface name and IPv6 prefix length	None, but could be used with a copy of DHCPv6_Prefix_Delegation_Configure.
serviceIdentifier	Dynamic WCCP service identifier number.	Wccp_Configure
tcp_conn_limit (Deprecated.)	Parameters used for configuring the TCP embryonic connection limits. Starting with version 6.3, configure these features in the Threat Defense Service Policy, which you can find on the Advanced tab of the access control policy assigned to the device.	TCP_Embryonic_Conn_Limit
tcp_conn_misc (Deprecated.)	Parameters used for configuring the TCP embryonic connection settings. Starting with version 6.3, configure these features in the Threat Defense Service Policy, which you can find on the Advanced tab of the access control policy assigned to the device.	TCP_Embryonic_Conn_Limit, TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (Deprecated.)	Parameters used for configuring the TCP embryonic connection timeouts. Starting with version 6.3, configure these features in the Threat Defense Service Policy, which you can find on the Advanced tab of the access control policy assigned to the device.	TCP_Embryonic_Conn_Timeout
tcpMssBytes	Maximum segment size in bytes.	Sysopt_basic
tcpMssMinimum	Checks whether to set maximum segment size (MSS), which is set only if this flag is true.	Sysopt_basic

Name	Description	Associated FlexConfig Object
threat_detection_statistics	Parameters used for threat detection statistics for TCP Intercept.	Threat_Detection_Configure
vxlan_Nve_Only	Parameters for configuring NVE-only on interface: • logical name of interface • IPv4 address (optional for routed interface) • IPv4 netmask (optional for routed interface)	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	Parameters used for configuring ports and NVE for VXLAN: • vxlan port • source interface (logical name) • type (peer or mcast) • Peer IP Address or default-mcast-group	VxLAN_Configure_Port_And_Nve
vxlan_Vni	Parameters used for creating VNI: • Interface number (1-10000) • segment-id (1-16777215) • nameif (Logical Name of the interface) • type (routed or transparent) • IP address (used in case of routed mode device) or bridge-group number (used in case of transparent mode device) • netmask (If device is in routed mode) or unused	VxLAN_Make_Vni
wccpPassword	WCCP password.	Wccp_Configure

Requirements and prerequisites for FlexConfig policies

This topic outlines the model support, domain requirements, and user role prerequisites required to configure and deploy FlexConfig policies.

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

Guidelines and limitations for FlexConfig

Be cautious with FlexConfig deployments, as configuration mistakes trigger rollbacks that can disrupt your network.

- If you make a mistake in the FlexConfig policy, the system will roll back all changes included in the deployment attempt that includes the failed FlexConfig. Because rollback due to a failed deployment includes clearing the configuration, this can be disruptive to your network.
- Consider timing deployments that include FlexConfig changes to non-business hours. Also, consider isolation the deployment so it includes just FlexConfig changes, and no other policy updates.

When you use the VxLAN_Make_VNI object, you must deploy the same FlexConfig to all units in a cluster or high availability pair before you form the cluster or high availability pair. The Management Center requires the VXLAN interfaces to match on all devices before forming the cluster or high availability pair.

The **webvpn keepout** command must be configured only within the global webvpn configuration mode. The webvpn group-policy attributes or username attributes configuration modes do not support the **keepout** command. Do not include the **keepout** command in a group-policy FlexConfig object.

If you configure any service that applies to connections, such as SIP inspection, go to the device CLI and enter the **clear conn** command to clear connections. When the connections are rebuilt, the new configuration is applied to the sessions.

QoS rules and service policy rules (in the access control policy) are translated to commands on the firewall. This includes creating policy maps. There can be only one policy map per interface. The system automatically combines QoS and service policy configurations in a single policy map per interface.

However, you can also create policy maps manually using FlexConfig. For lower-end firewalls, such as the Secure Firewall 3100, you can create up to 64 policy maps in the configuration. For more powerful firewalls, such as the Firepower 4100, you can create up to 128. Be careful not to exceed this limit, or deployment will fail. You can view the device configuration from the CLI or use the deployment transcript to see how rules are translated to commands.

Customize device configuration with FlexConfig policies

Use FlexConfig policies to customize the configuration of a Firewall Threat Defense device when standard configuration methods are insufficient.

Before using FlexConfig, try to configure all the policies and settings you need using the other features in Firewall Management Center. FlexConfig is a method of last resort to configure ASA-based features that are

compatible with Firewall Threat Defense but which are not otherwise configurable in Firewall Management Center.

Before you begin

Follow these steps to customize device configuration with FlexConfig policies:

Procedure

Step 1 Determine the CLI command sequence that you want to configure.

If you have a functioning configuration on an ASA device, use **show running-config** to get the sequence of commands that you need. Make adjustments to items such as interface names and IP addresses as needed.

If this is for a new feature, it is best to try to implement it on an ASA device in a lab setting to verify that you have the correct command sequence.

For more information, see the following topics:

- Recommended usage for FlexConfig policies, on page 922
- CLI commands in FlexConfig objects, on page 922

Step 2 Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

Examine the predefined FlexConfig objects to determine if any will be able to generate the commands you need. Click **View** (🔍) to see the object contents. If an existing object is close to what you want, start by making a copy of the object, and then edit the copy. See Predefined FlexConfig objects, on page 934.

Examining the objects will also give you an idea of the structure, command syntax, and expected sequencing for a FlexConfig object.

Note If you find any objects that you will use, either directly or as copies, examine the Variables list at the bottom of the object. Make note of the variable names, except those in all capitals that start with SYS, which are system variables. These variables are text objects that you will probably need to edit and define overrides for, especially if the default value column shows the object has no value.

Step 3 If you need to create your own FlexConfig objects, determine what variables you will need and create the associated objects.

The CLI you need to deploy might contain IP addresses, interface names, port numbers, and other parameters that you might want to adjust over time. These are best isolated into variables, which point to objects that contain the necessary values. You might also need variables for strings that are part of the configuration and could change over time.

Also, determine if you need different values for each device to which you will assign the policy. For example, you might want to configure the feature on three devices, but you might need to specify a different interface name or IP address on a given command for each of these devices. If you need to customize the object for each device, ensure that you enable overrides when creating the object and then define the override values per device.

See the list of topics for an explanation of the various types of variables and how to configure the related objects when necessary.

- FlexConfig variables, on page 926
- FlexConfig policy object variables, on page 932
- FlexConfig system variables, on page 933
- Configure FlexConfig text objects, on page 950

Step 4 If you are using the predefined FlexConfig objects, edit the text objects used as variables.

See Configure FlexConfig text objects, on page 950.

Step 5 (If necessary) Configure FlexConfig objects, on page 945.

You need to create objects only if the predefined objects cannot do the job.

Step 6 Configure the FlexConfig policy, on page 951.

a) Set target devices for a FlexConfig policy, on page 952.

You can also assign the policy to devices when you create the policy. The policy must have at least one assigned device before you can preview it.

b) Preview the FlexConfig policy, on page 953.

You must save changes before you can preview the policy.

Verify that the generated commands are the ones intended, and that all variables are resolving correctly.

Step 7 Choose **Deploy** > **Deployment** in the menu bar.

a) Select the devices assigned to the policy, and click **Deploy**.

Wait for deployment to complete.

Step 8 Verify the deployed configuration, on page 954.

Step 9 (If necessary) Remove features configured using FlexConfig, on page 956.

Unlike other types of policy, simply unassigning a FlexConfig from a device might not remove the related configuration. If you want to remove a FlexConfig-generated configuration, follow the cited procedure.

If you are removing a feature because it is now directly supported by the product, check Convert from FlexConfig to managed feature, on page 958.

Configure FlexConfig objects

Before you begin

Keep the following in mind:

- FlexConfig objects translate into commands that are then deployed to the device. These commands are already issued in global configuration mode. Therefore, do not include the **enable** and **configure terminal** commands as part of the FlexConfig object.

- Determine what types of variables you will need, and create any policy objects that you will require. You cannot create objects for variables while editing a FlexConfig object.
- Ensure that your commands do not conflict in any way with the VPN or access control configuration on the devices.
- If there is more than one set of commands for an interface, only the last set of commands is deployed. Therefore, we recommend you not use beginning and ending commands to configure interfaces. For an example of configuring interfaces, refer to the ISIS_Interface_Configuration predefined FlexConfig object.

There are several predefined FlexConfig objects that you can use directly, or you can make copies if you need to edit them. You can also create your own objects from scratch. A FlexConfig object's content can range from a single simple command string to elaborate CLI command structures that use variables and scripting commands to deploy commands whose content can differ from device to device or deployment to deployment.

You can also create FlexConfig policy objects when defining FlexConfig policies.

Procedure

Step 1 Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** .

Step 2 Do one of the following:

- Click **Add FlexConfig Object** to create a new object.
- Click **Edit** ( ) to edit an existing object.
- Click **View** ( ) to see the contents of a predefined object.
- If you want to edit a predefined object, click **Clone** ( ) to create a new object with the same contents.

Step 3 Enter a **Name** and optionally, a description for the object.

Step 4 In the object body area, enter the commands and instructions to produce the required configuration.

The object content is a sequence of scripting commands and configuration commands that generate a valid ASA software command sequence. The Firewall Threat Defense device uses ASA software commands to configure some features. For more information on scripting and configuration commands, refer to:

- Template scripts, on page 926
- CLI commands in FlexConfig objects, on page 922

You can use variables to supply information that can be known only at runtime, or which can differ from device to device. You simply type in processing variables, but you must use the **Insert** menu to add variables that are associated with policy objects or system variables, or which are secret keys. For a complete discussion of variables, refer to FlexConfig variables, on page 926 .

- To insert system variables, choose **Insert** > **Insert System Variable** > ***Variable Name*** . For a detailed explanation of these variables, see FlexConfig system variables, on page 933 .
- To insert policy object variables, choose **Insert** > **Insert Policy Object** > ***Object Type*** , selecting the appropriate type of object. Then, give the variable a name (which can be the same name as the associated policy object), select the object to associate with the variable, and click **Save** . For a detailed explanation

of these types, see FlexConfig policy object variables, on page 932 . For more detail on the procedure, see Add a policy object variable to a FlexConfig object, on page 948 .

- To insert secret key variables, choose **Insert** > **Secret Key** and define the variable name and value. For more detail on the procedure, see Configure secret keys, on page 949 .

Note You must use the **Insert** menu to create a new policy object or system variable. However, for subsequent uses of that variable, you must type it in, $ included. This is also true for system variables: the first time you use it, add it from the **Insert** menu. Then, type it out for subsequent uses. If you use the **Insert** menu more than once for a system variable, the system variable is added to the Variables list multiple times, and the FlexConfig will not validate, meaning you cannot save your changes. For processing variables (those not associated with a policy object or system variable), simply type in the variable. If you are adding a secret key, always use the **Insert** menu. Secret key variables do not show up in the Variables list.

Step 5 Choose the deployment frequency and type.

- **Deployment** —Whether to deploy the commands in the object **Once** or **Everytime** . The only way to choose the right option is to test the results of deployment.

  Start by selecting **Everytime** . Then, after you attach the object to a FlexConfig policy, deploy the configuration. After a successful deployment, come back to the FlexConfig policy and preview the configuration for one of the assigned devices as described in Preview the FlexConfig policy, on page 953 . If the section labeled `###CLI generated from managed features ###` contains commands that clear or negate the commands in the object, and the `###Flex-config Appended CLI ###` section contains the commands to reconfigure the feature, you know that **Everytime** is the right option.

  Even if you do not see negate commands, make some minor change to the device configuration, then run another deployment. If the deployment completes successfully, you can check the deployment transcript (see Verify the deployed configuration, on page 954). If you see that the commands were issued again (even when they were already configured) without error, then you can keep **Everytime** .

  Change to **Once** only if the system does not first negate the commands in the object before issuing them again, or if the deployment results in errors that are specific to the command. In some cases, the system does not allow you to issue a command that is already configured, but this is the exception.

  Some additional tips:

  - If the FlexConfig object points to system-managed objects such as network or ACL objects, choose **Everytime** . Otherwise, updates to the objects might not get deployed.
  - Use **Once** if the only thing you do in the object is to clear a configuration. Then, remove the object from the FlexConfig policy after the next deployment.

- **Type** —Select one of the following:
  - **Append** —(The default.) Commands in the object are put at the end of the configurations generated from the Firewall Management Center policies. You must use Append if you use policy object variables, which point to objects generated from managed objects. If commands generated for other policies overlap with those specified in the object, you should select this option so your commands are not overwritten. This is the safest option.

- **Prepend** —Commands in the object are put at the beginning of the configurations generated from the Firewall Management Center policies. You would typically use prepend for commands that clear or negate a configuration.

Step 6 (Optional.) Click **Validate** ( ) above the object body to check the integrity of the script.

The object is always validated when you click **Save**. You cannot save an invalid object.

Step 7 Click **Save** .

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Add a policy object variable to a FlexConfig object

Insert variables into a FlexConfig policy object that are associated with other types of policy object, allowing the variables to resolve to the names or content of the associated object when the FlexConfig is deployed to a device.

You can insert variables into a FlexConfig policy object that are associated with other types of policy object. When the FlexConfig is deployed to a device, these variables resolve to the names or content of the associated object.

Use the following procedure for the first use of a policy object variable in a FlexConfig object. If you need to refer to the object again, type in the variable (including the $ sign). To understand how to use these variables, see Variable processing, on page 927.

Before you begin

For information on editing a FlexConfig Object, see Configure FlexConfig objects, on page 945.

Procedure

Step 1 While editing a FlexConfig Policy Object, choose **Insert** > **Insert Policy Object** > ***Object Type***, selecting the appropriate type of object.

Step 2 Enter a name for the variable, and optionally, a description.

The name must be unique within the context of the FlexConfig object. It cannot include spaces. You are allowed to use the exact same name as the object associated with the variable.

Step 3 Select the object to associate with the variable and click **Add** to move it to the **Selected Object** list.

You can associate a variable with a single object only.

Note For text objects, you can select any of the predefined objects as needed. However, many of these objects have no default values. You must update the objects to add the required values either directly or as overrides for the device to which you will deploy the FlexConfig object. Trying to deploy a FlexConfig without updating these objects typically results in deployment errors.

Step 4 Click **Save**.

The variable appears in the Variables list at the bottom of the FlexConfig object editor.

Configure secret keys

Secret keys allow you to mask sensitive information such as passwords in FlexConfig objects, preventing the dissemination of sensitive information while providing special treatment for these variables.

A secret key is any single-string variable whose content you want to mask, such as passwords. The system provides special treatment for these variables to help you prevent the dissemination of sensitive information.

Secret key variables do not show up in the Variables list in the FlexConfig object.

Unlike other types of variables, you can use the **Insert** command every time you need to insert a given secret key variable. With respect to processing, these variables behave like single-value text object variables; see Single value variables, on page 927.

Note Any data defined in a secret key variable is masked from users except when previewing a FlexConfig policy. In addition, if you export a FlexConfig policy, the content of any secret key variable is erased. When you import the policy, you will need to manually edit each secret key variable to enter the data.

Before you begin

For information on editing a FlexConfig Object, see Configure FlexConfig objects, on page 945.

Procedure

Step 1 While editing a FlexConfig Policy Object, choose **Insert** > **Secret Key**.

Step 2 In the **Insert Secret Key** dialog box, do any of the following:

- To create a new key, click **Add Secret Key**, then fill in the following information and click **Add**.
  - **Secret Key Name**—The name of the variable. This name appears in the FlexConfig object prefixed with @.
  - **Password**, **Confirm Password**—The secret string, which is masked with asterisks as you type.
- To insert a secret key variable in the FlexConfig object, select the check box for the variable.

- To edit the value of a secret key variable, click **Edit** ( ) for the variable. Make your changes and click **Add**.
- To delete a secret key variable, click **Delete** ( ) for the variable.

Step 3 Click **Save**.

Configure FlexConfig text objects

Use text objects in FlexConfig objects as the target of policy object variables. During deployment, variables that point to text objects are replaced by the content of the text object.

Use text objects in FlexConfig objects as the target of policy object variables. You can use variables to supply information that can be known only at runtime, or which can differ from device to device. During deployment, variables that point to text objects are replaced by the content of the text object.

Text objects contain free-form strings, which can be keywords, interface names, numbers, IP addresses, and so forth. The content depends on how you will use the information within a FlexConfig script.

Before creating or editing a text object, determine exactly what content you will need. This includes how you intend to process the object, which will help you decide between creating a single string or multiple string object. Read the following topics:

- FlexConfig variables, on page 926
- Variable processing, on page 927

Procedure

Step 1 Choose **Objects** > **Object Management** > **FlexConfig** > **Text Object**.

Step 2 Do one of the following:

- Click **Add Text Object** to create a new object.
- Click **Edit** ( ) to edit an existing object. You are allowed to edit the predefined text objects, which is required if you intended to use the predefined FlexConfig objects.

Step 3 Enter a **Name** and optionally, a description for the object.

Step 4 (New objects only.) Choose a **Variable Type** from the drop-down list:

- **Single**—If the object should contain a single text string.
- **Multiple**—If the object should contain a list of text strings.

You cannot change the variable type after you save the object.

Step 5 If the variable type is **Multiple**, use the up and down arrows to specify a **Count**.

Rows are added or removed from the object as you change the number.

Step 6 Add content to the object.

You can either click in the text box next to a variable number and type in a value, or you can set up device overrides for each device that will be assigned a FlexConfig object that uses the text object. You can also do both, in which case the values configured in the base object act as default values in cases where an override does not exist for a given device.

When editing predefined objects, it is a good practice to use device overrides, so that the system defaults remain in place for other users who might need to use the object in different FlexConfig policies. The approach you take depends on the requirements of your organization.



Tip Some predefined objects require multiple values where each value serves a specific purpose. Read the description text carefully to determine the expected values in the object. In some cases, the instructions specify that you must use overrides instead of changing the base values. In the case of enableInspectProtocolList, you are prevented from entering protocols whose inspection is incompatible with Snort inspection.

If you decide to use device overrides, do the following.

a) Check the check box of **Allow Overrides**.
b) Expand the Overrides area (if necessary) and click **Add**.

   If an override already exists for the device, click edit for the override to change it.

c) On **Targets** in the Add Object Override dialog box, select the device for which you are defining values and click **Add** to move it to the Selected Devices list.
d) Click **Override**, adjust the **Count** as needed, then click in the variable fields and type in the values for the device.
e) Click **Add**.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Configure the FlexConfig policy

Configure a FlexConfig policy to manage device configurations using shared policies that can be assigned to multiple devices.

A FlexConfig policy contains two ordered lists of FlexConfig objects, one prepended list and one appended list. For an explanation of prepend/append, see Configure FlexConfig objects, on page 945.

FlexConfig policies are shared policies that you can assign to multiple devices.

Procedure

Step 1 Choose **Devices** > **FlexConfig**.

Step 2 Do one of the following:

- Click **New Policy** to create a new FlexConfig Policy. You are prompted to enter a name. Optionally, select devices in the Available Devices list and click **Add to Policy** to assign devices. Click **Save**.
- Click **Edit** ( ) to edit an existing Policy. You can change the name or description by clicking them in edit mode.
- Click **Copy** ( ) to create a new policy with the same contents. You are prompted for a name. Device assignments are not retained for the copy.
- Click delete to remove a policy you no longer need.

Step 3 Select the FlexConfig objects required for the policy from the **Available FlexConfig** list and click > to add them to the policy.

Objects are automatically added to the prepended or appended list based on the deployment type specified in the FlexConfig object.

To remove a selected object, click **Delete** ( ) next to an object.

Step 4 For each selected object, click **View** ( ) next to the object to identify the variables used in the object.

Except for system variables, which start with SYS, you need to ensure that the objects associated with the variables are not empty. A blank or brackets with nothing between them, [ ], indicate an empty object. You will need to edit these objects before deploying the policy.

Note If you use object overrides, those values will not show up in this view. Thus, an empty default value does not necessarily mean that you have not updated the object with the required values. Previewing the configuration will show whether the variables resolve correctly for a given device. See Preview the FlexConfig policy, on page 953.

Step 5 Click **Save**.

What to do next

- Set target devices for the policy; see Set target devices for a FlexConfig policy, on page 952.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Set target devices for a FlexConfig policy

This task allows you to assign or change device assignments for a FlexConfig policy after creation.

When you create a FlexConfig policy, you can select the devices that use the policy. You can subsequently change device assignments for the policy as described below.

Note Normally, when you unassign a policy from a device, the system automatically removes the associated configuration upon the next deployment. However, because FlexConfig objects are scripts for deploying customized commands, simply unassigning a FlexConfig policy from a device does not remove the commands that were configuring by the FlexConfig objects. If your intention is to remove FlexConfig-generated commands from a device's configuration, refer to Remove features configured using FlexConfig, on page 956.

Procedure

Step 1 Choose **Devices** > **FlexConfig** and edit a FlexConfig policy.

Step 2 Click **Policy Assignments**.

Step 3 On **Targeted Devices**, build your target list:

- Add—Choose one or more **Available Devices**, then click **Add to Policy** or drag and drop into the list of **Selected Devices**. You can assign the policy to devices, high availability pairs, and clustered devices.
- Delete—Click **Delete** ( ) next to a single device, or select multiple devices, right-click, then choose **Delete Selection**.

Step 4 Click **OK** to save your selection.

Step 5 Click **Save** to save the FlexConfig policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Preview the FlexConfig policy

The FlexConfig policy preview allows you to validate and troubleshoot your configuration before deployment. It translates FlexConfig objects into CLI commands and resolves variables based on device-specific configurations.

Preview a FlexConfig policy to see how the FlexConfig objects get translated into CLI commands. The preview shows the commands that will be generated for a selected device from the scripts and variables used in the FlexConfig objects. The variables are resolved based on the configuration for the device, so you get a clear idea of what will be deployed.

Use the preview to look for potential problems in the FlexConfig objects. Correct the objects until the preview shows the expected results.

You must preview the configuration separately for each device, because the variables can resolve differently based on the device configuration.

Procedure

Step 1 Choose **Devices** > **FlexConfig** and edit a FlexConfig policy.

Step 2 If there are any pending changes, click **Save**.

The preview shows results only for those FlexConfig objects that were in the most recently saved version of the policy. You must save the policy to see a preview of newly-added objects.

Step 3 Click **Preview Config**.

Step 4 Choose a device from the **Select Device** drop-down list.

The system retrieves information from the device and configured policies, and determines what CLI commands will be generated on the next deployment to the device. You can select the output and use Ctrl+C to copy it to the clipboard, where you can paste it into a text file for further analysis.

The preview includes the following sections:

- Flex-config Prepended CLI—These are the commands generated by FlexConfigs that are prepended to the configuration.
- CLI generated from managed features—These are commands generated for policies configured in the Firewall Management Center. Commands are generated for new or changed policies since the last successful deployment to the device. These commands do not represent all commands needed to implement the assigned policies. No commands in this section are generated from FlexConfig objects.
- Flex-config Appended CLI—These are the commands generated by FlexConfigs that are appended to the configuration.

Step 5 Click **Close** to close the preview dialog.

Verify the deployed configuration

This task helps you confirm that your FlexConfig policy deployment completed successfully and that the device configuration matches your expectations.

After you deploy a FlexConfig policy to a device, verify that the deployment was successful and that the resulting configuration is what you expected. Also, verify that the device is performing as expected.

Procedure

Step 1 To verify that deployment was successful:

Check the deployment status and review any error messages or warnings.

- Click **Notifications** in the menu bar, which is unnamed between **Deploy** and **System**.

  The icon looks like one of the following, and it might include a number if there are errors:

  - **Indicates No Warnings** — Indicates no warnings or errors are present on the system.

- Indicates **One or More Warnings** — Indicates one or more warnings and no errors are present on the system.
- **Indicates One or More Errors** — Indicates one or more errors and any number of warnings are present on the system.

- On **Deployments**, verify that the deployment was successful.
- To see more detailed information, especially for failed deployments, click **Show History**.
- Select the deployment job in the list of jobs in the left column.

  Jobs are listed in reverse chronological order, with the most recent job at the top of the list.

- Click download in the **Transcript** column for the device in the right column.

  The deployment transcript includes commands sent to the device, and any responses returned from the device. These response can be informative messages or error messages. For failed deployments, look for messages that indicate errors with the commands that you sent through FlexConfig. These errors can help you correct the script in the FlexConfig object that is trying to configure the commands.



Note There is no distinction made in the transcript between commands sent for managed features and those generated from FlexConfig policies.

For example, the following sequence shows that Firewall Management Center sent commands to configure GigabitEthernet0/0 with the logical name outside. The device responded that it automatically set the security level to 0. Firewall Threat Defense does not use the security level for anything. Messages relevant to FlexConfig are in the CLI Apply section of the transcript.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

Step 2 Verify that the deployed configuration includes the expected commands.

You can do this by making an SSH connection to the device's management IP address. Use the **show running-config** command to view the configuration.

Alternatively, use the CLI tool within Secure Firewall Management Center.

- Choose **System** (⚙) > **Health** > **Monitor** and click the name of the device.

  You might need to click the open/close arrow in the **Count** column in the Status table to see any devices.

- Click **Advanced Troubleshooting**.
- Click **Threat Defense CLI**.
- Select **show** as the command, and type **running-config** as the parameter.
- Click **Execute**.

  The running configuration appears in the text box. You can select the configuration and press Ctrl+C, then paste it into a text file for later analysis.

Step 3 Verify that the device is performing as expected.

Use the **show** commands related to the feature to see detailed information and statistics. For example, if you enabled additional protocol inspections, the **show service-policy** command provides this information. The exact commands to use are feature-dependent and should be mentioned in the ASA configuration guide and command reference you used to learn how to configure the feature.

If commands that show statistics indicate that numbers are not changing (for example, hit counts, connection counts, and so forth), the configuration might be valid but not meaningful. If you know that traffic is going through the device that should show up in statistics, look for what is missing in your configuration. For example, NAT or access rules might be dropping or changing traffic before a feature can act on it.

You can use the **show** commands from an SSH session or through the Firewall Management Center CLI tool.

However, if the **show** command that you need to use is not available directly within the Firewall Threat Defense CLI, you will need make an SSH connection to the device to use the commands. From the CLI, enter the following command sequence to enter Privileged EXEC mode within the diagnostic CLI. From there, you should be able to enter these otherwise unsupported **show** commands.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

Remove features configured using FlexConfig

This task allows you to manually remove configuration commands that were deployed using FlexConfig when unassigning the FlexConfig policy from a device might not remove all of the configuration.

If you decide you need to remove a set of configuration commands you configured using FlexConfig, you might need to manually remove that configuration. Unassigning the FlexConfig policy from a device might not remove all of the configuration.

To manually remove the configuration, you create new FlexConfig objects to clear or negate the configuration commands.

Before you begin

To determine if you need to manually remove some or all of the configuration generated by an object:

1. Examine the configuration preview, as described in Preview the FlexConfig policy, on page 953. If the **###CLI generated from managed features ###** section contains the clear or negate commands to remove all of the commands in the FlexConfig object, then you can simply remove the object from the FlexConfig policy, save, and redeploy.
2. Remove the object from the FlexConfig policy, save the change, then preview the configuration again. If the **###CLI generated from managed features ###** section still does not include the required clear or negate commands, you must follow this procedure to manually remove the configuration.

Follow these steps to remove features configured using FlexConfig:

Procedure

Step 1 Choose **Objects** > **Object Management** and create the FlexConfig Objects to clear or negate the configuration commands.

If a feature has a **clear** command that can remove all configuration settings, then use that command. For example, the predefined ISIS_Unconfigure_All object contains a single command that removes all ISIS-related configuration commands:

```
clear configure router isis
```

If there is not a **clear** command for the feature, you need to use the **no** form of each command you want to remove. For example, the predefined Sysopt_basic_negate object removes the commands configured through the predefined Sysopt_basic object.

```
no sysopt traffic detailed-statistics

no sysopt connection timewait
```

You would typically configure a FlexConfig object that removes configurations as a prepended, deploy once object.

Step 2 Choose **Devices** > **FlexConfig** and create a new FlexConfig policy or edit the existing policy.

If you want to preserve the FlexConfig policy that deploys the configuration commands, create a new policy specifically for negating the commands, and assign the devices to the policy. Then, add the new FlexConfig objects to the policy.

If you want to completely remove the FlexConfig configuration objects from all devices, you can simply delete those commands from the existing FlexConfig policy and replace them with the objects that negate the configuration.

Step 3 Click **Save** to save the FlexConfig policy.

Step 4 Click **Preview Config** and verify that the clear and negation commands are generating correctly.

Step 5 Choose **Deploy** > **Deployment** in the menu bar, select the device, and click **Deploy**.

Wait for deployment to complete.

Step 6 Verify that the commands were removed.

View the running configuration on the device to confirm that the commands are removed. For more detailed information, see Verify the deployed configuration, on page 954.

Step 7 While editing the FlexConfig policy, click **Policy Assignments** and remove the device. Optionally, remove the FlexConfig Objects from the policy.

Assuming that the FlexConfig policy simply removes the unwanted configuration commands, there is no need to keep the policy assigned to the device after the removal is complete.

However, if the FlexConfig policy retains options that you still want configured on the device, remove the negation objects from the policy. They are no longer needed.

Convert from FlexConfig to managed feature

This procedure converts deprecated FlexConfig commands to newly supported managed features after a software upgrade.

Each software release adds managed features to the product. These are features you configure directly through policies controlled outside of FlexConfig. This can deprecate FlexConfig commands that you are currently using. Your configurations are not automatically converted. After the upgrade, you cannot assign or create FlexConfig objects using the newly deprecated commands. After upgrading software, examine your FlexConfig policies and objects.

If a feature configured through FlexConfig becomes available as a managed feature, convert the configuration to the managed feature instead of using FlexConfig. In most cases, your existing FlexConfig configurations continue to work after the upgrade, and you can still deploy. However, using deprecated commands may cause deployment issues in certain situations. Configuring a feature in both the GUI and FlexConfig is not supported.

Note Use the migration tool instead of this procedure if the tool supports the feature configuration you are migrating.

Procedure

Step 1 Remove the FlexConfig, as explained in Remove features configured using FlexConfig, on page 956.

Step 2 Configure the settings in the newly supported managed feature.

The release notes have a list of new features for the release.

Examples for FlexConfig

This topic provides a collection of practical examples for implementing FlexConfig policies.

Configure precision time protocol (ISA 3000)

The Precision Time Protocol (PTP) is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. These device clocks are generally of varying precision and stability. The protocol is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

A PTP system is a distributed, networked system consisting of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks and transparent clocks. Non-PTP devices include network switches, routers and other infrastructure devices.

You can configure the Firewall Threat Defense device to be a transparent clock. The Firewall Threat Defense device does not synchronize its clock with the PTP clocks. The Firewall Threat Defense device will use the PTP default profile, as defined on the PTP clocks.

When you configure the PTP devices, you define a domain number for the devices that are meant to function together. Thus, you can configure multiple PTP domains, and then configure each non-PTP device to use the PTP clocks for one specific domain.

Before you begin

Determine the domain number configured on the PTP clocks that the device should use. This example assumes the PTP domain number is 10. Also, determine the interfaces through which the system can reach the PTP clocks in the domain.

These are the guidelines for configuring PTP.

- This feature is only available on the Cisco ISA 3000 appliance.
- Cisco PTP supports multicast PTP messages only.
- PTP is available only for IPv4 networks, not for IPv6 networks.
- PTP configuration is supported on physical Ethernet data interfaces, whether stand-alone or bridge group members. It is not supported on the management interface, subinterfaces, EtherChannels, Bridge Virtual Interfaces (BVI), or any other virtual interfaces.
- PTP flows on VLAN subinterfaces are supported, assuming the appropriate PTP configuration is present on the parent interface.
- You must ensure that PTP packets are allowed to flow through the device. PTP traffic is identified by UDP destination ports 319 and 320, and destination IP address 224.0.1.129, so any access control rule that allows this traffic should work.
- In Routed firewall mode, you must enable multicast routing for PTP multicast groups. In addition, if an interface on which you enable PTP is **not** in a bridge group, you must configure the interface to join the IGMP multicast group 224.0.1.129. If the physical interface is a bridge group member, you do not configure it to join the IGMP multicast group.

Follow these steps to configure Precision Time Protocol on an ISA 3000 device:

Procedure

Step 1 (Routed mode only) Enable Multicast routing, and configure the IGMP group for the interfaces.

In Routed mode, you must enable Multicast routing. In addition, for stand-alone physical interfaces, that is, those that are not bridge group members, you must also configure the interface to join the 224.0.1.129 IGMP group. You cannot configure bridge group members to join an IGMP group, but PTP configuration on bridge group members will work without the IGMP join.

Perform this procedure for each device on which you will configure PTP.



Note Write down the hardware names of each PTP-clock-facing interface on each device, for example, GigabitEthernet1/1.

a) Choose **Devices** > **Device Management**, and edit the device.
b) Click **Routing**.

c) Choose **Multicast Routing** > **IGMP**.
d) Check the **Enable Multicast Routing** check box.
e) Click **Join Group**.
f) Click **Add**, and in the **Add IGMP Join Group Parameters** dialog box, configure the following options and click **OK**.

- **Interface**—Select the PTP-clock-facing stand-alone interface.
- **Join Group**—Click **+** to add a new network object. Create a Host object with the address 224.0.1.129. When configuring additional interfaces, simply select this object. (See Create a network object, on page 2388.)

Repeat this step for each PTP-clock-facing stand-alone interface on the device.

g) Click **Save** on the Routing page.

Step 2 Create the FlexConfig object to enable PTP globally and on the interface.

This procedure assumes that the PTP-clock-facing interface is the same on every device you are configuring. If you have used different interfaces on different devices, you need to create separate objects for each distinct combination. For example, if you use GigabitEthernet1/1 on devices A and B, GigabitEthernet1/2 on devices C and D, and both GigabitEthernet1/1 and 1/2 on devices E and F, you need 3 separate FlexConfig objects, and subsequently, 3 separate FlexConfig policies (explained in the next step).

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.
b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Enable_PTP.
- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features. This ensures that any other changes you make to interface configuration are configured before these commands.
- **Object body**—In the object body, type the commands needed to configure PTP globally and on each PTP-clock-facing interface. For example, the commands needed for the global configuration for PTP domain 10 and the interface configuration on GigabitEthernet1/1 are:

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

The object body should look similar to the following:



Step 3 Create the FlexConfig policy and assign it to the devices.

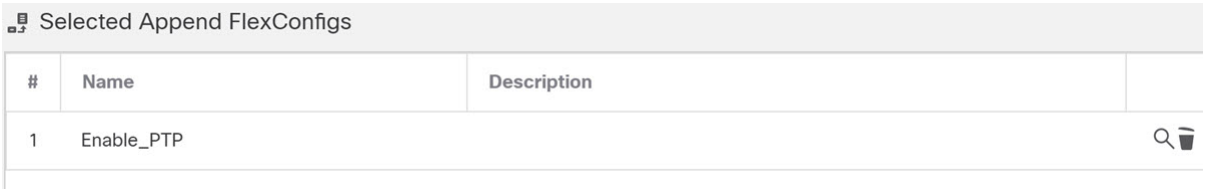
If you created multiple FlexConfig objects for different combinations of PTP-clock-facing interfaces, you need to create separate FlexConfig policies for each object, and assign those policies to the correct devices based on the interfaces you need to configure. Repeat this procedure for each group of devices.

a) Choose **Devices** > **FlexConfig**.
b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

   When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the PTP FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

   The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.
e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.
f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

   The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the PTP FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the PTP commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

Step 4 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration, on page 954.

Step 5 Verify the PTP configuration on each device.

From an SSH or Console session into each device, verify the PTP settings:

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
```

```
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

Configure automatic hardware bypass for power failure (ISA 3000)

Configure automatic hardware bypass to ensure network traffic continues to flow between interface pairs during power outages on ISA 3000 devices.

You can enable hardware bypass so that traffic continues to flow between an interface pair during a power outage. Supported interface pairs are copper interfaces GigabitEthernet 1/1 and 1/2; and GigabitEthernet 1/3 and 1/4. If you have a fiber Ethernet model, only the copper Ethernet pair (GigabitEthernet 1/1 and 1/2) supports hardware bypass.

When hardware bypass is active, traffic passes between these interface pairs at layer 1. The Firewall Threat Defense CLI will see the interfaces as being down. No firewall functions are in place, so make sure you understand the risks of allowing traffic to pass through the device.

In CLI Console or an SSH session, use the **show hardware-bypass** command to monitor the operational status.

Before you begin

For hardware bypass to work:

- You must place the interface pairs in the same bridge group.
- You must attach the interfaces to access ports on the switch. Do not attach them to trunk ports.

We recommend that you disable TCP sequence number randomization globally using the Threat Defense Service Policy attached to the access control policy assigned to the device. By default, the ISA 3000 rewrites the initial sequence number (ISN) of TCP connections passing through it to a random number. When hardware bypass is activated, the ISA 3000 is no longer in the data path and does not translate the sequence numbers. The receiving client receives an unexpected sequence number and drops the connection, so the TCP session needs to be re-established. Even with TCP sequence number randomization disabled, some TCP connections will have to be re-established because of the link that is temporarily down during the switchover.

Follow these steps to configure automatic hardware bypass for power failure:

Procedure

Step 1 Create the FlexConfig object to enable automatic bypass.

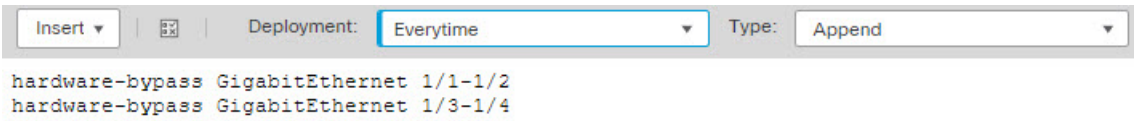
a. Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b. Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Enable_HW-Bypass.
- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to enable automatic hardware bypass. For example, the commands needed for both possible interface pairs:

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

The object body should look similar to the following:



Step 2 Create the FlexConfig policy and assign it to the devices.

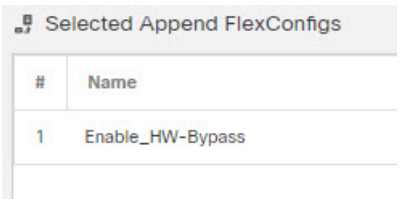
a. Choose **Devices** > **FlexConfig**.

b. Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c. Select the hardware bypass FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d. Click **Save**.

e. If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f. Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the hardware bypass FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the hardware bypass commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration, on page 954.

What to do next

If you want to manually invoke hardware bypass or manually turn it off, you need to create two FlexConfig objects:

- One that manually starts bypass, which would contain one or both of the following commands, depending on whether you want to invoke bypass for both pairs:

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- One that manually turns off bypass, which would contain one or both of the following commands:

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

You would then need to add one or the other object to the FlexConfig policy, and deploy changes, to either turn bypass on or off. You would also need to immediately remove the object from the FlexConfig policy after deployment. If you manually invoke bypass, you would then need to repeat the process to turn it off again. Thus, using this manual method requires frequent and careful editing of the FlexConfig policy and additional deployments.

Migrate FlexConfig policies

This task migrates ECMP, VXLAN, and EIGRP policies from FlexConfig objects to the management center UI to enable direct policy management.

Attention This section on migrating FlexConfig policies is applicable only for migrating ECMP, VXLAN, and EIGRP policies.

The ECMP, VXLAN, and EIGRP policies were configured using the FlexConfig objects and policies in earlier versions of the Firewall Management Center. You can now directly configure these policies in the management center UI. When you are upgrading the management center from earlier versions, the FlexConfig configuration is retained. However, to manage the policies from the UI, you must redo the configuration in the corresponding **Device (Edit)** > **Routing** page and remove the configuration from FlexConfig. To automate creation of the policies in the UI, Firewall Management Center provides an option to migrate the policies from FlexConfig to the UI. However, it does not remove the migrated policies from the FlexConfig. For post-migration procedure, refer to Step 7, on page 966.

Before you begin

- Ensure that the deployed FlexConfig policy is up-to-date and not out-of-date. The migration option will be available only if the policy is up-to-date on at least 1 device. Migration does not take place for those devices that have out-of-date policies.
- If the policy is configured in both FlexConfig and the management center:
  - Migration will not be initiated if the policy is already configured at **Device (Edit)** > **Routing**.
  - During deployment, the management center displays an error message. Example EIGRP migration error message—*EIGRP is configured through FlexConfig object and also under Device Listing ->Routing EIGRP for the device. Maintain the EIGRP configuration in either Routing EIGRP or FlexConfig.*
- If the network objects used in the policy exist in the management center, during migration, they are reused. During migration, when a network object that is matching the IP configuration is not available, a new network object is created as *bb* appended with a timestamp and integer, like ***bb_<timestamp>_<integer>***. For more than one such network object, the integer variable in the name would be incremented by one.

Follow these steps to migrate FlexConfig policies:

Procedure

Step 1 Choose **Devices** > **FlexConfig**, click **Edit** (✎) against the FlexConfig policy that you want to migrate.

Step 2 Click **Migrate Config**.

Note Once migration starts, both **Migrate Config** and FlexConfig **Edit** options are not available.

The **Migrate Config** option is not available, when:

- There are no applicable FlexConfig CLIs to be migrated.
- The FlexConfig policy is not associated with any FlexConfig objects.
- There are no devices that are associated with the FlexConfig policy.

Step 3 In the **Migrate Flex Configuration** dialog box, select the device to which you wish to migrate the configuration, and then click **Ok**.

The migration progress is displayed as task notification. When the migration is complete, click the *View Details* link and download the migration report (PDF format).

Step 4 To view the policy changes, choose **System** (⚙) > **Monitoring** > **Audit** and click on the *Flex Config Migration* message.

Step 5 To view the FlexConfig migration report, choose **System** (⚙) > **Monitoring** > **Audit** and click on the *Flex Config Migration* message. To view the complete migration report, click the **Report** icon.

Step 6 Verify the migrated configuration settings in the corresponding **Device (Edit)** > **Routing**. page.

Step 7 To remove the specific policy config from FlexConfig for the device, in the management center, do the following:

a) Identify the migrated FlexConfig policy for the device.
b) Use the copy option and create duplicate of the FlexConfig policy.
c) Remove the corresponding CLI objects from the duplicated FlexConfig policy.
d) Associate the device to the duplicated FlexConfig policy.

Step 8 Save and deploy the configuration.

History for FlexConfig

This reference provides a summary of feature changes by release for the FlexConfig policy.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	7.4.1	7.4.1	If the data plane process crashes, the system now reloads only the data plane process instead of rebooting the device. Along with the data plane process reload, Snort and a few other processes also get reloaded. However, if the data plane process crashes during bootup, the device follows the normal reload/reboot sequence, which helps avoid a reload process loop from occurring. This feature is enabled by default for both new and upgraded devices. New/modified CLI commands: **data-plane quick-reload**, **no data-plane quick-reload**, **show data-plane quick-reload status** Supported platforms: Firepower 1000/2100, Firepower 4100/9300 Platform restrictions: Not supported in multi-instance mode. See: *Cisco Secure Firewall Threat Defense Command Reference* and Cisco Secure Firewall ASA Series Command Reference.
Migration tool support.	7.3.0	Any	Support to migrate Flex configured ECMP, VXLAN, and EIGRP policies to management center was introduced. New/modified screens: **Devices** > **FlexConfig** > **Migrate FlexConfig**
Removal of BFD configuration in FlexConfig.	7.3.0	Any	Support to configure BFD policies directly in the management center user interface was introduced. Hence, FlexConfig support to configure BFD policies was removed.
Removal of priority-queue.	7.2.5	7.2.5	Support to configure priority-queue in threat defense was removed.
Removal of EIGRP configuration in FlexConfig.	7.2.0	Any	Support to configure EIGRP directly in the management center user interface was introduced. Hence, FlexConfig support to configure EIGRP policies was removed.
Removal of PBR configuration.	7.1.0	7.1.0	Support to configure the PBR directly in the FMC user interface was introduced. Hence, FlexConfig support to configure PBR for FTD 7.1 and higher was removed. New/modified commands: **policy-route route-map***routemap-object-name*.
Removal of ECMP zone creation support in FlexConfig.	7.1.0	Any	Support to configure the ECMP zones directly in the FMC user interface was introduced. Hence, FlexConfig support to configure ECMP zones was removed.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	6.5.0	Any	You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. We now allow you to include the **PTP** (interface mode) command, and the global commands **PTP mode e2etransparent** and **PTP domain**, in FlexConfig objects. New/modified commands: **show PTP**.
Deprecated FlexConfig objects.	6.3.0	Any	Several features that in previous releases you configured using FlexConfig are now directly supported in FMC. You need to remove these FlexConfig objects if you are using them, and convert your configuration to use the new objects. These are the deprecated FlexConfig objects and text objects. • **Default_DNS_Configure**, including the defaultDNSNameServerList and defaultDNSParameters text objects. Now, please configure DNS for the data interfaces using the Platform Settings policy. • **TCP_Embryonic_Conn_Limit**, and the tcp_conn_misc and tcp_conn_limit text objects. Configure these features in the FTD Service Policy, which you can find on the Advanced tab of the access control policy assigned to the device. • **TCP_Embryonic_Conn_Timeout**, and the tcp_conn_misc and tcp_conn_timeout text objects. Configure these features in the FTD Service Policy.

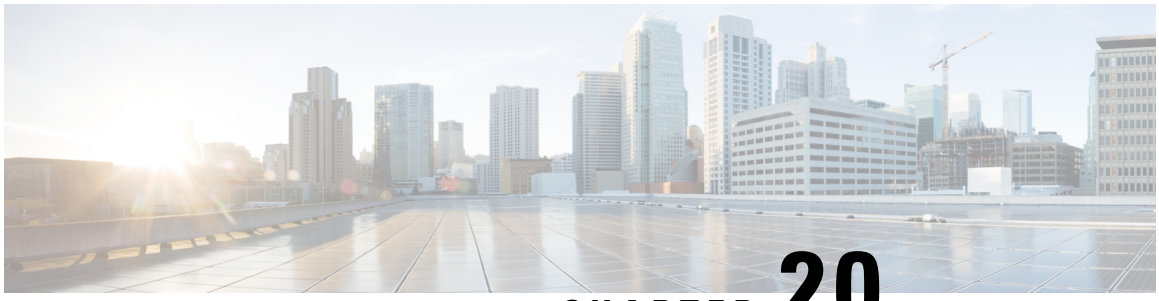
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
FlexConfig updates.	6.2.1	Any	As per the Government Certification requirements, all sensitive information like password, shared keys in system-provided or user-defined FlexConfig object should be masked using secret key variables. After you update the FMC to Version 6.2.1+, all sensitive information in FlexConfig Objects are converted to secret key variable format. In addition, these new FlexConfig templates are added: • **Default_DNS_Configure** template allows you to the default DNS group, which is used to resolve hostnames for commands or features that resolve names through the data interfaces. • **TCP Embryonic connection limit and timeout configuration** template allows you to configure embryonic connection limits/timeout CLIs to protect from SYN Flood DoSAttack. • **Turn on threat detection configure and clear** templates allow you to configure threat detection statistics for attacks intercepted by TCP Intercept. • **IPV6 router header inspection** template allows you to configure of IPV6 inspection header for selectively allow/block certain headers with different types (e.g. allowing RH Type 2,mobile). • **DHCPv6 prefix delegation** template allows you to configure one outside (PD client) and one inside interface (recipient of delegated prefix) for IPv6 prefix delegation.
FlexConfig.	6.2.0	Any	The FlexConfig feature allows you use the FMC to deploy ASA CLI template-based functionality to FTD devices. This feature allows you to enable some of the most valuable ASA functions that are not currently available on FTD devices. This functionality is structured as templates and objects that work together in a policy. The default templates are officially supported by Cisco TAC. New/modified screens: • **Devices** > **FlexConfig** • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Objects** • **Objects** > **Object Management** > **FlexConfig** > **Text Object**



PART IV

Routing

- Static and Default Routes, on page 973
- Virtual Routers, on page 991
- ECMP, on page 1047
- Bidirectional Forwarding Detection Routing, on page 1057
- OSPF, on page 1063
- EIGRP, on page 1095
- BGP, on page 1107
- RIP, on page 1129
- Multicast, on page 1137
- Policy-Based Routing, on page 1159



CHAPTER 20

Static and Default Routes

This chapter describes how to configure static and default routes on the Firewall Threat Defense.

- Static and default routes overview, on page 973
- Requirements and prerequisites for static routes, on page 976
- Guidelines for static and default routes, on page 976
- Add a static route, on page 977
- Reference for routing, on page 978

Static and default routes overview

To route traffic to a non-connected host or network, define a route to the host or network, using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, which is typically the next-hop router.

Default routes

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the Firewall Threat Defense sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

Default route configuration requirements

You should always define a default route.

The Firewall Threat Defense has separate routing tables for data interfaces and for management-only interfaces (including the special Linux Management interface). You can only add a default route for the data routing table. The Firewall Threat Defense automatically adds a default route in the management-only routing table that sends traffic to the Linux Management interface, where a separate route lookup occurs in the Linux routing table. You can add static routes to the Linux routing table that can be used by Management using the Firewall Threat Defense CLI **configure network static-routes** command.

Note The *default* Linux route is set with the **configure network ipv4** or **configure network ipv6** command.

Static routes

You might want to use static routes in the following cases:

Use cases for static routes

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the Firewall Threat Defense.
- You are using a feature that does not support dynamic routing protocols.
- Virtual routers use static routes to create route leaks. Route leaks enable flow of traffic from an interface of a virtual router to another interface in another virtual router. For more information, see Virtual router interconnection, on page 994.

Route to null0 interface to drop unwanted traffic

Access rules let you filter packets based on the information contained in their headers. A static route to the null0 interface is a complementary solution to access rules. You can use a null0 route to forward unwanted or undesirable traffic so the traffic is dropped.

Performance and routing benefits

Using static null0 routes provides a favorable performance profile. You can also use static null0 routes to prevent routing loops. BGP can leverage the static null0 route for Remotely Triggered Black Hole routing.



Note Though routing traffic to a null0 interface to blackhole it helps to drop unwanted traffic, this method increases the `no-route` ASP drops.

Route priorities

- Routes that identify a specific destination take precedence over the default route.
- When multiple routes exist to the same destination (either static or dynamic), then the administrative distance for the route determines priority. Static routes are set to 1, so they typically are the highest priority routes.
- When you have multiple static routes to the same destination with the same administrative distance, see Equal-cost multi-path routing, on page 987.
- For traffic emerging from a tunnel with the Tunneled option, this route overrides any other configured or learned default routes.

Transparent firewall mode and bridge group routes

For traffic that originates on the Firewall Threat Defense device and is destined through a bridge group member interface for a non-directly connected network, you need to configure either a default route or static routes so the Firewall Threat Defense device knows out of which bridge group member interface to send traffic. Traffic that originates on the Firewall Threat Defense device might include communications to a syslog server or SNMP server. If you have servers that cannot all be reached through a single default route, then you must configure static routes. For transparent mode, you cannot specify the BVI as the gateway interface; only member interfaces can be used. For bridge groups in routed mode, you must specify the BVI in a static route; you cannot specify a member interface. Refer to MAC address and route lookups, on page 77 for more information.

Static route tracking

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and configure a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

Static route tracking implementation

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the Firewall Threat Defense device goes down.

The Firewall Threat Defense device implements static route tracking by associating a static route with a monitoring target host on the destination network that the Firewall Threat Defense device monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. You can choose any network object as the target, but consider using one of these options:

- The address of the ISP gateway (for dual ISP support)
- The address of the next hop gateway (if you are concerned about gateway availability)
- A server on the target network, such as a syslog server, with which the Firewall Threat Defense device needs to communicate
- A persistent network object on the destination network

Note A PC that may be shut down at night is not a good choice.

You can configure static route tracking for statically defined routes or default routes obtained through DHCP or PPPoE. You can only enable PPPoE clients on multiple interfaces with route tracking configured.

Requirements and prerequisites for static routes

Requirement	Description
Model support	Firewall Threat Defense
Supported domains	Any
User roles	Admin Network Admin

Guidelines for static and default routes

Firewall mode and bridge groups

Configure static routes according to your firewall mode and interface requirements.

- In transparent mode, static routes must use the bridge group member interface as the gateway; you cannot specify the BVI.
- In routed mode, you must specify the BVI as the gateway; you cannot specify the member interface.
- Static route tracking is not supported for bridge group member interfaces or on the BVI.

Supported network address

Ensure your network addresses meet static route requirements.

- Static route tracking is not supported for IPv6.
- The Firewall Threat Defense does not support Class E routing, so a Class E network is not routable in static routes.

Clustering

Consider these limitations for clustering and multiple context mode configurations.

- In clustering, static route tracking is only supported on the control node.

Network object group

You cannot use a range of network objects or a network object group having a range of IP addresses in a static route.

ASP and RIB Route Entries

All routes and its distance installed on the device are captured in the ASP routing table. This is common for all static and dynamic routing protocols. Only the best distance route is captured in the RIB table.

Add a static route

A static route defines where to send traffic for specific destination networks. You should at a minimum define a default route. A default route is simply a static route with 0.0.0.0/0 as the destination IP address.

To configure routes for redundant manager access data interfaces, see Configure a redundant manager access data interface, on page 758.

Procedure

Step 1 To configure routes for redundant manager access data interfaces, see Configure a redundant manager access data interface, on page 758.

Step 2 Click **Routing**.

Step 3 (May be required) From the virtual routers drop-down list, select the virtual router for which you are configuring a static route.

Step 4 Select **Static Route**.

Step 5 Click **Add Routes**.

Step 6 Click **IPv4** or **IPv6** depending on the type of static route that you are adding.

Step 7 Choose the **Interface** to which this static route applies.

For transparent mode, choose a bridge group member interface name. For routed mode with bridge groups, you can choose either the bridge group member interface for the BVI name. To "black hole" unwanted traffic, choose the **Null0** interface.

For a device using virtual routing, you can select an interface that belongs to another virtual router. You can create such a static route if you want to leak traffic from this virtual router into the other virtual router. For more information, see Virtual router interconnection, on page 994.

Step 8 In the **Available Network** list, choose the destination network.

To define a default route, create an object with the address 0.0.0.0/0 and select it here.

Note Although you can create and choose a Network Object Group containing a range of IP addresses, the Firewall Management Center does not support using ranges in static routes.

Step 9 In the **Gateway** or **IPv6 Gateway** field, enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

When you are using static-route configuration for virtual routers to leak routes, do not specify the next hop gateway.

Step 10 In the **Metric** field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

The metric is a measurement of the "expense" of a route, based on the number of hops (hop count) to the network on which a specific host resides. Hop count is the number of networks that a network packet must traverse, including the destination network, before it reaches its final destination. The metric is used to compare

routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connected routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static route takes precedence. Connected routes always take precedence over static or dynamically discovered routes.

Step 11 (Optional) For a default route, click the **Tunneled** checkbox to define a separate default route for VPN traffic.

You can define a separate default route for VPN traffic if you want your VPN traffic to use a different default route than your non VPN traffic. For example, traffic incoming from VPN connections can be easily directed towards internal networks, while traffic from internal networks can be directed towards the outside. When you create a default route with the tunneled option, all traffic from a tunnel terminating on the device that cannot be routed using learned or static routes, is sent to this route. You can configure only one default tunneled gateway per device. ECMP for tunneled traffic is not supported.

Step 12 (IPv4 static route only) To monitor route availability, enter or choose the name of an SLA (service level agreement) Monitor object that defines the monitoring policy, in the **Route Tracking** field.

See Configure an SLA monitor, on page 2433.

Step 13 Click **Ok**.

Reference for routing

This section describes underlying concepts of how routing behaves within the Firewall Threat Defense.

Path determination

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Path determination process

Routing algorithms fill routing tables with a variety of information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables also can include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message sent between routers, informs other routers of the state of the sender links. Link information also can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

Supported route types

There are several route types that a router can use. The Firewall Threat Defense device uses the following route types:

- Static Versus Dynamic
- Single-Path Versus Multipath
- Flat Versus Hierarchical
- Link-State Versus Distance Vector

Static versus dynamic routing algorithms

Static routing algorithms are actually table mappings established by the network administrator. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Dynamic routing algorithms

Because static routing systems cannot react to network changes, they generally are considered unsuitable for large, constantly changing networks. Most of the dominant routing algorithms are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a default route for a router to which all unrouteable packets are sent), for example, can be designated to act as a repository for all unrouteable packets, ensuring that all messages are at least handled in some way.

Single-path versus multipath

Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are substantially better throughput and reliability, which is generally called load sharing.

Flat versus hierarchical routing

Some routing algorithms operate in a flat space, while others use routing hierarchies.

In a flat routing system, the routers are peers of all others. In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from non-backbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more non-backbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas.

In hierarchical systems, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

Link-state versus distance vector

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables.

Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. Distance vector algorithms know only about their neighbors. Typically, link-state algorithms are used in conjunction with OSPF routing protocols.

Supported internet protocols for routing

The Firewall Threat Defense device supports several internet protocols for routing. Each protocol is briefly described in this section.

The device supports these internet routing protocols:

- **Enhanced Interior Gateway Routing Protocol (EIGRP)**

  EIGRP is a Cisco proprietary protocol that provides compatibility and seamless interoperation with IGRP routers. An automatic-redistribution mechanism allows IGRP routes to be imported into Enhanced IGRP, and vice versa, so it is possible to add Enhanced IGRP gradually into an existing IGRP network.

- **Open Shortest Path First (OSPF)**

  OSPF is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF). OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area includes an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

- **Routing Information Protocol (RIP)**

  RIP is a distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system.

- **Border Gateway Protocol (BGP)**

  BGP is an interautonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

Routing tables

The Firewall Threat Defense uses separate routing tables for data traffic (through-the-device) and for management traffic (from-the-device). This section describes how the routing tables work. For information about the management routing table, see also Routing table for management traffic, on page 986.

How the routing table is populated

The Firewall Threat Defense routing table can be populated by statically defined routes, directly connected routes, and routes discovered by the dynamic routing protocols. Because the Firewall Threat Defense device can run multiple routing protocols in addition to having static and connected routes in the routing table, it is possible that the same route is discovered or entered in more than one manner.

Route selection criteria

When two routes to the same destination are put into the routing table, the one that remains in the routing table is determined as follows:

- If the two routes have different network prefix lengths (network masks), then both routes are considered unique and are entered into the routing table. The packet forwarding logic then determines which of the two to use.

  For example, if the RIP and OSPF processes discovered the following routes:

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  Even though OSPF routes have the better administrative distance, both routes are installed in the routing table because each of these routes has a different prefix length (subnet mask). They are considered different destinations and the packet forwarding logic determines which route to use.

- If the Firewall Threat Defense device learns about multiple paths to the same destination from a single routing protocol, such as RIP, the route with the better metric (as determined by the routing protocol) is entered into the routing table.

  Metrics are values associated with specific routes, ranking them from most preferred to least preferred. The parameters used to determine the metrics differ for different routing protocols. The path with the lowest metric is selected as the optimal path and installed in the routing table. If there are multiple paths to the same destination with equal metrics, load balancing is done on these equal cost paths.

- If the Firewall Threat Defense device learns about a destination from more than one routing protocol, the administrative distances of the routes are compared, and the routes with lower administrative distance are entered into the routing table.

Administrative Distances for Routes

You can change the administrative distances for routes discovered by or redistributed into a routing protocol. If two routes from two different routing protocols have the same administrative distance, then the route with the lower *default* administrative distance is entered into the routing table. In the case of EIGRP and OSPF routes, if the EIGRP route and the OSPF route have the same administrative distance, then the EIGRP route is chosen by default.

Administrative distance is a route parameter that the Firewall Threat Defense uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Because

the routing protocols have metrics based on algorithms that are different from the other protocols, it is not always possible to determine the best path for two routes to the same destination that were generated by different routing protocols.

Each routing protocol is prioritized using an administrative distance value. The following table shows the default administrative distance values for the routing protocols supported by the Firewall Threat Defense.

Table 68: Default Administrative Distance for Supported Routing Protocols

Route Source	Default Administrative Distance
Connected interface	0
VPN route	1
Static route	1
EIGRP Summary Route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal and local BGP	200
Unknown	255

The smaller the administrative distance value, the more preference is given to the protocol. For example, if the Firewall Threat Defense receives a route to a certain network from both an OSPF routing process (default administrative distance - 110) and a RIP routing process (default administrative distance - 120), the Firewall Threat Defense chooses the OSPF route because OSPF has a higher preference. In this case, the router adds the OSPF version of the route to the routing table.

A VPN advertised route (V-Route/RRI)) is equivalent to a static route with the default administrative distance 1. But it has a higher preference as with the network mask 255.255.255.255.

In this example, if the source of the OSPF-derived route was lost (for example, due to a power shutdown), the Firewall Threat Defense would then use the RIP-derived route until the OSPF-derived route reappears.

The administrative distance is a local setting. For example, if you change the administrative distance of routes obtained through OSPF, that change would only affect the routing table for the Firewall Threat Defense on which the command was entered. The administrative distance is not advertised in routing updates.

Administrative distance does not affect the routing process. The routing processes only advertise the routes that have been discovered by the routing process or redistributed into the routing process. For example, the RIP routing process advertises RIP routes, even if routes discovered by the OSPF routing process are used in the routing table.

Backup Dynamic and Floating Static Routes

A backup route is registered when the initial attempt to install the route in the routing table fails because another route was installed instead. If the route that was installed in the routing table fails, the routing table maintenance process calls each routing protocol process that has registered a backup route and requests them to reinstall the route in the routing table. If there are multiple protocols with registered backup routes for the failed route, the preferred route is chosen based on administrative distance.

Because of this process, you can create floating static routes that are installed in the routing table when the route discovered by a dynamic routing protocol fails. A floating static route is simply a static route configured with a greater administrative distance than the dynamic routing protocols running on the Firewall Threat Defense. When the corresponding route discovered by a dynamic routing process fails, the static route is installed in the routing table.

How forwarding decisions are made

A forwarding decision is a network routing process that

- determines the appropriate interface for packet transmission based on destination address matching in the routing table
- prioritizes routes with longer network prefix lengths when multiple matches exist, and
- directs packets through default routes when no specific routing table entries match the destination.

Forwarding decision process

Forwarding decisions are made as follows:

- If the destination does not match an entry in the routing table, the packet is forwarded through the interface specified for the default route. If a default route has not been configured, the packet is discarded.
- If the destination matches a single entry in the routing table, the packet is forwarded through the interface associated with that route.
- If the destination matches more than one entry in the routing table, then the packet is forwarded out of the interface associated with the route that has the longer network prefix length.

Note When a route change occurs, the Threat Defense re-evaluates the forwarding decision of established connections the next time a packet is seen on the flow.

The resulting behavior is determined by your configuration:

Configuration	Behavior	Outcome
Default (timeout floating-conn 0, no ECMP zone)	Retains the original egress path initially.	If that path can no longer resolve the destination, the flow is torn down after the conn-holddown period (default 15s) rather than waiting for an idle timeout.
Floating-Connection (timeout floating-conn configured)	Identifies a new optimal path on a different interface (outside the same ECMP zone).	The flow is torn down after the floating-conn timeout to allow for a fresh connection. Note: May trigger %FTD-6-110003 syslog messages.
ECMP Zone (Both interfaces in the same ECMP zone)	Dynamically updates the flow's egress interface.	The flow is switched to the new path atomically and non-disruptively.

Longest prefix match example

For example, a packet destined for 192.168.32.1 arrives on an interface with these routes in the routing table:

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

In this case, a packet destined to 192.168.32.1 is directed toward 10.1.1.2, because 192.168.32.1 falls within the 192.168.32.0/24 network. It also falls within the other route in the routing table, but 192.168.32.0/24 has the longest prefix within the routing table (24 bits verses 19 bits). Longer prefixes are always preferred over shorter ones when forwarding a packet.

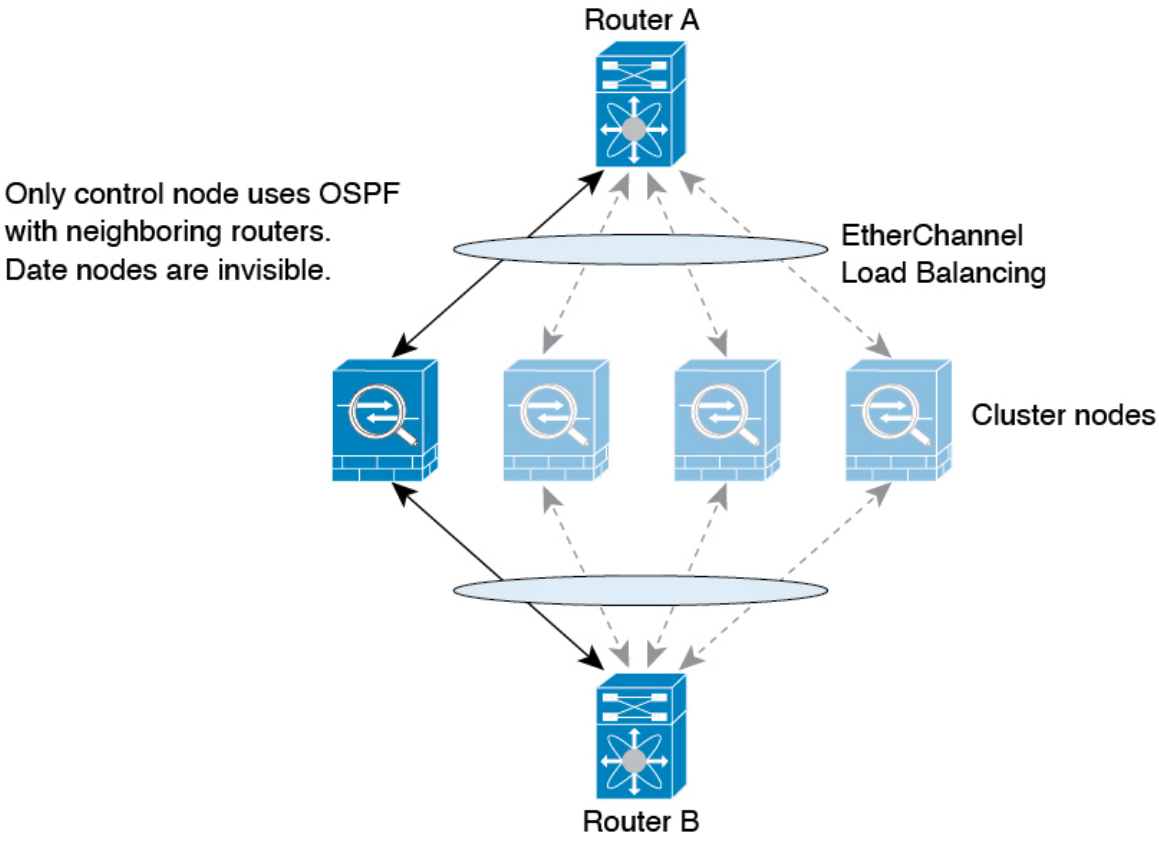
Dynamic routing and High availability

Dynamic routes are synchronized on the standby unit when the routing table changes on the active unit. This means that all additions, deletions, or changes on the active unit are immediately propagated to the standby unit. If the standby unit becomes active in an active/standby ready High availability pair, it will already have an identical routing table as that of the former active unit because routes are synchronized as a part of the High availability bulk synchronization and continuous replication processes.

Dynamic routing in Clustering

The routing process only runs on the control node, and routes are learned through the control node and replicated to data nodes. If a routing packet arrives at a data node, it is redirected to the control node.

Figure 351: Dynamic Routing in Spanned EtherChannel Mode



After the data node learn the routes from the control node, each node makes forwarding decisions independently.

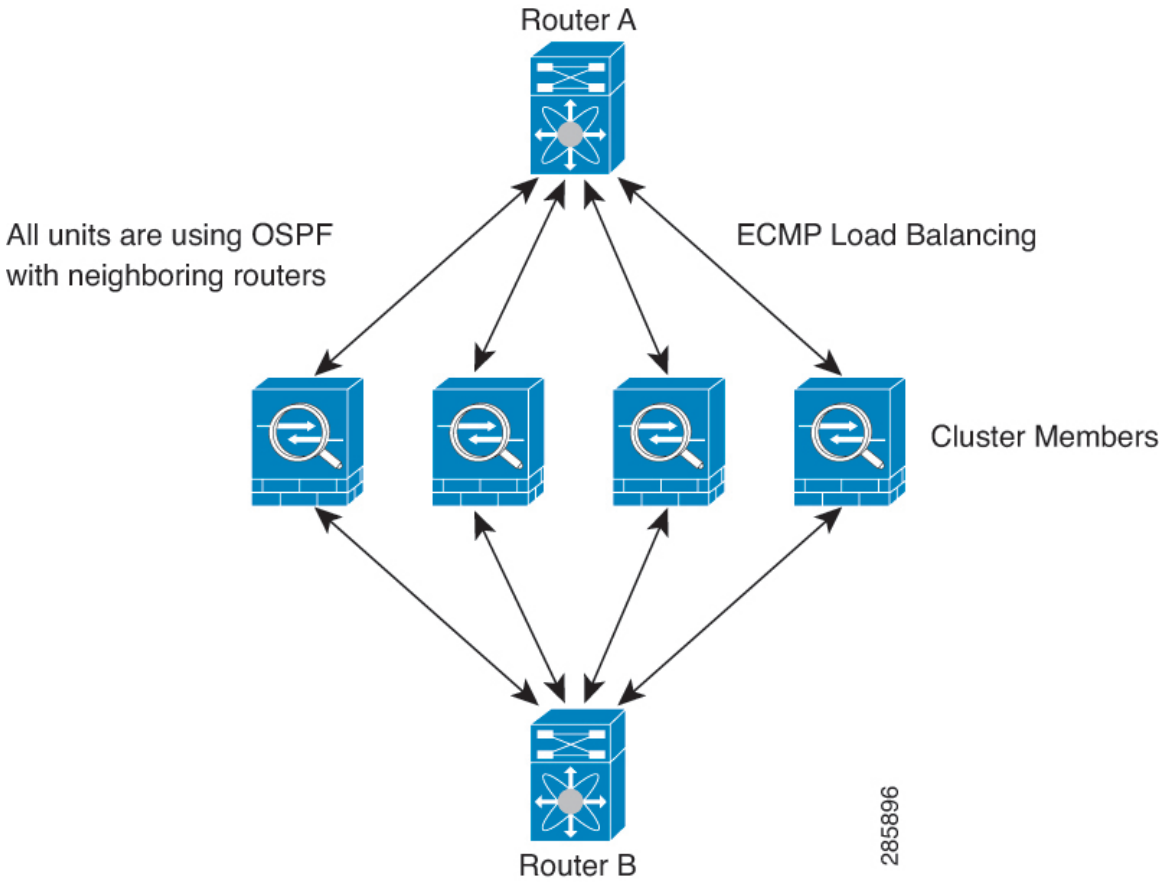
The OSPF LSA database is not synchronized from the control node to data nodes. If there is a control node switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.

Dynamic routing in individual interface mode

Learn how dynamic routing functions in individual interface mode, where each cluster node operates as a standalone router. Understand how to configure unique router IDs and manage traffic zones to ensure effective load balancing and prevent asymmetric routing in your network environment.

In Individual interface mode, each node runs the routing protocol as a standalone router, and routes are learned by each node independently.

Figure 352: Dynamic Routing in Individual Interface Mode



In the above diagram, Router A learns that there are 4 equal-cost paths to Router B, each through a node. ECMP is used to load balance traffic between the 4 paths. Each node picks a different router ID when talking to external routers.

You must configure a cluster pool for the router ID so that each node has a separate router ID.

EIGRP does not form neighbor relationships with cluster peers in individual interface mode.

Note If the cluster has multiple adjacencies to the same router for redundancy purposes, asymmetric routing can lead to unacceptable traffic loss. To avoid asymmetric routing, group all of these node interfaces into the same traffic zone. See Create an ECMP zone, on page 1049.

Routing table for management traffic

The Firewall Threat Defense device includes the following routing tables for from-the-device management traffic:

- Linux Management routing table—Special management traffic sourced from the Management interface such as Firewall Management Center communication, licensing communication, and database updates always uses the Linux Management routing table.
- Data routing table—All from-the-device traffic (as well as all through traffic) uses the data routing table by default. All regular data interfaces are part of this routing table. Most services let you choose a specific interface, so only routes associated with that interface are used.
- Management-only routing table—The Management interface and all data interfaces that you set to management-only are part of this routing table. To send from-the-device traffic from any of these interfaces, you must choose a specific management-only interface when you configure the service. An exception is for DNS lookups and ICMP (ping and traceroute): in these cases, the Firewall Threat Defense will use data and then fall back to management automatically if a route is not found. You can add static routes for management-only interfaces, but not for the special Management interface. The Firewall Threat Defense device automatically adds a default route for Management that forwards traffic to Linux, where a separate route lookup occurs in the Linux routing table. You can add static routes to the Linux routing table that can be used by Management using the Firewall Threat Defense CLI **configure network static-routes** command.

Note The *default* Linux route is set with the **configure network ipv4** or **configure network ipv6** command.

Note For devices that have not yet merged the Management and legacy Diagnostic interfaces, see refer to pre-7.3 versions of this guide.

Equal-cost multi-path routing

The Firewall Threat Defense supports Equal-Cost Multi-Path (ECMP) routing.

ECMP routing implementation

You can have up to 8 equal cost static or dynamic routes per interface. For example, you can configure multiple default routes on the outside interface that specify different gateways.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

In this case, traffic is load-balanced on the outside interface between 10.1.1.2, 10.1.1.3, and 10.1.1.4. Traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses, incoming interface, protocol, source and destination ports.

ECMP Across Multiple Interfaces Using Traffic Zones

If you configure traffic zones to contain a group of interfaces, you can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within each zone. For example, you can configure multiple default routes across three interfaces in the zone:

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

Similarly, your dynamic routing protocol can automatically configure equal cost routes. The Firewall Threat Defense load-balances traffic across the interfaces with a more robust load balancing mechanism.

When a route is lost, the device seamlessly moves the flow to a different route.

Routing GRE traffic

In Firewall Threat Defense, Generic Routing Encapsulation (GRE) traffic is managed using bi-directional flows. This means that each GRE session is represented by a single flow entry that handles both inbound and outbound traffic between endpoints. With bi-directional flows, only one route lookup is performed and both directions are mapped to the same interface. As a result, the system cannot make independent routing decisions for each direction, which may lead to sub-optimal routing in some scenarios.

About route maps

Route maps are used when redistributing routes into an OSPF, RIP, EIGRP or BGP routing process. They are also used when generating a default route into an OSPF routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Route map characteristics

Route maps have many features in common with widely known ACLs. These are some of the traits common to both:

- They are an ordered sequence of individual statements, and each has a permit or deny result. Evaluation of an ACL or a route map consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action associated with the statement match is performed.
- They are generic mechanisms. Criteria matches and match interpretation are dictated by the way that they are applied and the feature that uses them. The same route map applied to different features might be interpreted differently.

These are some of the differences between route maps and ACLs:

- Route maps are more flexible than ACLs and can verify routes based on criteria which ACLs can not verify. For example, a route map can verify if the type of route is internal.
- Each ACL ends with an implicit deny statement, by design convention. If the end of a route map is reached during matching attempts, the result depends on the specific application of the route map. Route maps that are applied to *redistribution* behave the same way as ACLs: if the route does not match any clause in a route map then the route redistribution is denied, as if the route map contained a deny statement at the end.

Permit and deny clauses

Route maps can have permit and deny clauses. The deny clause rejects route matches from redistribution. You can use an ACL as the matching criterion in the route map.

Route map and ACL clause interaction rules

Because ACLs also have permit and deny clauses, the following rules apply when a packet matches the ACL:

- ACL permit + route map permit: routes are redistributed.
- ACL permit + route map deny: routes are not redistributed.
- ACL deny + route map permit or deny: the route map clause is not matched, and the next route-map clause is evaluated.

Match and set clause values

Each route map clause has two types of values:

- A match value selects routes to which this clause should be applied.
- A set value modifies information that will be redistributed into the target protocol.

Route map evaluation process

For each route that is being redistributed, the router first evaluates the match criteria of a clause in the route map. If the match criteria succeeds, then the route is redistributed or rejected as dictated by the permit or deny clause, and some of its attributes might be modified by the values set from the set commands. If the match criteria fail, then this clause is not applicable to the route, and the software proceeds to evaluate the route against the next clause in the route map. Scanning of the route map continues until a clause is found that matches the route or until the end of the route map is reached.

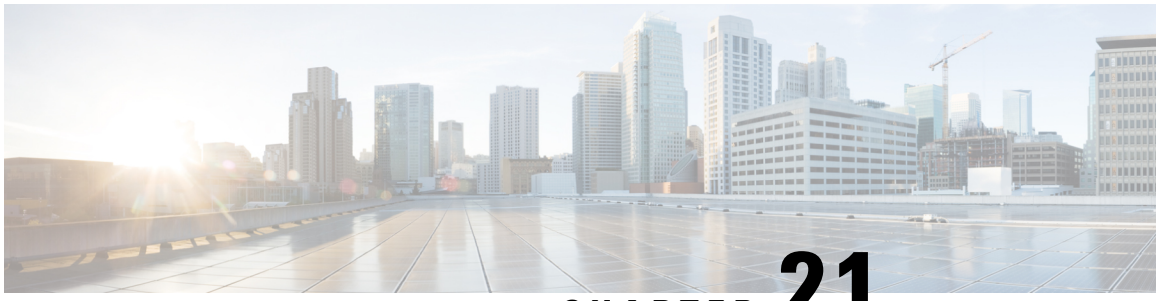
A match or set value in each clause can be missed or repeated several times, if one of these conditions exists:

- If several match entries are present in a clause, all must succeed for a given route in order for that route to match the clause (in other words, the logical AND algorithm is applied for multiple match commands).
- If a match entry refers to several objects in one entry, either of them should match (the logical OR algorithm is applied).
- If a match entry is not present, all routes match the clause.
- If a set entry is not present in a route map permit clause, then the route is redistributed without modification of its current attributes.



Note Do not configure a set entry in a route map deny clause because the deny clause prohibits route redistribution—there is no information to modify.

A route map clause without a match or set entry does perform an action. An empty permit clause allows a redistribution of the remaining routes without modification. An empty deny clause does not allow a redistribution of other routes (this is the default action if a route map is completely scanned, but no explicit match is found).



CHAPTER 21

Virtual Routers

This chapter describes underlying concepts about virtual routers and on how virtual routing behaves within the Secure Firewall Threat Defense.

- Virtual routers and virtual routing and forwarding (VRF), on page 991
- Maximum number of virtual routers by device model, on page 997
- Requirements and prerequisites for virtual routers, on page 999
- Guidelines and limitations for virtual routers, on page 999
- Manage virtual routers, on page 1001
- Create a virtual router, on page 1002
- Monitor virtual routers, on page 1006
- Configuration examples for virtual routers, on page 1006
- History for virtual routers, on page 1045

Virtual routers and virtual routing and forwarding (VRF)

A virtual router is a network virtualization feature that

- maintains separate routing tables for groups of interfaces
- provides clean separation in the traffic flowing through the device, and
- implements the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP).

Virtual router capabilities and configuration

Virtual routers provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general purpose corporate network.

When you create a virtual router, you assign interfaces to the router. You can assign a given interface to one, and only one, virtual router. You would then define static routes, and configure routing protocols such as OSPF or BGP, for each virtual router. You would also configure separate routing processes over your entire network, so that routing tables on all participating devices are using the same per-virtual-router routing process and tables. Using virtual routers, you create logically-separated networks over the same physical network to ensure the privacy of the traffic that runs through each virtual router.

Because the routing tables are separate, you can use the same, or overlapping, address spaces across the virtual routers. For example, you could use the 192.168.1.0/24 address space for two separate virtual routers, supported by two separate physical interfaces.

Note that there are separate management and data routing tables per virtual router. For example, if you assign a management-only interface to a virtual router, then the routing table for that interface is separate from the data interfaces assigned to the virtual router.

Virtual routers and dynamic VTI

You can create virtual routers, associate dynamic VTIs with these virtual routers, and extend the capabilities of dynamic VTIs in your network. You can associate dynamic VTIs either with global or user-defined virtual routers. You can assign a dynamic VTI to only one virtual router. For more information, refer to Virtual Routers and Dynamic VTI, on page 1368.

Virtual router applications

Virtual router applications are network implementation scenarios that

- isolate networks on shared resources through dedicated routing tables
- enable common security policy management across different departments or networks, and
- provide shared internet access for different departments or networks.

Global and user-defined virtual routers

This reference provides information about global and user-defined virtual routers, including their characteristics and the features supported by each type.

Global virtual routers

For a device with virtual routing capability, system creates a global virtual router by default. The system assigns all interfaces in your network to the global virtual router. A routed interface can belong to either a user-defined virtual router or a global virtual router. When you upgrade Firewall Threat Defense to a version which has virtual router capability, all its existing routing configuration becomes part of the global virtual router.

User-Defined virtual routers

A user-defined virtual router is the one defined by you. You can create more than one virtual router on a device. However, anytime, an interface can be assigned to only one user-defined virtual router. While some of the device features are supported on user-defined virtual routers, few of the features are supported only on the global virtual routers. User-defined virtual routers support route-based site-to-site VPN (static VTI) (static and dynamic VTI).

Supported features and monitoring policies

You can configure these features on the global virtual router only:

- OSPFv3
- RIP

- EIGRP
- IS-IS
- Multicast Routing
- Policy Based Routing (PBR)

ISIS and PBR are supported through Flex Config in Firewall Management Center (see Predefined FlexConfig objects, on page 934). Configure only global virtual router interfaces for these features.

DHCP server auto-configuration uses WINS/DNS server that is learned from an interface. This interface can only be a global virtual router interface.

You can configure these features separately for each user-defined virtual router:

- Static routes and their SLA monitors
- OSPFv2
- BGPv4/v6
- Integrated Routing and Bridging (IRB)
- SNMP

These features are used by the system when querying or communicating with the remote system (from-the-box traffic). These features use interfaces in the global virtual router only. That means, if you configure an interface for the feature, it must belong to the global virtual router. As a rule, anytime, if the system must look up a route to reach an external server for its own management purposes, it does the route lookup in the global virtual router.

- DNS server when used to resolve fully qualified names used in access control rules, or for resolving names for the **ping** command. If you specify **any** as the interface for a DNS server, the system considers interfaces in the global virtual router only.
- AAA server or identity realm when used with VPN. You can configure VPN on interfaces in the global virtual router only. Thus, the external AAA servers that are used for VPN, such as Active Directory, must be reachable through an interface in the global virtual router.

Virtual-router-aware policies

Virtual-router-aware policies are security policies that

- apply to interfaces from a single virtual router only
- use security zones whose memberships are constrained to interfaces assigned to a specific virtual router, and
- prevent policies from affecting all interfaces across all virtual routers when that is not desired.

Virtual router policy behavior

When you create a virtual router, the routing table for that virtual router is automatically separated from the global virtual router or any other virtual router. However, security policies are not automatically virtual-router-aware.

For example, if you write an access control rule that applies to "any" source or destination security zone, then the rule will apply to all interfaces across all virtual routers. This might in fact be exactly what you want. For example, all of your customers might want to block access to the same list of objectionable URL categories.

But, if you need to apply a policy to one of the virtual routers but not others, you need to create security zones that contain interfaces from that single virtual router only. Then, use the virtual-router-constrained security zones in the source and destination criteria of the security policy.

By using security zones whose memberships are constrained to the interfaces assigned to a single virtual router, you can write virtual-router-aware rules in these policies:

- Access control policy.
- Intrusion and file policies.
- SSL decryption policy.
- Identity policy and user-to-IP address mappings. If you use overlapping address spaces in virtual routers, ensure that you create separate realms for each virtual router and apply them correctly in the identity policy rules.

If you use overlapping address spaces in your virtual routers, you should use security zones to ensure that the right policies get applied. For example, if you use the 192.168.1.0/24 address space in two separate virtual routers, an access control rule that simply specifies the 192.168.1.0/24 network will apply to traffic in both virtual routers. If that is not the desired outcome, you can limit the application of the rule by also specifying the source/destination security zones for just one of the virtual routers.

Virtual router interconnection

Virtual router interconnection is a routing mechanism that

- enables traffic routing between virtual routers through route leaking,
- supports both manual static routes and dynamic BGP configurations, and
- allows network segmentation while maintaining controlled inter-segment communication.

Route leaking methods

You can configure the device to route traffic between virtual routers. This process of route leaking can be done manually by setting up static routes or dynamically through BGP settings.

Static route leaking involves manual configuration:

You can configure static routes to route traffic between virtual routers.

For example, if you have the outside interface in the global virtual router, you can set up static default routes in each of the other virtual routers to send traffic to the outside interface. Then, any traffic that cannot be routed within a given virtual router gets sent to the global router for subsequent routing.

Static routes between virtual routers are known as route leaks, because you are leaking traffic to a different virtual router. When you are leaking routes, say, VR1 routes to VR2, you can initiate connections from VR2 to VR1 only. For traffic to flow from VR1 to VR2, you must configure the reverse route. When you create a static route to an interface in another virtual router, you do not need to specify a gateway address. Simply select the destination interface.

For inter-virtual-router routes, the system does destination interface look-up in the source virtual router. Then, it looks up the MAC address of the next hop in the destination virtual router. Thus, the destination virtual router must have either a dynamic (learned) or static route for the selected interface for the destination address.

Configuring NAT rules that use source and destination interfaces in different virtual routers can also allow traffic to route between virtual routers. If you do not select the option for NAT to do a route lookup, the rule will simply send traffic out the destination interface with a NATed address whenever destination translation happens. However, the destination virtual router should have a route for the translated destination IP address so that next-hop lookup can succeed.

Though NAT rule leaks traffic from one virtual router to another, to ensure correct routing, we recommend that you configure a static route leak between these virtual routers for the translated traffic. Without the route leak, sometimes the rule may not match the traffic you expect it to match, and the translation may not be applied.

Virtual routing does not support a cascading or chain of route leaks. For example, assume that your Firewall Threat Defense has VR1, VR2, and VR3 virtual routers; VR3 is directly connected to a network - 10.1.1.0/24. Now, assume you configure a route leak in VR1 for network 10.1.1.0/24 through interface in VR2 and in VR2 define a route leak for 10.1.1.0/24 through VR3. This chain of route leaks will not allow traffic to hop from VR1 to VR2 and then exit from VR3. In case of route leaks, the route lookups first determine egress interface from input Virtual Router's routing table and then looks at the output of Virtual Router's routing table for next hop lookup. From both the lookups, egress interface should match. In our example, the egress interfaces will not be the same and hence the traffic does not pass through.

Use static inter VRF route with caution when the destination network is not a direct-connected subnet of the upstream (outgoing) VR. For example, assume two VRs - VR1 and VR2. While VR1 handles the outgoing traffic which gets the default route from its external peer through BGP or any dynamic routing protocol, and VR2 handles the incoming traffic which is configured with static inter VRF default route with VR1 as the next-hop. When VR1 loses the default route from its peer, VR2 will not able to detect that its upstream (outgoing) VR lost the default route and the traffic is still sent toward VR1 which will eventually get dropped without notifications. In this scenario, we recommend that you configure VR2 with dynamic route leak through BGP.

You can implement an inter-virtual-router route leak by exporting routes from a source virtual router (say VR1) to the source BGP table using route target extended community and then importing the same route target extended community from the source BGP table into the destination BGP table, which in turn is used by the destination virtual router (say, VR2). You can use the route maps for filtering the routes. The routes of global virtual router can also be leaked to user-defined virtual routers and vice versa. The BGP inter-virtual-router route leaking supports both ipv4 and ipv6 prefixes.

For details on configuring BGP route leaking, see Configure BGP route import and export, on page 1125.

BGP route leaking guidelines:

- Ensure that all the routes required for recursion are imported and present in the routing table of the ingress virtual router.
- ECMP is supported per virtual router. Hence, do not configure an ECMP across different virtual routers. The overlapping prefixes imported from different virtual routers cannot form an ECMP. That is, when you attempt to import routes with overlapping addresses from two different virtual routers to other virtual routers (a global virtual router or n user-defined virtual router), only one route (as per BGP best path algorithm, the first route that was advertised) is imported to the respective virtual routing table. For example, if a network 10.10.0.0/24, connected to VR1 is advertised through BGP to a global virtual router first, and later another network with the same address 10.10.0.0/24, connected to VR2 is also advertised through BGP to global virtual router, only the VR1 network route is imported to the global virtual routing table.

- OSPFv3 is not supported on user-defined virtual routers. Hence, do not configure BGPv6 to leak OSPFv3 user-defined virtual routers to global virtual router. However, you can configure BGPv6 to leak OSPFv3 global virtual router routes to user-defined virtual router through redistribution.
- It is recommended to keep VTI interface, protected internal interfaces (loopback interface if supported for VTI) to be part of same virtual router to prevent the need for route leak.

Best practice for overlapping IP addresses

Virtual router creates multiple instances of routing tables that are independent, thereby, the same or overlapping IP addresses can be used without conflicts. Firewall Threat Defense allows the same network to be part of two or more virtual routers. This involves multiple policies to be applied at the interface or at the virtual router level.

Limitations with overlapping IP addresses

When using an overlapping IP address in multiple virtual routers, to ensure proper application of the policy, you have to modify policies or rules for some of the features. Such features require you to use more specific interface either by splitting existing security zone or using new interface group as the need be.

- Network Map—Modify the network discovery policy to exclude some overlapping IP segments to ensure that there is no overlapping IP address being mapped.
- Identity Policy—The identity feed source cannot differentiate among virtual routers; to overcome this limitation, map overlapping address spaces or virtual routers in different realms.
- Access Policy—Apply rules on specific interfaces to ensure that different policies are applied on overlapping IP segments.
- Prefilter Policy—Apply rules on specific interfaces to ensure that different policies are applied on overlapping IP segments.
- QoS/Rate Limit—Apply rules on specific interfaces to ensure that different policies are applied on overlapping IP segments.
- SSL Policy—Apply rules on specific interfaces to ensure that different policies are applied on overlapping IP segments.

Unsupported features with overlapping IP addresses

These features are not supported with overlapping IP addresses:

- ISE SGT-based Rule in AC Policy—The static security group tag (SGT) to IP address mappings downloaded from Cisco Identity Services Engine (ISE) are not virtual-router-aware. Set up separate ISE systems per virtual router if you need to create different SGT mappings per virtual router. This is not necessary if you intend to map the same IP addresses to the same SGT number in each virtual router.
- Overlapping DHCP server pools are not supported across virtual routers.
- Events and Analytics—Many of the Firewall Management Center analytics are dependent on network map and identity mappings which cannot differentiate if the same IP address belongs to two different end hosts. Hence, these analytics are not accurate when there are overlapping IP segments existing in same device but different virtual routers.

Other than few exceptions, the routing functions and most of the NGFW and IPS capability does not get impacted by the overlapping IP addresses.

Configuring SNMP on user-defined virtual routers

In addition to supporting SNMP on the management interface and Global virtual router data interfaces, Secure Firewall Threat Defense now allows you to configure SNMP host on user-defined virtual routers.

Summary

The key components involved in configuring SNMP on user-defined virtual routers are:

- Device interfaces: Physical or logical interfaces that need to be configured and enabled
- Virtual router: User-defined virtual router configured on specific interfaces
- SNMP hosts: Network management stations that receive SNMP polling and traps
- Secure Firewall Threat Defense: The target device where configurations are deployed

Workflow

The SNMP configuration on user-defined virtual routers involves these stages:

1. Configure device interfaces.
2. Configure virtual router on an interface.
3. Configure SNMP hosts on a virtual router interface.



Note SNMP is not virtual router-aware. Hence, while configuring SNMP server on the user-defined virtual router, ensure that the network address is not an overlapping IP address.

4. Deploy configurations to Secure Firewall Threat Defense.

   On successful deployment, the SNMP polling and traps are sent to the Network Management Station through the virtual router interface.

Maximum number of virtual routers by device model

The maximum number of virtual routers you can create depends on the device model. The following table shows the maximum supported virtual routers per model. You can confirm the maximum for your system by entering the **show vrf counters** command, which displays the maximum number of user-defined virtual routers for your platform (not including the global virtual router). The numbers below include both user and global routers. For Firepower 4100/9300 devices, these values apply to native mode.

For platforms that support multi-instance capability, such as the Firepower 4100/9300, determine the maximum number of virtual routers per container instance by dividing the maximum virtual routers by the number of cores on the device, and then multiplying by the number of cores assigned to the instance, rounding down to the nearest whole number. For example, if the platform supports a maximum of 100 virtual routers, and it has

70 cores, then each core would support a maximum of 1.43 virtual routers (rounded). Thus, an instance assigned 6 cores would support 8.58 virtual routers, which rounds down to 8, and an instance assigned 10 cores would support 14.3 virtual routers (rounding down, 14).

Device Model	Maximum Virtual Routers
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Secure Firewall 4215	100
Secure Firewall 4225	100
Secure Firewall 4245	100
Firepower 9300 appliance, all models	100
Firewall Threat Defense Virtual, all platforms	30
ISA 3000	10

Related Topics

Requirements and prerequisites for container instances, on page 250

Requirements and prerequisites for virtual routers

This reference provides the essential requirements and prerequisites that must be met before deploying and configuring virtual routers in your network environment.

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

Network Admin

Security Approver

Guidelines and limitations for virtual routers

Firewall mode guidelines

Use virtual routers on routed firewall mode only.

Interface guidelines

Configure interfaces for virtual routers according to these guidelines:

- Assign an interface to only one virtual router.
- A virtual router can have any number of interfaces that are assigned to it.
- Assign only routed interfaces with logical names and VTIs to a user-defined virtual router.
- If you want to change a virtual router interface to a non-routed mode, remove the interface from the virtual router, and then change its mode.
- You can assign an interface to a virtual router, either from a global virtual router or from another user-defined virtual router.
- Do not assign these interfaces to a user-defined virtual router:
  - Members of EtherChannel.
  - Members of Redundant interfaces.
  - Members of BVI.
- VTI is a route-based VPN. When the tunnel is established, control the traffic that uses VTI for encryption through routing. Static routing, as well as dynamic routing with BGP, OSPFv2/v3, or EIGRP is supported.

- Do not use interfaces that belong to user-defined virtual routers in policy-based site-to-site or remote access VPNs.
- A dynamic VTI and its corresponding protected network interface must be part of the same virtual router.
- You must map the borrow IP interface and the dynamic VTI to the same virtual router.
- User-defined virtual routers support only BGPv4/v6 and OSPFv2 routing protocols.
- A tunnel source interface can be in a different user-defined virtual router than that associated with the dynamic VTI.

Follow these precautions when moving interfaces between virtual routers:

- If a route using the interface that is being moved or its virtual router is deleted, exist in source or destination virtual router table, remove the routes before the interface movement or virtual router deletion.
- As separate routing tables are maintained for each virtual router, when an interface is moved from one virtual router to another virtual router, be it global or user-defined, the system removes the IP address configured on the interface temporarily. All existing connections on the interface are terminated. Thus, moving interfaces between virtual routers have drastic effect on the network traffic. Hence take precautionary measures before you move interfaces.

Global virtual router guidelines

Consider these guidelines for global virtual routers:

- The interfaces which are named and not part of other virtual routers, are part of the global virtual router.
- Do not remove routed interfaces from global virtual router.
- Do not modify global virtual router.
- Generally, after configuring interfaces, if you un-register and register back to same or another Firewall Management Center, interface configuration is imported back from device. With virtual router support, there is a restriction—the IP address for only global virtual router interfaces is retained.

Clustering guidelines

Consider these limitations when using virtual routers with clustering:

- When the control unit link fails due to failure of its interfaces, the unit removes all leaked routes of its interfaces from the global routing table and propagates the inactive connected and static routes to other units of the cluster. This results in removal of those leaked routes from the routing table in other units. These removal takes place prior to another unit becoming a new control unit, which takes approximately 500 ms. When another unit becomes the new control unit, these routes are learned and added back to the routing tables through BGP convergence. Thus, till the convergence time, approximately one minute, the leaked routes are not available for the routing events to take place.
- When a control role change occurs in a cluster, the leaked routes learnt through BGP is updated with the best ECMP path. However, the non-best ECMP path is removed from the cluster routing table only after the BGP reconvergence timer elapses, that is 210 seconds. Thus, till the BGP reconvergence timer elapse, the old, non-best ECMP path persist as preferred route for routing events.

Additional guidelines

Follow these additional guidelines when configuring virtual routers:

- While configuring BGP for virtual routers, you can redistribute the routes belonging to different protocols within the same virtual routers. For example, OSPF VR2 routes cannot be imported into BGP VR1. You can only redistribute OSPF VR2 into BGP VR2, and then configure a route leak between BGP VR2 and BGP VR1.
- Do not use IPv6 ACL for filtering the routes in the route map. Only prefix list is supported.
- Security Intelligence Policy—The Security Intelligence policy is not virtual-router-aware. If you add an IP address, URL, or DNS name to the block list, it is blocked for all virtual routers. This limitation is applicable on the interface having security zones.
- NAT Rules—Do not mix interfaces in NAT rules. In virtual routing, if the specified source and destination interface objects (interface groups or security zones) have interfaces that belong to different virtual routers, the NAT rule diverts traffic from one virtual router through another virtual router. The NAT does the route lookup in the virtual router table for the inbound interface only. If necessary, define static routes in the source virtual router for the destination interface. If you leave the interface as **any**, the rule applies to all interfaces regardless of virtual router membership.
- DHCP Relay—Interconnecting virtual routers for DHCP relay is not supported. For example, if DHCP relay client is enabled on VR1 interface and DHCP relay server is enabled on VR2 interface, the DHCP requests will not be forwarded outside of VR2 interface.
- Recreating a deleted virtual router—When you recreate a virtual router that was deleted less than 10 seconds earlier, an error message appears stating that deletion of the virtual router is in progress. If you want to recreate a deleted virtual router successively, use a different name for the new virtual router.
- The Threat Defense Snort engine maintains state for each traffic flow and is designed to inspect each flow exactly once. Duplicate or double inspection is unsupported when repeated traffic maps to the same Snort flow key, because the subsequent instance is associated with the existing per-flow state and may be identified as an anomaly.

  This can occur when a flow re-enters the device through a different interface or VLAN, is rerouted by an ACI fabric with different VLAN tags, or traverses VRF cross-VLAN paths. The resulting drop may appear in packet-tracer or capture output as:

  ```
  Drop-reason: (stream) Blocked or blacklisted by the stream preprocessor.
  ```

  If a flow-identifying attribute differs such that the traffic maps to a different Snort flow key, Snort can process the flows independently. However, differences in fields that are not part of the flow key do not create a separate flow.

  From an optimal network architecture perspective, each traffic flow, in both directions, should traverse the Snort engine only once. If duplicate inspection cannot be avoided, use a prefilter or fastpath rule to bypass Snort inspection for the affected flows.

Manage virtual routers

When you click **Manage Virtual Routers** on the Virtual Routers pane, the Manage Virtual Routers page appears. This page displays the existing virtual routers on the device and the associated interfaces. On this page, you can **Add Virtual Router** ( ) to the device. You can also **Edit** ( ) and **Delete** ( ) user-defined

virtual routers. You cannot edit or remove a global virtual router. You can only **View** (🔍) the details of a global virtual router.

Create a virtual router

Create a virtual router to enable network segmentation and manage routing configurations independently within the firewall device.

Virtual routers allow you to segment network traffic and create separate routing domains within a single firewall device, providing enhanced network management and security isolation.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **Manage Virtual Routers**.

Step 4 Click **Add Virtual Router** (+).

Step 5 In the Add Virtual Router box, enter a name and description for the virtual router.

Note If you are creating a virtual router that was deleted less than 10 seconds earlier, an error message appears stating that deletion of the virtual router is in progress. If you want to create a deleted virtual router successively, use a different name for the new virtual router.

Step 6 Click **Ok**.

The Routing page appears, displaying the newly created virtual router page.

The virtual router is successfully created and appears in the routing configuration interface, ready for further configuration.

What to do next

- Configure a Virtual Router.

Configure a virtual router

Configure a virtual router to assign interfaces and set up routing policies for network traffic management and routing capabilities on your device.

You can assign interfaces to a user-defined virtual router and configure the routing policies for the device. Though you cannot manually add or remove interfaces for a global virtual router, you can configure the routing policies for the device interfaces.

Before you begin

- To configure routing policies for a user-defined virtual router, add a router. See Create a virtual router, on page 1002.
- All routing configuration settings of a non-virtual routing capable device are also available for a global virtual router. For information on the settings, see Routing Settings.
- Only limited routing protocols are supported for a user-defined virtual router.

Procedure

Step 1 From the **Devices** > **Device Management** page, edit the virtual-router supported device. Navigate to **Routing**.

For information on the modifications to the routing page, see Modifications to the Firewall Management Center web interface routing page.

Step 2 From the drop-down list, select the desired virtual router.

Step 3 In the **Virtual Router Properties** page, modify the description as needed.

Step 4 To add interfaces, select the interface under the **Available Interfaces** box, and then click **Add**.

Remember these guidelines:

- Only interfaces with a logical name are listed under the **Available Interfaces** box. You can edit the interface and provide a logical name in **Interfaces**. Remember to save the changes for the settings to take effect.
- Only interfaces of global virtual routers are available for assigning; the **Available Interfaces** box lists only interfaces that are not assigned to any other user-defined virtual routers. You can assign physical interfaces, subinterfaces, redundant interfaces, bridge groups, VTIs, and EtherChannels to a virtual router, but not their member interfaces. Because the member interfaces cannot be named, they cannot be used in virtual routing.

  You can assign the diagnostic interface to the global virtual router only.

Step 5 To save the interface settings, click **Save**.

Step 6 To configure the routing policy for the virtual router, click the respective names to open the corresponding settings page:

- **OSPF**—Only OSPFv2 is supported on the user-defined virtual router. All other settings for OSPFv2 are as applicable as for a non-virtual-router-aware interface, except that **Interface** allows you to select only the interfaces of the virtual router that you are configuring. You can define the OSPFv3 and OSPFv2 routing policies for a global virtual router. For information on the OSPF settings, see OSPF, on page 1063.
- **RIP**—You can configure RIP routing policies only for a global virtual router. For information on RIP settings, see RIP, on page 1129.
- **BGP**—This page displays the BGP general settings that you have configured in **Settings**:
  - You cannot modify any of those general settings on this page, except for the router ID settings. You can override the router ID settings that were defined in the **Settings** page by editing them on this page.

- To configure other BGP IPv4 or IPv6 settings, you must enable the BGP option in **BGP** page under **General Settings**.
- BGP configuration for both IPv4 and IPv6 address family are supported for global router and the user-defined virtual router.

For information on configuring BGP settings, see BGP, on page 1107.

- **Static Route**—Use this setting to define where to send traffic for a specific destination network. You can also use this setting to create an inter-virtual-router static route. You can create a leak of connected or static route by using the interfaces of user-defined or global virtual routers. **FMC prefixes** to an interface to indicate that it is belonging to another virtual router and can be used for a route leak. For the route leak to be successful, do not specify next hop gateway.

  The Static Route table displays the virtual router whose interface is used for a route leak in the **Leaked from Virtual Router** column. If it is not a route leak, the column displays N/A.

  Irrespective of which virtual router the static route belongs, a Null0 interface is listed along with the interfaces of the same virtual router to which the static route belongs.

  For information on static route settings, see Static and Default Routes, on page 973.

- **Multicast**—You can configure multicast routing policies only for a global virtual router. For information on multicast settings, see Multicast, on page 1137.

Step 7 To save the routing policy settings, click **Save**.

The virtual router is configured with the assigned interfaces and routing policies you specified.

What to do next

- Modify a virtual router.
- Remove a virtual router.

Modify a virtual router

This task allows you to update the configuration settings of virtual routers to meet changing network requirements.

You can modify the description and other routing policies of a virtual router.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **Manage Virtual Routers**.

All virtual routers along with the assigned interfaces are displayed in the **Virtual Routers** page.

Step 4 To modify a virtual router, click **Edit** (✎) against the desired virtual router.

Note You cannot modify the general settings of the global virtual router. Hence, edit is not available for the global router; instead a **View** ( ) is provided to view the settings.

Step 5 To save the changes, click **Save**.

The virtual router configuration is updated with your changes.

What to do next

- Remove a virtual router.

Remove Virtual Routers

Remove virtual routers when they are no longer needed or when consolidating routing configurations. This helps maintain a clean and efficient network routing structure.

Virtual routers provide network segmentation and routing isolation. When removing virtual routers, all associated interfaces automatically move to the global virtual router, and all routing policies are deleted.

Before you begin

- You cannot delete the Global virtual router. Hence, the delete option is not available for the Global virtual router.
- You can remove multiple virtual routers at a time.
- All the routing policies of the deleted virtual router are also deleted.
- All the interfaces of the deleted virtual router move to the global virtual router.
- If there are any restrictions on the movement of interfaces, such as overlapping IPs, route conflicts, and so on, you can remove the router only after resolving the conflicts.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **Manage Virtual Routers**.

All virtual routers along with the mapped interfaces are displayed in the **Virtual Routers** page.

Step 4 To remove a virtual router, click **Delete** ( ) against the desired virtual router.

Step 5 To remove multiple routers, holding the CTRL key, click the virtual routers that you want to delete. Right-click, and then click **Delete**.

Step 6 To save the changes, click **Save**.

The selected virtual routers are removed from the device configuration. All interfaces from the deleted virtual routers are automatically moved to the global virtual router, and all associated routing policies are permanently deleted.

Monitor virtual routers

To monitor and troubleshoot virtual routers, log into the device CLI and use these commands:

- **show vrf**: Displays the details of the virtual routers and their associated interfaces.
- **show route vrf** <*vrf_name*>: Displays the routing details of a virtual router.
- **show run router BGP all**: Displays the BGP routing details of all virtual router.
- **show run router BGP vrf** <*vrf_name*>: Displays the BGP routing details of a virtual router.
- **show crypto ipsec sa/show crypto ikev2 sa**: Displays the details of the tunnel and the associated virtual router.
- You can monitor the tunnels in the Site-to site monitoring dashboard (**Overview > Site to Site VPN**).

  In the **Tunnel Status** widget, hover over a topology, click View and click **Packet Tracer** to view and troubleshoot the threat defense VPN tunnels.

Configuration examples for virtual routers

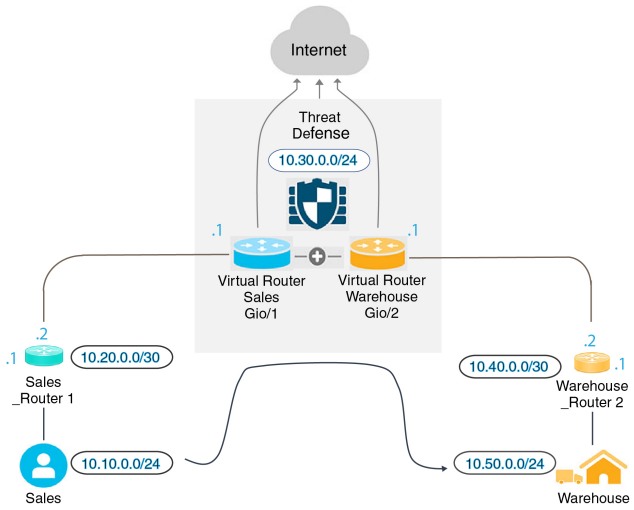
Route to a distant server through virtual routers

This task enables network separation while maintaining connectivity to servers across different virtual routing domains. You can create multiple virtual routers to maintain separate routing tables for groups of interfaces and interconnect them to reach hosts that are multiple hops away.

In virtual routing, you can create multiple virtual routers to maintain separate routing tables for groups of interfaces, thereby achieve network separation. In some scenarios, you may need to access a server that is reachable only through a separate virtual router. This example provides the procedure that interconnects virtual routers to reach to a host that is multiple hops away.

Consider an example, where a member of the sales department of a garment company wants to look up at the stock maintained by the warehousing department of its factory unit. In a virtual routing environment, you need to leak route between virtual routers where destination (warehousing department) is multiple hops away from sales department. This route leaking is done by adding multihop route leak, where, you configure a static route in Sales virtual router(source) to an interface in Warehouse virtual router (destination). As the destination network is multi-hop away, you also need to configure the Warehouse virtual router with the route to the destination network, namely 10.50.0.0/24.

Figure 353: Interconnecting two virtual routers - an example



Before you begin

This example assumes that you have already configured Sales_Router1 to route traffic from 10.20.0.1/30 interface to 10.50.0.5/24.

Follow these steps to route to a distant server through virtual routers:

Procedure

Step 1 Configure the inside interface (Gi0/1) of the device to be assigned to Sales virtual router.

a) Choose **Devices** > **Device Management**, click the device name, and click **Interfaces**.

b) Edit the Gi0/1 interface.

- **Name**—For this example, VR-Sales.
- Select the **Enabled** checkbox.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.
- **IP Address**—Enter 10.30.0.1/24.

c) Click **Ok**.

d) Click **Save**.

Step 2 Configure the inside interface (Gi0/2) of the device to be assigned to Warehouse virtual router.

a) Choose **Devices** > **Device Management**, click the device name, and click **Interfaces**.

b) Edit the Gi0/2 interface.

- **Name**—For this example, VR-Warehouse.
- Select the **Enabled** checkbox.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.

- **IP Address**—Leave it blank. The system does not allow you to configure interfaces with same IP address (10.30.0.1/24), as you are yet to create user-defined virtual routers.

c) Click **Ok**.
d) Click **Save**.

Step 3 Create Sales and Warehouse virtual routers and assign their interfaces.

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Manage Virtual Routers**.
c) Click **Add Virtual Router** and create Sales.
d) Click **Add Virtual Router** and create Warehouse.
e) Select Sales from virtual router drop-down, in **Virtual Router Properties**, add VR-Sales as **Selected Interface** and save.
f) Select Warehouse from virtual router drop-down, in **Virtual Router Properties**, add VR-Warehouse as **Selected Interface** and save.

Step 4 Revisit the VR-Warehouse interface configuration.

a) Choose **Devices** > **Device Management**, click the device name, and click **Interfaces**.
b) Click **Edit** against VR-Warehouse interface. Specify the IP Address as 10.30.0.1/24. The system now allows you to configure with same IP address of VR-Sales, because the interfaces are seperately assigned to two different virtual routers.
c) Click **Ok**.
d) Click **Save**.

Step 5 Create network objects for the warehouse server—10.50.0.0/24, and for the warehouse gateway— 10.40.0.2/30.

a) Choose **Objects** > **Object Management**.
b) Choose **Add Network** > **Add Object**.

- **Name**—For this example, Warehouse-Server.
- **Network**—Click Network and enter 10.50.0.0/24.

c) Click **Save**.
d) Choose **Add Network** > **Add Object**.

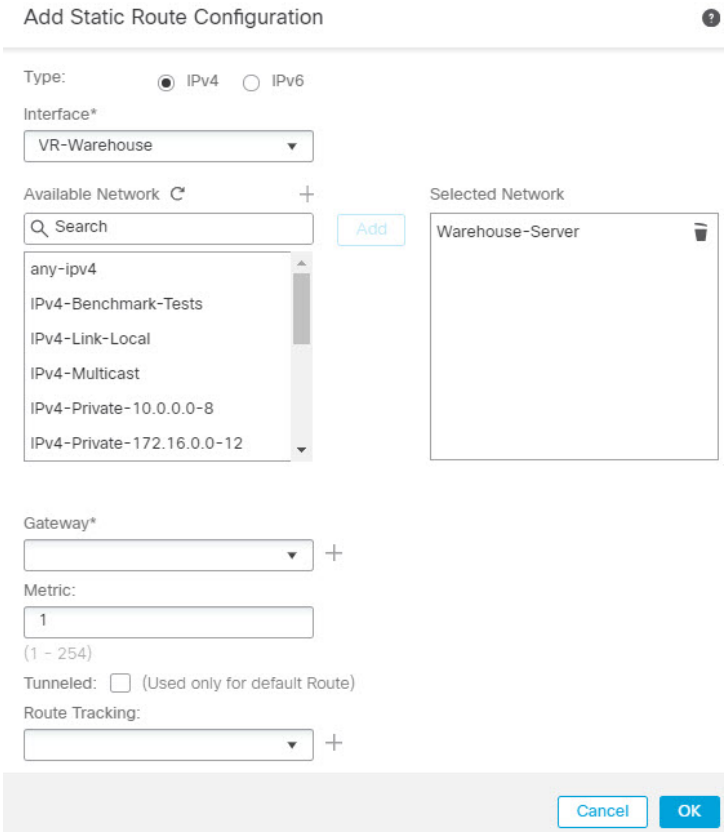
- **Name**—For this example, Warehouse-Gateway.
- **Network**—Click Host and enter 10.40.0.2.

e) Click **Save**.

Step 6 Define the route leak in Sales that points to the VR-Warehouse interface.

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Choose **Routing**.
c) Choose Sales virtual router from the drop-down, and then click **Static Route**.
d) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select VR-Warehouse.
- **Network**—Select the Warehouse-Server object.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, do not select the gateway.

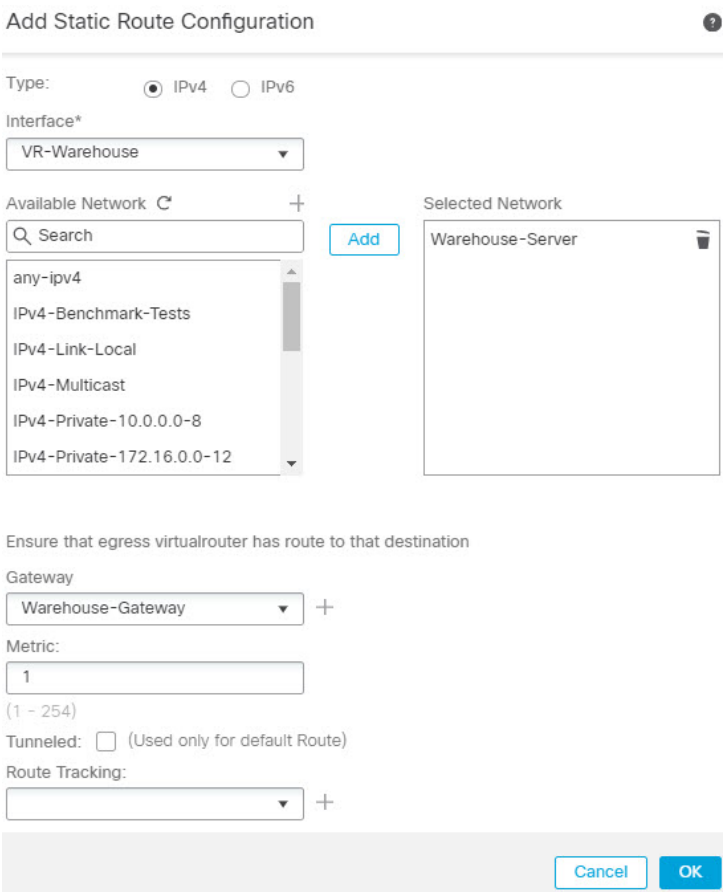


e) Click **Ok**.
f) Click **Save**.

Step 7 In the Warehouse virtual router, define the route that points to the Warehouse Router 2 gateway.

a) Choose Warehouse virtual router from the drop-down, and then click **Static Route**.
b) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select VR-Warehouse.
- **Network**—Select the Warehouse-Server object.
- **Gateway**—Select the Warehouse-Gateway object.



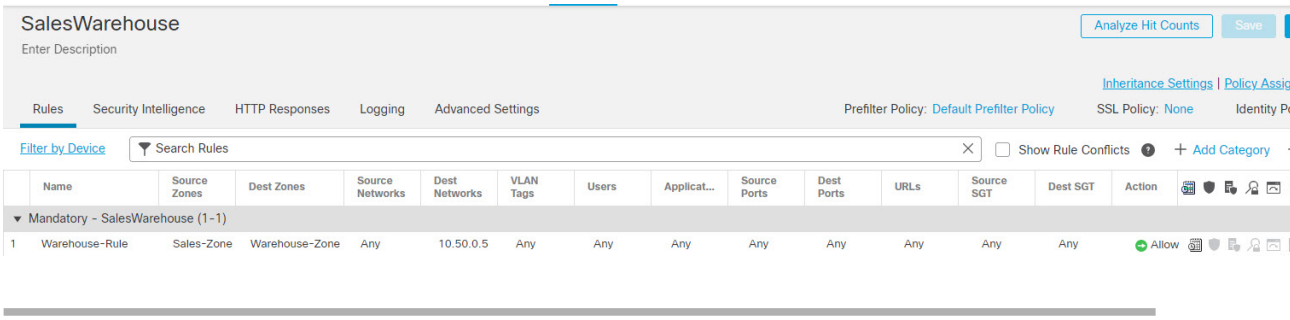
c) Click **Ok**.

d) Click **Save**.

Step 8 Configure access control rule that allows access to the warehouse server. For creating the access control rule, you need to create security zones. Use **Objects** > **Object Management** > **Interface**. Choose **Add** > **Security Zone** and create security zones for VR-Sales and VR-Warehouse; for Warehouse-Server network object, create a Warehouse-Server interface group (Choose **Add** > **Interface Group**).

Step 9 Choose **Policies** > **Access Control heading** > **Access Control** and configure an access control rule to allow traffic from the source interfaces in the Sales virtual router to the destination interfaces in the Warehouse virtual router for the destination Warehouse-Server network object.

For example, if the interfaces in Sales are in the Sales-Zone security zone, and those in Warehouse are in the Warehouse-Zone security zone, the access control rule would look similar to this:



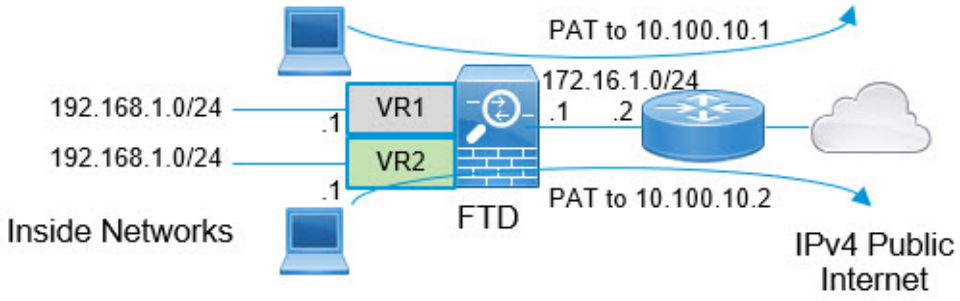
The route leak configuration enables traffic from the Sales virtual router to reach the warehouse server through the Warehouse virtual router. The access control rule allows the required traffic between the security zones.

How to Provide Internet Access with Overlapping Address Spaces

Ensure that endpoints using the same IP address space in different virtual routers can securely access the internet by implementing NAT/PAT policies

When using virtual routers, you can have the same network address for interfaces that reside in separate routers. However, because the IP addresses routed in these separate virtual routers are the same, apply NAT/PAT rules for each interface with separate NAT/PAT pools to ensure that return traffic goes to the correct destination. This example provides the procedure to configure the virtual routers and NAT/PAT rules to manage the overlapping address spaces.

For example, interfaces vr1-inside and vr2-inside on Firewall Threat Defense is defined to use the IP address 192.168.1.1/24, managing endpoints on their segment in the 192.168.1.0/24 network. To allow Internet access from two virtual routers that use the same address space, you need to apply NAT rules separately to the interfaces within each virtual router, ideally using separate NAT or PAT pools. You could use PAT to translate the source addresses in VR1 to 10.100.10.1, and for those in VR2, to 10.100.10.2. The following illustration shows this setup, where the Internet-facing outside interface is part of the global router. You must define the NAT/PAT rules with the source interface (vr1-inside and vr2-inside) explicitly selected—using “any” as the source interface makes it impossible for the system to identify the correct source because the same IP address could exist on two different interfaces.



Note Even if you have some interfaces within virtual routers that does not use overlapping address spaces, define the NAT rule with the source interface to make troubleshooting easier, and to ensure a cleaner separation between traffic from the virtual routers that is Internet-bound.

Procedure

Step 1 Configure the inside interface of the device for VR1:

a) Choose **Devices** > **Device Management**, click the device name, and then click **Interfaces** .

b) Edit the interfaces that you want to assign to VR1:

- **Name**—For this example, vr1-inside.
- Select the **Enabled** checkbox.

- In **IPV4**, for **IP Type**, choose **Use Static IP** .
- **IP Address**—Enter 192.168.1.1/24.

c) Click **Ok** .
d) Click **Save** .

Step 2 Configure the inside interface of the device for VR2:

a) Choose **Devices** > **Device Management** , click the device name, and then click **Interfaces** .
b) Edit the interfaces that you want to assign to VR2:

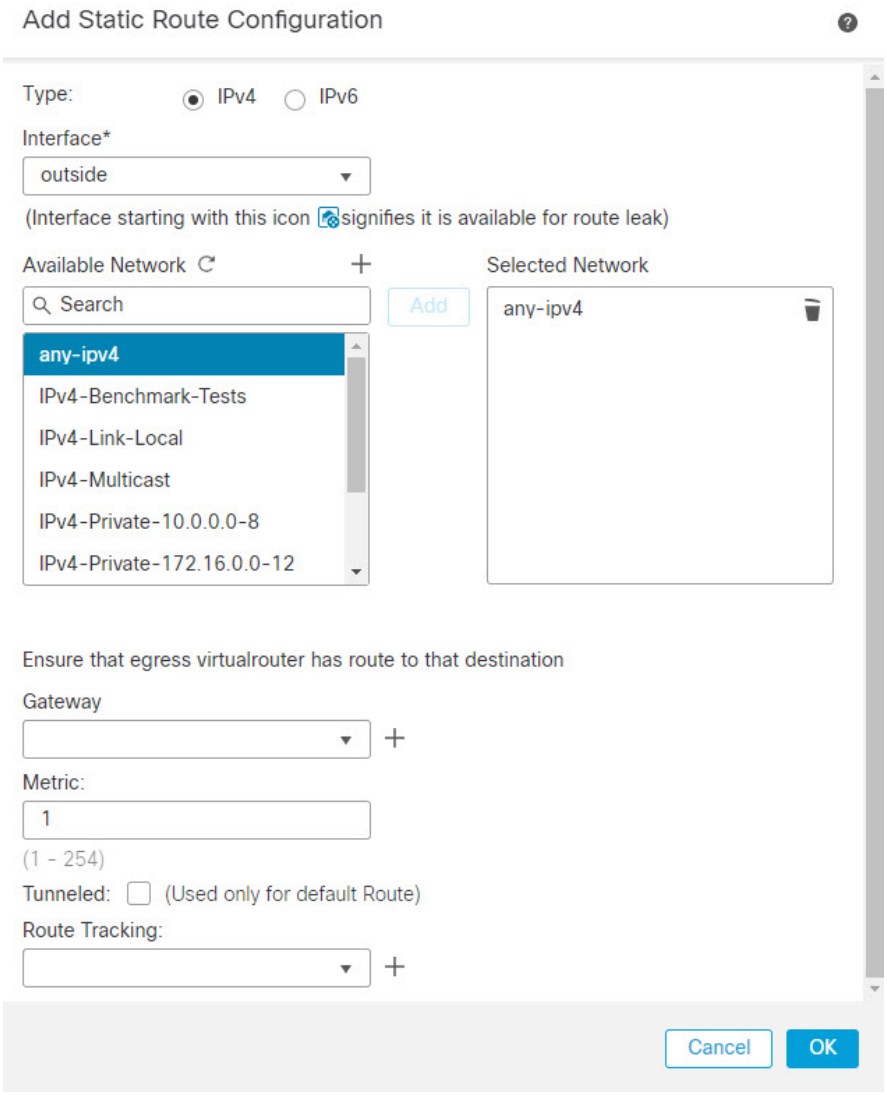
- **Name** —For this example, vr2-inside.
- Select the **Enabled** checkbox.
- In **IPV4** , for **IP Type** , choose **Use Static IP** .
- **IP Address** —Leave it blank. The system does not allow you to configure interfaces with same IP address, as you are yet to create user-defined virtual routers.

c) Click **Ok** .
d) Click **Save** .

Step 3 Configure VR1 and the static default route leak to the outside interface:

a) Choose **Devices** > **Device Management** , and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Manage Virtual Routers** . Click **Add Virtual Router** and create VR1.
c) For VR1, in **Virtual Router Properties** , assign vr1-inside and save.
d) Click **Static Route**.
e) Click **Add Route**. In **Add Static Route Configuration** , specify the following:

- **Interface** —Select the outside interface of the global router.
- **Network** —Select the any-ipv4 object. This network is the default route for any traffic that cannot be routed within VR1.
- **Gateway** —Leave it blank. When leaking a route into another virtual router, do not provide a Gateway.

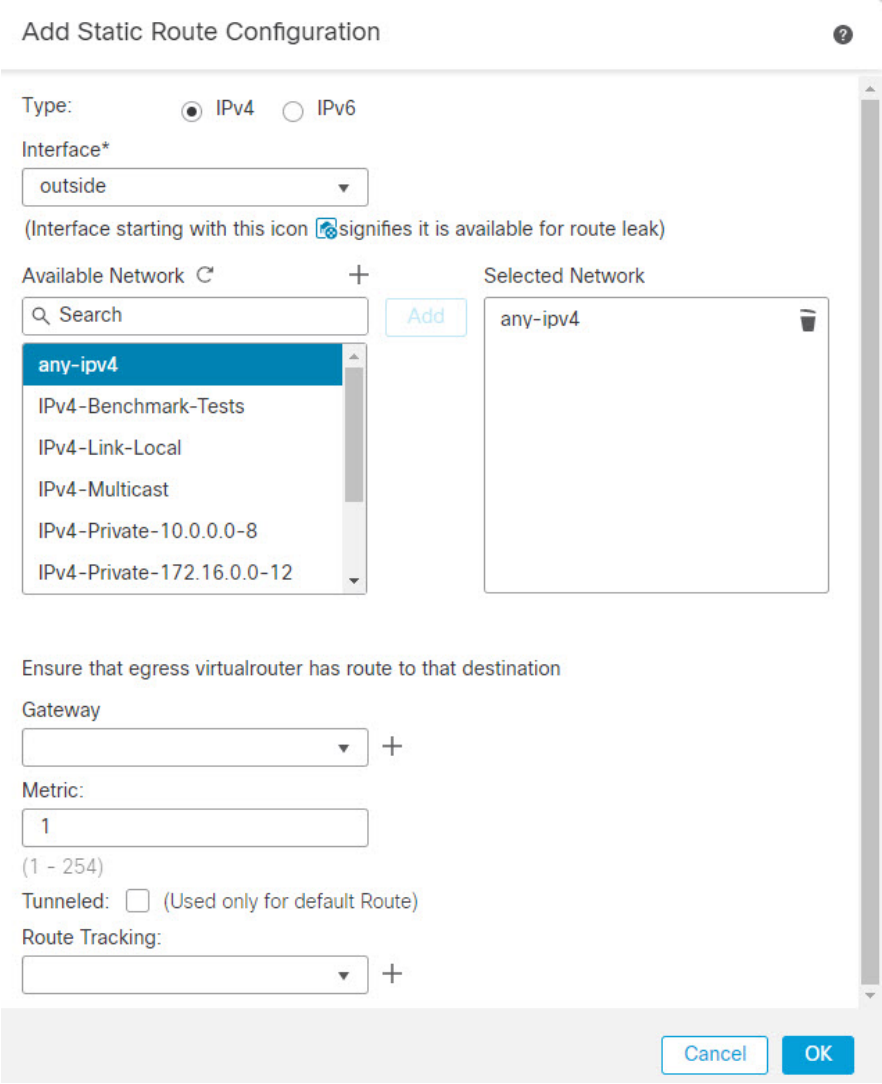


f) Click **Ok**.
g) Click **Save**.

Step 4 Configure VR2 and the static default route leak to the outside interface:

a) Choose **Devices** > **Device Management** , and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Manage Virtual Routers**. Click **Add Virtual Router** and create VR2.
c) For VR2, in **Virtual Router Properties**, assign vr2-inside and save.
d) Click **Static Route**.
e) Click **Add Route**. In **Add Static Route Configuration** , specify the following:

- **Interface** —Select the outside interface of the global router.
- **Network** —Select the any-ipv4 object. This network is the default route for any traffic that cannot be routed within VR2.
- **Gateway** —Leave it blank. When leaking a route into another virtual router, do not select the Gateway.



f) Click **Ok**.

g) Click **Save**.

Step 5 Configure IPv4 static default route, namely 172.16.1.2 on the outside interface of the global router:

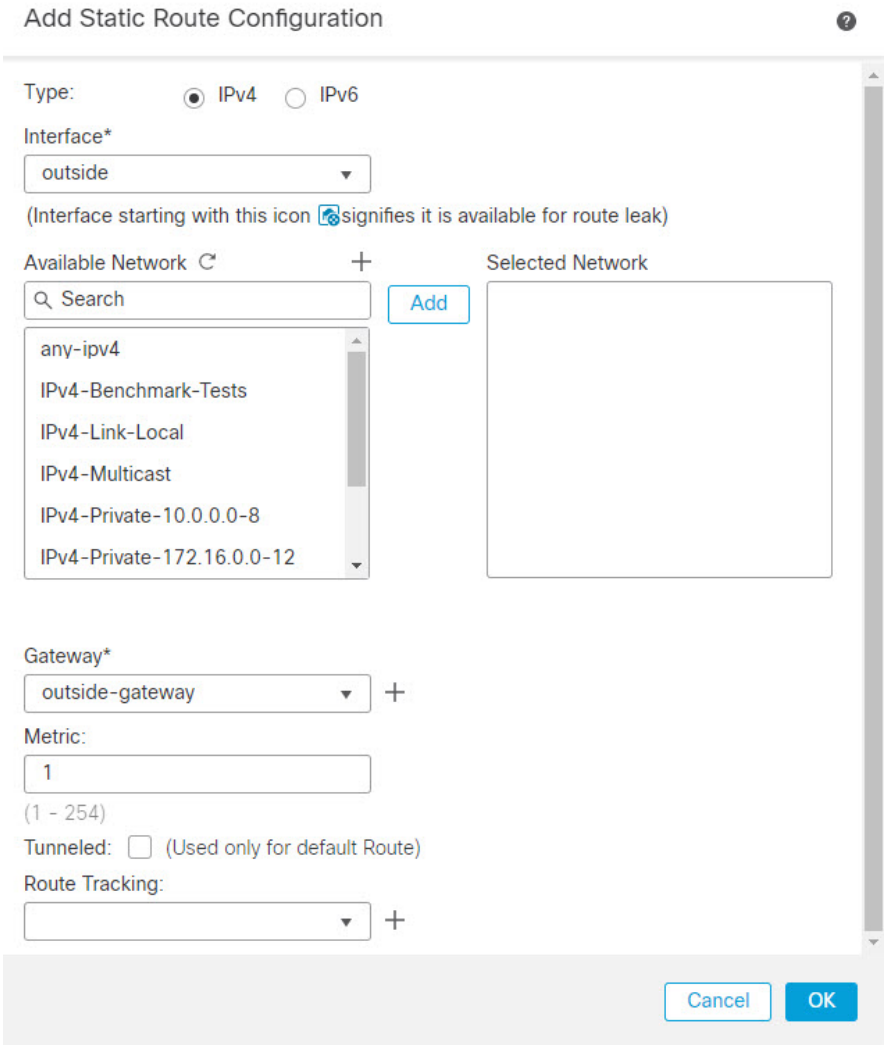
a) Choose **Devices** > **Device Management** , and edit the Firewall Threat Defense device.

b) Choose **Routing** and edit global router properties.

c) Click **Static Route** .

d) Click **Add Route** . In **Add Static Route Configuration** , specify the following:

- **Interface** —Select the outside interface of the global router.
- **Network** —Select the any-ipv4 object. This will be the default route for any IPv4 traffic.
- **Gateway** —If already created, select the host name from the drop-down. If the object is not yet created, click **Add** and define the host object for the IP address of the gateway at the other end of the network link on the outside interface, in this example, 172.16.1.2. After you create the object, select it in the Gateway field.



e) Click **Ok** .
f) Click **Save** .

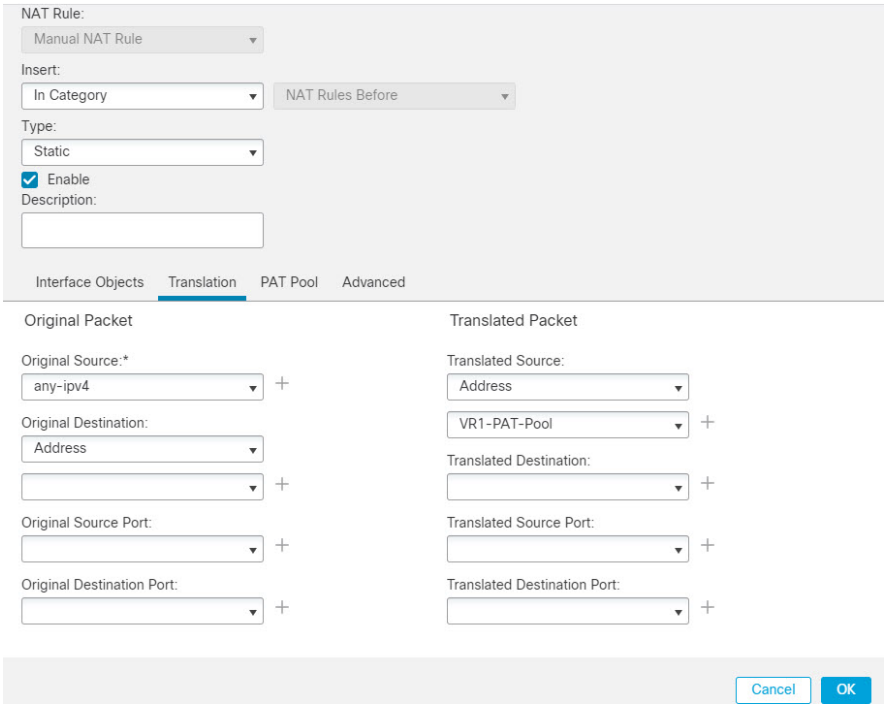
Step 6 Revisit the vr2-inside interface configuration:

a) Choose **Devices** > **Device Management** , click the device name, and then click **Interfaces** .
b) Click **Edit** against vr2-inside interface. Specify the IP Address as 192.168.1.1/24. The system now allows you to configure with same IP address of vr1-inside, because the interfaces are separately assigned to two different virtual routers.
c) Click **Ok** .
d) Click **Save** .

Step 7 Create the NAT rule to PAT inside to outside traffic of VR1 to 10.100.10.1.

a) Choose **Devices** > **NAT**.
b) Click **New Policy** > **Threat Defense NAT**.
c) Enter InsideOutsideNATRule as the NAT policy name, and select the Firewall Threat Defense device. Click **Save** .
d) In InsideOutsideNATRule page, click **Add Rule** and define the following:

- **NAT Rule** —Select Manual NAT Rule.
- **Type** —Select Dynamic.
- **Insert** —Above, if any dynamic NAT rule exists.
- Click **Enabled** .
- In **Interface Objects** , select vr1-interface object and click **Add to Source** (If the object is not available, create one in **Objects** > **Object Management** > **Interface**), and select outside as **Add to Destination** .
- In **Translation** , for **Original Source** , select any-ipv4. For **Translated Source** , click **Add** and define host object VR1-PAT-Pool with 10.100.10.1. Select VR1-PAT-Pool as shown in the figure below:



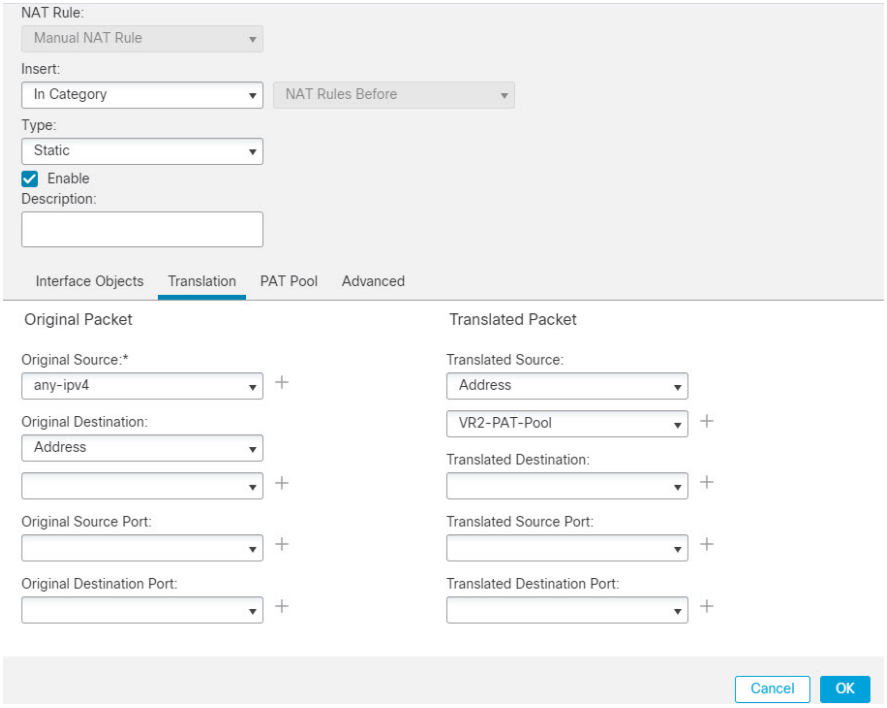
e) Click **Ok** .
f) Click **Save** .

Step 8 Add NAT rule to PAT inside to outside traffic of VR2 to 10.100.10.2.

a) Choose **Devices** > **NAT** .
b) Edit InsideOutsideNATRule to define the VR2 NAT rule:

- **NAT Rule** —Select Manual NAT Rule.
- **Type** —Select Dynamic.
- **Insert** —Above, if any dynamic NAT rule exists.
- Click **Enabled** .

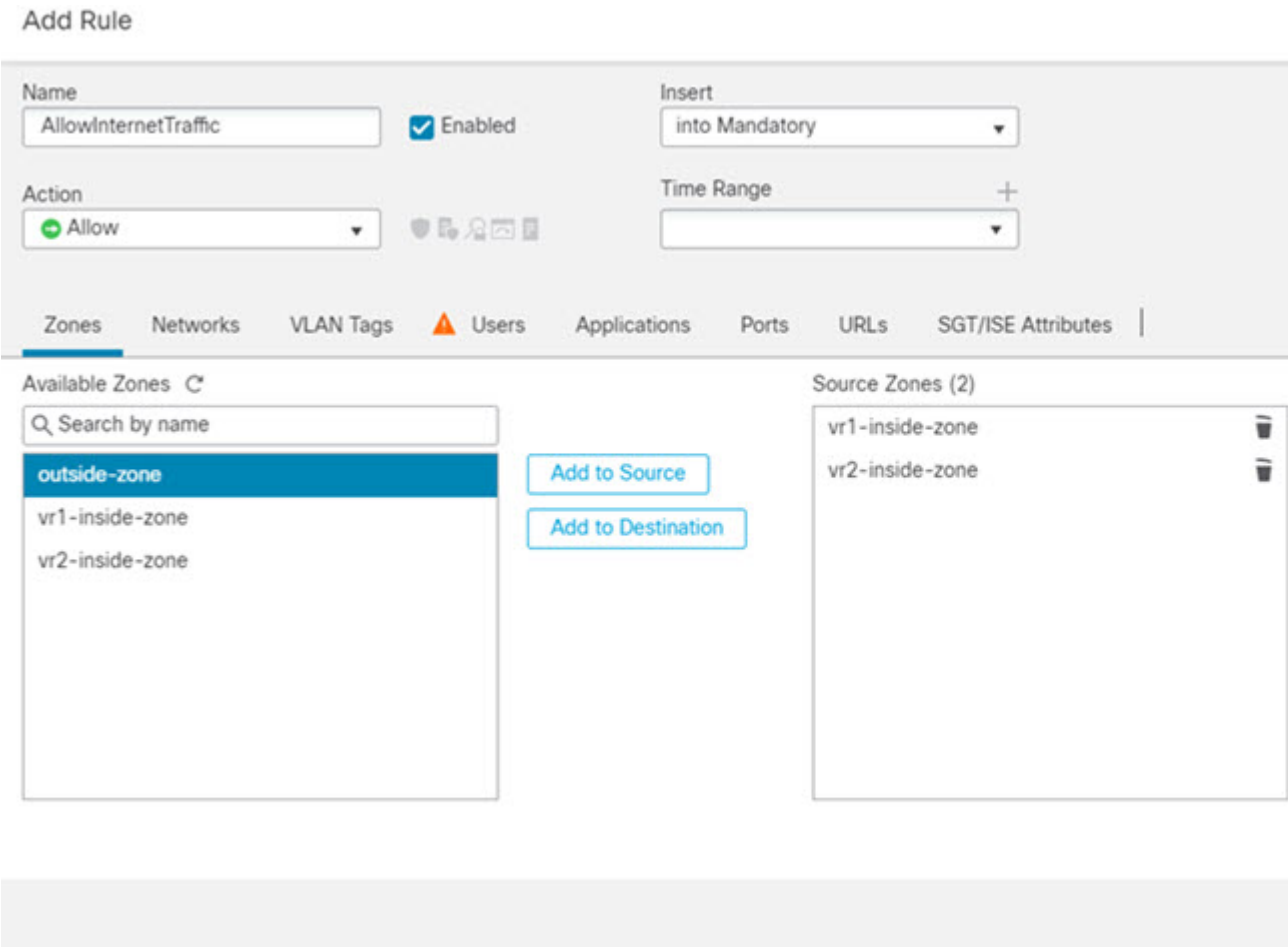
- In **Interface Objects** , select vr2-interface object and click **Add to Source** (If the object is not available, create one in **System** (⚙) > **Configuration** > **Management Interfaces**), and select outside as **Add to Destination** .
- In **Translation** , for **Original Source** , select any-ipv4. For **Translated Source** , click **Add** and define host object VR2-PAT-Pool with 10.100.10.2. Select VR2-PAT-Pool as shown in the figure below:



c) Click **Ok** .
d) Click **Save** .

Step 9 To configure the access control policy that allows traffic from the vr1-inside and vr2-inside interfaces to the outside interface, you need to create security zones. Use **Objects** > **Object Management** > **Interface** . Choose **Add** > **Security Zone** and create security zones for vr1-inside, vr2-inside, and outside interfaces. Choose **Policies** > **Access Control heading** > **Access Control** and configure an access control rule to allow traffic from vr1-inside-zone and vr2- inside-zone to outside-zone.

Assuming that you create zones named after the interfaces, a basic rule that allows all traffic to flow to the Internet will look like the following. You can apply other parameters to this access control policy:

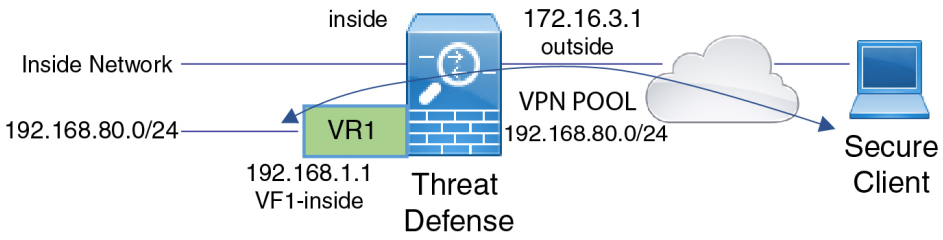


Allow RA VPN access to internal networks in virtual routing

Allow Secure Client users to connect to user-defined virtual router networks by configuring route leaks between the global virtual router and user-defined virtual routers.

On virtual routing-enabled devices, RA VPN is supported only on global virtual router interfaces. This example provides the procedure that allows your Secure Client user to connect to user-defined virtual router networks.

In the following example, the RA VPN (Secure Client) user connects to the outside interface of Firewall Threat Defense at 172.16.3.1, and is given an IP address within the pool of 192.168.80.0/24. The user can access the inside network of only the global virtual router. To allow traffic flow through the network of the user-defined virtual router VR1, namely 192.168.1.0/24, leak the route by configuring the static routes on global and VR1.



Before you begin

This example assumes that you have already configured the RA VPN, defined the virtual routers, and configured and assigned the interfaces to the appropriate virtual routers.

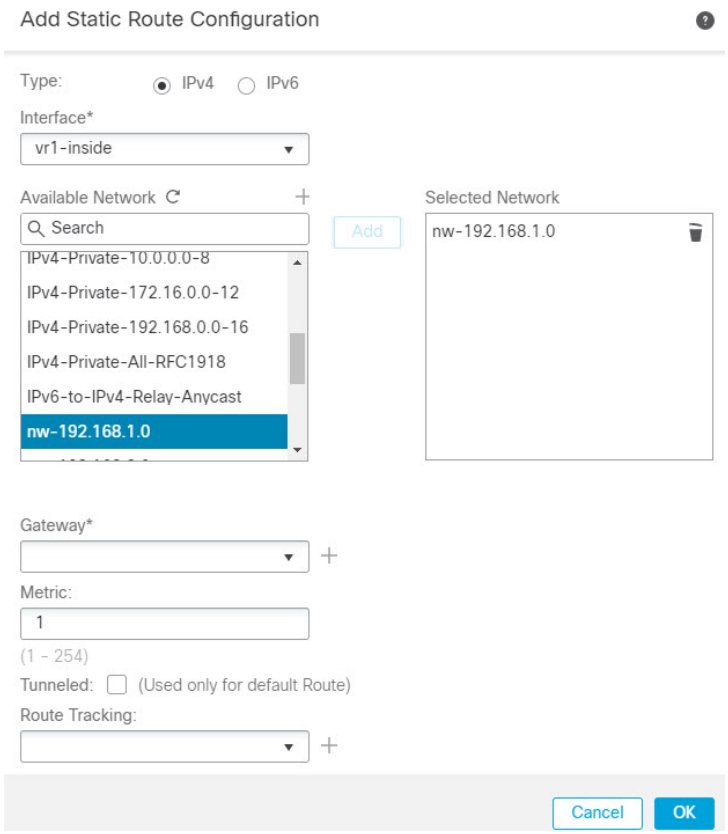
Follow these steps to allow RA VPN access to internal networks in virtual routing:

Procedure

Step 1 Configure route leak from Global virtual router to the user-defined VR1:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Click **Routing**. By default, the Global routing properties page appears.
c) Click **Static Route**.
d) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the VR1 inside interface.
- **Network**—Select the VR1 virtual router network object. You can create one using the **Add Object** option.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, does not select the gateway.



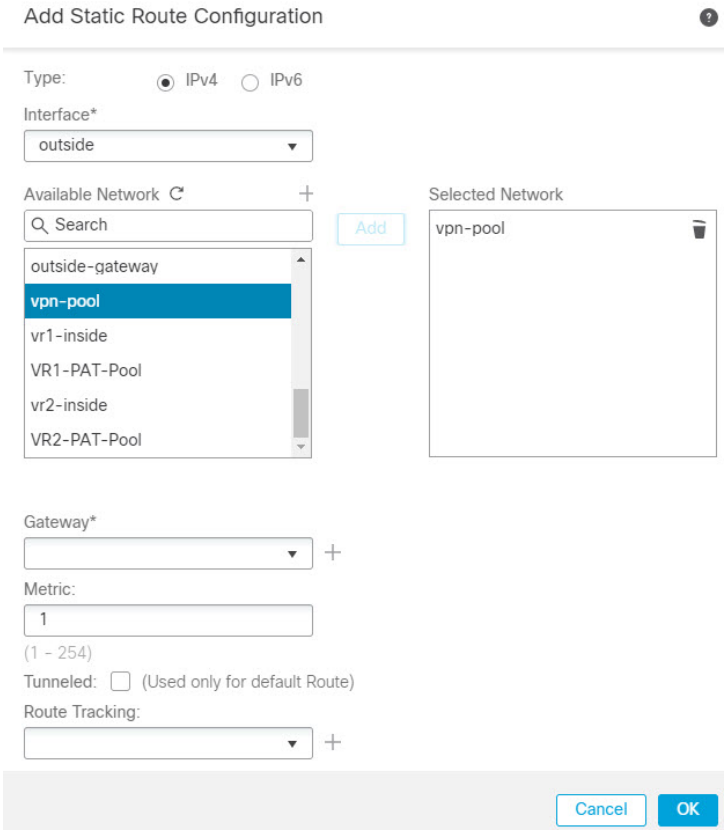
The route leak allows Secure Client assigned IP addresses in the VPN pool to access the 192.168.1.0/24 network in the VR1 virtual router.

e) Click **Ok**.

Step 2 Configure the route leak from VR1 to the Global virtual router:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Click **Routing** and from the drop-down, select VR1.
c) Click **Static Route**.
d) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the outside interface of the global router.
- **Network**—Select the global virtual router network object.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, does not select the gateway.



The configured static route allows endpoints on the 192.168.1.0/24 network (VR1) to initiate connections to Secure Client assigned IP addresses in the VPN pool.

e) Click **Ok**.

Secure Client users can now access networks in both the global virtual router and the user-defined VR1 virtual router through the configured route leaks.

What to do next

If RA VPN address pool and the IP addresses in the user-defined virtual router overlap, you must also use static NAT rules on the IP addresses to enable proper routing. Alternatively, you can change your RA VPN address pool so that there is no overlap.

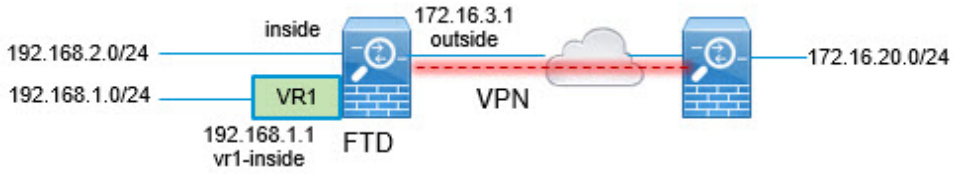
Secure traffic from networks in multiple virtual routers over a site-to-site VPN

This task allows you to secure connections from or to networks hosted within user-defined virtual routers over the site-to-site VPN by configuring route leaking between virtual routers and updating the VPN connection profile.

On virtual routing-enabled devices, Site-to-Site VPN is supported only on global virtual router interfaces. You cannot configure it on an interface that belongs to a user-defined virtual router. This procedure allows you to secure the connections from or to networks hosted within user-defined virtual routers over the site-to-site

VPN. You also need to update the site-to-site VPN connection to include the user-defined virtual routing networks.

Let us consider a scenario, where, a site-to-site VPN is configured between a branch office network to a company headquaters network; the Firewall Threat Defense in the branch office having virtual routers. In this case, the site-to-site VPN is defined on the outside interface of the branch office at 172.16.3.1. This VPN includes the inside network 192.168.2.0/24 without extra configuration, because the inside interface is also part of the global virtual router. But, to provide site-to-site VPN services to the 192.168.1.0/24 network, which is part of the VR1 virtual router, you must leak the route by configuring the static routes on global and VR1, and add the VR1 network to the site-to-site VPN configuration.



Before you begin

This example assumes that you have already configured the site-to-site VPN between the 192.168.2.0/24 local network and the 172.16.20.0/24 external network, defined the virtual routers, and configured and assigned the interfaces to the appropriate virtual routers.

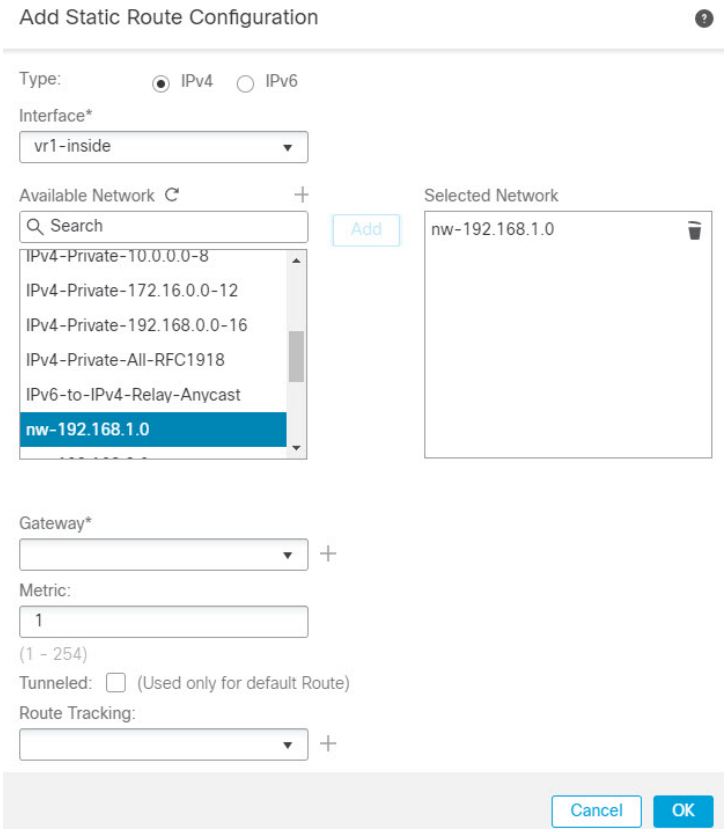
Follow these steps to secure traffic from networks in multiple virtual routers over a site-to-site VPN:

Procedure

Step 1 Configure route leak from the Global virtual router to the user-defined VR1:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Click **Routing**. By default, the Global routing properties page appears.
c) Click **Static Route**.
d) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the VR1 inside interface.
- **Network**—Select the VR1 virtual router network object. You can create one using the **Add Object** option.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, do not select the gateway.



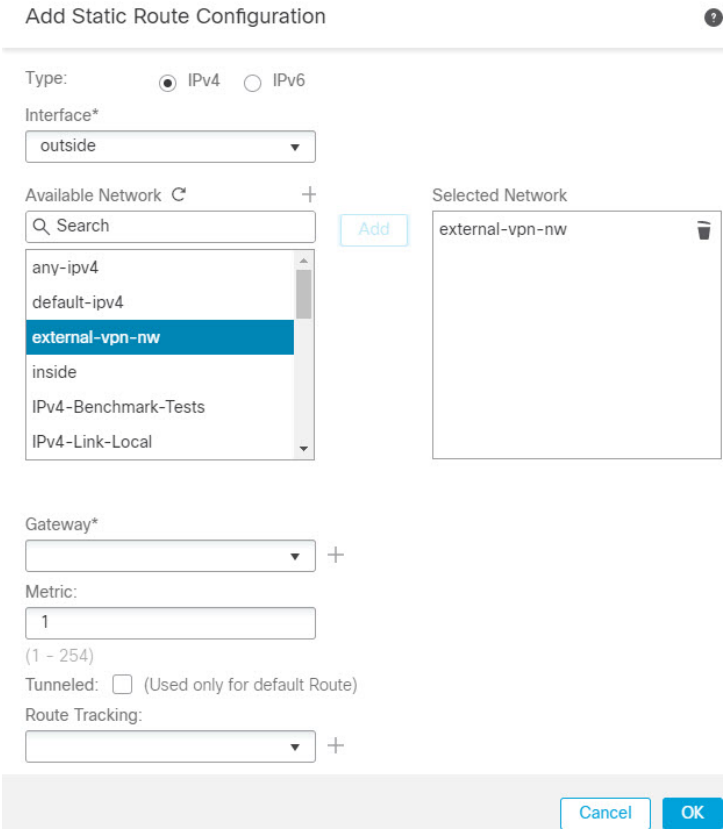
The route leak allows endpoints protected by the external (remote) end of the site-to-site VPN to access the 192.168.1.0/24 network in the VR1 virtual router.

e) Click **Ok**.

Step 2 Configure the route leak from VR1 to the Global virtual router:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Click **Routing** and from the drop-down, select VR1.
c) Click **Static Route**.
d) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the outside interface of the global router.
- **Network**—Select the global virtual router network object.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, do not select the gateway.

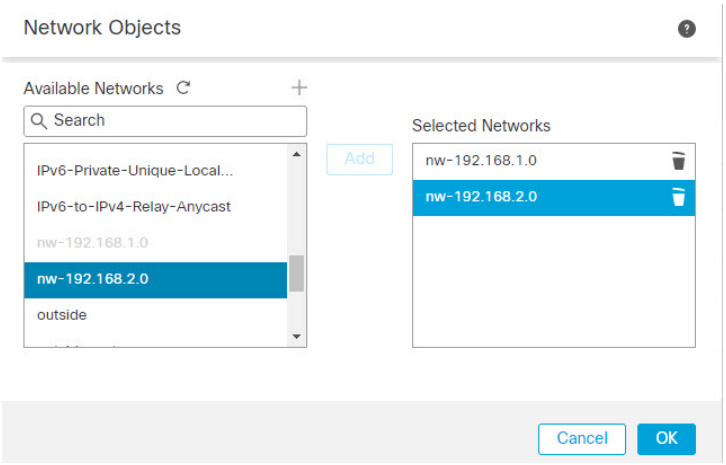


This static route allows endpoints on the 192.168.1.0/24 network (VR1) to initiate connections that will traverse the site-to-site VPN tunnel. For this example, the remote endpoint that is protecting the 172.16.20.0/24 network.

e) Click **Ok**.

Step 3 Add the 192.168.1.0/24 network to the site-to-site VPN connection profile:

a) Choose **Devices** > **VPN** > **Site to Site**, and edit the VPN Topology.
b) In **Endpoints**, edit Node A endpoint.
c) In **Edit Endpoint**, in the **Protected Networks** field, click **Add New Network Object**.
d) Add the VR1 network object with 192.168.1.0 network:



e) Click **Ok** and save the configuration.

The route leaking configuration allows traffic from networks in user-defined virtual routers to traverse the site-to-site VPN tunnel securely, enabling connectivity between the VR1 network and remote networks protected by the VPN.

Secure traffic from networks with multiple virtual routers over a site-to-site VPN with dynamic VTI

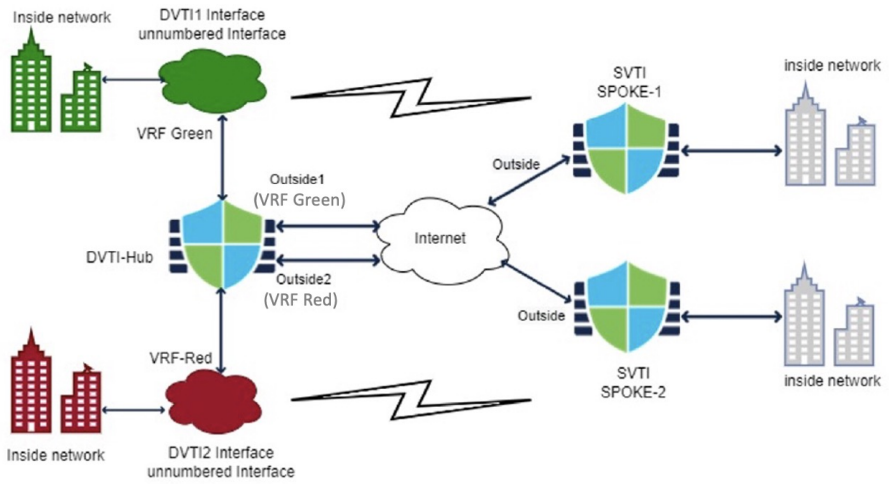
This task enables ISPs to create virtual routers and associate dynamic VTIs with these virtual routers to extend the capabilities of dynamic VTIs in their network. You can associate dynamic VTIs either with global or user-defined virtual routers.

ISPs have different segmented networks for different customers. You can create virtual routers, associate dynamic VTIs with these virtual routers, and extend the capabilities of dynamic VTIs in your network. You can associate dynamic VTIs either with global or user-defined virtual routers. A single threat defense device can act as a dynamic VTI hub with a global or one or more user-defined virtual routers. Each user-defined virtual router can be one customer network.

Let us consider an example where route-based site-to-site VPNs are configured between two company headquarter networks and their two branch office networks. The ISP's threat defense, a dynamic VTI hub, manages the two company headquarter networks with two user-defined virtual routers: VRF green and VRF red. The dynamic VTI hub establishes a site-to-site VPN between:

- Customer 1 (VRF green) and Branch 1 (SVTI spoke 1)
- Customer 2 (VRF red) and Branch 2 (SVT2 spoke 2)

Figure 354: Site-to-Site VPNs with multiple virtual routers and dynamic VTI



Procedure

Step 1 Configure a dynamic VTI interface on the hub.

a) Choose **Devices** > **Device Management** and edit the threat defense device.
b) Choose **Add Interfaces > Virtual Tunnel Interface**.
c) Select the **Tunnel Type** as **Dynamic**.
d) Specify the interface name as DVTI1 and configure all the parameters for the dynamic VTI.
e) Click **Save**
f) Repeat steps 1a - e to configure the second dynamic VTI on the hub, DVTI2.

Step 2 Configure static VTI on spoke 1.

a) Choose **Devices** > **Device Management** and edit the threat defense device.
b) Select **Add Interfaces > Virtual Tunnel Interface**.
c) Select the **Tunnel Type** as **Static**.
d) Specify the interface name as SVTI spoke-1 and configure all the parameters for the static VTI.
e) Click **Save**
f) Repeat steps 2a - e to configure the static VTI on spoke 2: SVTI spoke-2.

Step 3 Configure a route-based site-to-site VPN between hub and SVTI spoke 1.

a) Choose **Devices** > **VPN** > **Site to Site** and click **+ Site To Site VPN**.
b) Enter a name for the VPN topology in the **Topology Name** field.
c) Choose **Route Based (VTI)** and select **Hub and Spoke** as the network topology.
d) Click the **Endpoints** tab.
e) Configure the hub and the spoke (DVTI1 and SVTI spoke-1) and their routing policies.
f) Configure the **IKE**, **IPsec**, and **Advanced** options for the VPN, if required.
g) Click **Save**.
h) Repeat steps 3a - g to configure the second route-based site-to-site VPN topology between hub (DVTI2) and SVTI spoke 2.

Step 4 Configure the two virtual routers.

a) Choose **Devices** > **Device Management** and edit the threat defense device.
b) Click **Routing**.
c) Click **Manage Virtual Routers**.
d) Click **Add Virtual Router**.

Specify the name as VRF green and provide a description for the virtual router.

e) Repeat steps 4a - d to configure VRF red.

Step 5 Assign all the interfaces to the virtual routers.

a) From the drop-down list, select the virtual router.
b) In the **Virtual Router Properties** page, select the interfaces listed under the **Available Interfaces** box.

Assign the dynamic VTI interface along with the other interfaces.

c) Click **Add**.

Step 6 Repeat steps 5a - c for VRF red.

Step 7 Configure the routing policy for the virtual router.

a) From the drop-down list, select the virtual router.
b) Click **Static Route** or one of the dynamic routing protocols.
c) Configure the routing parameters.
d) Click **Save**.

You have successfully configured networks with multiple virtual routers over a site-to-site VPN with dynamic VTI, enabling ISPs to manage different segmented networks for different customers through virtual routers.

What to do next

Select the hub and spoke devices and click **Deploy**. After the deployment, you can monitor the VPN tunnels in the Site-to site monitoring dashboard (**Overview** > **Dashboards** > **Site to Site VPN**).

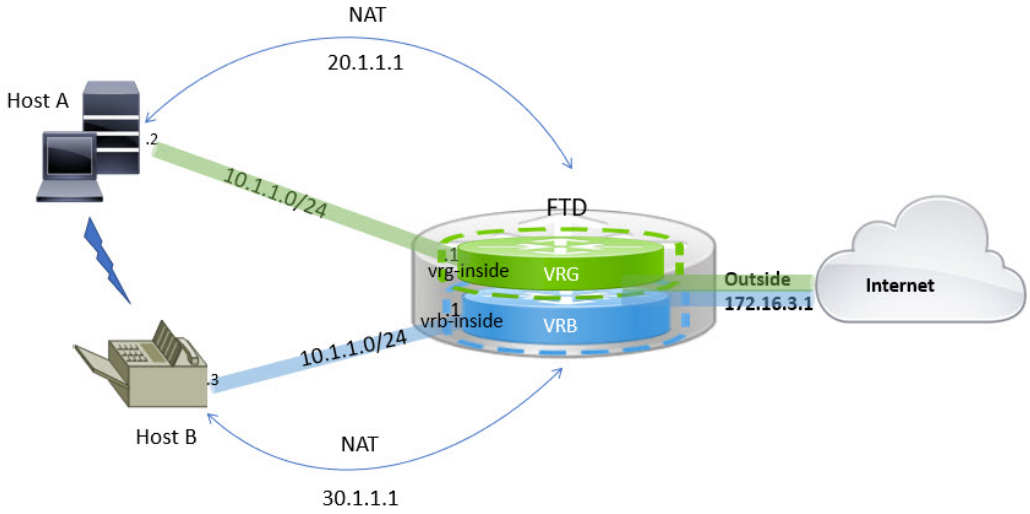
You can also use the commands listed in Monitor virtual routers, on page 1006 to view and troubleshoot the virtual router.

Route traffic between two overlapping network hosts in virtual routing

Configure NAT rules to manage overlapping network hosts and enable communication between hosts on different virtual routers that have the same network address.

You can configure hosts on the virtual routers that have same network address. If the hosts want to communicate, you can configure twice NAT. This example provides the procedure to configure the NAT rules to manage the overlapping network host.

In the following example, two hosts Host A and Host B belong to different virtual routers: VRG (interface VRG-inside), VRB (interface VRB-inside) respectively with the same subnet 10.1.1.0/24. For both the hosts to communicate, create a NAT policy where, VRG-Host interface object would use a mapped NAT address - 20.1.1.1, and VRB-Host interface object would use a mapped NAT address - 30.1.1.1. Thus, Host A uses 30.1.1.1 to communicate to Host B; Host B uses 20.1.1.1 to reach Host A.



Before you begin

This example assumes that you have already configured:

- VRG-inside and VRB-inside interfaces are associated with virtual routers: VRG and VRB respectively and VRG-inside and VRB-inside interfaces configured with same subnet address (say, 10.1.1.0/24).
- Interfaces zones VRG-Inf, VRB-Inf created with VRG-inside and VRB-inside interfaces respectively.
- Host A in VRG with VRG-inside as default gateway; Host B in VRB with VRB-inside as default gateway.

Follow these steps to route traffic between two overlapping network hosts in virtual routing:

Procedure

Step 1 Create the NAT rule to handle traffic from Host A to Host B. Choose **Devices** > **NAT**.

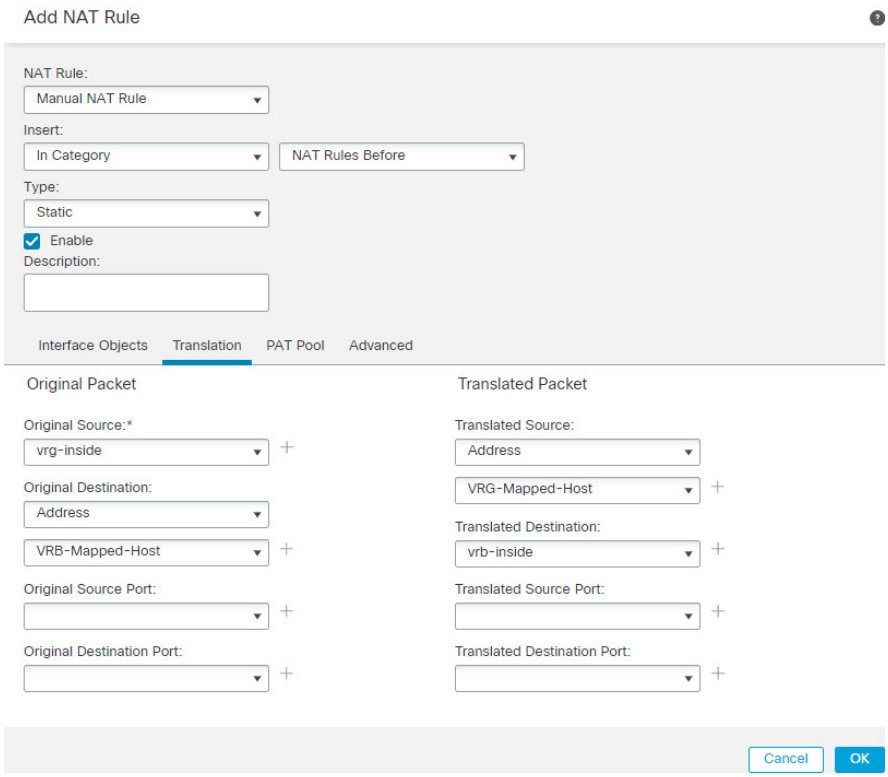
Step 2 Click **New Policy** > **Threat Defense NAT**.

Step 3 Enter a NAT policy name, and select the Firewall Threat Defense device. Click **Save**.

Step 4 In the NAT page, click **Add Rule** and define the following:

- **NAT Rule**—Select Manual NAT Rule.
- **Type**—Select Static.
- **Insert**—Select Above, if any NAT rule exists.
- Click **Enabled**.
- In **Interface Objects**, select VRG-Inf object and click **Add to Source** (If the object isn't available, create one in **Objects** > **Object Management** > **Interface**), and select VRB-Inf object and click **Add to Destination**.
- In **Translation**, select the following:
  - **Original Source**, select VRG-inside.

- **Original Destination**, click **Add** and define object VRB-Mapped-Host with 30.1.1.1. Select VRB-Mapped-Host.
- **Translated Source**, click **Add** and define object, VRG-Mapped-Host with 20.1.1.1. Select VRG-Mapped-Host.
- **Translated Destination**, select VRB-inside as shown in the following figure:



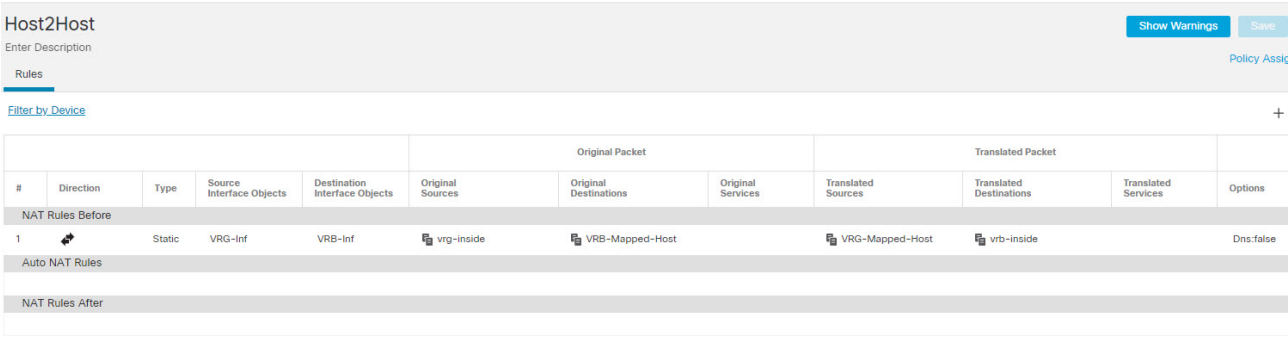
When you run the **show NAT detail** command on the Firewall Threat Defense device, you will see an output similar to this:

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

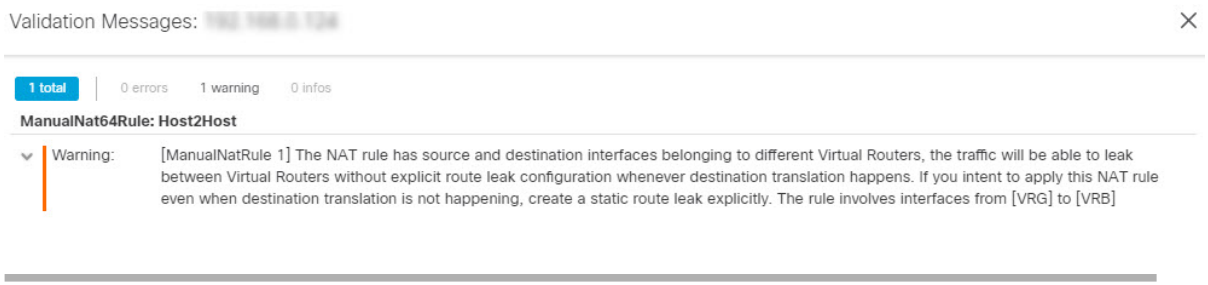
Step 5 Click **Ok**.

Step 6 Click **Save**.

The NAT rule looks like this:



When you deploy the configuration, a warning message appears:



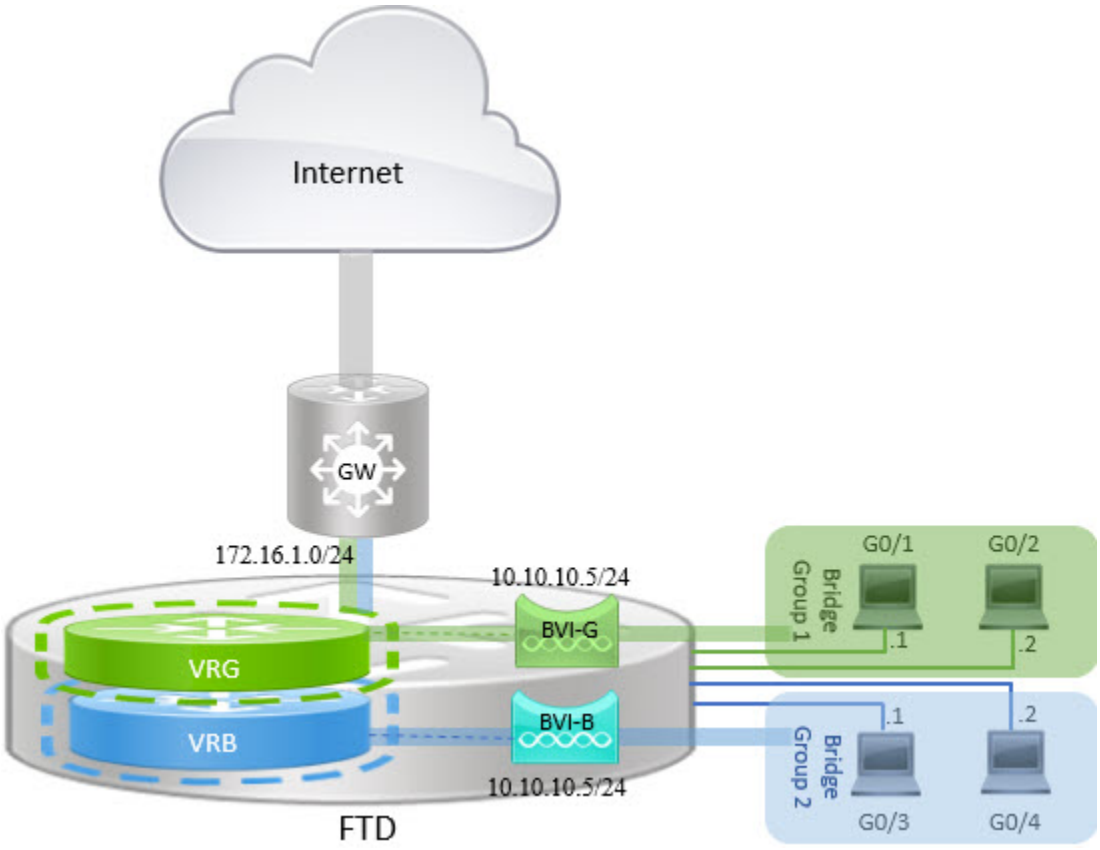
The NAT rule is configured to enable communication between Host A and Host B on overlapping network addresses. Host A uses 30.1.1.1 to communicate with Host B, and Host B uses 20.1.1.1 to reach Host A.

Manage overlapping segments in routed firewall mode with BVI interfaces

This task allows you to deploy single Firewall Threat Defense between multiple overlapping networks transparently and/or deploy the firewall between the hosts of same network by configuring BVI per virtual router.

BVI is a virtual interface within a router that acts like a normal routed interface. It does not support bridging, but represents the comparable bridge group to routed interfaces within the router. All the packets coming in or going out of these bridged interfaces, pass through the BVI interface. The interface number of the BVI is the number of the bridge group that the virtual interface represents.

In the following example, BVI-G is configured in VRG and Bridge Group 1 is the routed interface for interfaces G0/1 and G0/2. Similarly, BVI-B is configured in VRB and Bridge Group 2 is the routed interface for interfaces G0/3 and G0/4. Consider that both BVIs have the same IP subnet address, say 10.10.10.5/24. Because of virtual routers, the network is isolated on the shared resources.



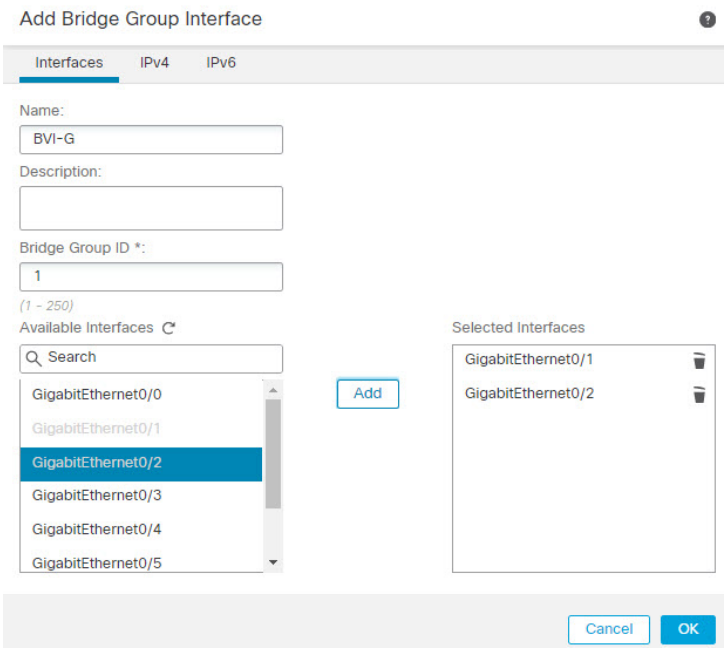
Procedure

Step 1 Choose **Devices** > **Device Management**. Edit the required device.

Step 2 In **Interfaces**, choose **Add Interfaces** > **Bridge Group Interface**.

a) Enter the following details for BVI-G:

- **Name**—For this example, BVI-G.
- **Bridge Group ID**—For this example, 1.
- **Available Interface**—Select the interfaces.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.
- **IP Address**—Enter 10.10.10.5/24.

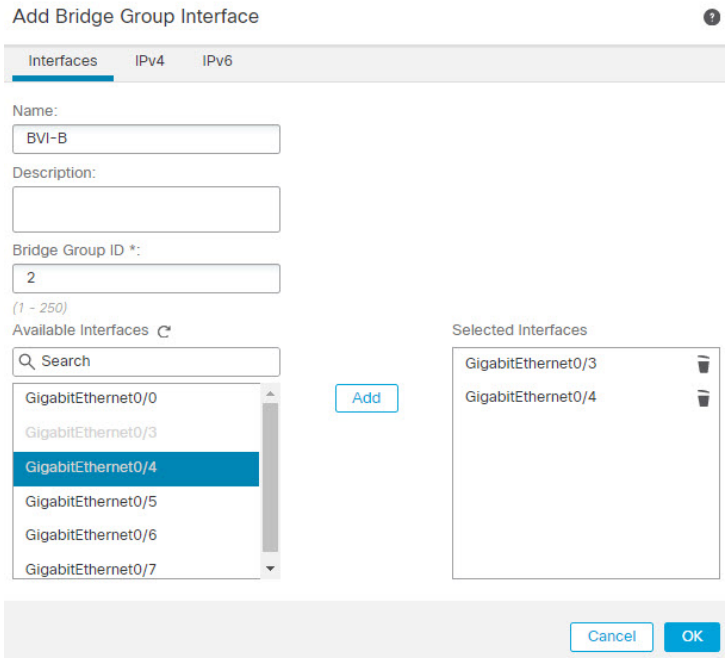


b) Click **Ok**.

c) Click **Save**.

a) Enter the following details for BVI-B:

- **Name**—For this example, BVI-B.
- **Bridge Group ID**—For this example, 2.
- **Available Interface**—Select the sub interfaces.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.
- **IP Address**—Leave this field empty as the system does not allow two interfaces to have overlapping IP address. You can revisit the Bridge Group and provide the same IP address after aligning it under a virtual router.



b) Click **Ok**.

c) Click **Save**.

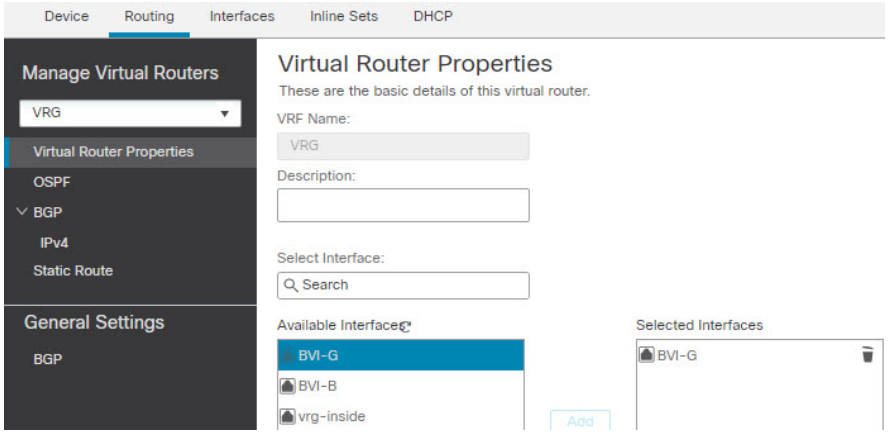
Step 3 Create virtual router, say VRG, and select BVI-G as its network:

a) Choose **Devices** > **Device Management**.

b) Edit the device, and choose **Routing** > **Manage Virtual Routers**.

c) Click **Add Virtual Router**. Enter a name for the virtual router and click **Ok**.

d) In **Virtual Routing Properties**, select **BVI-G** and click **Add**.



e) Click **Save**.

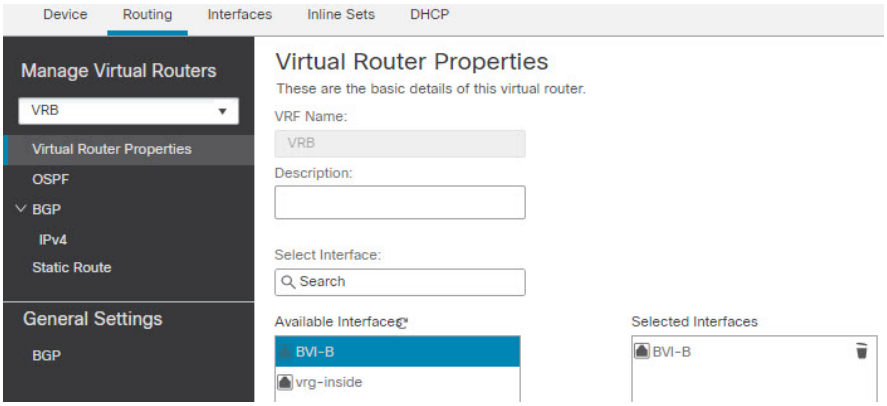
Step 4 Create virtual router, say VRB, and select BVI-B as its network:

a) Choose **Devices** > **Device Management**.

b) Edit the device, and choose **Routing** > **Manage Virtual Routers**.

c) Click **Add Virtual Router**. Enter a name for the virtual router and click **Ok**.

d) In **Virtual Routing Properties**, select **BVI-B** and click **Add**.



e) Click **Save**.

Step 5 Revisit the BVI-B configuration:

a) Choose **Devices** > **Device Management**, edit the device and click **Interfaces**.

b) Click **Edit** against BVI-B interface. Specify the IP Address as 10.10.10.5/24. The system now allows you to configure with same IP address of BVI-G, because the interfaces are seperately assigned to two different virtual routers.

c) Click **Ok**.

d) Click **Save**.

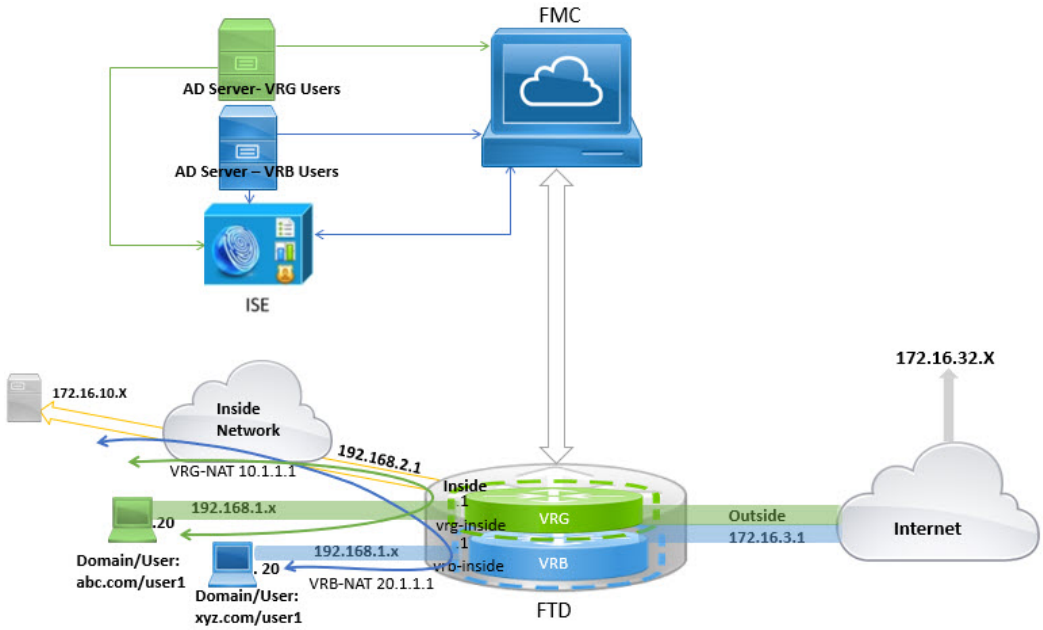
If you want to enable inter-BVI communication, use an external router as default gateway. In overlapping BVI scenarios, as in this example, use twice NAT external router as gateway to establish inter-BVI traffic. When configuring NAT for the members of a bridge group, you specify the member interface. You cannot configure NAT for the bridge group interface (BVI) itself. When doing NAT between bridge group member interfaces, you must specify the real and mapped addresses. You cannot specify "any" as the interface.

You have successfully configured BVI interfaces per virtual router to manage overlapping segments in routed firewall mode. The virtual routers isolate the network on shared resources, allowing the use of same IP subnet addresses for both BVIs.

Configure user authentication with overlapping networks

This task enables you to configure user authentication in virtual routing environments where multiple virtual routers share overlapping IP addresses and user networks. The configuration allows users from different domains to access shared resources while maintaining proper access control.

In virtual routing, you can configure multiple virtual routers with overlapping IP and overlapping users. In the example, VRG, and VRB are the virtual routers with overlapping IP - 192.168.1.1/24. The users on two different domains are also on overlapping network IP 192.168.1.20. For VRG and VRB users to access the shared server 172.16.10.X, leak routes to the global virtual router. Use source NAT to handle the overlapping IP. For controlling the access from VRG and VRB users, you must set user authentication in Firewall Management Center. Firewall Management Center uses realms, Active Directories, Identity source, and Identity rules and policies for authenticating user identity. Because Firewall Threat Defense does not have direct role in authenticating users, user access is managed only through the access control policy. For controlling traffic from the overlapping users, use Identity policy and rules to create access control policy.



Before you begin

This example assumes that you have:

- Two AD servers for the VRG and VRB users.
- ISE with the two AD servers added.

Follow these steps to configure user authentication with overlapping networks:

Procedure

Step 1 Configure the inside interface of the device for VRG:

a) Choose **Devices** > **Device Management**, click the device name, and then click **Interfaces**.

b) Edit the interfaces that you want to assign to VRG:

- **Name**—For this example, VRG-inside.
- Select the **Enabled** checkbox.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.
- **IP Address**—Enter 192.168.1.1/24.

c) Click **Ok**.

d) Click **Save**.

Step 2 Configure the inside interface of the device for VRB:

a) Choose **Devices** > **Device Management** > **Interfaces**.

b) Edit the interfaces that you want to assign to VRB:

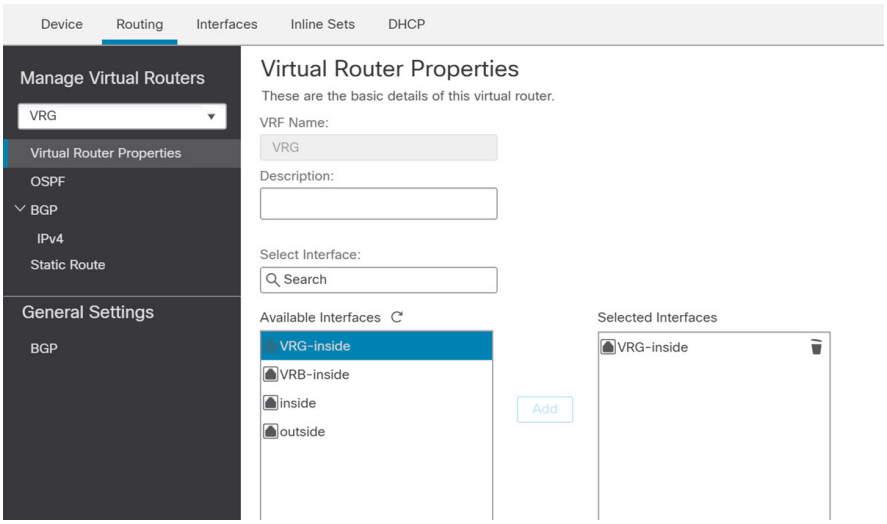
- **Name**—For this example, VRB-inside.

- Select the **Enabled** checkbox.
- In **IPV4**, for **IP Type**, choose **Use Static IP**.
- **IP Address**—Leave it blank. The system doesn't allow you to configure interfaces with same IP address, as you're yet to create user-defined virtual routers.

c) Click **Ok**.
d) Click **Save**.

Step 3 Configure VRG and the static default route leak to the inside interface of the Global router for the VRG users to access the common server 172.16.10.1:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Manage Virtual Routers**. Click **Add Virtual Router** and create VRG.
c) For VRG, in **Virtual Router Properties**, assign VRG-inside and save.



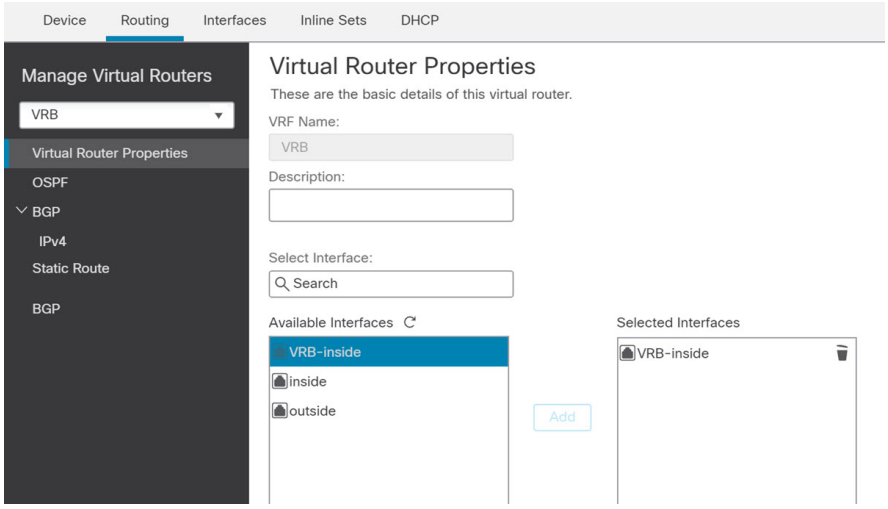
d) Click **Static Route**.
e) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the inside interface of the global router.
- **Network**—Select the any-ipv4 object.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, do not select a gateway.

f) Click **Ok**.
g) Click **Save**.

Step 4 Configure VRB and the static default route leak to the inside interface of the Global router for the VRB users to access the shared server 172.16.10.x:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Manage Virtual Routers**. Click **Add Virtual Router** and create VRB.
c) For VRB, in **Virtual Router Properties**, assign VRB-inside and save.



d) Click **Static Route**.

e) Click **Add Route**. In **Add Static Route Configuration**, specify the following:

- **Interface**—Select the inside interface of the global router.
- **Network**—Select the any-ipv4 object.
- **Gateway**—Leave it blank. When leaking a route into another virtual router, do not select a gateway.

f) Click **Ok**.

g) Click **Save**.

Step 5 Revisit the VRB-inside interface configuration:

a) Choose **Devices** > **Device Management**, click the device name, and then click **Interfaces**.

b) Click **Edit** against VRB-inside interface. Specify the IP Address as 192.168.1.1/24. The system now allows you to configure with the same IP address as that of VRG-inside, because the interfaces are seperately assigned to two different virtual routers.

c) Click **Ok**.

d) Click **Save**.

Step 6 Add NAT rules for the source objects VRG and VRB. Click **Devices** > **NAT**.

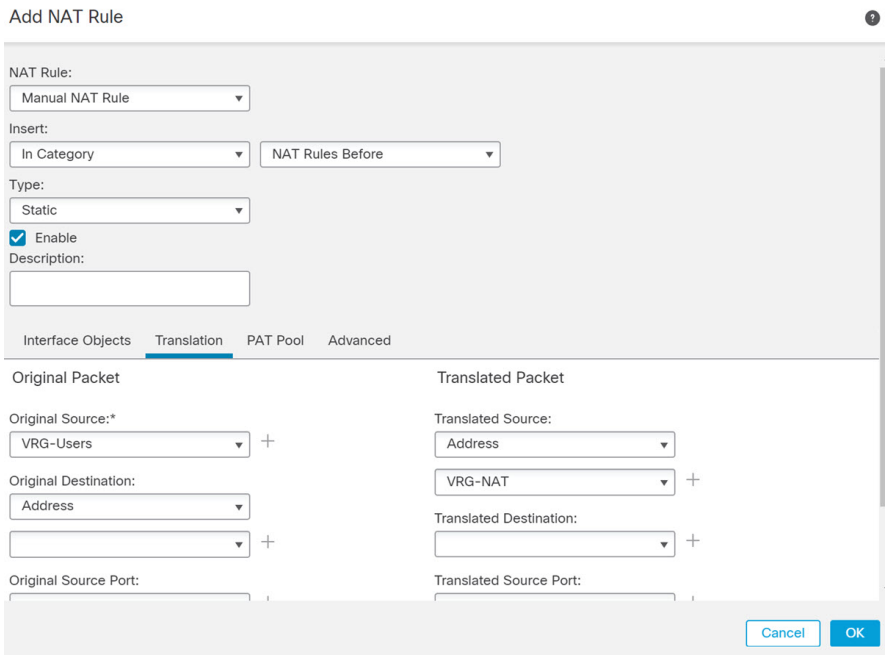
Step 7 Click **New Policy** > **Threat Defense NAT**.

Step 8 Enter a NAT policy name, and select the Firewall Threat Defense device. Click **Save**.

Step 9 In the NAT page, click **Add Rule** and define the following source NAT for VRG:

- **NAT Rule**—Select Manual NAT Rule.
- **Type**—Select Static.
- **Insert**—Select Above, if any NAT rule exists.
- Click **Enabled**.
- In **Interface Objects**, select VRG-Inside object and click **Add to Source** (If the object is not available, create one in **Objects** > **Object Management** > **Interface**), and select Global-Inside object and click **Add to Destination**.
- In **Translation**, select the following:

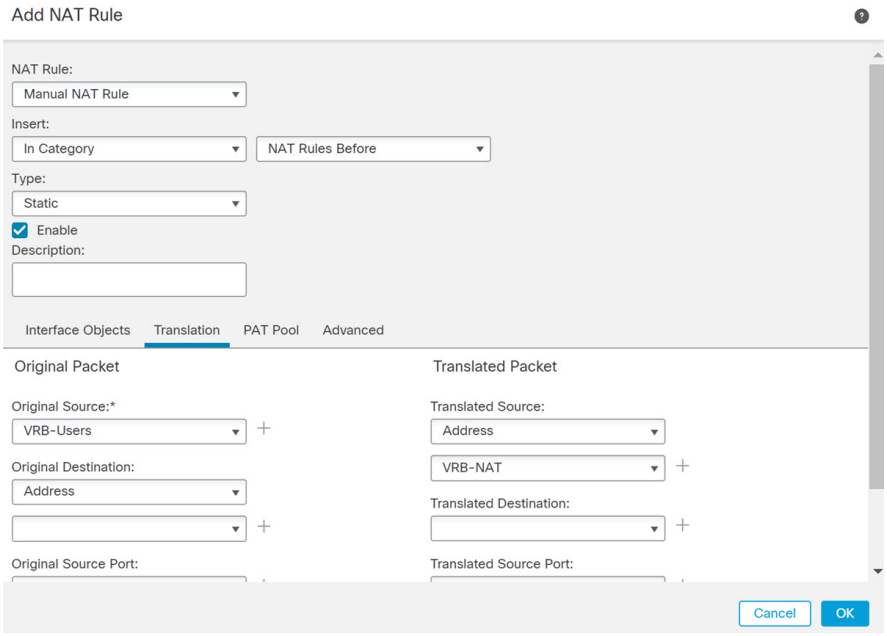
- **Original Source**, select VRG-Users.
- **Translated Source**, click **Add** and define object, VRG-NAT with 10.1.1.1. Select VRG-NAT as shown in the figure:



Step 10 Click **Ok**.

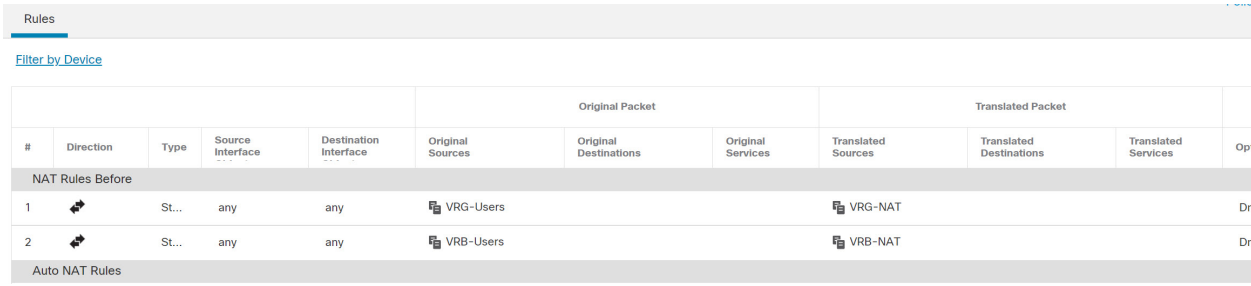
Step 11 In the NAT page, click **Add Rule** and define the following source NAT for VRB:

- **NAT Rule**—Select Manual NAT Rule.
- **Type**—Select Static.
- **Insert**—Select Above, if any NAT rule exists.
- Click **Enabled**.
- In **Interface Objects**, select VRB-Inside object and click **Add to Source** (If the object is not available, create one in **Objects** > **Object Management** > **Interface**), and select Global-Inside object and click **Add to Destination**.
- In **Translation**, select the following:
  - **Original Source**, select VRB-Users.
  - **Translated Source**, click **Add** and define object, VRB-NAT with 20.1.1.1. Select VRB-NAT as shown in the figure:



Step 12 Click **Save**.

The NAT rule looks like this:



Step 13 Add the two unique AD servers in Firewall Management Center one for each VRG and VRB users—choose **System** > **Integration** > **Realms**.

Step 14 Click **New Realm** and complete the fields. For detailed information on the fields, see Realm fields, on page 1844.

Step 15 For controlling the access from VRG and VRB users, define 2 Active Directories, see Realm directory and synchronize fields, on page 1848see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860

Step 16 Add ISE in Firewall Management Center—choose **System** > **Integration** > **Identity Sources**.

Step 17 Click **Identity Services Engine** and complete the fields. For detailed information on the fields, see Configure ISE/ISE-PIC for user control using a realm, on page 1917.

Step 18 Create Identity policy, rules, and then define access control policy for controlling access of overlapping users from VRG and VRB.

You have successfully configured user authentication for virtual routers with overlapping networks. VRG and VRB users can now access the shared server through proper NAT translation and authentication controls, with distinct identity policies managing access for each user group.

Interconnect virtual routers using BGP

This task enables you to configure BGP settings to leak routes among virtual routers (Global and user-defined virtual routers) by using route targets and route maps to share routes between different virtual routing instances.

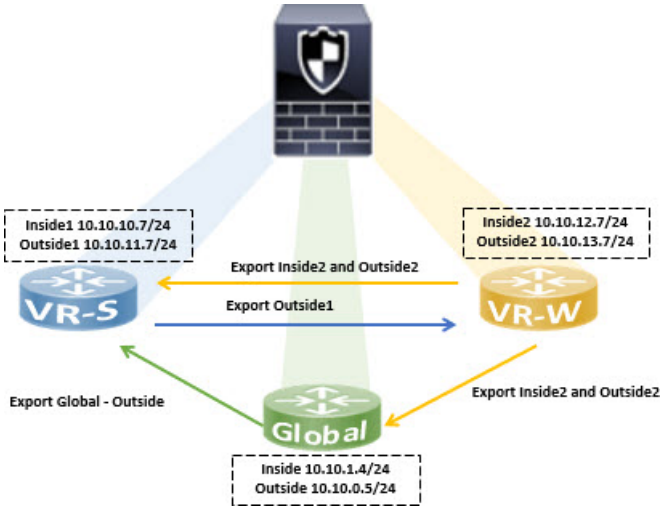
You can now configure BGP settings on a device to leak the routes among virtual routers (Global and user-defined virtual routers). The route target of the source virtual router is exported to the BGP table, which, in turn is imported to the destination virtual router. The route map is used to share the Global virtual routes with the user-defined virtual routers and vice versa. Note that all import or export of the routes to the BGP table is configured at the user-defined virtual router, including the Global virtual routes.

Consider the firewall device of a factory is configured with virtual routers and interfaces:

- Global virtual router is configured with Inside (10.10.1.4/24) and Outside (10.10.0.5/24)
- VR-S (Sales) virtual router is configured with Inside1 (10.10.10.7/24) and Outside1 (10.10.11.7/24)
- VR-W (Warehouse) virtual router is configured with Inside2 (10.10.12.7/24) and Outside2 (10.10.13.7/24)

Assume that you want the routes of warehouse (VR-W) to be leaked with sales (VR-S) and Global, and the outside interface routes of VR-S to VR-W. Similarly, you want the outside interface routes of the Global router to be leaked to sales (VR-S). This example demonstrates the BGP configuration procedure to achieve interconnecting the routers:

Figure 355: Interconnect virtual routers using BGP settings



Before you begin

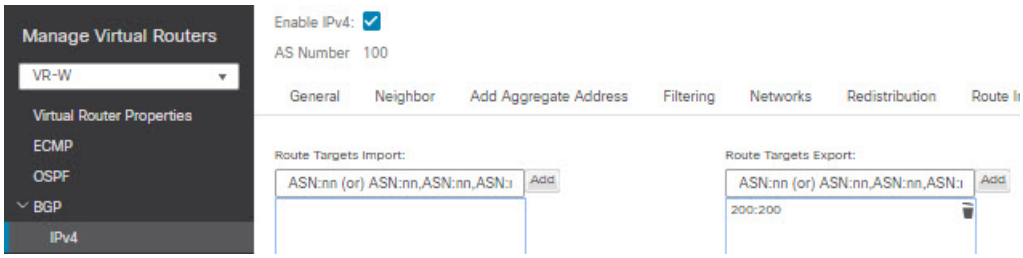
- Create the virtual routers—VR-S and VR-W.
- Enable BGP and for each virtual router Configure BGP for redistribution of connected routes.

Follow these steps to interconnect virtual routers using BGP:

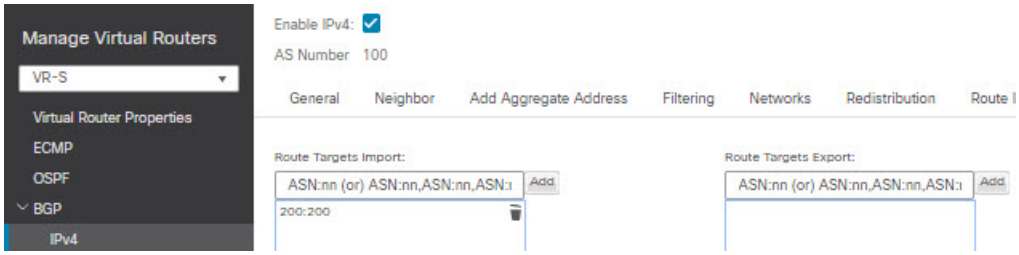
Procedure

Step 1 Configure VR-W to export its routes tagging them with a route target to VR-S:

a) Choose **Devices** > **Device Management**, edit device, and then click the **Routing** tab.
b) From the virtual router drop-down, select VR-W. Then click **BGP** > **IPv4** > **Route Import/Export**.
c) To leak the VR-W routes to VR-S, tag the routes with a route target, so that the VR-W routes are exported to its BGP table with the route target marked on them. In the **Route Targets Export** field, enter a value, say, *200:200*. Click **Add**:



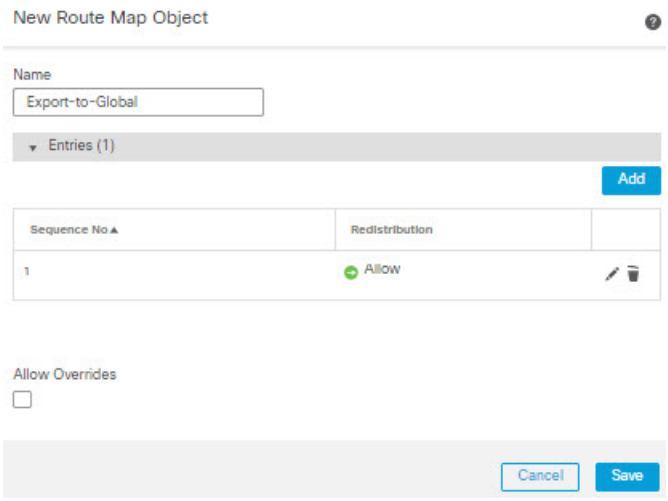
d) From the virtual router drop-down, select VR-S. Then click **BGP** > **IPv4** > **Route Import/Export**.
e) To receive the leaked routes from VR-W, configure the Import Route Target to import the VR-W routes that are marked with the route target from the (peer or redistributed) BGP table. In the **Route Targets Import** field, enter the same route target value that you had configured for VR-W, *200:200*. Click **Add**.



Note If you want to conditionalize routes to be leaked from VR-W, you can specify the match criteria in the route map object, and choose it in the **User Virtual Router Export Route Map**. Similarly, if you want to conditionalize the routes to be imported to VR-S from the BGP table, you can use the **User Virtual Router Import Route Map**. This procedure is explained in Step 3.

Step 2 Configure VR-W to export its routes to the Global virtual router:

a) You need to create a route map that would allow the VR-W routes to be exported to the Global routing table. Choose **Objects** > **Object Management** > **Route Map**.
b) Click **Add Route Map**, give a name, say *Export-to-Global*, and then click **Add**.
c) Specify a **Sequence Number**, say 1, and then choose Allow from the **Redistribution** drop-down list:

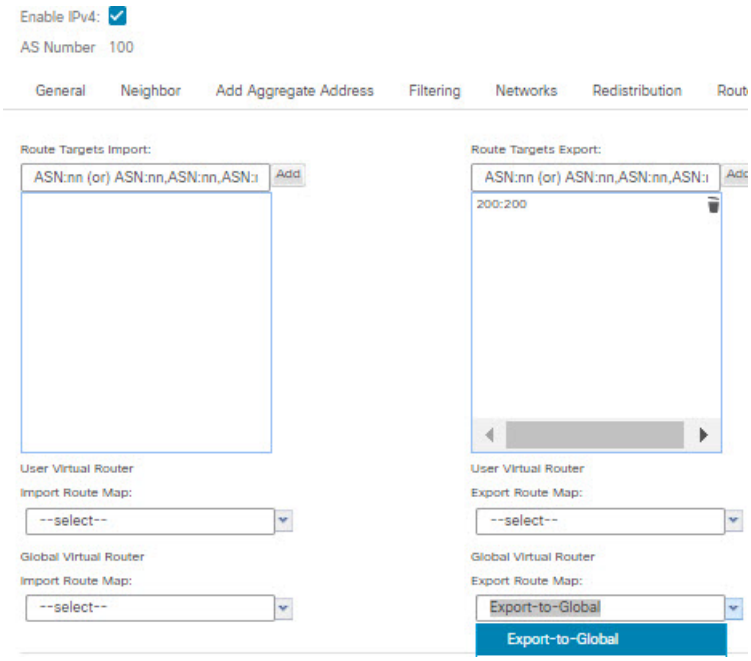


d) Click **Save**.

In this example, all the VR-W routes are leaked to the Global routing table. Hence, no match criteria is configured for the route map.

e) Navigate to the **Routing** tab of the device, and select VR-W. Click **BGP** > **IPv4** > **Route Import/Export**.

f) From the **Global Virtual Router Export Route Map** drop-down list, choose Export-to-Global:



Step 3 To leak only the Outside1 routes of VR-S to VR-W:

a) From the virtual router drop-down, select VR-S and then click **BGP** > **IPv4** > **Route Import/Export**.

b) To leak the VR-S routes to VR-W, tag the routes with a route target, so that the VR-S routes are exported to its BGP table with the route target marked on them. In the **Route Targets Export** field, enter a value, say, *100:100*. Click **Add**.

c) From the virtual router drop-down, select VR-W, and choose **BGP** > **IPv4** > **Route Import/Export**. To receive the leaked routes from VR-S, configure the Import Route Target to import the VR-S routes that are marked with the route target from the (peer or redistributed) BGP table. In the **Route Targets Import** field, enter the VR-S route target value, *100:100*. Click **Add**.

d) Now, you need to conditionalize that only the Outside1 routes of VR-S to be leaked to VR-W. Choose **Objects** > **Object Management** > **Prefix Lists** > **IPv4 Prefix List**. Click **Add IPv4 Prefix List**, give a name, say *VRS-Outside1-Only*, and then click **Add**.

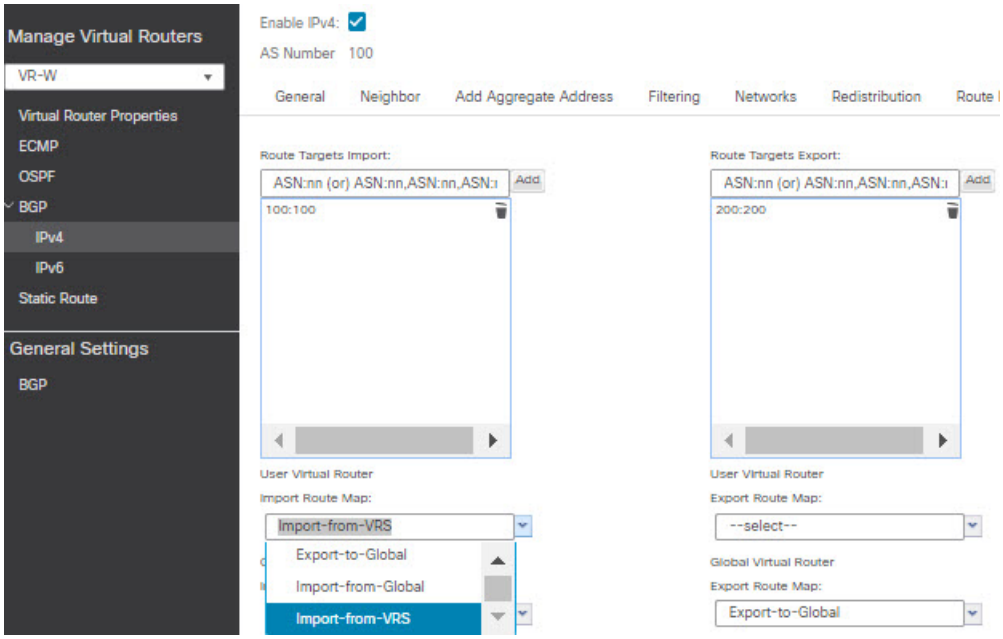
e) Specify a **Sequence Number**, say 1, and then choose Allow from the **Redistribution** drop-down list. Enter the IP Address (first two octets) of the VR-S Outside1 interface and then click **Save**.

f) Create a route map with the match clause with the prefix list. Click **Route Map**. Click **Add Route Map**, give a name, say *Import-from-VRS*, and then click **Add**.

g) Specify a **Sequence Number**, say 1, and then choose Allow from the **Redistribution** drop-down list.

h) In the **Match Clause** tab, click **IPv4**. Under **Address** tab, click **Prefix List**. Under **Available IPv4 Prefix List**, select VRS-Outside1-Only, and then click **Add**.

i) Navigate to the **Routing** tab of the device, and select VR-W. Click **BGP** > **IPv4** > **Route Import/Export**. From the **Global Virtual Router Import Route Map** drop-down list, choose Import-from-VRS:



Step 4 Configure VR-S to import the Outside routes of Global virtual router:

Note To leak routes to or from a Global virtual router, you must configure the source or destination user defined virtual router respectively. Thus, in this example, VR-S is the destination router that imports the routes from Outside interface of the Global virtual router.

a) Choose **Objects** > **Object Management** > **Prefix Lists** > **IPv4 Prefix List**.

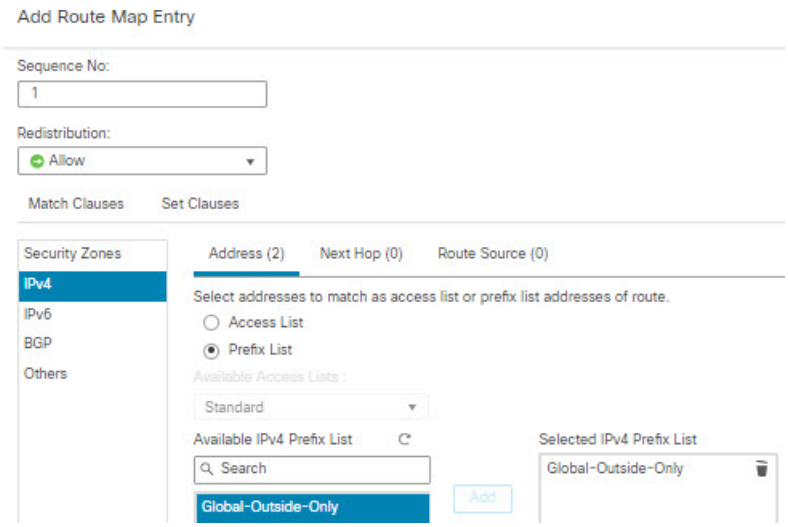
b) Click **Add IPv4 Prefix List**, give a name, say *Global-Outside-Only*, and then click **Add**. Specify a **Sequence Number**, say 1, and then choose Allow from the **Redistribution** drop-down list.

c) Enter the IP Address (first two octets) of the Global Outside interface:



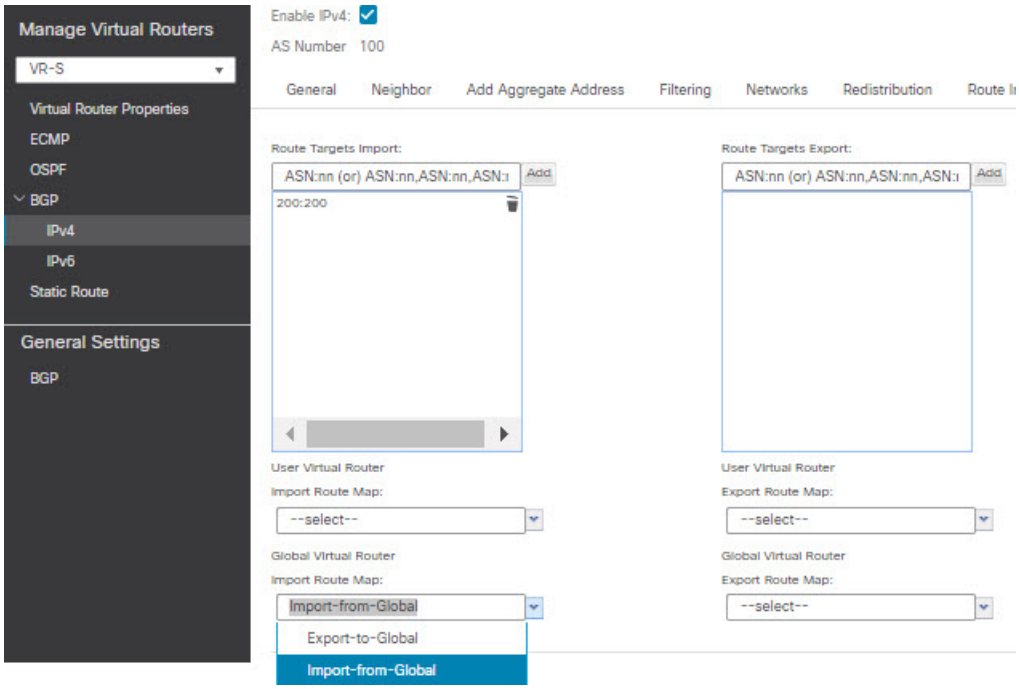
Then click **Save**.

d) Click **Route Map**. Click **Add Route Map**, give a name, say *Import-from-Global*, and then click **Add**.
e) Specify a **Sequence Number**, say 1, and then choose Allow from the **Redistribution** drop-down list.
f) In the **Match Clause** tab, click **IPv4**. Under **Address** tab, click **Prefix List**.
g) Under **Available IPv4 Prefix List**, select Global-Outside-Only, and then click **Add**:



Then click **Save**.

h) Navigate to the **Routing** tab of the device, and select VR-S. Click **BGP** > **IPv4** > **Route Import/Export**.
i) From the **Global Virtual Router Import Route Map** drop-down list, choose Import-from-Global:



Step 5 **Save** and **Deploy**.

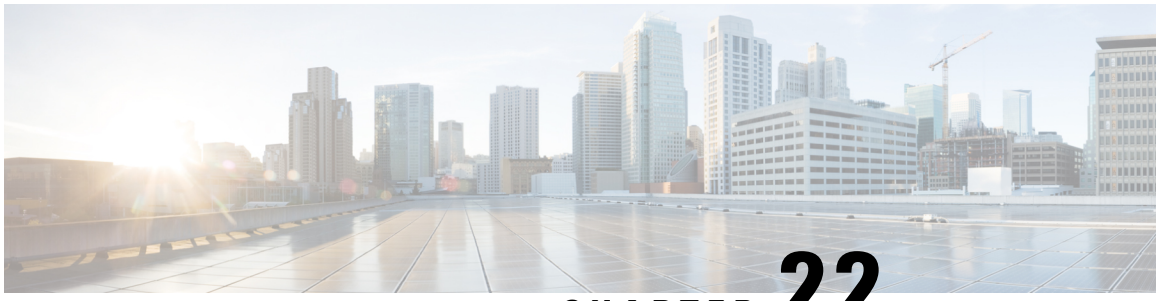
The BGP configuration is complete and routes are now leaked among the virtual routers according to the configured route targets and route maps. VR-W routes are exported to VR-S and Global, VR-S Outside1 routes are exported to VR-W, and Global Outside routes are imported to VR-S.

History for virtual routers

This reference provides a comprehensive history of virtual router features introduced across different versions, including feature descriptions, minimum version requirements, and implementation details.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Virtual routing with dynamic VTI.	7.4	7.4	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device management** > **Edit Device** > **Routing** > **Virtual Router Properties** > **Dynamic VTI interfaces under Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices.
Virtual router support for the ISA 3000.	7.0	7.0	You can configure up to 10 virtual routers on the ISA 3000.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
SNMP support on user-defined virtual routers	7.0	7.0	You can now configure SNMP on user-defined virtual routers.
Bulk removal of virtual routers.	6.7	6.6	You can remove multiple virtual routers from threat defense at a time. New/modified screens: **Devices** > **Device Management** > **Routing** > **Manage Virtual Routers**
Virtual routers and VRF-Lite for threat defense.	6.6	6.6	You can now create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). The maximum number of virtual routers you can create ranges from five to 100, and depends on the device model.. New/modified screens: **Devices** > **Device Management** edit device **Routing** tab New/modified CLI commands: . • **show VRF** • Added the [**VRF** *name* | **all**] keyword set to these CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show BGP**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters** Platform restrictions: Not supported on the Firepower 1010 and ISA 3000.



CHAPTER 22

ECMP

Equal Cost Multi-Path (ECMP) is a routing strategy that allows a router to forward packets along multiple paths of equal cost to a destination.

- Enables load balancing across multiple network paths.
- Utilizes routing protocols to determine path cost.
- Increases total available bandwidth for traffic flows.

- ECMP routing methods, on page 1047
- Guidelines and limitations for ECMP, on page 1048
- Manage ECMP zones for virtual routers, on page 1049
- Create an ECMP zone, on page 1049
- Configure an equal cost static route, on page 1050
- Modify an ECMP zone, on page 1051
- Remove an ECMP zone, on page 1052
- Configure ECMP zones on your device, on page 1053
- History for ECMP in Secure Firewall Threat Defense, on page 1056

ECMP routing methods

ECMP is a routing method that

- enables traffic distribution across multiple equal-cost paths,
- supports up to 8 equal cost static or dynamic routes across up to 8 interfaces within each zone, and
- uses traffic zones per virtual router to contain a group of interfaces.

Multiple default routes configuration

This example shows multiple default routes configured across three interfaces in the zone:

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2

route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2

route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

Guidelines and limitations for ECMP

Follow these principles for effective ECMP zone configuration:

Firewall mode limitations

Use ECMP zones only in routed firewall mode.

Interface restrictions

Do not use dVTI or Loopback interfaces with ECMP zones.

ECMP zone configuration limits

Follow these limits when configuring ECMP zones:

- Devices can have a maximum of 256 ECMP zones.
- You can associate only 8 interfaces per ECMP zone.
- An interface can be a member of only one ECMP zone.

Interface management limitations

Do not remove interfaces or delete zones actively used for routing:

- You cannot remove an interface that is associated with an equal cost static route from the ECMP zone.
- You cannot delete an ECMP zone if its interface has equal cost static routes associated with it.

Supported interface types

Use only routed interfaces for ECMP zones. Do not associate these interface types with an ECMP zone:

- BVI interface.
- Member interfaces in an EtherChannel.
- Failover or state link interface.
- Management-only or management-access interfaces.
- Cluster control link interface.
- VNIs.
- VLAN interfaces.
- Interfaces in a remote access VPN configuration with SSL enabled.

Feature compatibility limitations

Consider these feature limitations when using ECMP zones:

- DHCP Relay is not supported on interfaces in an ECMP zone.
- Dual ISP/WAN Firewall Threat Defense Deployment—Create a single ECMP zone for the primary and secondary data interfaces, enabling static routes with identical metric values.

- The Firewall Threat Defense does not support ECMP with NAT in IPsec sessions—a standard IPsec virtual private network (VPN) tunnel does not work with NAT points in the delivery path of IPsec packets.

Manage ECMP zones for virtual routers

The ECMP page lets you manage existing ECMP zones linked with virtual routers. When you click **ECMP** on the **Routing** pane, the ECMP page displays the current ECMP zones, including the associated interfaces, for the selected virtual router. On this page, you can add new ECMP zones to the virtual router. You can also **Edit** ( ) and **Delete** ( ) ECMP zones.

You can perform these actions:

- Create an ECMP zone, on page 1049
- Configure an equal cost static route, on page 1050
- Modify an ECMP zone, on page 1051
- Remove an ECMP zone, on page 1052

Create an ECMP zone

Create an ECMP zone to enable load balancing across multiple equal-cost paths in a virtual router configuration.

ECMP zones are created per virtual router. Only interfaces that belong to the virtual router where the ECMP is being created can be associated with the ECMP zone.

Procedure

Step 1 Navigate to **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 From the virtual router drop-down, select the virtual router in which you want to create the ECMP zone.

You can create ECMP zones in the global virtual router and user-defined virtual routers. For information on creating virtual routers, refer to Create a virtual router, on page 1002.

Step 4 Click **ECMP**.

Step 5 Click **Add**.

Step 6 In the **Add ECMP** box, enter a name for the ECMP zone.

Note The ECMP name must be unique on the routed device.

Step 7 Under the **Available Interfaces** box, select the interface and click **Add**.

- Only interfaces belonging to the virtual router where you are creating the ECMP can be associated with it. Interfaces must have a logical name to be displayed; edit the interface and save to set a logical name.

- From Version 10.0, ECMP is supported on dynamic VTIs (DVTIs) of hub devices in SD-WAN VPN topologies. When enabled on a DVTI, it is automatically added to a system-generated ECMP zone, so DVTIs do not appear under **Available Interfaces**.

Step 8 Click **OK**.

The ECMP page displays your newly created ECMP zone.

Step 9 Click **Save** and **Deploy** the configuration.

You can associate the ECMP zone interfaces with equal cost static route by defining them with same destination and metric value but with a different gateway.

What to do next

- Configure an equal cost static route, on page 1050
- Modify an ECMP zone, on page 1051
- Remove an ECMP zone, on page 1052

Configure an equal cost static route

Configure equal cost static routes to enable load balancing across multiple interfaces with the same destination and metric value within an ECMP zone.

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	Firewall Threat Defense and Firewall Threat Defense Virtual	Any	Admin/Network Admin/Security Approver

You can assign interfaces of a virtual router, both global and user-defined, to an ECMP zone for the device.

Before you begin

- To configure an equal cost static route for an interface, ensure that it is associated with an ECMP zone. For more information, refer to Create an ECMP zone, on page 1049.
- All routing configuration settings of a non-VRF-capable device are also available for a global virtual router.
- You cannot define a static route for interfaces with the same destination and metric without associating the interfaces with an ECMP zone.

Procedure

Step 1 From the **Devices** > **Device Management** page, edit the Firewall Threat Defense device. Click the **Routing** tab.

Step 2 From the drop-down list, select the virtual router whose interfaces are associated with an ECMP zone.

Step 3 To configure the equal cost static route for the interfaces, click **Static Route**.

Step 4 Either click **Add Route** to add a new route, or click **Edit** (✎) for an existing route.

Step 5 From the **Interface** drop-down, select the interface that belongs to the virtual router and is associated with an ECMP zone.

Step 6 Select the destination network from the **Available Networks** box and click **Add**.

Step 7 Enter a gateway for the network.

Step 8 Enter a metric value. It can be a number that ranges between 1 and 254.

Step 9 To save the settings, click **Save**.

To configure equal cost static routing, repeat these steps to configure the static route for another interface in the same ECMP zone with the same destination network and metric value. Remember to provide a different gateway.

The equal cost static routes are configured for the interfaces associated with the ECMP zone, enabling load balancing across multiple paths.

What to do next

- Modify an ECMP zone, on page 1051
- Remove an ECMP zone, on page 1052

Modify an ECMP zone

Use this procedure when you need to make changes to an existing ECMP zone configuration on your device.

Follow these steps to modify an ECMP zone:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **ECMP**.

ECMP zones with their associated interfaces appear.

Step 4 To modify an ECMP zone, click **Edit** (✎) next to the desired ECMP zone. In the **Edit ECMP** dialog box, you can make changes to the ECMP name or associated interfaces.

- ECMP Name: Ensure that the ECMP name you enter is unique.
- Interfaces: Add or remove one or more interfaces as needed.

Note An interface must not belong to more than one ECMP zone, and it should not be linked to an equal-cost static route.

Step 5 Click **OK**.

Step 6 Click **Save**.

The ECMP zone shows your updated settings.

What to do next

- Configure an equal cost static route, on page 1050
- Remove an ECMP zone, on page 1052

Remove an ECMP zone

ECMP zones group interfaces for equal-cost multipath routing. You may need to remove an ECMP zone when reconfiguring your network topology or when the zone is no longer required.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **ECMP**.

The ECMP zones with associated interfaces appear.

Step 4 To remove an ECMP zone, click **Delete** ( ) next to the ECMP zone.

Note You cannot delete the ECMP zone if it has interfaces associated with equal-cost static routes.

Step 5 Click **Delete** in the confirmation message.

Step 6 Click **Save** to apply changes.

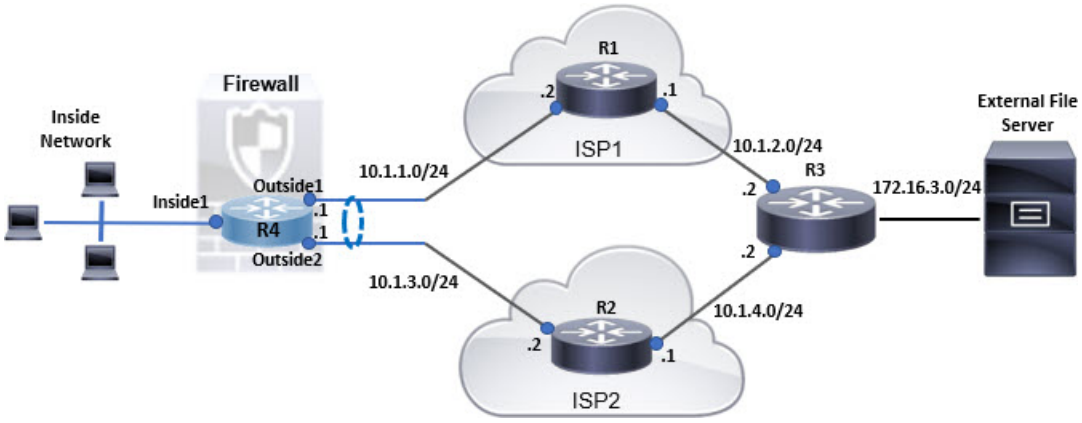
The ECMP zone is removed from the device configuration and is no longer available for routing operations.

Configure ECMP zones on your device

Configure Equal-Cost MultiPath (ECMP) to enable efficient traffic handling through the device with support for asymmetric routing, load balancing, and traffic rerouting when a path becomes unavailable.

This example demonstrates how to use Firewall Management Center to configure ECMP zones on Firewall Threat Defense such that the traffic flowing through the device is handled efficiently. With ECMP configured, Firewall Threat Defense maintains the routing table on a per-zone basis, enabling efficient packet re-routing. Thus, ECMP supports asymmetric routing, load balancing, and traffic rerouting when a path becomes unavailable. In this example, R4 records the two paths to reach the external file server.

Figure 356: Configuration example for ECMP



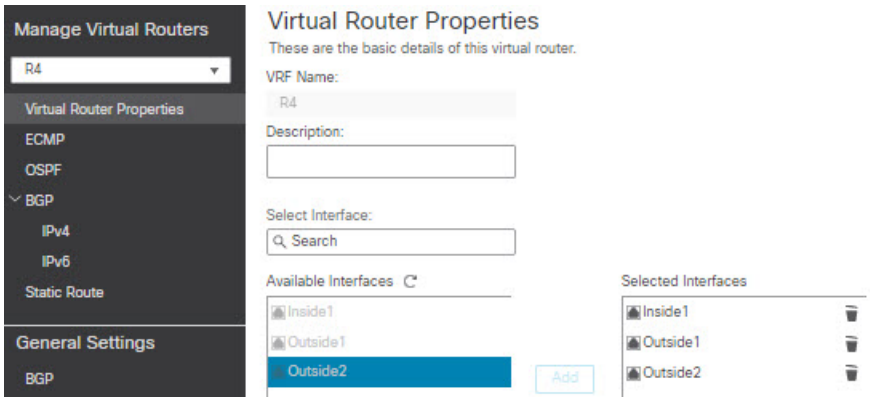
Follow these steps to configure ECMP on your device:

Procedure

Step 1 Create a virtual router.

Set up a new router on *R4* with interfaces: *Inside1*, *Outside1*, and *Outside2*. For more information, refer to Create virtual router.

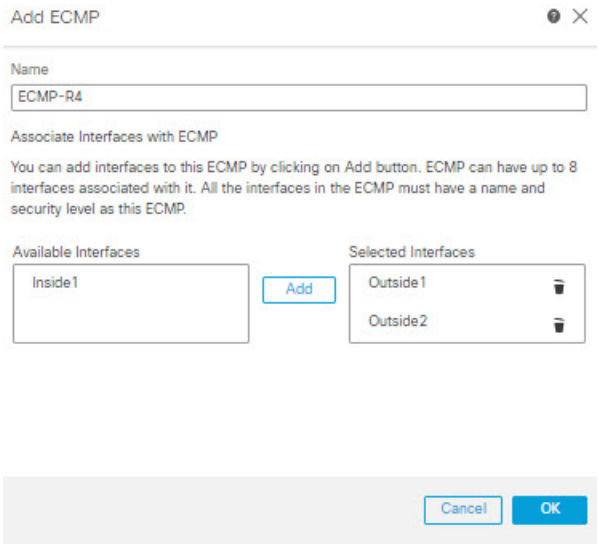
Figure 357: Configuring R4 virtual router



Step 2 Create ECMP zones:

a) In the **Routing** tab, choose R4 user-defined virtual router, and then click **ECMP**.
b) Click **Add**.
c) Enter an ECMP name and from the **Available Interfaces** list, choose *Outside1* and *Outside2*:

Figure 358: Creating ECMP zone

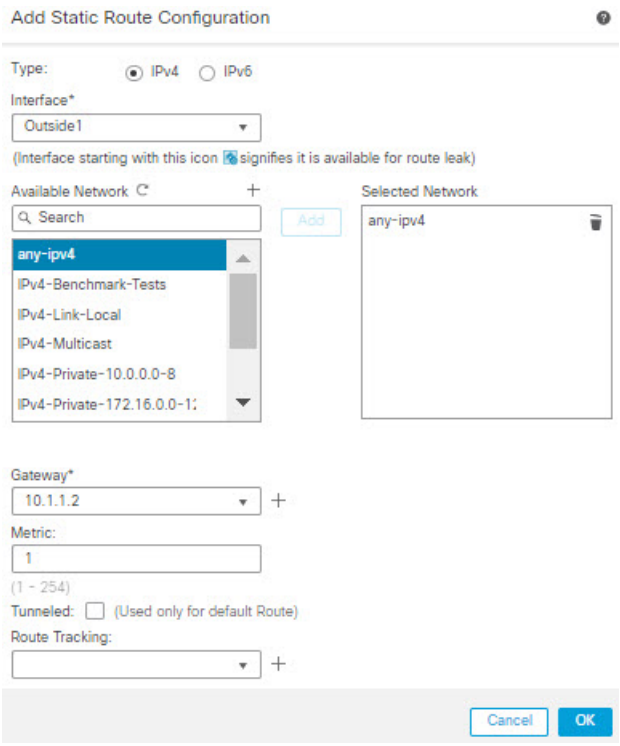


d) Click **OK**.
e) Click **Save**.

Step 3 Create static routes for the zone interfaces:

a) In the **Routing** tab, click **Static Route**.
b) From the **Interface** drop-down list, select Outside1.
c) Under **Available Network**, choose any-ipv4 and click **Add**.
d) Specify the next-hop address in the **Gateway** field, 10.1.1.2.

Figure 359: Configuring static route for Outside1



e) Configure the static route for Outside2 by repeating Step 3b through Step 3d.

Ensure that you specify the same metric but different gateways for the static routes:

Figure 360: Configured static routes of ECMP zone interfaces



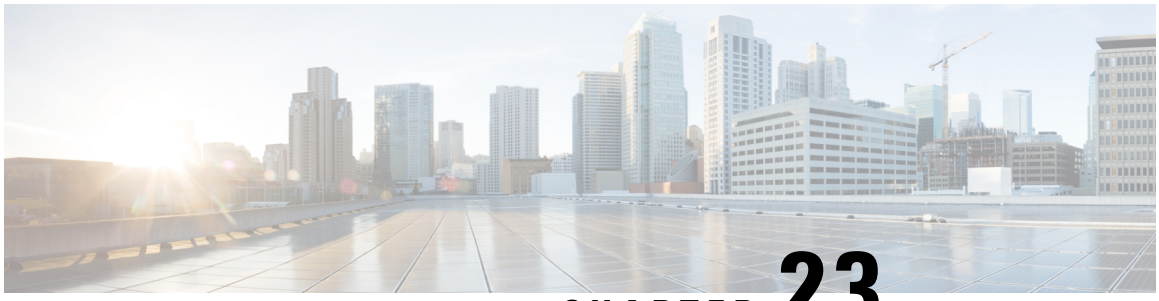
Step 4 Save and deploy the changes to apply ECMP routing to your device.

Network packets will now utilize efficient routes to reach their destination R3, either through R4>R1>R3 or R4>R2>R3, according to the ECMP algorithm configuration. If the R1>R3 route becomes unavailable, traffic can be rerouted through R2, which helps reduce disruption during path failure. Additionally, return traffic from R3 can arrive on *Outside2* even if the original packet was sent through *Outside1*. When network traffic is heavy, R4 distributes the network load between two specified routes to maintain balanced traffic.

History for ECMP in Secure Firewall Threat Defense

This reference provides the history of Equal-Cost Multi-Path (ECMP) features, focusing on key enhancements introduced in various releases and their implementation specifics.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
ECMP support as Routing Policy	7.1	Any	Secure Firewall Threat Defense supports ECMP routing through FlexConfig policies. Group interfaces into traffic zones to refine ECMP routing in Secure Firewall Management Center. New/modified screens: **Devices** > **Device Management** > **Routing** > **ECMP**



CHAPTER 23

Bidirectional Forwarding Detection Routing

This chapter describes how to configure Firewall Threat Defense to use the Bidirectional Forwarding Detection (BFD) routing protocol.

- BFD routing protocol, on page 1057
- Guidelines for BFD routing, on page 1057
- Configure BFD, on page 1059
- History for BFD routing, on page 1062

BFD routing protocol

A BFD routing protocol is a detection protocol that

- provides fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols
- operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems, and
- carries packets in the payload of the encapsulating protocol appropriate for the media and the network.

Why BFD?

BFD provides a consistent failure detection method for network administrators in addition to fast forwarding path failure detection.

Network administrators can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms. This makes network profiling and planning easier, and reconvergence time is consistent and predictable.

Guidelines for BFD routing

Context mode guidelines

BFD is supported on all Firewall Threat Defense platforms and is available in multi-instance mode.

Firewall mode guidelines

BFD is supported in routed firewall mode and not in transparent mode.

Failover and cluster guidelines

- BFD is not supported on failover interfaces.
- In clustering, BFD is supported only on the control node.

Routing and protocol guidelines

- OSPFv2, OSPFv3, IS-IS, BGP IPv4, and BGP IPv6 protocol are supported.

  For BFD support on IS-IS, using FlexConfig CLI configure BFD on IS-IS interfaces (Physical Interfaces, Sub-Interfaces, Port-Channels only):

```
For IPv6
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  ipv6 router isis
  isis ipv6 bfd
exit

For IPv4
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  isis
  isis bfd
exit
```

  EIGRP protocol is not supported.
- BFD for static routes is not supported. You can configure BFD on interfaces that belong only to virtual routers.
- Only named interfaces are supported.
- BFD on BVI, VTI, and loopback interfaces are not supported.

Single-hop guidelines

- Echo mode is disabled by default. You can enable echo mode on single-hop only.
- Echo mode is not supported for IPv6.
- Use only a single-hop template to configure a single-hop policy.
- Authentication of the single-hop template is optional.
- You cannot configure multiple BFDs on the same interface.

Multi-hop guidelines

- Do not configure the source IP address also as the destination IP address.

- Source and destination address should have same IP type—IPV4 or IPV6.
- Only network objects of host or network type are allowed.
- Use only a multi-hop template to configure a multi-hop policy.
- Authentication is mandatory for the multi-hop template.

Upgrade guidelines

When you upgrade to version 7.3 and the previous version has any FlexConfig BFD policies, the management center displays a warning message during deployment. However, it does not stop the deployment process. After post-upgrade deployment, to manage the BFD policies from the UI (**Device (Edit)** > **Routing** > **BFD**), you must configure BFD policies in the **Device (Edit)** > **Routing** > **BFD** page and remove the configuration from the FlexConfig policy for the device.

Configure BFD

This task enables and configures the Bidirectional Forwarding Detection (BFD) routing policy on your system to provide rapid detection of faults in the forwarding path.

Before you begin

Ensure you have access to the system where you want to configure BFD.

Follow these steps to configure BFD:

Procedure

Step 1 Create Configure a BFD template, on page 2358.

Step 2 Configure BFD policies, on page 1059.

Step 3 Configure BFD support in the BGP neighbor settings; see, Configure BGP Neighbor Settings.

BFD is enabled and configured on your system.

Configure BFD policies

BFD policies are used to provide rapid failure detection for interfaces associated with virtual routers. Configuring BFD templates allows you to monitor connectivity and quickly identify link failures.

- Enable fast failure detection for routing interfaces.
- Support both single-hop and multi-hop BFD configurations.

You can bind a BFD template to an interface belonging to a virtual router, or to a source and destination address pair.

Before you begin

- BFD policy is configurable only on interfaces that belong to virtual routers. See Configure interfaces to a virtual router.

To configure BFD policies, complete these steps.

Procedure

Step 1 From the **Devices** > **Device Management** page, edit the virtual-router supported device. Navigate to **Routing**.

Step 2 From the drop-down list, select the desired virtual router, and then click **BFD**.

Step 3 To configure a BFD on the interface, click the **Single-Hop** tab or **Multi-Hop** tab.



Note For a single-hop policy, the BFD template is configured on an interface; for a multi-hop policy, the BFD template is configured on a source and destination address pair.

Step 4 Click **Add**. To modify the configured BFD policy, click **Edit** ( ).



Note When you edit the interface mapping with BFD template to replace it with a new BFD template, the Firewall Management Center uses a **no** command to remove the template mapping from interface and applies the new template to the interface which causes a BFD flap which may also lead to an OSPFv2, OSPFv3, or BGP flap. However, if the BFD intervals are higher, the BFD flap might not occur. Alternatively, to avoid the flapping, you can delete the existing BFD template mapping; deploy the interface, and then add the new BFD template to the interface and deploy the configuration.

- See Configure a single-hop BFD policy, on page 1060.
- See Configure a multi-hop BFD policy, on page 1061.

After completing this task, BFD policies are configured on the selected interfaces or address pairs.

Configure a single-hop BFD policy

You can configure a single-hop BFD policy only on an interface that belongs to a virtual router. This task is relevant when you need to apply BFD for rapid link failure detection on specific interfaces.

Before you begin

- Create single-hop BFD templates. You cannot configure single-hop BFD policy on interfaces that use a multi-hop template.

Follow these steps to configure a single-hop BFD policy:

Procedure

Step 1 In the **Single-Hop** tab, click **Add** or **Edit**.

Step 2 In the **Add BFD Single-Hop** dialog box, configure the following:

a) The **Interface** drop-down list displays interfaces belonging to virtual routers. Select the interface you want to configure with the BFD policy.

b) The **Template Name** drop-down list displays single-hop templates. Select the template that you want to apply.

If you have not created a single-hop template, use **Add** (+) and create a single-hop BFD template.

Step 3 Click **OK** and **Save** the configuration.

The single-hop BFD policy is applied to the selected interface. The interface will now use the specified BFD template for single-hop operations.

Configure a multi-hop BFD policy

Configure a multi-hop BFD policy to enable monitoring of connectivity between specific source and destination address pairs. This configuration helps to monitor links that traverse multiple hops in your network.

Before you begin

- Create multi-hop BFD templates. You cannot configure multi-hop BFD policy using a single-hop template.

Follow these steps to configure a multi-hop BFD policy:

Procedure

Step 1 In the **Add BFD Multi-Hop** dialog box, configure the following:

a) Click the BFD source address type:**IPv4** or **IPv6** radio button.

b) The **Source Address** drop-down list displays the network objects. Select the source address for the BFD policy; do not choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note The created network object's IP type should match with the selected source IP type.

c) The **Destination Address** drop-down list displays network objects. Select the destination address for the BFD; do not choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note The created network object's IP type should match with the selected source IP type.

Attention Do not select the network object that has the same IP address as that of the source address.

d) The **Template Name** drop-down list displays multi-hop templates. Select the template to apply to the BFD policy.

If you have not created a multi-hop template, use **Add** (+) and create a multi-hop BFD template.

Step 2 Click **OK** and **Save** the configuration.

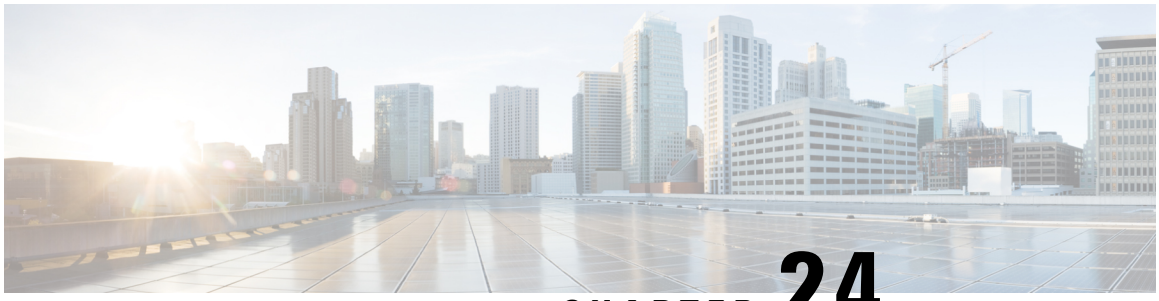
The multi-hop map (table view) is displayed on the **Multi-Hop** tab page.

History for BFD routing

The History table summarizes the introduction and evolution of the BFD routing in Cisco Firewall Management Center across releases, enabling quick tracking of feature availability and changes.

Table 69: Feature history for BFD routing

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
BFD support for IS-IS	7.4	7.4	You can configure BFD on IS-IS interfaces using FlexConfig CLI.
BFD support for OSPF	7.4	7.4	You can enable BFD on interfaces that use OSPF version 2 and OSPF version 3. New/modified screens: • **Configuration** > **Device Setup** > **Routing** > **OSPFv2** • **Configuration** > **Device Setup** > **Routing** > **OSPFv3**
BFD configuration	7.4	7.4	In the previous releases, BFD was configurable on threat defense only through FlexConfig. FlexConfig no longer supports BFD configuration. You can now configure BFD policies for threat defense in the management center UI. In threat defense, BFD is supported only on the BGP protocol. New/modified screens: **Devices** > **Device Management** > **Routing** > **BFD**.



CHAPTER 24

OSPF

This chapter describes how to configure the Firewall Threat Defense to route data, perform authentication, and redistribute routing information using the Open Shortest Path First (OSPF) routing protocol.

- OSPF, on page 1063
- Requirements and prerequisites for OSPF, on page 1067
- Guidelines for OSPF, on page 1067
- OSPFv2 configuration, on page 1070
- OSPFv3 configuration, on page 1083
- History for OSPF, on page 1093

OSPF

This chapter describes how to configure the Firewall Threat Defense to route data, perform authentication, and redistribute routing information using the Open Shortest Path First (OSPF) routing protocol.

OSPF routing

OSPF is an interior gateway routing protocol that

- uses link states rather than distance vectors for path selection,
- propagates link-state advertisements rather than routing table updates, and
- converges more quickly than RIP networks because only LSAs are exchanged instead of the entire routing tables.

OSPF characteristics and features

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

The advantages of OSPF over RIP include these characteristics:

- OSPF link-state database updates are sent less frequently than RIP updates, and the link-state database is updated instantly, rather than gradually, AS stale information is timed out.

- Routing decisions are based on cost, which is an indication of the overhead required to send packets across a certain interface. The Firewall Threat Defense device calculates the cost of an interface based on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The disadvantage of shortest path first algorithms is that they require a lot of CPU cycles and memory.

The Firewall Threat Defense device can run two processes of OSPF protocol simultaneously on different sets of interfaces. You might want to run two processes if you have interfaces that use the same IP addresses (NAT allows these interfaces to coexist, but OSPF does not allow overlapping addresses). Or you might want to run one process on the inside and another on the outside, and redistribute a subset of routes between the two processes. Similarly, you might need to segregate private addresses from public addresses.

You can redistribute routes into an OSPF routing process from another OSPF routing process, a RIP routing process, or from static and connected routes configured on OSPF-enabled interfaces.

The Firewall Threat Defense device supports these OSPF features:

- Intra-area, inter-area, and external (Type I and Type II) routes.
- Virtual links.
- LSA flooding.
- Authentication to OSPF packets (both password and MD5 authentication).
- Configuring the Firewall Threat Defense device AS a designated router or a designated backup router. The Firewall Threat Defense device also can be set up AS an ABR.
- Stub areas and not-so-stubby areas.
- Area boundary router Type 3 LSA filtering.

OSPF supports both MD5 and clear text neighbor authentication. Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (such AS RIP) can potentially be used by attackers to subvert routing information.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts AS a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses LSAs to send information about available routes to other OSPF routers. Using ABR Type 3 LSA filtering, you can have separate private and public areas with the ASA acting AS an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other, which allows you to use NAT and OSPF together without advertising private networks.



Note Only Type 3 LSAs can be filtered. If you configure the Firewall Threat Defense device AS an ASBR in a private network, it will send Type 5 LSAs describing private networks, which will get flooded to the entire AS, including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either AS default or Type 5 AS external LSAs. However, you need to configure

static routes for the private networks protected by the Firewall Threat Defense device. Also, you should not mix public and private networks on the same Firewall Threat Defense device interface.

You can have two OSPF routing processes, one RIP routing process, and one EIGRP routing process running on the Firewall Threat Defense device at the same time.

OSPF support for fast hello packets

OSPF support for fast hello packets is a feature that

- provides a way to configure the sending of hello packets in intervals less than one second, and
- results in faster convergence in an Open Shortest Path First (OSPF) network.

OSPF fast hello packets configuration prerequisites

OSPF must be configured in the network already or configured at the same time as the OSPF Support for Fast Hello Packets feature.

OSPF hello interval and dead interval

OSPF hello interval and dead interval are configurable time parameters that

- maintain connectivity between OSPF neighbors through regular hello packet exchanges,
- detect neighbor failures when hello packets are not received within the specified timeframes, and
- must be consistent across all routers within the same network to ensure proper operation.

Hello interval and dead interval configuration details

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non broadcast link.

Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

OSPF fast hello packets

OSPF fast hello packets are hello packets that

- are sent at intervals of less than 1 second,
- are achieved by using the OSPF dead-interval command with a dead interval set to 1 second, and
- use a hello-multiplier value set to the number of hello packets sent during that 1 second.

Fast hello packet behavior

When fast hello packets are configured on the interface, these behaviors occur:

- The hello interval advertised in the hello packets that are sent out this interface is set to 0.
- The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See OSPF hello interval and dead interval, on page 1065.

Benefits of OSPF fast hello packets

A fast hello packet is an OSPF protocol feature that

- reduces network convergence time by enabling routers to detect changes in the network faster,
- allows rapid detection of lost neighbors within one second, and
- enhances reliability in LAN environments where neighbor loss may not be detected at the Open Systems Interconnection (OSI) physical or data-link layer.

The benefit of OSPF Fast Hello Packets is that your OSPF network can react swiftly to changes, minimizing downtime and improving overall network stability. This feature is particularly useful in scenarios where routers may not detect lost neighbors via traditional methods, allowing OSPF to maintain accurate routing tables.

If a router on a LAN segment is powered off or disconnected and the physical and data-link layers do not signal neighbor loss, OSPF fast hello packets will detect the neighbor's disappearance within one second.

OSPFv2 and OSPFv3 implementation differences

A protocol distinction is a protocol category that

- prevents backward compatibility between OSPFv2 and OSPFv3,
- requires both OSPF versions to run simultaneously for IPv4 and IPv6 routing, and
- allows OSPFv2 and OSPFv3 to coexist without interacting with each other.

OSPFv3 additional features

OSPFv3 provides additional features that include:

- Protocol processing per link.
- Removal of addressing semantics.
- Addition of flooding scope.
- Support for multiple instances per link.
- Use of the IPv6 link-local address for neighbor discovery and other features.

- LSAs expressed as prefix and prefix length.
- Addition of two LSA types.
- Handling of unknown LSA types.
- Authentication support using the IPsec ESP standard for OSPFv3 routing protocol traffic, as specified by RFC-4552.

Requirements and prerequisites for OSPF

This reference provides the requirements and prerequisites that must be met before configuring OSPF on supported devices.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for OSPF

Context mode guidelines

OSPFv2 supports single and multiple context mode.

- OSPFv2 instances cannot form adjacencies with each other across shared interfaces because, by default, inter-context exchange of multicast traffic is not supported across shared interfaces. However, you can use the static neighbor configuration under OSPFv2 process configuration under OSPFv2 process to bring up OSPFv2 neighbourship on a shared interface.
- Inter-context OSPFv2 on separate interfaces is supported.
- **(For point-to-point topology)** In a multiple context mode, you can configure static OSPFv2 neighbors to advertise OSPFv2 routes over a point-to-point, non-broadcast network. For a successful OSPF adjacency formation, when you remove and reconfigure OSPF on a shared interface, execute the commands in this order: Remove the OSPF configuration using **no router <OSPF name>**, and then remove the OSPF point-to-point non-broadcast configuration on the interface using **no OSPF network point-to-point non-broadcast**. When you reconfigure OSPF on the shared interface, configure the OSPF router using **router <OSPF name>**, and then configure the interface with **OSPF network point-to-point non-broadcast**.
- OSPFv3 supports single mode only.

Key chain authentication guidelines

OSPFv2 supports key chain authentication on both single and multiple mode, both in physical and virtual modes. However, in multiple mode, you can configure the key chain only in context mode.

- The rotating keys are applicable only for OSPFv2 protocol. OSPF area authentication with key chain is not supported.
- The existing MD5 authentication without time range in OSPFv2 is still supported along with new rotating keys.
- Though the platform supports SHA1 and MD5 cryptographic algorithms, only MD5 cryptographic algorithm is used for authentication.

Firewall mode guidelines

OSPF supports routed firewall mode only. OSPF does not support transparent firewall mode.

High availability Guidelines

OSPFv2 and OSPFv3 support Stateful High availability.

IPv6 guidelines

OSPFv2 does not support IPv6, while OSPFv3 provides IPv6 support with specific authentication and routing capabilities.

- OSPFv2 does not support IPv6.
- OSPFv3 supports IPv6.
- OSPFv3 uses IPv6 for authentication.
- The Firewall Threat Defense device installs OSPFv3 routes into the IPv6 RIB, provided it is the best route.

OSPFv3 hello packets and GRE

Typically, OSPF traffic does not pass through GRE tunnel. When OSPFv3 on IPv6 is encapsulated inside GRE, the IPv6 header validation for security check such as Multicast Destination fails. The packet is dropped due to the implicit security check validation, as this packet has destination IPv6 multicast.

- You may define a pre-filter rule to bypass GRE traffic. However, with pre-filter rule, inner packets would not be interrogated by the inspection engine.

Clustering guidelines

OSPFv2 and OSPFv3 have specific limitations and behaviors in clustering environments.

- OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment.
- In Spanned interface mode, dynamic routing is not supported on management-only interfaces.
- In Individual interface mode, make sure that you establish the control and data units as either OSPFv2 or OSPFv3 neighbors.

- In Individual interface mode, OSPFv2 adjacencies can only be established between two contexts on a shared interface on the control unit. Configuring static neighbors is supported only on point-to point-links; therefore, only one neighbor statement is allowed on an interface.
- When a control role change occurs in the cluster, specific behavior occurs based on interface mode. In spanned interface mode, the router process is active only on the control unit and is in a suspended state on the data units. Each cluster unit has the same router ID because the configuration has been synchronized from the control unit. As a result, a neighboring router does not notice any change in the router ID of the cluster during a role change. In individual interface mode, the router process is active on all the individual cluster units. Each cluster unit chooses its own distinct router ID from the configured cluster pool. A control role change in the cluster does not change the routing topology in any way.

Multiprotocol label switching (MPLS) and OSPF guidelines

When a MPLS-configured router sends Link State (LS) update packets containing opaque Type-10 link-state advertisements (LSAs) that include an MPLS header, authentication fails and the appliance silently drops the update packets, rather than acknowledging them. Eventually the peer router will terminate the neighbor relationship because it has not received any acknowledgments.

- Make sure that non-stop forwarding (NSF) is disabled on the appliance to ensure that the neighbor relationship remains stable. Navigate to the **Non Stop Forwarding** page in Firewall Management Center (**Devices** > **Device Management (select the desired device)** > **Routing** > **OSPF** > **Advanced** > **Non Stop Forwarding**). Ensure the **Non Stop Forwarding Capability** boxes are not checked.

These guidelines apply to MPLS environments where opaque LSAs might cause authentication failures.



Note The Firepower 4100/9300 models may have high latency when using MPLS because they lack load balancing across multiple receiving queues.

Bidirectional and forwarding detection (BFD) and OSPF guidelines

You can enable BFD on specific interface types with OSPFv2 and OSPFv3.

- You can enable BFD on OSPFv2 and OSPFv3 interfaces (Physical Interfaces, Sub-Interfaces, and Port-Channels).
- BFD is not supported on VTI Tunnels, DVTI Tunnels, Loopback, Switchport, VNI, VTEP, and IRB interfaces.

Route redistribution guidelines

Route redistribution with prefix lists and between routing domains requires specific configuration considerations.

- Redistribution of route maps with IPv4 prefix list on OSPFv2 is supported. However, redistribution of route maps with IPv6 prefix list on OSPFv3 is not supported. Use an access list in the route map on OSPF for redistribution.
- When OSPF is configured on a device that is a part of EIGRP network or vice versa, ensure that OSPF-router is configured to tag the route (EIGRP does not support route tag yet). When redistributing OSPF into EIGRP and EIGRP into OSPF, a routing loop occurs when there is an outage on one of the links, interfaces, or even when the route originator is down. To prevent the redistribution of routes from one domain back into the same domain, a router can tag a route that belongs to a domain while it is

redistributing, and those routes can be filtered on the remote router based on the same tag. Because the routes will not be installed into the routing table, they will not be redistributed back into the same domain.

Additional guidelines

OSPFv2 and OSPFv3 support various features and have specific limitations in different deployment scenarios.

- OSPFv2 and OSPFv3 support multiple instances on an interface.
- OSPFv3 supports encryption through ESP headers in a non-clustered environment.
- OSPFv3 supports Non-Payload Encryption.
- OSPFv2 supports Cisco NSF Graceful Restart and IETF NSF Graceful Restart mechanisms as defined in RFCs 4811, 4812 & 3623 respectively.
- OSPFv3 supports Graceful Restart mechanism as defined in RFC 5187.
- There is a limit to the number of intra area (type 1) routes that can be distributed. For these routes, a single type-1 LSA contains all prefixes. Because the system has a limit of 35 KB for packet size, 3000 routes result in a packet that exceeds the limit. Consider 2900 type 1 routes to be the maximum number supported.
- For a device using virtual routing, you can configure OSPFv2 and OSPFv3 for a global virtual router. However, you can configure only OSPFv2 for a user-defined virtual router.
- To avoid adjacency flaps due to route updates being dropped if the route update is larger than the minimum MTU on the link, ensure that you configure the same MTU on the interfaces on both sides of the link.
- OSPFv3 drops the LS update if the packet size exceeds 8190. As a result, the neighbourship is terminated. Hence, configure the switch with the "ospfv3 MTU-ignore" command to avoid neighbourship termination.

OSPFv2 configuration

This section describes the tasks involved in configuring an OSPFv2 routing process. For a device using virtual routing, you can configure OSPFv2 for global as well as for user-defined virtual routers.

Configure OSPF areas, ranges, and virtual links

Complete the configuration of OSPF by defining areas, assigning route summarization ranges, and creating virtual links to connect discontiguous OSPF areas.

You can configure several OSPF area parameters, which include setting authentication, defining stub areas, and assigning specific costs to the default summary route. You can enable up to two OSPF process instances. Each OSPF process has its own associated areas and networks. Authentication provides password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the ABR into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

For a virtual-router-aware device, choose the virtual router from the virtual routers drop-down list.

Step 3 Click **OSPF** and configure the following on the **OSPF** page:

- Check the check box of **Process 1**. You can enable up to two OSPF process instances for each context /virtual router. You must choose an OSPF process to be able to configure the Area parameters.

  If the device is using virtual routing, the ID fields display the unique process IDs generated for the chosen virtual router.

- Choose the **OSPF Role** from the drop-down list, and enter a description for it in the next field. The options are **Internal Router**, **ABR**, **ASBR**, and **ABR & ASBR**. For a description of the OSPF roles, refer to OSPF routing, on page 1063.

Step 4 Select **Area** > **Add**.

You can click **Edit** ( ) , or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 5 Configure the following area options for each OSPF process:

- **OSPF Process**: Choose the process ID. For a device using virtual routing, the drop-down lists the unique process IDs generated for the selected virtual router.
- **Area ID**: Designation of the area for which routes are to be summarized.
- **Area Type**: Choose one of the following:
  - **Normal**: (Default) Standard OSPF area.
  - **Stub**: A stub area does not have any routers or areas beyond it. Stub areas prevent Autonomous System (AS) External LSAs (Type 5 LSAs) from being flooded into the stub area. When you create a stub area, you can prevent summary LSAs (Types 3 and 4) from being flooded into the area by not checking the **Summary Stub** check box.
  - **NSSA**: Makes the area a not-so-stubby area (NSSA). NSSAs accept Type 7 LSAs. You can disable route redistribution by not checking the **Redistribute** check box and checking the **Default Information Originate** check box. You can prevent summary LSAs from being flooded into the area by not checking the **Summary NSSA** check box.
- **Metric Value**: The metric used for generating the default route. The default value is 10. Valid metric values range from 0 through 16777214.
- **Metric Type**: The metric type is the external link type that is associated with the default route that is advertised into the OSPF routing domain. The available options are 1 for a Type 1 external route or 2 for a Type 2 external route.
- **Available Network**: Choose one of the available networks and click **Add** , or click **Add** ( ) to add a new network object. For the procedure for adding networks, refer to Networks, on page 2386.

- **Authentication**: Choose the OSPF authentication:
  - **None**: (Default) Disables OSPF area authentication.
  - **Password**: Provides a clear text password for area authentication, which is not recommended where security is a concern.
  - **MD5**: Allows MD5 authentication.
- **Default Cost**: The default cost for the OSPF area, which is used to determine the shortest paths to the destination. Valid values range from 0 through 65535. The default value is 1.
- Click **OK** to save the area configuration.

Step 6 Select **Range** > **Add**.

- Choose one of the available networks and whether to advertise, or
- Click **Add** (+) to add a new network object. For the procedure for adding networks, refer to Networks, on page 2386.
- Click **OK** to save the range configuration.

Step 7 Select **Virtual Link**, click **Add** (+), and configure the following options for each OSPF process:

- **Peer Router**: Choose the IP address of the peer router. To add a new peer router, click **Add** (+). For the procedure for adding networks, refer to Networks, on page 2386.
- **Hello Interval**: The time in seconds between the hello packets sent on an interface. The hello interval is an unsigned integer that is to be advertised in the hello packets. The value must be the same for all routers and access servers on a specific network. Valid values range from 1 through 65535. The default is 10.

  The smaller the hello interval, the faster topological changes are detected, but the more traffic is sent on the interface.
- **Transmit Delay**: The estimated time in seconds that is required to send an LSA packet on the interface. The integer value must be greater than zero. Valid values range from 1 through 8192. The default is 1.

  LSAs in the update packet have their own ages incremented by this amount before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links.
- **Retransmit Interval**: The time in seconds between LSA retransmissions for adjacencies that belong to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay, and can range from 1 through 65535. The default is 5.

  When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links.
- **Dead Interval**: The time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The dead interval is an unsigned integer. The default is four times the hello interval, or

40 seconds. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 through 65535.

- **Authentication**: Choose the OSPF virtual link authentication from the following:
  - **None**: (Default) Disables virtual link area authentication.
  - **Area Authentication**: Enables area authentication using MD5. Click **Add**, and enter the key ID, key, confirm the key, and then click **OK**.
  - **Password**: Provides a clear text password for virtual link authentication, which is not recommended where security is a concern.
  - **MD5**: Allows MD5 authentication. Click **Add**, and enter the key ID, key, confirm the key, and then click **OK**.

Note Ensure to enter only numbers as the MD5 key ID.

  - **Key Chain**: Allows key chain authentication. Click **Add**, and create the key chain, and then click **Save**. For detailed procedure, refer to Create a key chain object, on page 2385. Use the same authentication type (MD5 or Key Chain) and key ID for the peers to establish a successful adjacency.
  - Click **OK** to save the virtual link configuration.

Step 8 Click **Save** on the **Routing** page to save your changes.

OSPF is configured with designated areas, summarized ranges, and any necessary virtual links. Routing updates are generated based on your configuration.

Configure OSPF redistribution

This task enables you to control the redistribution of routes between the OSPF routing processes on your Firewall Threat Defense device.

The Firewall Threat Defense device can control the redistribution of routes between the OSPF routing processes. The rules for redistributing routes from one routing process into an OSPF routing process are displayed. You can redistribute routes discovered by EIGRP, RIP and BGP into the OSPF routing process. You can also redistribute static and connected routes into the OSPF routing process.

Before you begin

Follow these steps to configure OSPF redistribution:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF**.

Step 5 From **OSPF Role** drop-down, choose role.

Step 6 Click **Redistribution** > **Add**.

You can click **Edit** (), or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 7 Configure the following redistribution options for each OSPF process:

- **OSPF Process**: Choose the process ID. For a device using virtual routing, this drop-down list displays the unique process IDs generated for the selected virtual router.
- **Route Type**: Choose one of the following types:
  - **Static**: Redistributes static routes to the OSPF routing process.
  - **Connected**: Redistributes connected routes (routes established automatically by virtue of having the IP address enabled on the interface) to the OSPF routing process. Connected routes are redistributed AS external to the device. You can select whether to use subnets under the Optional list.
  - **OSPF**: Redistributes routes from another OSPF routing process, for example, internal, external 1 and 2, NSSA external 1 and 2, or whether to use subnets. You can select these options under the Optional list.
  - **BGP**: Redistribute routes from the BGP routing process. Add the AS number and whether to use subnets.
  - **RIP**: Redistributes routes from the RIP routing process. You can select whether to use subnets under the Optional list.

Note As a user-defined virtual router does not support RIP, you cannot redistribute routes from RIP.

  - **EIGRP**: Redistribute routes from the EIGRP routing process. Add the AS number and whether to use subnets.

- **Metric Value**: Metric value for the routes being distributed. The default value is 10. Valid values range from 0 to 16777214.

  When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

- **Metric Type**: The metric type is the external link type that is associated with the default route that is advertised into the OSPF routing domain. The available options are 1 for a Type 1 external route or 2 for a Type 2 external route.
- **Tag Value**: Tag specifies the 32-bit decimal value attached to each external route that is not used by OSPF itself, but which may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP. For other protocols, zero is used. Valid values are from 0 to 4294967295.

- **RouteMap**: Checks for filtering the importing of routes from the source routing protocol to the current routing protocol. If this parameter is not specified, all routes are redistributed. If this parameter is specified, but no route map tags are listed, no routes are imported. Or you can add a new route map by clicking **Add** (+). To add a new route map, refer to Configure Route Map Entry.

Step 8 Click **OK** to save the redistribution configuration.

Step 9 Click **Save** on the Routing page to save your changes.

OSPF redistribution is now configured for the selected OSPF process with the specified route types and parameters.

Configure OSPF Inter-Area filtering

Configure ABR type 3 LSA filtering to control which prefixes are sent between different OSPF areas and restrict other prefixes to their local OSPF area.

ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one OSPF area to another OSPF area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number. By default, sequence numbers are automatically generated in increments of 5, beginning with 5.

Before you begin

Follow these steps to configure OSPF inter-area filtering:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF**.

Step 5 Select **InterArea** > **Add**.

You can click **Edit** (✎), or use the right-click menu to cut, copy, past, insert, and delete inter-areas.

Step 6 Configure these inter-area filtering options for each OSPF process:

- **OSPF Process**: For a device using virtual routing, the drop-down lists the unique process IDs generated for the selected virtual router.
- **Area ID**: The area for which routes are to be summarized.
- **PrefixList**: The name of the prefix. To add a new prefix list object, see Step 5.

- **Traffic Direction**: Inbound or outbound. Choose Inbound to filter LSAs coming into an OSPF area, or Outbound to filter LSAs coming out of an OSPF area. If you are editing an existing filter entry, you cannot modify this setting.

Step 7 Click **Add** (+), and enter a name for the new prefix list, and whether to allow overrides.

You must configure a prefix list before you can configure a prefix rule.

Step 8 Click **Add** to configure prefix rules, and configure these parameters:

- **Action**: Select **Block** or **Allow** for the redistribution access.
- **Sequence No**: The routing sequence number. By default, sequence numbers are automatically generated in increments of 5, beginning with 5.
- **IP Address**: Specify the prefix number in the format of IP address/mask length.
- **Min Prefix Length**: (Optional) The minimum prefix length.
- **Max Prefix Length**: (Optional) The maximum prefix length.
- Click **OK** to save the inter-area filtering configuration.

Step 9 Click **Save** on the Routing page to save your changes.

The OSPF inter-area filtering configuration is saved and applied to control LSA distribution between the specified OSPF areas according to the configured prefix lists and traffic direction settings.

Configure OSPF filter rules

Configure OSPF filter rules to improve control of route distribution between OSPF areas by allowing only specified prefixes to be sent from one area to another area while restricting all other prefixes.

You can configure ABR Type 3 LSA filters for each OSPF process. ABR Type 3 LSA filters allow only specified prefixes to be sent from one area to another area and restrict all other prefixes. You can apply this type of area filtering out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF area at the same time. OSPF ABR Type 3 LSA filtering improves your control of route distribution between OSPF areas.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF**.

Step 5 Select **Filter Rule** > **Add**.

You can click **Edit** (✎), or use the right-click menu to cut, copy, past, insert, and delete filter rules.

Step 6 Configure the following filter rule options for each OSPF process:

- **OSPF Process**: For a device using virtual routing, the drop-down lists the unique process IDs generated for the selected virtual router.
- **Access List**: The access list for this OSPF process. To add a new standard access list object, click **Add** (+) and refer to Configure a standard ACL object, on page 2355.
- **Traffic Direction**: Choose In or Out for the traffic direction being filtered. Choose In to filter LSAs coming into an OSPF area, or Out to filter LSAs coming out of an OSPF area. If you are editing an existing filter entry, you cannot modify this setting.
- **Interface**: The interface for this filter rule.

Step 7 Click **OK** to save the filter rule configuration.

Step 8 Click **Save** on the Routing page to save your changes.

The OSPF filter rules are configured and saved, enabling controlled route distribution between OSPF areas based on the specified access list and traffic direction settings.

Configure OSPF summary addresses

Configure OSPF summary addresses to decrease the size of the OSPF link-state database by advertising a single route for all redistributed routes that are included for a specified network address and mask.

When routes from other protocols are redistributed into OSPF, each route is advertised individually in an external LSA. However, you can configure the Firewall Threat Defense device to advertise a single route for all the redistributed routes that are included for a specified network address and mask. This configuration decreases the size of the OSPF link-state database. Routes that match the specified IP address mask pair can be suppressed. The tag value can be used as a match value for controlling redistribution through route maps.

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. Summary routes help reduce the size of the routing table.

Using summary routes for OSPF causes an OSPF ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by the address. Only routes from other routing protocols that are being redistributed into OSPF can be summarized.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF**.

Step 5 Select **Summary Address** > **Add**.

You can click **Edit** (✎) to edit, or use the right-click menu to cut, copy, past, insert, and delete summary addresses.

Step 6 Configure the following summary address options for each OSPF process:

- **OSPF Process**: For a device using virtual routing, the drop-down lists the unique process IDs generated for the selected virtual router.
- **Available Network**: The IP address of the summary address. Select one from the Available networks list and click **Add**, or to add a new network, click **Add** (+). See Networks, on page 2386 for the procedure for adding networks.
- **Tag**: A 32-bit decimal value that is attached to each external route. This value is not used by OSPF itself, but may be used to communicate information between ASBRs.
- **Advertise**: Advertises the summary route. Uncheck this check box to suppress routes that fall under the summary address. By default, this check box is checked.

Step 7 Click **OK** to save the summary address configuration.

Step 8 Click **Save** on the Routing page to save your changes.

The OSPF summary address configuration is saved and the device will advertise a single route for all redistributed routes that are included for the specified network address and mask.

Configure OSPF interfaces and neighbors

You can change some interface-specific OSPFv2 parameters, if necessary. You are not required to change any of these parameters, but the following interface parameters must be consistent across all routers in an attached network: the hello interval, the dead interval, and the authentication key. If you configure any of these parameters, be sure that the configurations for all routers on your network have compatible values.

You need to define static OSPFv2 neighbors to advertise OSPFv2 routes over a point-to-point, non-broadcast network. This feature lets you broadcast OSPFv2 advertisements across an existing VPN connection without having to encapsulate the advertisements in a GRE tunnel.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF**.

Step 5 Select **Interface** > **Add**.

You can click **Edit** (✎), or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 6 Configure the following Interface options for each OSPF process:

- **Interface**: The interface you are configuring.

Note If the device is using virtual routing, this drop-down list displays only those interfaces that belong to the router.

- **Default Cost**: The cost of sending a packet through the interface. The default value is 10.
- **Priority**: The designated router for a network. Valid values range from 0 to 255. The default value is 1. Entering 0 for this setting makes the router ineligible to become the designated router or backup designated router.

  When two routers connect to a network, both attempt to become the designated router. The device with the higher router priority becomes the designated router. If there is a tie, the router with the higher router ID becomes the designated router. This setting does not apply to interfaces that are configured as point-to-point interfaces.
- **MTU Ignore—OSPF** checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency is not established.
- **Database Filter**: Use this setting to filter the outgoing LSA interface during synchronization and flooding. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. In a fully meshed topology, this flooding can waste bandwidth and lead to excessive link and CPU usage. Checking this check box prevents OSPF flooding of the LSA on the selected interface.
- **Database Filter**: Use this setting to filter the outgoing LSA interface during synchronization and flooding. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. In a fully meshed topology, this flooding can waste bandwidth and lead to excessive link and CPU usage. Checking this check box prevents OSPF flooding of the LSA on the selected interface.
- **Hello Interval**: Specifies the interval, in seconds, between hello packets sent on an interface. Valid values range 1–8192 seconds. The default value is 10 seconds.

  The smaller the hello interval, the faster topological changes are detected, but more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface.
- **Transmit Delay**: Estimated time in seconds to send an LSA packet on the interface. Valid values range 1–65535 seconds. The default is 1 second.

  LSAs in the update packet have their ages increased by the amount specified by this field before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links.
- **Retransmit Interval**: Time in seconds between LSA retransmissions for adjacencies that belong to the interface. The time must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds. The default is 5 seconds.

  When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links.
- **Dead Interval**: Time period in seconds for which hello packets must not be seen before neighbors indicate that the router is down. The value must be the same for all nodes on the network and can range 1–65535.

- **Hello Multiplier**: Specifies the number of Hello packets to be sent per second. Valid values are 3–20.
- **Point-to-Point**: Lets you transmit OSPF routes over VPN tunnels.
- **Authentication**: Choose the OSPF interface authentication from the following:
  - **None**: (Default) Disables interface authentication.
  - **Area Authentication**: Enables interface authentication using MD5. Click **Add**, and enter the key ID, key, confirm the key, and then click **OK**.
  - **Password**: Provides a clear text password for virtual link authentication, which is not recommended where security is a concern.
  - **MD5**: Allows MD5 authentication. Click **Add**, and enter the key ID, key, confirm the key, and then click **OK**.

Note Enter only letters, numbers, and special characters for the MD5 key ID. Do not enter spaces; spaces are truncated in management center.

  - **Key Chain**:Allows key chain authentication. Click **Add**, and create the key chain, and then click **Save**. For detailed procedure, refer to Create a key chain object, on page 2385. Use the same authentication type (MD5 or Key Chain) and key ID for the peers to establish a successful adjacency.
- **Enable BFD**: Allows you to enable BFD on this interface.
- **Enter Password**: The password you configure if you choose Password as the type of authentication.
- **Confirm Password**: Confirm the password that you chose.

Step 7 Select **Neighbor** > **Add**.

You can click **Edit** (), or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 8 Configure the following parameters for each OSPF process:

- **OSPF Process**: Choose 1 or 2.
- **Neighbor**: Choose one of the neighbors in the drop-down list, or click **Add** () to add a new neighbor; enter the name, description, network, whether to allow overrides, and then click **Save**.
- **Interface**: Choose the interface associated with the neighbor.

Step 9 Click **OK** and click **Save** to save the changes.

OSPF interface and neighbor configuration is completed. The configured parameters are applied to the selected interfaces and neighbors, enabling OSPF routing functionality on the specified network segments.

Configure OSPF Advanced Properties

Enable advanced OSPF features for optimized routing behavior and enhanced protocol reliability.

The Advanced Properties allows you to configure options, such as syslog message generation, administrative route distances, an LSA timer, and graceful restarts.

Graceful Restarts

The Firewall Threat Defense device may experience some known failure situations that should not affect packet forwarding across the switching platform. The Non-Stop Forwarding (NSF) capability allows data forwarding to continue along known routes, while the routing protocol information is being restored. This capability is useful when there is a scheduled hitless software upgrade. You can configure graceful restart on OSPFv2 by using either using NSF Cisco (RFC 4811 and RFC 4812) or NSF IETF (RFC 3623).

Note NSF capability is also useful in HA mode and clustering.

Configuring the NSF graceful-restart feature involves two steps; configuring capabilities and configuring a device as NSF-capable or NSF-aware. A NSF-capable device can indicate its own restart activities to neighbors and a NSF-aware device can help a restarting neighbor.

A device can be configured as NSF-capable or NSF-aware, depending on some conditions:

- A device can be configured as NSF-aware irrespective of the mode in which it is.
- A device has to be in either Failover or Spanned Etherchannel (L2) cluster mode to be configured as NSF-capable.
- For a device to be either NSF-aware or NSF-capable, it should be configured with the capability of handling opaque Link State Advertisements (LSAs)/ Link Local Signaling (LLS) block as required.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 (For a virtual-router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring OSPF.

Step 4 Click **OSPF** > **Advanced**.

Step 5 Select **General**, and configure the following:

- **Router ID**: Choose Automatic or IP Address (appears for non-cluster and a cluster in spanned etherchannel mode) or Cluster Pool (appears for a cluster in individual interface mode) for the router ID. If you choose IP address, enter the IP address in the adjacent field. If you choose Cluster Pool, choose the IPv4 cluster pool value in the adjacent drop-down field. For information on creating the cluster pool address, see Configure address pools, on page 2356 .
- **Ignore LSA MOSPF**: Suppresses syslog messages when the route receives unsupported LSA Type 6 multicast OSPF (MOSPF) packets.
- **RFC 1583 Compatible**: Configures RFC 1583 compatibility as the method used to calculate summary route costs. Routing loops can occur with RFC 1583 compatibility enabled. Disable it to prevent routing loops. All OSPF routers in an OSPF routing domain should have RFC compatibility set identically.

- **Adjacency Changes**: Defines the adjacency changes that cause syslog messages to be sent.

  By default, a syslog message is generated when an OSPF neighbor goes up or down. You can configure the router to send a syslog message when an OSPF neighbor goes down and also a syslog for each state.

  - **Log Adjacency Changes**: Causes the Firewall Threat Defense device to send a syslog message whenever an OSPF neighbor goes up or down. This setting is checked by default.
  - **Log Adjacency Change Details**: Causes the Firewall Threat Defense device to send a syslog message whenever any state change occurs, not just when a neighbor goes up or down. This setting is unchecked by default.

- **Administrative Route Distance**: Allows you to modify the settings that were used to configure administrative route distances for **inter-area**, **intra-area**, and **external** IPv6 routes. The administrative route distance is an integer from 1 to 254. The default is 110.
- **LSA Group Pacing**: Specifies the interval in seconds at which LSAs are collected into a group and refreshed, check summed, or aged. Valid values range from 10 to 1800. The default value is 240.
- **Enable Default Information Originate**: Check the **Enable** check box to generate a default external route into an OSPF routing domain and configure the following options:
  - **Always advertise the default route**: Ensures that the default route is always advertised.
  - **Metric Value**: Metric used for generating the default route. Valid metric values range from 0 to 16777214. The default value is 10.
  - **Metric Type**: The external link type that is associated with the default route that is advertised into the OSPFv3 routing domain. Valid values are 1 (Type 1 external route) and 2 (Type 2 external route). The default is Type 2 external route.
  - **RouteMap**: Choose the routing process that generates the default route if the route map is satisfied or click **Add** (+) to add a new one. See Configure Route Map Entry to add a new route map.

Step 6 Click **OK** to save the general configuration.

Step 7 Select **Non Stop Forwarding**, and configure Cisco NSF graceful restart for OSPFv2, for an NSF-capable or NSF-aware device.

Note There are two graceful restart mechanisms for OSPFv2, Cisco NSF and IETF NSF. Only one of these graceful restart mechanisms can be configured at a time for an OSPF instance. An NSF-aware device can be configured as both Cisco NSF helper and IETF NSF helper but a NSF-capable device can be configured in either Cisco NSF or IETF NSF mode at a time for an OSPF instance.

a) Check the **Enable Cisco Non Stop Forwarding Capability** check box.
b) (Optional) Check the **Cancel NSF restart when non-NSF-aware neighboring networking devices are detected** check box if required.
c) (Optional) Make sure the **Enable Cisco Non Stop Forwarding Helper** mode check box is unchecked to disable the helper mode on an NSF-aware device.

Step 8 Configure IETF NSF Graceful Restart for OSPFv2, for an NSF-capable or NSF-aware device: .

a) Check the **Enable IETF Non Stop Forwarding Capability** check box.

b) In the **Length of graceful restart interval (seconds)** field, enter the restart interval in seconds. The default value is 120 seconds. For a restart interval below 30 seconds, graceful restart will be terminated.
c) (Optional) Make sure the **Enable IETF nonstop forwarding (NSF) for helper mode** check box is unchecked to disable the IETF NSF helper mode on an NSF-aware device.
d) **Enable Strict Link State advertisement checking**: When enabled, it indicates that the helper router will terminate the process of restarting the router if it detects that there is a change to a LSA that would be flooded to the restarting router, or if there is a changed LSA on the retransmission list of the restarting router when the graceful restart process is initiated.
e) **Enable IETF Non Stop Forwarding**: Enables non stop forwarding, which allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. OSPF uses extensions to the OSPF protocol to recover its state from neighboring OSPF devices. For the recovery to work, the neighbors must support the NSF protocol extensions and be willing to act as "helpers" to the device that is restarting. The neighbors must also continue forwarding data traffic to the device that is restarting while protocol state recovery takes place.

Advanced OSPF settings are applied. The device now uses customized OSPF general and graceful restart properties for improved routing behavior, syslog management, and protocol resilience.

OSPFv3 configuration

OSPFv3 configuration is a routing process setup that

- enables IPv6 routing functionality on network devices,
- involves multiple configuration tasks to establish the routing process, and
- supports configuration only for global virtual routers in virtual routing environments.

Virtual routing limitations

For a device using virtual routing, you can configure OSPFv3 only for its global virtual router and not for its user-defined virtual router.

Configure OSPFv3 Areas, Route Summaries, and Virtual Links

Use this task to enable OSPFv3, create routing areas, set up route summaries, and configure virtual links for advanced routing scenarios on the Cisco Secure Firewall Management Center (FMC). These steps allow for flexible IPv6 routing and help ensure optimal path calculation and efficient management.

Before you begin

Have admin access to Cisco Secure Firewall Management Center.

- Have admin access to Cisco Secure Firewall Management Center.
- Know the IP addresses and roles for devices to be configured.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Navigate to the **Routing** tab, and click **OSPFv3** in the left pane.

Step 3 By default **Enable Process 1** is selected. You can enable up to two OSPF process instances.

Step 4 Choose the OSPFv3 role from the drop-down list, and enter a description for it. The options are **Internal**, **ABR**, **ASBR**, and **ABR and ASBR**. For descriptions of the OSPFv3 roles, refer to OSPF routing, on page 1063.

Step 5 Select **Area** > **Add**.

Click **Edit** ( ), or use the right-click menu to cut, copy, past, insert, and delete areas.

Select **General**, and configure the following options for each OSPF process:

a) **Area ID**: The area for which routes are to be summarized.
b) **Cost**: The metric or cost for the summary route, which is used during OSPF SPF calculations to determine the shortest paths to the destination. Valid values range from 0 to 16777215.
c) **Type**: Specifies Normal, NSSA, or Stub. If you select Normal, there are no other parameters to configure. If you select Stub, you can choose to send summary LSAs in the area. If you select NSSA, you can configure the next three options:

- **Allow Sending summary LSA into this area**: Allows the sending of summary LSAs into the area.
- **Imports routes to normal and NSSA area**: Allows redistribution to import routes to normal and not to stubby areas.
- **Defaults information originate**: Generates a default external route into an OSPFv3 routing domain.

d) **Metric**: Metric used for generating the default route. The default value is 10. Valid metric values range from 0 to 16777214.
e) **Metric Type**: The metric type is the external link type that is associated with the default route that is advertised into the OSPFv3 routing domain. The available options are 1 for a Type 1 external route or 2 for a Type 2 external route. Click **OK** to save the general configuration.

Step 6 (Not applicable for Internal OSPFv3 Role) Select **Route Summary** > **Add Route Summary**.

Click **Edit** ( ), or use the right-click menu to cut, copy, past, insert, and delete route summaries.

Configure the following route summary options for each OSPF process:

- **IPv6 Prefix/Length**: The IPv6 prefix. To add a new network object, click **Add** ( ). For the procedure for adding networks, refer to, Networks, on page 2386.
- **Cost**: The metric or cost for the summary route, which is used during OSPF SPF calculations to determine the shortest paths to the destination. Valid values range from 0 to 16777215.
- **Advertise**: Advertises the summary route. Uncheck this check box to suppress routes that fall under the summary address. By default, this check box is checked.

  Click **OK** to save the route summary configuration.

Step 7 (Not applicable for Internal OSPFv3 Role) Select **Virtual Link**, click **Add Virtual Link** , and configure the following options for each OSPF process:

- **Peer RouterID**: Choose the IP address of the peer router. To add a new network object, click **Add** (+). For the procedure to add networks, refer to Networks, on page 2386.
- **TTL Security**: Enables TTL security check. The value for the hop-count is a number from 1 to 254. The default is 1.

  OSPF sends outgoing packets with an IP header Time to Live (TTL) value of 255 and discards incoming packets that have TTL values less than a configurable threshold. Because each device that forwards an IP packet decrements the TTL, packets received via a direct (one-hop) connection have a value of 255. Packets that cross two hops have a value of 254, and so on. The receive threshold is configured in terms of the maximum number of hops that a packet may have traveled.
- **Dead Interval**: The time in seconds that hello packets are not seen before a neighbor indicates that the router is down. The default is four times the hello interval, or 40 seconds. Valid values range from 1 to 65535.

  The dead interval is an unsigned integer. The value must be the same for all routers and access servers that are attached to a common network.
- **Hello Interval**: The time in seconds between the hello packets sent on an interface. Valid values range from 1 to 65535. The default is 10.

  The hello interval is an unsigned integer that is to be advertised in the hello packets. The value must be the same for all routers and access servers on a specific network. The smaller the hello interval, the faster topological changes are detected, but the more traffic is sent on the interface.
- **Retransmit Interval**: The time in seconds between LSA retransmissions for adjacencies that belong to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay, and can range from 1 to 65535. The default is 5.

  When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links.
- **Transmit Delay**: The estimated time in seconds that is required to send an LSA packet on the interface. The integer value must be greater than zero. Valid values range from 1 to 8192. The default is 1.

  LSAs in the update packet have their own ages incremented by this amount before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links.

  Click **OK** to save the virtual link configuration.

Step 8 Click **Save** on the **Router** page to save your changes.

Configure OSPFv3 redistribution

Configure OSPFv3 redistribution to control how routes are redistributed between OSPF routing processes and other routing protocols on the Secure Firewall Threat Defense device.

The Secure Firewall Threat Defense device can control the redistribution of routes between the OSPF routing processes. The rules for redistributing routes from one routing process into an OSPF routing process are displayed. You can redistribute routes discovered by EIGRP, RIP and BGP into the OSPF routing process. You can also redistribute static and connected routes into the OSPF routing process.

Before you begin

Follow these steps to configure OSPFv3 redistribution:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **Routing** > **OSPF**.

Step 3 Select **Redistribution**, and click **Add**.

You can click **Edit** (), or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 4 Configure the following redistribution options for each OSPF process:

- **Source Protocol**—The source protocol from which routes are being redistributed. The supported protocols are connected, OSPF, Static, EIGRP, and BGP. If you choose OSPF, you must enter the Process ID in the **Process ID** field. If you choose BGP, you must add the AS number in the **AS Number** field.
- **Metric**—Metric value for the routes being distributed. The default value is 10. Valid values range from 0 to 16777214.

  When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
- **Metric Type**—The metric type is the external link type that is associated with the default route that is advertised into the OSPF routing domain. The available options are 1 for a Type 1 external route or 2 for a Type 2 external route.
- **Tag**—Tag specifies the 32-bit decimal value attached to each external route that is not used by OSPF itself, but which may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP. For other protocols, zero is used. Valid values are from 0 to 4294967295.
- **Route Map**—Checks for filtering the importing of routes from the source routing protocol to the current routing protocol. If this parameter is not specified, all routes are redistributed. If this parameter is specified, but no route map tags are listed, no routes are imported. Or you can add a new route map by clicking **Add** (). See Configure a route map, on page 2415 for the procedure to add a new route map.
- **Process ID**—The OSPF process ID, either 1 or 2.

Note The Process ID is enabled the OSPFv3 process is redistributing a route learned by another OSPFv3 process.

- **Match**—Enables OSPF routes to be redistributed into other routing domains:

- **Internal** for routes that are internal to a specific autonomous system.
- **External 1**for routes that are external to the autonomous system, but are imported into OSPFv3 AS Type 1 external routes.
- **External 2** for routes that are external to the autonomous system, but are imported into OSPFv3 AS Type 2 external routes.
- **NSSA External 1** for routes that are external to the autonomous system, but are imported into OSPFv3 in an NSSA for IPv6 AS Type 1 external routes.
- **NSSA External 2** for routes that are external to the autonomous system, but are imported into OSPFv3 in an NSSA for IPv6 AS Type 2 external routes.

Step 5 Click **OK** to save the redistribution configuration.

Step 6 Click **Save** on the Routing page to save your changes.

The OSPFv3 redistribution configuration is saved and routes are redistributed according to the specified parameters.

What to do next

Continue with Configure OSPFv3 summary prefixes, on page 1087.

Configure OSPFv3 summary prefixes

Configure OSPFv3 summary prefixes to control route advertisement and suppression based on IPv6 prefix and mask pairs.

You can configure the Firewall Threat Defense device to advertise routes that match a specified IPv6 prefix and mask pair.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **Routing** > **OSPFv3**.

Step 3 Select **Summary Prefix** > **Add**.

You can click **Edit** ( ), or use the right-click menu to cut, copy, past, insert, and delete summary prefixes.

Step 4 Configure the following summary prefix options for each OSPF process:

- **IPv6 Prefix/Length**: The IPv6 prefix and prefix length label. Select one from the list or click **Add** ( ) to add a new network object. For the procedure to add networks, refer to Networks, on page 2386.
- **Advertise**: Advertises routes that match the specified prefix and mask pair. Uncheck this check box to suppress routes that match the specified prefix and mask pair.
- (Optional) **Tag**: A value that you can use as a match value for controlling redistribution through route maps.

Step 5 Click **OK** to save the summary prefix configuration.

Step 6 Click **Save** on the Routing page to save your changes.

The OSPFv3 summary prefix configuration is saved and will control route advertisement based on your specified settings.

Configure OSPFv3 interfaces, authentication, and neighbors

Set up OSPFv3 routing, authentication, and neighbor relationships to support IPv6 dynamic network routing.

You can change certain interface-specific OSPFv3 parameters, if necessary. You are not required to change any of these parameters, but the following interface parameters must be consistent across all routers in an attached network: the hello interval and the dead interval. If you configure any of these parameters, be sure that the configurations for all routers on your network have compatible values.

For a successful implementation of OSPFv3 authentication with Nexus switches, ensure that you have the compatible version of the switch, for example, Nexus 3000, 7000, and 9000 series switches.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **Routing** > **OSPFv3**.

Step 3 Select **Interface** > **Add**.

You can click **Edit** to edit, or use the right-click menu to cut, copy, past, insert, and delete areas.

Step 4 Configure the following interface options for each OSPFv3 process:

- **Interface**: The interface you are configuring.
- **Enable OSPFv3**: Enables OSPFv3.
- **OSPF Process**: Choose 1 or 2.
- **Area**: The area ID for this process.
- **Instance**: Specifies the area instance ID to be assigned to the interface. An interface can have only one OSPFv3 area. You can use the same area on multiple interfaces, and each interface can use a different area instance ID.

Step 5 Select **Properties**, and configuring the following options for each OSPFv3 process:

- **Filter Outgoing Link Status Advertisements**: Filters outgoing LSAs to an OSPFv3 interface. All outgoing LSAs are flooded to the interface by default.
- **Filter Outgoing Link Status Advertisements**: Filters outgoing LSAs to an OSPFv3 interface. All outgoing LSAs are flooded to the interface by default.
- **Disable MTU mismatch detection**: Disables the OSPF MTU mismatch detection when DBD packets are received. OSPF MTU mismatch detection is enabled by default.

- **Flood Reduction**: Changes normal LSAs into Do Not Age LSAs, so that they don't get flooded every 3600 seconds across areas.

  OSPF LSAs are refreshed every 3600 seconds. In large OSPF networks, this can lead to large amounts of unnecessary LSA flooding from area to area.

- **Point-to-Point Network**: Lets you transmit OSPF routes over VPN tunnels. When an interface is configured as point-to-point, non-broadcast, the following restrictions apply:
  - You can define only one neighbor for the interface.
  - You need to manually configure the neighbor.
  - You need to define a static route pointing to the crypto endpoint.
  - If OSPF over a tunnel is running on the interface, regular OSPF with an upstream router cannot be run on the same interface.
  - You should bind the crypto map to the interface before specifying the OSPF neighbor to ensure that the OSPF updates are passed through the VPN tunnel. If you bind the crypto map to the interface after specifying the OSPF neighbor, use the **clear local-host all** command to clear OSPF connections so that the OSPF adjacencies can be established over the VPN tunnel.

- **Broadcast**: Specifies that the interface is a broadcast interface. By default, this check box is checked for Ethernet interfaces. Uncheck this check box to designate the interface as a point-to-point, nonbroadcast interface. Specifying an interface as point-to-point, nonbroadcast lets you transmit OSPF routes over VPN tunnels.

- **Cost**: Specifies the cost of sending a packet on the interface. Valid values for this setting range from 0 to 255. The default value is 1. Entering 0 for this setting makes the router ineligible to become the designated router or backup designated router. This setting does not apply to interfaces that are configured as point-to-point, nonbroadcast interfaces.

  When two routers connect to a network, both attempt to become the designated router. The device with the higher router priority becomes the designated router. If there is a tie, the router with the higher router ID becomes the designated router.

- **Priority**: Determines the designated router for a network. Valid values range from 0 to 255.

- **Dead Interval**: Time period in seconds for which hello packets must not be seen before neighbors indicate that the router is down. The value must be the same for all nodes on the network and can range from 1 to 65535.

- **Hello Interval**: Time period in seconds between OSPF packets that the router will send before adjacency is established with a neighbor. Once the routing device detects an active neighbor, the hello packet interval changes from the time specified in the poll interval to the time specified in the hello interval. Valid values range from 1 to 65535 seconds.

- **Retransmit Interval**: Time in seconds between LSA retransmissions for adjacencies that belong to the interface. The time must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds. The default is 5 seconds.

- **Transmit Delay**: Estimated time in seconds to send a link-state update packet on the interface. Valid values range from 1 to 65535 seconds. The default is 1 second.

- **Enable BFD**: Allows you to enable BFD on this interface.

Step 6 Select **Authentication**, and configure the following options for each OSPFv3 process:

- **Type**: Type of authentication. The available options are Area, Interface, and None. The None option indicates that no authentication is used.
- **Security Parameters Index**: A number from 256 to 4294967295. Configure this if you chose Interface as the type.
- **Authentication**: Type of authentication algorithm. Supported values are SHA-1 and MD5. Configure this if you chose Interface as the type.
- **Authentication Key**: When MD5 authentication is used, the key must be 32 hexadecimal digits (16 bytes) long. When SHA-1 authentication is used, the key must be 40 hexadecimal digits (20 bytes) long.
- **Encrypt Authentication Key**: Enables encryption of the authentication key.
- **Include Encryption**: Enables encryption.
- **Encryption Algorithm**: Type of encryption algorithm. Supported value is DES. The NULL entry indicates no encryption. Configure this if you chose **Include Encryption**.
- **Encryption Key**: Enter the encryption key. The key length must be a hexadecimal string. When AES-256-CBC authentication is used, the key must be 130 hexadecimal digits. Configure this if you chose **Include Encryption**.
- **Encrypt Key**: Enables the key to be encrypted.

Step 7 Click **OK** to save the authentication configuration.

Step 8 Select **Neighbor**, click **Add**, and configure the following options for each OSPFv3 process:

- **Link Local Address**: The IPv6 address of the static neighbor.
- **Cost**: Enables cost. Enter the cost in the **Cost** field, and check the **Filter Outgoing Link State Advertisements** if you want to advertise.
- (Optional) **Poll Interval**: Enables the poll interval. Enter the **Priority** level and the **Poll Interval** in seconds.
- Click **Add** to add the neighbor.

Step 9 Click **OK** to save the Interface configuration.

OSPFv3 interface, authentication, and neighbor settings are configured on the device. OSPFv3 processes will operate according to the specified parameters.

Configure OSPFv3 Advanced Properties

Enable and fine-tune OSPFv3 advanced properties to optimize routing, ensure stability, and automate operations for your device

The Advanced Properties allows you to configure options, such as syslog message generation, administrative route distances, passive OSPFv3 routing, LSA timers, and graceful restarts.

Graceful Restarts

The Firewall Threat Defense device may experience some known failure situations that should not affect packet forwarding across the switching platform. The Non-Stop Forwarding (NSF) capability allows data forwarding to continue along known routes, while the routing protocol information is being restored. This capability is useful when there is a scheduled hitless software upgrade. You can configure graceful restart on OSPFv3 using graceful-restart (RFC 5187).



Note NSF capability is also useful in HA mode and clustering.

Configuring the NSF graceful-restart feature involves two steps; configuring capabilities and configuring a device as NSF-capable or NSF-aware. A NSF-capable device can indicate its own restart activities to neighbors and a NSF-aware device can help a restarting neighbor.

A device can be configured as NSF-capable or NSF-aware, depending on some conditions:

- A device can be configured as NSF-aware irrespective of the mode in which it is.
- A device has to be in either Failover or Spanned Etherchannel (L2) cluster mode to be configured as NSF-capable.
- For a device to be either NSF-aware or NSF-capable, it should be configured with the capability of handling opaque Link State Advertisements (LSAs)/ Link Local Signaling (LLS) block as required.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **OSPFv3** > **Advanced**.

Step 3 For **Router ID**, choose **Automatic** or **IP Address** (appears for non-cluster and a cluster in spanned etherchannel mode) or **Cluster Pool** (appears for a cluster in individual interface mode). If you choose **IP Address**, enter the IPv6 address in the **IP Address** field. If you choose **Cluster Pool**, choose the IPv6 cluster pool value from the **Cluster Pool** down-down list. For information on creating the cluster pool address, refer to Configure address pools, on page 2356.

Check the **Ignore LSA MOSPF** check box if you want to suppress syslog messages when the route receives unsupported LSA Type 6 multicast OSPF (MOSPF) packets.

Step 4 Select **General**, and configure the following:

- **Adjacency Changes**: Defines the adjacency changes that cause syslog messages to be sent.

  By default, a syslog message is generated when an OSPF neighbor goes up or down. You can configure the router to send a syslog message when an OSPF neighbor goes down and also a syslog for each state.

  - **Adjacency Changes**: Causes the Firewall Threat Defense device to send a syslog message whenever an OSPF neighbor goes up or down. This setting is checked by default.
  - **Include Details**: Causes the Firewall Threat Defense device to send a syslog message whenever any state change occurs, not just when a neighbor goes up or down. This setting is unchecked by default.

- **Administrative Route Distances**: Allows you to modify the settings that were used to configure administrative route distances for inter-area, intra-area, and external IPv6 routes. The administrative route distance is an integer from 1 to 254. The default is 110.
- **Default Information Originate**: Check the **Enable** check box to generate a default external route into an OSPFv3 routing domain and configure the following options:
  - **Always Advertise**: Will always advertise the default route whether or not one exists.
  - **Metric**: Metric used for generating the default route. Valid metric values range from 0 to 16777214. The default value is 10.
  - **Metric Type**: The external link type that is associated with the default route that is advertised into the OSPFv3 routing domain. Valid values are 1 (Type 1 external route) and 2 (Type 2 external route). The default is Type 2 external route.
  - **Route Map**: Choose the routing process that generates the default route if the route map is satisfied or click **Add** (+) to add a new one. See Configure a route map, on page 2415 to add a new route map.

    Click **OK** to save the general configuration.

Step 5 Select **Passive Interface**, select the interfaces on which you want to enable passive OSPFv3 routing from the **Available Interfaces** list, and click **Add** to move them to the **Selected Interfaces** list.

Passive routing assists in controlling the advertisement of OSPFv3 routing information and disables the sending and receiving of OSPFv3 routing updates on an interface.

Click **OK** to save the passive interface configuration.

Step 6 Select **Timer**, and configure the following LSA pacing and SPF calculation timers:

- **Arrival**: Specifies the minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 6000,000 milliseconds. The default is 1000 milliseconds.
- **Flood Pacing**: Specifies the time in milliseconds at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 to 100 milliseconds. The default value is 33 milliseconds.
- **Group Pacing**: Specifies the interval in seconds at which LSAs are collected into a group and refreshed, check summed, or aged. Valid values range from 10 to 1800. The default value is 240.
- **Retransmission Pacing**: Specifies the time in milliseconds at which LSAs in the retransmission queue are paced. The configurable range is from 5 to 200 milliseconds. The default value is 66 milliseconds.
- **LSA Throttle**: Specifics the delay in milliseconds to generate the first occurrence of the LSA. The default value is 0 millisecond. The minimum specifies the minimum delay in milliseconds to originate the same LSA. The default value is 5000 milliseconds. The maximum specifies the maximum delay in milliseconds to originate the same LSA. The default value is 5000 milliseconds.

Note For LSA throttling, if the minimum or maximum time is less than the first occurrence value, then OSPFv3 automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPFv3 automatically corrects to the minimum delay value.

- **SPF Throttle**: Specifies the delay in milliseconds to receive a change to the SPF calculation. The default value is 5000 milliseconds. The minimum specifies the delay in milliseconds between the first and second SPF calculations. The default value is 10000 milliseconds. The maximum specifies the maximum wait time in milliseconds for SPF calculations. The default value is 10000 milliseconds.

Note For SPF throttling, if the minimum or maximum time is less than the first occurrence value, then OSPFv3 automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPFv3 automatically corrects to the minimum delay value.

Click **OK** to save the LSA timer configuration.

Step 7 Select **Non Stop Forwarding ngf**, and check the **Enable graceful-restart helper** check box. This is checked by default. Uncheck this to disable the graceful-restart helper mode on an NSF-aware device.

Check the **Enable link state advertisement** check box to enable strict link state advertisement checking.

When enabled, it indicates that the helper router will terminate the process of restarting the router if it detects that there is a change to a LSA that would be flooded to the restarting router, or if there is a changed LSA on the retransmission list of the restarting router when the graceful restart process is initiated.

Check the **Enable graceful-restart (Use when Spanned Cluster or Failover Configured)** check box and enter the graceful-restart interval in seconds. The range is 1-1800. The default value is 120 seconds. For a restart interval below 30 seconds, graceful restart will be terminated.

Click **OK** to save the graceful restart configuration.

Step 8 Click **Save** on the **Routing** page to save your changes.

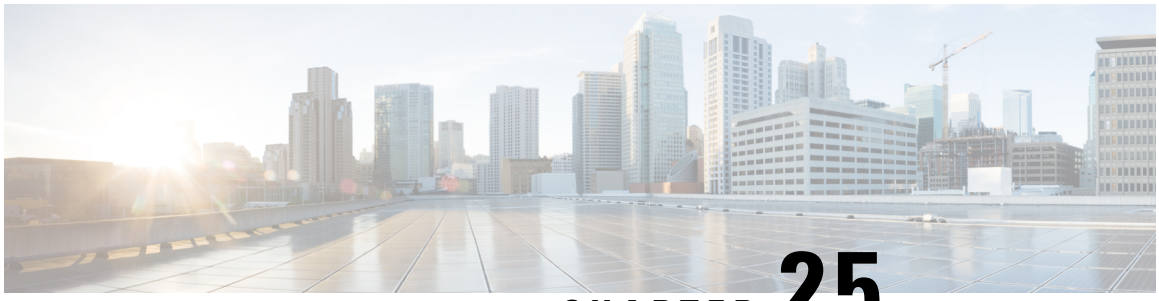
The device is configured with your OSPFv3 advanced properties. All changes are applied, enhancing routing resilience, logging, and failover handling.

History for OSPF

This reference provides a summary of the key features introduced in OSPF and the versions in which they became available, along with details about their implementation.

Table 70: Feature history for OSPF

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
BFD Support for OSPF v2 and v3	7.4	7.4	You can enable BFD on OSPFv2 and OSPFv3 interfaces. New/modified screens: • **Configuration** > **Device Setup** > **Routing** > **OSPFv2** • **Configuration** > **Device Setup** > **Routing** > **OSPFv3**



CHAPTER 25

EIGRP

EIGRP is a routing protocol that

- enables routers to efficiently exchange information,
- maintain network topology tables, and
- ensures secure data path selection and communication across networks.

EIGRP Operational Overview

This section covers the configuration of the Firewall Threat Defense to perform these routing tasks:

- Route data traffic
- Perform authentication
- Redistribute routing information

- EIGRP routing, on page 1095
- Requirements and prerequisites for EIGRP, on page 1096
- Guidelines and limitations for EIGRP routing, on page 1097
- Configure EIGRP routing on firewall devices, on page 1098
- History for EIGRP, on page 1106

EIGRP routing

An Enhanced Interior Gateway Routing Protocol (EIGRP) is a routing protocol that

- sends updates only when network topology changes, not at regular intervals,
- offers rapid convergence and supports variable-length subnet masks, and
- supports partial updates and multiple network layer protocols.

EIGRP capabilities and operations

EIGRP stores all neighbor routing tables for quick adaptation to alternate routes. If a suitable route does not exist, EIGRP queries its neighbors to discover an alternate route. It propagates these queries through the network to locate a route. EIGRP's support for variable-length subnet masks allows routes to be automatically

summarized on a network boundary. Additionally, EIGRP can be configured to summarize any bit boundary at any interface.

EIGRP sends partial updates when route metrics change, limiting propagation to necessary routers, which minimizes bandwidth use compared to protocols that send periodic full updates.

To learn about routers on attached networks, EIGRP uses neighbor discovery through multicast hello packets to announce their presence on the network. When a new neighbor is detected through hello packets, a topology table exchange occurs.

EIGRP hello packets are normally sent as multicast messages and do not require explicit replies. For manually configured static neighbors, hello packets are sent as unicast messages to the specified neighbor.

Once this neighbor relationship is established, routing updates are exchanged only on topology changes. The relationship persists through regular multicast hello packets, with devices expected to respond within advertised hold times. Hold time is the time within which threat defense can expect to receive a hello packet from that neighbor. If the device does not receive a hello packet within the advertised hold time, it considers the neighbor unavailable.

EIGRP employs mechanisms like neighbor discovery/recovery, Reliable Transport Protocol (RTP), and Diffusing Update Algorithm (DUAL) for route computations. DUAL retains all routes to a destination, selecting the least-cost route for packet forwarding while retaining others in case of network changes. If the main route fails, another route is chosen from the feasible successors. A successor is a neighboring router that is used for packet forwarding that has a least-cost path to a destination. DUAL utilizes a feasibility condition to ensure that the path is not part of a routing loop.

If a feasible successor is not found in the topology table, a route recomputation takes place. During route recomputation, DUAL queries the EIGRP neighbors for a route. The query is propagated to successive neighbors. If a feasible successor is not found, an unreachable message is returned.

During route recomputation, DUAL marks the route as active. By default, threat defense waits for three minutes to receive a response from its neighbors. If the device does not receive a response from a neighbor, the route is marked as stuck-in-active. All routes in the topology table that point to the unresponsive neighbor as a feasible successor are removed.

Requirements and prerequisites for EIGRP

This topic provides the necessary prerequisites and requirements for deploying EIGRP within a Cisco network environment.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines and limitations for EIGRP routing

Firewall mode guidelines

Use routed firewall mode only for EIGRP routing.

Device guidelines

Configure only one EIGRP process per device.

- EIGRP can be configured through management center UI on Firewall Threat Defense version 6.6 and later.

Interface guidelines

Use only routed interfaces with logical names and IP addresses for EIGRP routing processes.

- EIGRP can only incorporate interfaces from the global virtual router. EIGRP can learn, filter, and redistribute routes across routing protocols in the global virtual router.
- Supports physical, EtherChannel, redundant, and subinterfaces only. However, the members of EtherChannel interfaces are not supported.
-
- Passive interfaces cannot be configured as neighbor interfaces.

IP address and network objects support

Use only IPv4 addresses and standard access list objects for EIGRP configuration.

- Ranges, FQDNs, and wildcard masks are not supported.

Redistribution guidelines

Configure route tagging to prevent routing loops when redistributing between EIGRP and OSPF.

- BGP, OSPF, and RIP in the global virtual router can redistribute routes toward EIGRP.
- EIGRP can redistribute to BGP, OSPF, RIP, Static, and Connected in the global virtual router.
- When EIGRP is configured on a device that is a part of an OSPF network or vice versa, ensure that the OSPF router is configured to tag the route (EIGRP does not support route tag).

  When redistributing EIGRP into OSPF and OSPF into EIGRP, a routing loop can occur when there is an outage on one of the links, interfaces, or even when the route originator is down. To prevent the redistribution of routes from one domain back into the same domain, a router can tag a route that belongs to a domain while it is redistributing, and those routes can be filtered on the remote router based on the same tag. Because the routes will not be installed into the routing table, they will not be redistributed back into the same domain.

Deployment process guidelines

Disable and redeploy EIGRP when changing the AS number to prevent deployment failures.

To effectively change the AS number of an existing EIGRP setup, you should disable and redeploy EIGRP configurations to avoid repeated deployments and ensure error-free deployment processes.

Upgrade guidelines

Migrate FlexConfig EIGRP policies to UI management after upgrading to version 7.2 and later.

When you upgrade to version 7.2 and later, and if the previous version includes any FlexConfig EIGRP policies, the management center displays a warning message during deployment. It does not stop the deployment process; a warning message is displayed. After deployment, to manage the EIGRP policies from the UI (**Devices** > **Device Management**, click the **Edit** (✎) icon. Then, click **Routing>EIGRP**), you must redo the configuration in the **EIGRP** page and remove the configuration from FlexConfig. To automate policy creation in the UI, Firewall Management Center provides an option to migrate the policies from FlexConfig to the UI. For more information, refer to Migrate FlexConfig policies, on page 964.

Configure EIGRP routing on firewall devices

Enable EIGRP on a firewall device for efficient routing within an autonomous system.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click the **Routing** tab.

Step 3 Under Global, click **EIGRP**.

Step 4 Check the **Enable EIGRP** check box to enable the EIGRP routing process.

Step 5 In the **AS Number** field, enter the autonomous system (AS) number for the EIGRP process.

Valid values are from 1 to 65535. The AS number identifies the local EIGRP routing domain and must match on EIGRP neighbors.

Step 6 To configure other EIGRP properties, refer to these topics for detailed steps:

a. Configure EIGRP settings, on page 1099.

b. Configure EIGRP neighbors settings, on page 1099.

c. Configure EIGRP filter rules, on page 1100.

d. Configure EIGRP redistribution settings, on page 1101.

e. Configure EIGRP summary address settings, on page 1102.

f. Configure EIGRP interfaces settings, on page 1103.

g. Configure EIGRP advanced settings, on page 1104.

The firewall device is now configured with the base EIGRP process and the designated AS number. It can participate in EIGRP routing after the required interfaces, networks, and related settings are configured.

Configure EIGRP settings

Use this procedure when you need to set up EIGRP routing protocol parameters on your device. EIGRP configuration includes enabling automatic network summarization, selecting networks that participate in the routing process, and configuring passive interfaces that do not exchange routing updates.

Procedure

Step 1 On the **EIGRP** page, click the **Setup** tab.

Step 2 Check the **Auto Summary** check box to enable EIGRP to summarize at network boundaries.

Note Enabling Auto Summary can cause routing problems if you have noncontiguous networks.

Step 3 In the **Available Networks/Hosts** box, select the networks or hosts that should participate in the EIGRP routing process, and then click **Add**. To add a new network object, click **Add** (+). For detailed instructions on adding networks, refer to Networks, on page 2386.

Step 4 To configure passive interfaces, check the **Passive Interface** check box. In EIGRP, a passive interface does not send or receive routing updates.

a) To specify selective interfaces as passive, click the **Selected Interface** radio button. In the **Available Interfaces** box, select the interfaces, and click **Add**.

b) To specify all interfaces as passive, click the **All Interfaces** radio button.

Step 5 Click **Save**.

The EIGRP settings are configured and saved. The routing protocol will operate according to the specified configuration, including automatic summarization behavior, network participation, and passive interface settings.

Configure EIGRP neighbors settings

Define static neighbors for the EIGRP process. This results in unicast hello packets being sent to that neighbor.

Procedure

Step 1 On the **EIGRP** page, click the **Neighbors** tab.

Step 2 Click +**Add**.

Step 3 Select the interface through which the neighbor is available from the **Interface** drop-down list.

Step 4 Select the IP address of the static neighbor from the **Neighbor** drop-down list.

Step 5 To add a new network object, click +. For instructions on adding network objects, refer to Networks, on page 2386.

Step 6 Click **OK**.

Step 7 Click **Save**.

The EIGRP static neighbor is configured, and hello packets are sent as unicast to the specified neighbor through the designated interface.

Configure EIGRP filter rules

Filter rules provide granular control over EIGRP route advertisements and acceptances, allowing you to manage network traffic flow and routing table contents based on specific criteria such as interface or protocol type.

To configure EIGRP filter rules, perform these steps:

Procedure

Step 1 On the **EIGRP** page, click the **Filter Rules** tab.

Step 2 Click **Add**.

Step 3 In the **Add Filter Rules** dialog box, select the direction for the rule from the **Filter Direction** drop-down list:

- **Inbound**: The rule filters routes received in incoming EIGRP updates.
- **Outbound**: The rule filters routes advertised in outgoing EIGRP updates.

Step 4 Under **Type**, choose one of these options:

- To select the interface to which the filtering rule applies, click **Interface**, and then select the interface from the **Select Interface** drop-down list. Select the access list from the **Access List** drop-down list. The list defines the networks that are to be received and suppressed in routing updates. To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object, on page 2355. Click **OK**.

Note You cannot apply EIGRP filtering rules on VTI interfaces.

- (This option is enabled only if you choose **Outbound** filter direction.) To select the protocol to which the filtering rule applies, click **Protocol** and then select BGP, RIP, Static, Connected, or OSPF from the **Select Protocol** drop-down list. You can specify the relevant **Process ID** for BGP and OSPF protocols. Select the access list from the **Access List** drop-down list. The list defines the networks that are to be received and suppressed in routing updates. To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object, on page 2355. Click **OK**.

Step 5 Click **Save**.

The EIGRP filter rule is configured and applied to control route filtering based on the specified direction, interface, protocol, and access list criteria.

Configure EIGRP redistribution settings

Define rules to redistribute routes from other routing protocols to the EIGRP routing process to enable route sharing across different routing protocols.

To configure EIGRP redistribution settings, perform these steps:

Procedure

Step 1 On the **EIGRP** page, click the **Redistribution** tab.

Step 2 Click **Add**.

Step 3 In the **Add Redistribution** dialog box, from the **Protocol** drop-down list, select the source protocol from which the routes are being redistributed:

- **BGP**: Redistributes routes discovered by the BGP routing process to EIGRP. Specify the relevant **Process ID**.
- **RIP**: Redistributes routes discovered by the RIP routing process to EIGRP.
- **Static**: Redistributes static routes to the EIGRP routing process. Static routes within a network statement scope automatically redistribute to EIGRP, without additional rules. Specify the metric when redistributing static routes to VTI interfaces in EIGRP. You do not need to specify the metric for static routes pointing to other types of interfaces.
- **Connected**: Redistributes connected routes (routes established automatically by virtue of having IP address enabled on the interface) to the EIGRP routing process. Connected routes that fall within the scope of a network statement are automatically redistributed to EIGRP; you do not need to define a redistribution rule for them.
- **OSPF**: Redistributes routes discovered by the OSPF routing process to EIGRP. Specify the relevant **Process ID**. If you select this protocol, the Match options on this dialog box become available under **Optional OSPF Redistribution**:
  - **Internal**: Routes that are internal to a specific AS.
  - **External1**: Routes that are external to the AS and imported into OSPF as a Type 1 external route.
  - **External2**: Routes that are external to the AS and imported into the selected process as a Type 2 external route.
  - **Nsaa-External1**: Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes.
  - **Nsaa-External2**: (NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes.

Note These options are not available when redistributing static, connected, RIP, or BGP routes.

Step 4 Under **Optional Metrics**, enter the relevant values:

- **Bandwidth**: The minimum bandwidth of the route in kilobits per second. Valid values range from 1 to 4294967295.
- **Delay Time**: The routing delay in tens of microseconds. Valid values range from 0 to 4294967295.
- **Reliability**: The likelihood of successful packet transmission is expressed as a number 0 through 255. The value 255 indicates 100 percent reliability; 0 means no reliability.
- **Loading**: The effective bandwidth of the route. Valid values range from 1 to 255. 255 indicates 100 percent loading.
- **MTU**: The smallest permissible value for the maximum transmission unit of the path. Valid values range from 1 to 65535.
- **Route Map**: Select the route map object to apply to the redistribution entry from the **Route Map** drop-down list. To create a new route map object, click +. For instructions on adding a new route map, refer to Configure Route Map Entry.

Step 5 Click **OK**.

Step 6 Click **Save**.

The EIGRP redistribution settings have been configured and saved. Routes from the selected source protocol will be redistributed to EIGRP according to the specified rules and metrics.

Configure EIGRP summary address settings

You can configure summary addresses for each interface. If you want to create summary addresses that do not occur at a network boundary, you should manually define them. Alternatively, you can use summary addresses with automatic route summarization disabled. If more specific routes are available in the routing table, EIGRP advertises the summary address with a metric equal to the minimum of all specific routes.

Procedure

Step 1 On the **EIGRP** page, click the **Summary Address** tab.

Step 2 Click +**Add**.

Step 3 From the **Interface** drop-down list, select the interface from which the summary address is advertised.

Step 4 From the **Network** drop-down list, select the network object with a specific IP address and network mask to be summarized. To add a new network, click +. For detailed instructions for adding networks, refer to Networks, on page 2386.

Step 5 In the **Administrative Distance** field, enter the administrative distance of the summary route. Valid values range from 1 to 255.

Step 6 Click **OK**.

Step 7 Click **Save**.

The EIGRP summary address settings are configured and saved. EIGRP will advertise the summary address from the specified interface with the configured administrative distance.

Configure EIGRP interfaces settings

Manage interface settings to optimize routing operations.

To configure EIGRP interface settings, perform these steps:

Procedure

Step 1 On the **EIGRP** page, click the **Interfaces** tab.

Step 2 Click **Add**.

Step 3 Select the appropriate interface from the **Interface** drop-down list.

Step 4 In the **Hello Interval** field, enter the hello interval in seconds for EIGRP packets on an interface. Valid values range from 1 to 65535. The default value is 5 seconds.

Step 5 In the **Hold Time** field, enter the hold time that is advertised by the device in EIGRP hello packets. Valid values range from 1 to 65535. The default value is 15 seconds.

To enable EIGRP split-horizon on the interface, check the **Split Horizon** check box.

Step 6 In the **Delay Time** field, enter the delay time in tens of microseconds. Valid values are from 1 to 16777215.

Note This option is not supported in multi-context mode devices.

Step 7 Specify authentication properties:

- **Enable MD5 Authentication**: Check the check box to use the MD5 hash algorithm for authentication of EIGRP packets.
- **Key Type**: Select one key type from the drop-down list:
  - **None**: Indicates that no authentication is required.
  - **Unencrypted**: Indicates that the key string is a clear text password for authentication.
  - **Encrypted**: Indicates that the key string is an encrypted password for authentication.
  - **Auth Key**: Indicates that the key string is an EIGRP authentication key.
- **Key ID**: The ID of the key that is used to authenticate EIGRP updates. Enter a numerical key identifier. Valid values range from 0 to 255.

- **Key**: An alphanumeric character string up to 17 characters. For an encrypted authentication type, this field should have a minimum of 17 characters.
- **Confirm Key**: Re-enter the key.

Step 8 Click **OK**.

Step 9 Click **Save**.

The EIGRP interface settings that you configured are saved. The interface uses the specified hello interval, hold time, split-horizon setting, delay time, and authentication parameters for EIGRP routing operations.

Configure EIGRP advanced settings

Configure EIGRP advanced settings to optimize routing behavior and performance in your network.

To configure EIGRP advanced settings, perform these steps:

Procedure

Step 1 On the **EIGRP** page, click the **Advanced** tab.

Step 2 Under **Default Route Information**, specify the sending and receiving of default route information in EIGRP updates.

- (Appears for non-cluster and cluster in spanned etherchannel mode)**Router ID (IP Address)**: Enter the ID used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. Specify a global address for the router ID to prevent this issue. Each EIGRP router requires a unique value.
- (Appears only for a cluster in individual interface mode)**IPv4 Address Pool**: Select the relevant cluster pool value (IPv4 address pool object). To create the address pool, refer to Configure address pools, on page 2356.
- **Accept Default Route Info**: Check the check box to configure EIGRP to accept default route information.
  - **Access List**: From the **Access List** drop-down list, specify a standard access list that defines the networks that are allowed and the networks that are not when receiving default route information.

    To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object, on page 2355.
- **Send Default Route Info**: Check the check box to configure EIGRP to advertise exterior default routing information.
  - **Access List**: From the **Access List** drop-down list, specify a standard access list that defines the networks that are allowed and the networks that are not when sending default route information.

    To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object, on page 2355.

Step 3 Under **Administrative Distance**, specify:

- **Internal Distance**: Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values range from 1 to 255. The default value is 90.
- **External Distance**: Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values range from 1 to 255. The default value is 170.

Step 4 Under **Adjacency Changes**, specify:

- **Log Neighbor Changes**: Check the check box to enable the logging of EIGRP neighbor adjacency changes.
- **Log Neighbor Warnings**: Check the check box to enable the logging of EIGRP neighbor warning messages.
- (Optional) Enter the time interval (in seconds) between repeated neighbor warning messages. Valid values range from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Step 5 Under **Stub**, to enable the device as an EIGRP stub routing process, click one or more of the EIGRP stub routing processes check boxes:

- **Receive only**: Configures the EIGRP stub routing process to receive route information from the neighbor routers but not send route information to the neighbors. If this option is selected, you cannot select any of the other stub routing options.
- **Connected**: Advertises connected routes.
- **Redistributed**: Advertises redistributed routes.
- **Static**: Advertises static routes.
- **Summary**: Advertises summary routes.

Step 6 Under **Default Metrics**, define the default metrics for routes redistributed to the EIGRP routing process:

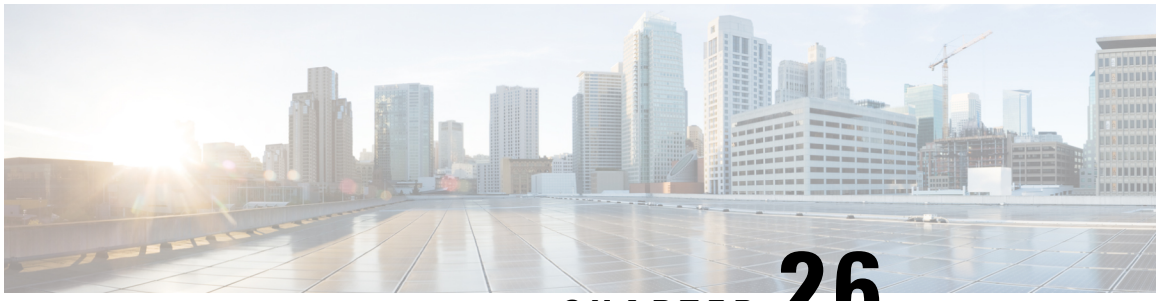
- **Bandwidth**: The minimum bandwidth of the route in kilobits per second. Valid values range from 1 to 4294967295.
- **Delay Time**: The route delay in tens of microseconds. Valid values range from 0 to 4294967295.
- **Reliability**: The likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 indicates 100 percent reliability; 0 means no reliability.
- **Loading**: The effective bandwidth of the route. Valid values range from 1 to 255; 255 indicates 100 percent loading.
- **MTU**: The smallest allowed value for the maximum transmission unit of the path. Valid values range from 1 to 65535.

EIGRP advanced settings are configured according to your specifications, optimizing routing behavior and performance.

History for EIGRP

This reference provides historical data about EIGRP version compatibility and configuration changes across various releases.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
EIGRP configuration	7.2	Any	In the previous releases, EIGRP was configured on threat defense only through FlexConfig. FlexConfig no longer supports EIGRP configuration. Configuration of EIGRP settings for threat defense is now available in the management center UI. New/modified screens: **Devices** > **Device Management** > **Routing** > **EIGRP**.



CHAPTER 26

BGP

This section describes how to configure the Firewall Threat Defense to route data, perform authentication, and redistribute routing information using the Border Gateway Protocol (BGP).

- BGP, on page 1107
- Requirements and prerequisites for BGP, on page 1111
- Guidelines for BGP, on page 1111
- Configure BGP, on page 1112
- History for BGP, on page 1127

BGP

Border Gateway Protocol (BGP) is an inter- and intra-autonomous system routing protocol that

- operates within and between autonomous systems (networks or groups of networks under common administration with common routing policies),
- exchanges routing information for the Internet, and
- serves as the protocol used between Internet service providers (ISPs).

Routing tables

A routing table is a network database that

- records paths to destination networks based on exchanged routing information
- updates dynamically as neighbors share new or modified routing routes, and
- determines the optimal path to a destination without requiring periodic updates.

BGP attributes for route selection

Routes learned via BGP have several attributes that determine the best path when multiple routes to a destination exist. The most important BGP attributes include:

- Weight: A Cisco-defined attribute that is local to a router. It is not advertised to neighboring routers. Among multiple routes to the same destination, the route with the highest weight is preferred.

- Local preference: This attribute selects an exit point from the local autonomous system (AS) and is shared throughout the local AS. If multiple exit points exist, the one with the highest local preference attribute is chosen for a specific route.
- Multi-exit discriminator: The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric. It is referred to as a suggestion because the external AS that is receiving the MEDs may also be using other BGP attributes for route selection. The route with the lower MED metric is preferred.
- Origin: The origin attribute indicates how BGP learned about a particular route. The origin attribute can have one of three possible values and is used in route selection.
  - IGP: The route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.
  - EGP: The route is learned via the Exterior Border Gateway Protocol (EBGP).
  - Incomplete: The origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP.
- AS_PATH: When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed. Only the route with the shortest AS_PATH list is installed in the IP routing table.
- Next hop: The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS. However, when the next hop is in the same subnet the peering address of the EBGP peer, the next hop is not modified. This behavior is referred to as the third-party next hop.

  Use the **next-hop-self** command when redistributing VPN-advertised routes to IBGP as peers to ensure that the routes are redistributed with the correct next hop IP.
- Community: The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. The predefined community attributes are as follows:
  - no-export: Do not advertise this route to EBGP peers.
  - no-advertise: Do not advertise this route to any peer.
  - internet: Advertise this route to the Internet community; all routers in the network belong to it.



Note As loop detection is done by scanning the full AS_PATH (as specified in the AS_PATH attribute), and checking that the AS number of the local system does not appear in the AS_PATH. By default, EBGP advertises the learned routes to the same peer to prevent additional CPU cycles on the device in performing loop checks and to avoid delays in the existing outgoing update tasks.

BGP usage scenarios

BGP usage scenarios are network configurations that

- enable ISPs to exchange customer and ISP routes between autonomous systems using External BGP (EBGP),
- allow service providers to exchange routes within an autonomous system using Interior BGP (IBGP), and
- support IPv6 prefix routing over IPv6 networks.

BGP implementation contexts

Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

BGP can also be used for carrying routing information for IPv6 prefix over IPv6 networks.

BGP path selection

BGP path selection is a routing process that selects only one path as the best path when BGP receives multiple advertisements for the same route from different sources, puts the selected path in the IP routing table, and propagates the path to its neighbors using specific criteria in order of precedence.

BGP path selection criteria

BGP uses these criteria, in the order presented, to select a path for a destination:

1. If the path specifies a next hop that is inaccessible, drop the update. Otherwise, prefer the path with the largest weight.
2. If the weights are the same, prefer the path with the largest local preference. If the local preferences are the same, prefer the path that was originated by BGP running on this router.
3. If no route was originated, prefer the route that has the shortest AS_PATH. If all paths have the same AS_PATH length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).
4. If the origin codes are the same, prefer the path with the lowest MED attribute. If the paths have the same MED, prefer the external path over the internal path.
5. If the paths are still the same, prefer the path through the closest IGP neighbor.
6. Determine if multiple paths require installation in the routing table for BGP multipath, on page 1109.
7. If both paths are external, prefer the path that was received first (the oldest one).
8. Prefer the path with the lowest IP address, as specified by the BGP router ID. If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.
9. Prefer the path that comes from the lowest neighbor address.

BGP multipath

BGP multipath is a BGP feature that

- allows installation into the IP routing table of multiple equal-cost BGP paths to the same destination prefix,
- enables traffic to the destination prefix to be shared across all installed paths, and
- does not affect best path selection algorithm.

BGP multipath requirements

These paths are installed in the table together with the best path for load-sharing. BGP multipath does not affect best path selection. For example, a router still designates one of the paths as the best path, according to the algorithm, and advertises this best path to its BGP peers.

In order to be candidates for multipath, paths to the same destination need to have these characteristics equal to the best-path characteristics:

- Weight
- Local preference
- AS-PATH length
- Origin code
- Multi Exit Discriminator (MED)
- One of these:
  - Neighboring AS or sub-AS (before the addition of the BGP Multipaths)
  - AS-PATH (after the addition of the BGP multipaths)

Some BGP multipath features put additional requirements on multipath candidates:

- The path should be learned from an external or confederation-external neighbor (eBGP).
- The IGP metric to the BGP next hop should be equal to the best-path IGP metric.

These are the additional requirements for internal BGP (iBGP) multipath candidates:

- The path should be learned from an internal neighbor (iBGP).
- The IGP metric to the BGP next hop should be equal to the best-path IGP metric, unless the router is configured for unequal-cost iBGP multipath.

BGP inserts up to *n* most recently received paths from multipath candidates into the IP routing table, where *n* is the number of routes to install in the routing table, as specified when you configure BGP multipath. The default value, when multipath is disabled, is 1.

For unequal-cost load balancing, you can also use BGP Link Bandwidth.



Note The equivalent next-hop-self is performed on the best path that is selected among eBGP multipaths before it is forwarded to internal peers.

Requirements and prerequisites for BGP

This reference provides the requirements and prerequisites necessary for configuring BGP on supported devices.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for BGP

Context mode guidelines

Consider these context mode requirements when implementing BGP.

- Supported in single and multiple context modes.
- Only one Autonomous System (AS) number is supported for all contexts.

Firewall mode guidelines

Does not support transparent firewall mode. BGP is supported only in routed mode.

IPv6 guidelines

Supports IPv6.

Additional guidelines

Consider these additional operational requirements and limitations.

- For BGP, the next hop IP address for the routes is the network IP address and not 0.0.0.0.
- The system does not add a route entry for the IP address received over PPPoE in the CP route table. BGP always looks into the CP route table for initiating the TCP session, hence BGP does not form TCP session.

  Thus, BGP over PPPoE is not supported.
- BGP is not supported on management-only or BVI interfaces.
- To avoid adjacency flaps due to route updates being dropped if the route update is larger than the minimum MTU on the link, ensure that you configure the same MTU on the interfaces on both sides of the link.

- BGP with PATH MTU (PMTU) can cause adjacency flaps if MTU discovery fails, especially with ECMP routing. Hence, be cautious while using BGP, PMTU, and ECMP as packet drops can occur if MTU discovery fails due to any reason.
- The BGP table of the member unit is not synchronized with the control unit table. Only its routing table is synchronized with the control unit routing table.
- Enable the graceful timeout feature when you use BGP on Firewall Threat Defense devices that are configured in high availability mode. Enabling this feature reduces packet drops that occur due to issues related to BGP convergence.
- When you configure a route-based site-to-site VPN using static or dynamic VTI interfaces, ensure that the TTL hop count is greater than one if you use BGP as the routing protocol.
- On Firewall Threat Defense devices, changing a large number of BGP neighbors from iBGP to eBGP in a single deployment can fail. During deployment, Firewall Management Center can remove and re-create the same peer in immediate succession, and the deployment can fail if the previous peer deletion is still in progress. To avoid this issue, split the changes across multiple deployments. Remove or modify a subset of neighbors, deploy the configuration, and then apply additional neighbor changes in subsequent deployments.

Configure BGP

Configure BGP routing protocol to establish peering relationships and control route advertisement between autonomous systems.

BGP configuration involves multiple components including basic settings, neighbor relationships, route filtering, and redistribution policies.

Procedure

Step 1 Configure basic BGP settings, on page 1113

Step 2 Configure BGP general settings, on page 1115

Step 3 Configure BGP Neighbor Settings, on page 1117

Step 4 Configure BGP aggregate address settings, on page 1121

Step 5 Configure BGPv4 filtering settings, on page 1122

Note The Filtering section is applicable only to IPv4 settings

Step 6 Configure BGP network settings, on page 1123

Step 7 Configure BGP redistribution settings, on page 1123

Step 8 Configure BGP route injection settings, on page 1124

Step 9 Configure BGP route import and export, on page 1125

BGP is configured with all necessary settings, enabling dynamic routing and proper route exchange between autonomous systems.

Configure basic BGP settings

Enable and customize BGP settings to control routing behavior and improve network operations.

You can set many basic settings for BGP.

For a device using virtual routing, the basic settings described in this section must be configured in the **BGP** page under **General Settings**. For more information, refer to Modifications to the Firewall Management Center web interface routing page.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **Routing** and do the following:

a) (For a virtual-router-aware device) Under **General Settings**, click **BGP**.

b) Check the **Enable BGP** check box to enable the BGP routing process.

c) In the **AS Number** field, enter the autonomous system (AS) number for the local BGP process. The AS number internally includes multiple autonomous numbers. Valid values are from 1 to 4294967295 or from 1.0 to 65535.65535 when a dot notation is used. The AS number is a uniquely assigned value that identifies each network on the Internet.

d) In the **Router Id** drop-down list, choose **Automatic** or **Manual** (appears for non-cluster and a cluster in spanned etherchannel mode) or **Cluster Pool** (appears for a cluster in individual interface mode). If you choose **Automatic**, the highest-level IP address on the Firewall Threat Defense device is used as the router ID. If you choose **Manual**, enter the IP address in the **IP Address** field. If you choose **Cluster Pool**, enter the cluster pool value in the **Cluster Pool** field. For more information on creating the cluster pool address, refer to Configure address pools, on page 2356..

e) To use a fixed router ID, choose **Manual** and enter an IPv4 address in the **IP Address** field. The default value is **Automatic**. For a virtual router-aware device, you can override the router ID settings in the **Virtual Routers** > **BGP** page.

Step 3 (Optional) Edit the various BGP settings, starting with **General**. The defaults for these settings are appropriate in most cases, but you can adjust them to fit the needs of your network. Click **Edit** ( ) to edit the settings in the group:

a) Enter a **Scanning Interval** for BGP routers for next-hop validation. Valid values are from 5 to 60 seconds. The default value is 60.

b) In the **Number of AS numbers in AS_PATH attribute of received routes** field, enter the maximum number of AS numbers allowed in the AS_PATH attribute of received routes. An AS_PATH attribute is a sequence of intermediate AS numbers between source and destination routers that form a directed route for packets to travel. Valid values are between 1 and 254. The default value is **None**.

c) Check the **Log Neighbor Changes** check box to enable logging of BGP neighbor changes (up or down) and resets. This helps in troubleshooting network connectivity problems and measuring network stability. This is enabled by default.

d) Check the **Use TCP path MTU discovery** check box to use the Path MTU determining technique to determine the maximum transmission unit (MTU) size on the network path between two IP hosts. This avoids IP fragmentation. This is enabled by default.

e) Check the **Reset session upon failover** check box to reset the external BGP session immediately upon link failure. This is enabled by default.

f) Check the **Enforce the first AS is peer's AS for EBGP routes** check box to discard incoming updates received from external BGP peers that do not list their AS number as the first segment in the AS_PATH attribute. This prevents a misconfigured or unauthorized peer from misdirecting traffic by advertising a route as if it was sourced from another autonomous system. This is enabled by default.

g) Check the **Use dot notation for AS number** check box to split the full binary 4-byte AS number into two words of 16 bits each, separated by a dot. AS numbers from 1 to 65535 are represented as decimal numbers, and AS numbers greater than 65535 are represented using dot notation. This is disabled by default.

Enter a value for the aggregate timer (in seconds) in the **Aggregate Timer** field. Valid values are 0 or any value between 6 and 60. The default value is 30.

h) Check the **BGP community new format (AA:NN)** check box to configure BGP to display community values in the AA:NN format, where AA represents the autonomous system number, and NN represents the community number, each being 2 bytes long. This format conforms to RFC-1997. By default, BGP communities are displayed as a single 32-bit decimal number.

i) Click **OK**.

Step 4 (Optional) Edit the **Best Path Selection** section:

a) Enter a value for **Default local preference** between 0 and 4294967295. The default value is 100. Higher values indicate higher preference. This preference is sent to all routers and access servers in the local autonomous system.

b) Check the **Allow comparing MED from different neighbors** check box to allow the comparison of Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. This is disabled by default.

c) Check the **Compare Router ID for identical EBGP paths** check box to compare similar paths received from external BGP peers during the best path selection process and switch the best path to the route with the lowest router ID. This is disabled by default.

d) Check the **Pick the best-MED path among paths advertised by neighbor AS** check box to enable MED comparison among paths learned from confederation peers. The comparison between MEDs is made only if no external autonomous systems are there in the path. This is disabled by default.

e) Check the **Treat missing MED as the least preferred path** check box to consider the missing MED attribute as having a value of infinity, making the path the least desirable; therefore, a path with a missing MED is least preferred. This is disabled by default.

f) Click **OK**.

Step 5 (Optional) Edit the **Neighbor Timers** section:

a) Enter the time interval for which the BGP neighbor remains active after not sending a keepalive message in the **Keepalive interval** field. At the end of this keepalive interval, the BGP peer is declared dead, if no messages are sent. The default value is 60 seconds.

b) Enter the time interval for which the BGP neighbor remains active while a BGP connection is being initiated and configured in the **Hold time** field. The default value is 180 seconds. Specify a value from 0 to 65535.

c) (Optional) Enter the minimum time interval for which the BGP neighbor remains active while a BGP connection is being initiated and configured in the **Min Hold time** field. Specify a value from 3 to 65535.

Note A hold time of less than 20 seconds increases the possibility of peer flapping.

d) Click **OK**.

Step 6 In the **Next Hop** section, optionally check the **Address tracking** check box to enable BGP next hop address tracking and enter the **Delay Interval** between checks on updated next-hop routes installed in the routing table. Click **OK**.

Note The **Next Hop** section is applicable only to IPv4 settings.

Step 7 (Optional) Edit the **Graceful Restart** section:

Note This section is available only when the Firewall Threat Defense device is in failover or spanned cluster mode. This is done so that there is no drop in packets in the traffic flow, when one of the devices in the failover setup fails.

a) Check the **Enable Graceful Restart** check box to enable Firewall Threat Defense peers to avoid a routing flap following a switchover.
b) Specify the time duration that Firewall Threat Defense peers will wait to delete stale routes before a BGP open message is received in the **Restart Time** field. The default value is 120 seconds. Valid values are between 1 and 3600 seconds.
c) Enter the time duration that the Firewall Threat Defense will wait before deleting stale routes after an end of record (EOR) message is received from the restarting Firewall Threat Defense in the **Stalepath Time** field. The default value is 360 seconds. Valid values are between 1 and 3600 seconds.
d) Click **OK** and then click **Save**.

Step 8 To view the BGP basic settings, from the virtual routers drop-down, select the desired router, and then click **BGP**.

This page displays the basic settings that are configured in the **Settings** page. You can edit the router ID settings on this page.

Step 9 To edit the router ID settings, modify the IP address in the **IP Address** fields. The modified value overrides the router ID settings that were configured on the **BGP** page under **General Settings**.

The device is configured with basic BGP settings, enabling BGP routing, specifying the AS number, router ID, and any custom parameters you set.

Configure BGP general settings

Configure route maps, administrative route distances, synchronization, next-hop, and packet forwarding for BGP to optimize routing performance in your network.

The defaults for these settings are appropriate in most cases, but you can adjust them to fit the needs of your network.

Procedure

Step 1 On the **Device Management** page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, select the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 In the **General** tab, update the following sections:

a) In the **Setting** section, enter or select a **RouteMap** object and click **OK**.

Note The **RouteMap** field is applicable only to IPv4 settings.

b) In the **Administrative Route Distances** section, update the following as required, and click **OK**:

- **External**: Enter the administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255. The default value is 20.
- **Internal**: Enter administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255. The default value is 200.
- **Local**: Enter administrative distance for local BGP routes. Local routes are routes originated by the local BGP process, such as networks specified with the network router configuration command or routes redistributed into BGP from another routing process. The range of values for this argument is from 1 to 255. The default value is 200.

c) In the **Routes and Synchronization** section, update the following as required, and click **OK**:

- (Optional) **Generate default routes**: Check the check box of this option to configure default-information originate.
- (Optional) **Summarize subnet routes into network level routes**: Check the check box of this to configure automatic summarization of subnet routes into network-level routes. This check box is applicable only to IPv4 settings.
- (Optional) **Advertise inactive routes**: Check the check box of this to advertise routes that are not installed in the routing information base (RIB).
- (Optional) **Synchronize between BGP and IGP systems**: Check the check box of this to enable synchronization between BGP and your Interior Gateway Protocol (IGP) system. Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.
- (Optional) **Redistribute IBGP into IGP**: Check the check box of this to configure IBGP redistribution into an interior gateway protocol (IGP), such as OSPF.

d) In the **Forward Packets Over Multiple Paths** section, update the following as required and click **OK**:

- (Optional) **Number of Paths**: Enter the maximum number of Border Gateway Protocol routes that can be installed in a routing table. The range of values are from 1 to 8. The default value is 1.
- (Optional) **IBGP Number of Paths**: Enter the maximum number of parallel internal Border Gateway Protocol (IBGP) routes that can be installed in a routing table. The range of values are from 1 to 8. The default value is 1.

Step 5 Click **Save**.

BGP general settings are configured with your specified route maps, administrative distances, synchronization options, and multi-path forwarding parameters.

Configure BGP Neighbor Settings

Define and customize BGP neighbor connections on your device for efficient routing and advanced peer management.

A BGP router must connect with each of its peers before exchanging updates. These peers are called BGP neighbors. Perform this procedure to define BGP IPv4 or IPv6 neighbors and neighbor settings.

Procedure

Step 1 On the **Device Management** page, click **Routing**.

(For a virtual router-aware device) From the virtual routers drop-down list, choose the virtual router for which you are configuring BGP.

Step 2 Choose **BGP** > **IPv4** or **IPv6**. Click **Neighbor**.

Step 3 Click **Add** to define BGP neighbors and neighbor settings.

a) Enter the BGP neighbor **IP address**. This IP address is added to the BGP neighbor table. When you are configuring BGP IPv6 on static VTI, enter the virtual tunnel IP address of the neighbor. Choose the BGP neighbor **Interface**.



Note The **Interface** field is only applicable to IPv6 settings.

b) Enter the autonomous system to which the BGP neighbor belongs, in the **Remote AS** field. Check the **Enabled address** check box to enable communication with this BGP neighbor. Further neighbor settings will be configured only if the **Enabled address** check box is selected.

c) (Optional) Check the **Shutdown administratively** check box to disable a neighbor or peer group.

d) (Optional) Check the **Configure graceful restart (failover / spanned mode)** check box to enable configuration of the BGP graceful restart capability for this neighbor. After selecting this option, you must check the **Enable graceful restart** check box to specify whether graceful restart should be enabled or disabled for this neighbor.

Note

- The graceful restart is enabled only when the device is in HA mode or when L2 cluster (all nodes from the same network) is configured.
- The graceful restart option for BGPv6 is enabled only on Firewall Threat Defense Version 7.3+.
- If you configure graceful restart only at General Settings and not at BGP IPv6, the global General Settings configuration persists.
- If you configure graceful restart at General Settings and also at BGP IPv6, the global General Settings configuration is overridden by the BGP IPv6 configuration settings.

e) (Optional) To enable configuration of the BFD support for BGP, from the **BFD Fallover** drop-down list, choose the BFD type—single-hop, multi-hop, or auto-detect-hop. This selection registers the BGP neighbor to receive forwarding path detection failure messages from BFD. Choose None if you do not want to have BFD support.

f) (Optional) Enter a **Description** for the BGP neighbor.

g) (Optional) From the **Update Source** drop-down list, choose an interface to source the BGP packets.

You can choose a loopback address as this interface to overcome path failures. You can also choose any physical, port-channel, or a sub-interface.

Step 4 (Optional) In **Filtering Routes**, use access lists, route maps, prefix lists and AS path filters as required, to distribute BGP Neighbor information. Update the following sections:

a) Choose or select the appropriate incoming or outgoing **Access List** to distribute BGP neighbor information.

Note Access lists are only applicable to IPv4 settings.

b) Choose or select the appropriate incoming or outgoing **Route Maps** to apply a route map to incoming or outgoing routes.

c) Choose or select the appropriate incoming or outgoing **Prefix List** to distribute BGP neighbor information.

d) Choose or select the appropriate incoming or outgoing **AS path filter** to distribute BGP neighbor information.

e) Check the check box of **Limit the number of prefixes allowed from the neighbor** to control the number of prefixes that can be received from a neighbor.

- Enter the maximum number of prefixes allowed from a specific neighbor in the **Maximum Prefixes** field.
- Enter the percentage (of maximum) at which the router starts to generate a warning message in the **Threshold Level** field. Valid values are integers between 1 and 100. The default value is 75.

f) Check the **Control prefixes received from the peer** check box to specify additional controls for the prefixes received from a peer. Do one of the following:

- Check the **Terminate peering when prefix limit is exceeded** check box to stop the BGP neighbor when the prefix limit is reached. Specify the interval after which the BGP neighbor will restart in the **Restart interval** field.

- Check the **Give only warning message when prefix limit is exceeded** check box to generate a log message when the maximum prefix limit is exceeded. Here, the BGP neighbor will not be terminated.

g) Click **OK**.

Step 5 (Optional) In **Routes**, specify miscellaneous Neighbor route parameter. Proceed to update the following:

a) Enter the minimum interval (in seconds) between the sending of BGP routing updates in the **Advertisement Interval** field. Valid values are between 1 and 600.

b) Check the **Remove private AS numbers from outbound routing updates** check box to exclude the private AS numbers from being advertised on outbound routes.

c) Check the **Generate default routes** check box to allow the local router to send the default route 0.0.0.0 to a neighbor to use as a default route. Enter or Select the route map that allows the route 0.0.0.0 to be injected conditionally in the **Route map** field.

d) To add conditionally advertised routes, click Add Row +. In the Add Advertised Route dialog box, do the following:

1. Add or choose a route map in the **Advertise Map** field, that will be advertised if the conditions of the exist map or the non-exist map are met.
2. Click **Exist Map** and choose a route map from the Route Map Object Selector. This route map is compared with the routes in the BGP table, to determine whether the advertise map route is advertised.
3. Click **Non-Exist Map** and choose a route map from the Route Map Object Selector. This route map is compared with the routes in the BGP table, to determine whether the advertise map route is advertised.
4. Click **OK**.

Step 6 In **Timers**, check the **Set timers for the BGP peer** check box to set the keepalive frequency, hold time, and minimum hold time.

- **Keepalive interval**: Enter the frequency (in seconds) with which Firewall Threat Defense sends keepalive messages to the neighbor. Valid values are between 0 and 65535. The default value is 60 seconds.
- **Hold time**: Enter the interval (in seconds) after not receiving a keepalive message that Firewall Threat Defense declares a peer dead. Valid values are between 0 and 65535. The default value is 180 seconds.
- **Min hold time**: (Optional) Enter the minimum interval (in seconds) after not receiving a keepalive message that Firewall Threat Defense declares a peer dead. Valid values are between 3 and 65535. The default value is 3 seconds.



Note A hold time of less than 20 seconds increases the possibility of peer flapping.

Step 7 In **Advanced**, update the following:

a) (Optional) Check the **Enable Authentication** check box to enable MD5 authentication on a TCP connection between two BGP peers.

1. Choose an encryption type from the **Enable Encryption** drop-down list.
2. Enter a password in the **Password** field. Reenter the password in the **Confirm Password** field. The password is case-sensitive and can be up to 25 characters long when the service password-encryption

command is enabled and up to 81 characters long when the service password-encryption command is not enabled. The string can contain any alphanumeric characters, including spaces.

Note You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.

b) (Optional) Select the **Send Community attribute to this neighbor** check box to specify that community attributes should be sent to the BGP neighbor
c) (Optional) Select the **Use FTD as next hop for this neighbor** check box to configure the router as the next-hop for a BGP speaking neighbor or peer group.
d) Select the **Disable Connection Verification** check box to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address. When deselected (default), a BGP routing process will verify the connection of single-hop eBGP peering session (TTL=254) to determine if the eBGP peer is directly connected to the same network segment by default. If the peer is not directly connected to same network segment, connection verification will prevent the peering session from being established.
e) Select **Allow connections with neighbor that is not directly connected** to accept and attempt BGP connections to external peers residing on networks that are not directly connected. (Optional) Enter the time-to-live in the **TTL hops** field. Valid values are between 1 and 255. However, for eBGP multi-hop neighborship configuration, you must enter the **TTL hops** value. Alternatively, select **Limited number of TTL hops to neighbor**, to secure a BGP peering session. Enter the maximum number of hops that separate eBGP peers in the **TTL hops** field. Valid values are between 1 and 254.
f) (Optional) Select the **Use TCP MTU path discovery** check box to enable a TCP transport session for a BGP session.
g) Choose the TCP connection mode from the **TCP Transport Mode** drop-down list. Options are Default, Active, or Passive.
h) (Optional) Enter a **Weight** for the BGP neighbor connection.
i) Select the **BGP Version** that Firewall Threat Defense will accept from the drop-down list. The version can be set to 4-Only to force the software to use only Version 4 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Step 8 Update **Migration**, only if AS migration is considered.

Note The AS migration customization should be removed after transition has been completed.

a) (Optional) Check the **Customize the AS number for routes received from the neighbor** check box to customize the AS_PATH attribute for routes received from an eBGP neighbor.
b) Enter the local autonomous system number in the **Local AS number** field. Valid values are any valid autonomous system number from 1 to 4294967295 or 1.0 to 65535.65535.
c) (Optional) Check the **Do not prepend local AS number to routes received from neighbor** check box to prevent the local AS number from being prepended to any routes received from eBGP peer.
d) (Optional) Check the **Replace real AS number with local AS number in routes received from neighbor** check box to replace the real autonomous system number with the local autonomous system number in the eBGP updates. The autonomous system number from the local BGP routing process is not prepended.

e) (Optional) Check the **Accept either real AS number or local AS number in routes received from neighbor** check box to configure the eBGP neighbor to establish a peering session using the real autonomous system number (from the local BGP routing process) or by using the local autonomous system number.

Step 9 Click **OK**, and then click **Save**.

The BGP neighbor and its associated advanced settings are configured. The device can now establish and manage BGP sessions as specified, ensuring effective routing and network reachability.

Configure BGP aggregate address settings

Route aggregation combines the attributes of several different routes so that only a single route is advertised, reducing the number of routes that need to be advertised.

BGP neighbors store and exchange routing information and the amount of routing information increases as more BGP speakers are configured. Route aggregation is the process of combining the attributes of several different routes so that only a single route is advertised. Aggregate prefixes use the classless interdomain routing (CIDR) principle to combine contiguous networks into one classless SET of IP addresses that can be summarized in routing tables. As a result fewer routes need to be advertised. Use the Add/Edit Aggregate Address dialog box to define the aggregation of specific routes into one route.

Procedure

Step 1 When editing the Firewall Threat Defense device, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 Click **Add Aggregate Address**.

Step 5 Enter a value for the aggregate timer (in seconds) in the **Aggregate Timer** field. Valid values are 0 or any value between 6 and 60. The default value is 30.

Step 6 Click ( )**Add** and update the **Add Aggregate Address** dialog box:

a) **Network**: Enter an IPv4 address or select the desired network/hosts objects.
b) **Attribute Map**: (Optional) Enter or select the route map used to SET the attribute of the aggregate route.
c) **Advertise Map**: (Optional) Enter or select the route map used to select the routes to create AS_SET origin communities.
d) **Suppress Map**: (Optional) Enter or select the route map used to select the routes to be suppressed.
e) **Generate AS SET path Information**: (Optional) Check the check box to enable generation of autonomous system SET path information.
f) **Filter all routes from updates**: (Optional) Check the check box to filter all more-specific routes from updates.
g) Click **OK**.

The BGP aggregate address settings are configured and fewer routes need to be advertised due to route aggregation.

What to do next

- For BGPv4 settings, proceed to Configure BGPv4 filtering settings, on page 1122.
- For BGPv6 settings, proceed to Configure BGP network settings, on page 1123.

Configure BGPv4 filtering settings

Configure filtering settings to filter routes or networks received in incoming BGP updates and restrict routing information that the router learns or advertises.

Filtering settings are used to filter routes or networks received in incoming BGP updates. Filtering is used to restrict routing information that the router learns or advertises.

Before you begin

Filtering is only applicable for a BGP IPv4 routing policy.

Follow these steps to configure BGPv4 filtering settings:

Procedure

Step 1 On the Device Management page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4**.

Step 4 Click **Filtering**.

Note The **Filtering** field is applicable only to IPv4 settings.

Step 5 Click (+)**Add** and update the **Add Filter** dialog box:

a) **Access List**: Choose an access control list that defines which networks are to be received and which are to be suppressed in routing updates.

b) **Direction**: (Optional) Choose a direction that specifies if the filter should be applied to inbound updates or outbound updates.

c) **Protocol**: (Optional) Choose the routing process for which you want to filter: None, BGP, Connected, OSPF, RIP, or Static.

d) **Process ID**: (Optional) Enter the process ID for the OSPF routing protocol.

e) Click **OK**.

Step 6 Click **Save**.

BGPv4 filtering settings are configured to filter routes or networks based on the specified access control list and filtering criteria.

Configure BGP network settings

Configure BGP network settings to control which networks are advertised by the BGP routing process and to apply route map filters for network advertisement.

Network settings are used to add networks that will be advertised by the BGP routing process and route maps that will be examined to filter the networks to be advertised.

Procedure

Step 1 On the **Device Management** page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 Click **Networks**.

Step 5 Click **Add** and update the **Add Networks** dialog box:

a) **Network**: Choose the network to be advertised by the BGP routing processes.



Note For a network prefix to be advertised, a route to the device must exist on the routing table.

To add a new network object, refer to Create a network object, on page 2388.

b) (Optional) **Route Map**: Enter or choose a route map that should be examined to filter the networks to be advertised. If not specified, all networks are redistributed. To add a new route map object, refer to Configure a route map, on page 2415.

c) Click **OK**.

Step 6 Click **Save**.

The BGP network settings are configured with the specified networks and route maps for advertisement filtering.

Configure BGP redistribution settings

Configure redistribution settings to define the conditions for redistributing routes from another routing domain into BGP.

Redistribution settings allow you to define the conditions for redistributing routes from another routing domain into BGP.

Procedure

Step 1 On the **Device Management** page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 Click **Redistribution**.

Step 5 Click **Add** and update the **Add Redistribution** dialog:

a) **Source Protocol**: Select the protocol from which you want to redistribute routes into the BGP domain from the Source Protocol drop-down list.

Note User-defined virtual routers do not support redistributing routes from RIP.

b) **Process ID**: Enter the identifier for the selected source protocol. Applies to the OSPF protocol. For devices using virtual routing, this drop-down lists the process ID assigned for the virtual router for which you are configuring the BGP settings.

c) **Metric**: (Optional) Enter a metric for the redistributed route.

d) **Route Map**: Enter or select a route map that should be examined to filter the networks to be redistributed.

If not specified, all networks are redistributed. To create a new route map object, click **Add** (+). For the procedure to add a new route map, see Configure Route Map Entry.

e) **Match**: The conditions used for redistributing routes from one routing protocol to another. The routes must match the selected condition to be redistributed. You can choose one or more conditions. These options are enabled only when OSPF is chosen as the Source Protocol.

- Internal
- External 1
- External 2
- NSSA External 1
- NSSA External 2

f) Click **OK**.

The BGP redistribution settings are configured and routes from the specified source protocol are redistributed into the BGP domain according to the defined conditions.

Configure BGP route injection settings

Configure BGP route injection settings to control which routes are conditionally injected into the BGP routing table based on defined criteria.

Route injection settings allow you to define the routes to be conditionally injected into the BGP routing table.

Procedure

Step 1 On the **Device Management** page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 Click **Route Injection**.

Step 5 Click **Add** and update the **Add Route Injection** dialog box:

a) **Inject Map**: Enter or select the route map that specifies the prefixes to inject into the local BGP routing table. To create a new route map object, click **Add** (+). For the procedure to add a new route map, see Configure Route Map Entry.

b) **Exist Map**: Enter or select the route map containing the prefixes that the BGP speaker will track.

c) **Injected routes will inherit the attributes of the aggregate route**: Check this box to configure the injected route to inherit attributes of the aggregate route.

d) Click **OK**.

Step 6 Click **Save**.

The BGP route injection settings are configured and the specified routes will be conditionally injected into the BGP routing table according to the defined route maps.

Configure BGP route import and export

This task enables you to implement inter-virtual-router route leaking in BGP by importing or exporting routes using route target extended communities, allowing controlled sharing of routes between virtual routers.

In BGP, you can implement an inter-virtual-router route leak by importing or exporting routes using the route target extended community of the destination and source virtual routers respectively. You can use a route map to filter the desired route targets instead of leaking the entire routing table. You can also leak the routes of global virtual router to user-defined virtual routers and vice versa.

- You can configure BGP to leak routes between two user-defined virtual routers using the route target extended communities:
  - Tag the routes with the route targets from the source virtual router using route target export.
  - Import the routes that are matching the route targets into the destination virtual router using route target import.
  - Optionally, you can filter routes from source virtual router or to destination virtual router using export or import route maps respectively. You can configure route map with match extended community list for filtering the routes. Similarly, you can configure route map with set extended community route targets to tag the routes with the route target extended community.
- To import routes from the global virtual router to a user-defined virtual router, specify the IPv4/IPv6 route map in Global Virtual Router Import Route Map to import to the user-defined virtual router.
- To export routes from a user-defined virtual router to the global virtual router, in addition to exporting the route targets, you can also specify the Global Virtual Router Export Route Map to export from the user-defined virtual router.

The BGP inter-virtual-router route leaking supports both IPv4 and IPv6 prefixes.

Before you begin

- Create virtual routers.
- Enable BGP on the virtual router.
- Configure BGP, on page 1112.

Follow these steps to configure BGP route import/export settings:

Procedure

Step 1 On the Device Management page, click **Routing**.

Step 2 (For a virtual-router-aware device) From the virtual routers drop-down, choose the virtual router for which you are configuring BGP.

Step 3 Choose **BGP** > **IPv4** or **IPv6**.

Step 4 (Supported for virtual routers only) Click **Route Import/Export**.

Step 5 In the **Route Targets Import** field, enter the route target extended community that you want to match for the routes to be imported. On deployment, the routes of the destination virtual router that match this value are imported to the source virtual router's BGP table.

Note
- The route target must be in **ASN:nn** format.
- You can enter multiple route targets as comma-separated values.
- This value can range from 0:1 to 65534:65535.

Step 6 In the **Route Targets Export** field, enter the route target extended community to tag the source virtual router's routes with the route target value. On deployment, the routes of the source virtual router are tagged with this value.

Note
- The route target must be in **ASN:nn** format.
- You can enter multiple route targets as comma separated values.
- This value can range from 0:1 to 65534:65535.

Step 7 Route maps help you to narrow down the routes to be shared instead of leaking the entire routing table. Route map filtering is applied on the list of routes that are obtained with the specified route target values:

a) (Optional) Under **User Virtual Router**, choose the route map from the **Import Route Map** drop-down list to filter the routes at the destination virtual router.

Note The user virtual router import route map is effective only when the route targets import is configured.

b) (Optional) Under **User Virtual Router**, choose the route map from the **Export Route Map** drop-down list to filter the routes at the source virtual router before the routes are exported to other virtual routers.

Note You can use the match and set clauses in the route map with the route target extended community lists for filtering based on other criteria or tagging the routes with the route target community values. For more information, refer to Configure a route map, on page 2415.

Step 8 To share the routes between a user-defined virtual router and global virtual router, specify the route map under the **Global Virtual Router**:

a) To leak the global virtual router routes to the user-defined virtual router, select the route map from the **Import Route Map** drop-down list. The IPv4 or IPv6 route map is imported to the user-defined virtual router.

b) To leak the user-defined virtual router routes to the global virtual router, select the route map from the **Export Route Map** drop-down list. The IPv4 or IPv6 route map is exported to the global virtual router.

Note You must specify the route targets for export apart from specifying the route map.

Note You can use the match clause of the route map object to filter the routes for leaking. For more information, refer to Configure a route map, on page 2415.

Step 9 Follow the procedure (Step 3 to Step 8) to configure relevant BGP route import and export settings for other virtual routers as well. Click **Save**, then **Deploy** to apply your import/export settings.

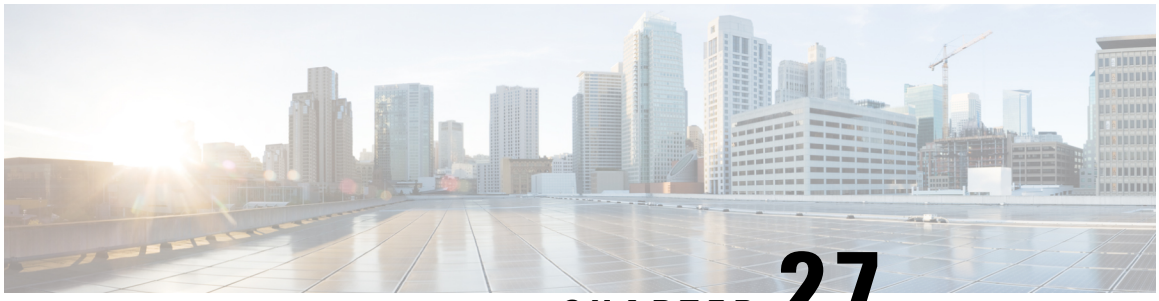
When the packets flow into the ingress virtual router, BGP imports the routes from the destination virtual routers that have the matching route target value and if a route map is also configured, the routes are further filtered and used to identify the best path routes for routing the packets.

History for BGP

This reference provides the history and version information for BGP features and enhancements, including minimum required versions and implementation details.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Graceful restart support on BGPv6	7.4	Any	You can configure graceful restart on BGPv6 for Secure Firewall Threat Defense version 7.3 and later. New/modified screens: **Routing** > **BGP** > **IPv6** > **Add/Edit Neighbor**.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Loopback interface support for BGP	7.4	Any	You can use a loopback interface for BGP. New/modified screens: **Routing** > **BGP** > **IPv4 or IPv6** > **Add/Edit Neighbor**.
BGP configuration to interconnect virtual routers	7.1	Any	You can configure BGP settings to dynamically leak routes among user-defined virtual routers, and between global virtual router and user-defined virtual routers. The import and export routes feature was introduced to exchange routes among the virtual routers by tagging them with route targets and optionally, filtering the matched routes with route maps. This BGP feature is accessible only when you select a user-defined virtual router. New/modified screens: For a selected user-defined virtual router, **Devices** > **Device Management** > **Routing** > **BGPv4/v6** > **Route Import/Export** tab.
BGPv6 support for user-defined virtual routers	7.1	Any	Secure Firewall Threat Defense now supports configuring BGPv6 on user-defined virtual routers. New/modified screens: For a selected user-defined virtual router, **Devices** > **Device Management** > **Routing** > **BGPv6** page.



CHAPTER 27

RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol that

- enables devices to exchange routing information,
- supports authentication mechanisms, and
- facilitates redistribution of routing information.

RIP Configuration Constraints

There are constraints when deploying RIP on the Firewall Threat Defense:

- RIP configuration is restricted to the global virtual router and is not supported for user-defined virtual routers.

- RIP, on page 1129
- Requirements and prerequisites for RIP, on page 1132
- Guidelines for RIP, on page 1132
- Configure RIP, on page 1133

RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol that

- uses hop count as the metric for path selection,
- exchanges RIP broadcasts with neighboring devices to dynamically learn and advertise routes, and
- includes four basic components: routing update process, RIP routing metrics, routing stability, and routing timers.

RIP characteristics and versions

RIP is a widely used routing protocol. It sends routing updates at regular intervals and when the network topology changes. These updates provide information about network reachability and the number of hops to each destination..

You can configure RIP with less effort than OSPF, but it generates more network traffic. RIP supports both Version 1 and Version 2.

Secure Firewall Threat Defense device supports both RIP Version 1 and Version 2. RIP Version 1 does not send subnet masks with its updates; Version 2 supports variable-length subnet masks and neighbor authentication to ensure trusted routing information exchanges.

RIP offers simple configuration and adapts to topology changes. In contrast, static routes require manual updates for each change. RIP, however, incurs higher network and processing overhead compared to static routing.

How RIP routing updates work

Summary

Key components in the RIP routing update process include:

- RIP routers: Send and receive routing update messages to maintain network topology information
- Routing tables: Store the best routes to destinations with associated metric values
- Routing update messages: Contain network topology changes and route information
- Metric values: Determine the best path, with routers maintaining only the lowest metric route

Workflow

The process involves these stages:

1. RIP routers send routing-update messages at regular intervals and when the network topology changes.
2. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop.
3. RIP routers maintain only the best route to a destination, which is the route with the lowest metric value.
4. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates occur independently from regularly scheduled RIP router updates.

RIP routing metric

A RIP routing metric is a network measurement that

- calculates the distance between a source and a destination network,
- assigns a hop count value, typically 1, to each hop in a network path from the source to the destination, and
- updates the routing table when new routing data is received, using the sender's IP address as the next hop.

RIP stability features

RIP stability features are routing mechanisms that

- prevent routing loops by setting a limit on the number of hops in a path from source to destination,
- provide stability despite potentially rapid changes in network topology, and
- include split horizon and hold-down mechanisms to prevent incorrect routing information propagation.

Additional stability mechanisms

The maximum number of hops allowed in a path is 15. If a routing update shows a new or changed entry, the system increases the metric value to infinity (16), which makes the network destination unreachable. This stability mechanism limits the maximum diameter of a RIP network to fewer than 16 hops.

RIP timers

RIP timers are network protocol mechanisms that

- regulate RIP performance through timed intervals for routing updates and route management,
- control when routes are marked invalid, placed in holddown, or flushed from the routing table, and
- help prevent network congestion by managing the timing of routing updates across devices.

RIP timer stages

RIP uses numerous timers to regulate its performance. These are the timer stages for RIP:

- Update: The routing-update timer is the interval between periodic routing updates. This is how often the device sends routing updates. Generally, set to 30 seconds, a small random delay added to prevent simultaneous route updates.
- Invalid: Each routing table entry has a route-timeout timer for the last valid update. The route is marked invalid and moves to holddown once the timer expires. The default is 180 seconds (3 minutes).
- Holddown: The period the system waits before accepting any new updates for invalid routes. The default is 180 seconds (3 minutes).
- Flush: The route-flush timer marks the period from when the system receives the last valid update until the route is discarded and removed from the routing table. The default is 240 seconds (4 minutes).

RIP timer sequence when adjacent router interface goes down

When an adjacent router goes down, routing updates stop, and the Invalid and Flush timers start increasing. In the first 180 seconds, nothing will happen. After 180 seconds, the Invalid timer expires, marks the route invalid, and the Holddown timer begins, holding the route for 60 seconds.

If there is no routing update for the adjacent router's status (that is, it is still down), the route enters into the Flush state. In total, the system has waited for 240 seconds from the last update (180 seconds for the Invalid timer and 60 seconds for Holddown timer), and then the system flushes the route. Even if the adjacent router's interface comes up immediately, the system waits for the Holddown timer to complete the 120-second period before accepting updates.

Requirements and prerequisites for RIP

These requirements and prerequisites must be met for configuring RIP on supported firewall models.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for RIP

IPv6 guidelines

RIP does not support IPv6.

RIP version 2 guidelines

Consider these guidelines for RIP Version 2 configuration:

- If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP Version 2 updates to the interface.
- With RIP Version 2, the Secure Firewall Threat Defense device transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
- When RIP Version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP Version 2 configuration is removed from an interface, that multicast address is unregistered.

RIP limitations

These are the limitations of RIP:

- The Secure Firewall Threat Defense device cannot pass RIP updates between interfaces.
- RIP Version 1 does not support variable-length subnet masks.
- RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
- RIP convergence is relatively slow compared to other routing protocols.
- You can only enable a single RIP process on the Secure Firewall Threat Defense device.

Configure RIP

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection.

Use this procedure to define networks, manage redistribution, and apply interface-specific filtering or broadcast parameters.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select **Routing** and select **RIP** from the table of contents.

Check the **Enable RIP** check box to configure the RIP settings.

Choose the RIP versions for sending and receiving RIP updates from the **RIP Version** drop-down list:

- **Receive Version 1 & 2, Send Version 1**
- **Send & Receive Version 1**
- **Send & Receive Version 2**

Step 3 (Optional) Check the **Generate Default Route** check box to generate a default route for distribution, based on the route map that you specify.

a) Specify a route map name to use for generating default routes, in the **Route Map** field.

Generate the default route 0.0.0.0/0 for distribution when a route map is specified in the **Route Map** field.

Step 4 When you choose Send and Receive Version 2, the **Enable Auto Summary** option is available. When the **Enable Auto Summary** check box is checked, automatic route summarization is enabled. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.



Note RIP Version 1 always uses automatic summarization—you cannot disable it.

Step 5 Click **Networks**. Define one or more networks for RIP routing. Enter IP address(es), or enter or select the desired Network/Hosts objects. There is no limit to the number of networks you can add to the security appliance configuration. Interfaces belonging to the defined network will participate in the RIP routing. The RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.



Note RIP only supports IPv4 objects.

Step 6 (Optional) Click **Passive Interface**. Use this option to specify passive interfaces on the appliance, and by extension the active interfaces. The device receives RIP routing broadcasts on passive interfaces, using that

information to populate its routing tables, but does not broadcast routing updates on passive interfaces. Interfaces that are not designated as passive receive and send updates.

Step 7 Click **Redistribution** to manage redistribution routes. These are the routes that are being redistributed from other routing processes into the RIP routing process.

a) Click **Add** to specify redistribution routes.

b) Choose the routing protocol to redistribute into the RIP routing process, in the **Protocol** drop-down list. Available options are **Static**, **Connected**, **OSPF**, **BGP**, and **EIGRP**.

Note For OSPF, specify the process ID in the **Process ID** field. For BGP, specify the AS number in the **AS Number** field. When you choose the Connected option in the **Protocol** drop-down list, you can redistribute directly connected networks into the RIP routing process.

c) (Optional) If you are redistributing OSPF routes into the RIP routing process, you can select specific types of OSPF routes to redistribute in the **Match** drop-down list. Ctrl-click to select multiple types:

- **Internal**: Routes internal to the autonomous system (AS) are redistributed.
- **External 1**: Type 1 routes external to the AS are redistributed.
- **External 2**: Type 2 routes external to the AS are redistributed.
- **NSSA External 1**: Type 1 routes external to a not-so-stubby area (NSSA) are redistributed.
- **NSSA External 2**: Type 2 routes external to an NSSA are redistributed.

Note The default is match Internal, External 1, and External 2.

d) Select the RIP metric type to apply to the redistributed routes in the **Metric** drop-down list. The three choices are:

- **Transparent**: Use the current route metric.
- **Specified Value**: Assign a specific metric value from 0 to 16 in the **Metric Value** field.
- **None**: No metric is specified. Do not use any metric value, to apply to redistributed routes.

Note **None** option is applicable only for **Static** and **Connected** protocols.

e) (Optional) Enter the name of a route map that must be satisfied, in the **Route Map** field before the route can be redistributed into the RIP routing process. Routes are redistributed only if IP address matches an allow statement in the route map address list. To create a new route map object, click **Add** (+). See Configure Route Map Entry for the procedure to add a new route map.

f) Click **OK**.

Step 8 (Optional) Click **Filtering** to manage filters for the RIP policy. In this section, filters are used to prevent routing updates through an interface, control the advertising of routes in routing updates, control the processing of routing updates and filtering sources of routing updates.

a) Click **Add** to add RIP filters.

b) Select the type of traffic to be filtered - Inbound or Outbound in the **Traffic Direction** field.



Note If traffic direction is inbound, you can only define an Interface filter.

c) Specify whether the filter is based on an Interface or a Route, by selecting appropriate option in the **Filter On** field. If you click **Interface**, you can enter or choose the name of the interface on which routing updates are to be filtered. If you click **Route**, you can choose the route type:

- **Static**: Only static routes are filtered.
- **Connected**: Only connected routes are filtered.
- **OSPF**: Only OSPFv2 routes discovered by the specified OSPF process are filtered. Enter the Process ID of the OSPF process to be filtered.
- **BGP**: Only BGPv4 routes discovered by the specified BGP process are filtered. Enter the value in the **Process ID** field.
- **EIGRP**: Only EIGRP routes are filtered.

d) In the **Access List** field, enter or choose the name of one or more access control lists (ACLs) that define the networks to be allowed or removed from RIP route advertisements. To add a new standard access list object, click **Add** (+) and see Configure a standard ACL object, on page 2355.

e) Click **OK**.

Step 9 (Optional) Click **Broadcast** to add or edit interface configurations. Using Broadcast, you can override the global RIP versions to send or receive per interface. You can also define the authentication parameters per interface if you want to implement authentication to ensure valid RIP updates.

a) Click **Add** to add interface configurations.

b) Enter or choose an interface defined on this appliance in the **Interface** field.

c) In the Send option, select the appropriate boxes to specify sending updates using the RIP **Version 1**, **Version 2**, or both. These options let you override, for the specified interface, the global Send versions specified.

d) In the Receive option, select the appropriate boxes to specify accepting updates using the RIP **Version 1**, **Version 2**, or both. These options let you override, for the specified interface, the global Receive versions specified.

e) Select the **Authentication** used on this interface for RIP broadcasts.

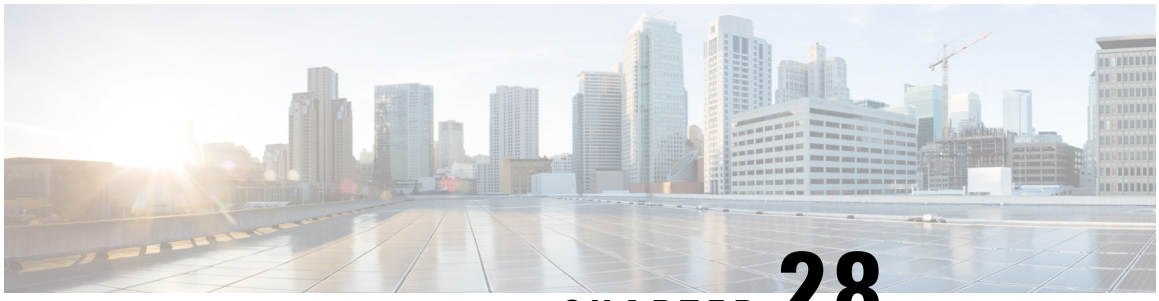
- **None**: No authentication
- **MD5**: Employ MD5
- **Clear Text**: Employ clear-text authentication

If you choose MD5 or Clear Text, you must also provide the following authentication parameters.

- **Key ID**: The ID of the authentication key; valid values are from 0 to 255.

- **Key**: The key used by the chosen authentication method; can contain up to 16 characters.
- **Confirm**: Enter the authentication key again to confirm.

f) Click **OK**.



CHAPTER 28

Multicast

This chapter describes how to configure the Secure Firewall Threat Defense device to use the multicast routing protocol.

- Multicast routing, on page 1137
- Prerequisites for Multicast Routing, on page 1142
- Guidelines for multicast routing, on page 1142
- Configure IGMP features, on page 1143
- Configure PIM features, on page 1149
- Configure multicast routes, on page 1155
- Configure multicast boundary filters, on page 1156

Multicast routing

Multicast routing is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications include videoconferencing, corporate communications, distance learning, and distributing software, stock quotes, and news.

Multicast routing applications and protocols

Multicast routing protocols send source traffic to multiple receivers efficiently, without adding extra load on the source or receivers, and use less network bandwidth than other technologies. Multicast packets are replicated in the network by Firewall Threat Defense device enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols, which results in the most efficient delivery of data to multiple receivers possible.

The Firewall Threat Defense device supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single Firewall Threat Defense device.

Note The UDP and non-UDP transports are both supported for multicast routing. However, the non-UDP transport has no FastPath optimization.

IGMP Protocol

IP hosts use the Internet Group Management Protocol (IGMP) to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP uses group addresses (Class D IP address) as group identifiers. Host group address can be in the range of 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is never assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

Note When you enable multicast routing on the Firewall Threat Defense device, IGMP Version 2 is automatically enabled on all interfaces.

Query Messages to Multicast Groups

The Firewall Threat Defense device sends query messages to discover which multicast groups have members on the networks attached to the interfaces. Members respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Query messages are addressed to the all-systems multicast group, which has an address of 224.0.0.1, with a time-to-live value of 1.

These messages are sent periodically to refresh the membership information stored on the Firewall Threat Defense device. If the Firewall Threat Defense device discovers that there are no local members of a multicast group still attached to an interface, it stops forwarding multicast packets for that group to the attached network, and it sends a prune message back to the source of the packets.

By default, the PIM designated router on the subnet is responsible for sending the query messages. By default, they are sent once every 125 seconds.

When changing the query response time, by default, the maximum query response time advertised in IGMP queries is 10 seconds. If the Firewall Threat Defense device does not receive a response to a host query within this amount of time, it deletes the group.

Stub multicast routing

Stub multicast routing provides dynamic host registration and facilitates multicast routing.

When configured for stub multicast routing, the Firewall Threat Defense device acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the Firewall Threat Defense device forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the Firewall Threat Defense device cannot be configured for PIM sparse or bidirectional mode. Enable PIM on the interfaces that participate in IGMP stub multicast routing.

The Firewall Threat Defense device supports both PIM-SM and bidirectional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees, each rooted at a single Rendezvous Point (RP) per multicast group. Optionally, it creates shortest-path trees for each multicast source.

PIM multicast routing

Bidirectional PIM is a variant of PIM-SM that builds bidirectional shared trees connecting multicast sources and receivers.

DF election process

Bidirectional trees are built using a Designated Forwarder (DF) election process operating on each link of the multicast topology. With the assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point (RP) and then along the shared tree to receivers. This process does not require source-specific state. The DF election takes place during RP discovery and provides a default route to the RP.



Note If the Firewall Threat Defense device is the PIM RP, use the untranslated outside address of the Firewall Threat Defense device as the RP address.

PIM sparse mode

PIM Sparse Mode (PIM-SM) is a PIM mode that forwards traffic only when specifically requested by receivers. It uses a central Rendezvous Point (RP) to coordinate the multicast traffic forwarding between the multicast source and the destination. RP is a router that serves as the meeting point for the source and the receivers. Multicast sources register with the RP through their first hop router. They send a copy of the multicast traffic to the receivers through the RP.

PIM source specific multicast support

Firewall Threat Defense device can forward source specific multicast traffic (e.g., for groups in the 232.x.x.x range) even though they do not support PIM-SSM configuration or Internet Group Management Protocol version 3 (IGMPv3).

SSM is classified as a data delivery mechanism for one-to-many applications such as IPTV. The SSM model uses a concept of "channels" denoted by an (S,G) pair, where S is a source address and G is an SSM destination address. Subscribing to a channel is achieved by using a group management protocol such as IGMPv3. SSM enables a receiving client, once it has learned about a particular multicast source, to receive multicast streams directly from the source rather than receiving it from a shared Rendezvous Point (RP). Access control mechanisms are introduced within SSM, providing a security enhancement that is not available with current sparse or sparse-dense mode implementations.

Limitation:

- Firewall Threat Defense device cannot act as the last-hop router for SSM multicast because it does not support IGMPv3 (which receivers use to join SSM groups).

  If the Firewall Threat Defense device is the last-hop, it will ignore IGMPv3 join messages from receivers for SSM groups, and SSM forwarding will not work.

- Static multicast routes on Firewall Threat Defense device do not work for SSM range (232.x.x.x).

Workaround:

For Cisco Firewall Threat Defense device firewall to forward SSM-related multicast traffic, you must add a multicast-capable layer 3 device (such as a router or switch) that supports PIM and IGMPv3 on the same network segment as the receivers.

How it Works:

- Receivers register their SSM group joins (IGMPv3) with this layer 3 device.
- This layer 3 device sends PIM join messages towards the Firewall Threat Defense device.
- The Firewall Threat Defense device receives these PIM messages and dynamically learns multicast routes.
- SSM multicast traffic is then properly forwarded by the Firewall Threat Defense device, since it is no longer the last-hop device.

Multicast Bidirectional PIM

Multicast bidirectional PIM is useful for networks that have many sources and receivers talking to each other simultaneously and where each participant can become both the source and receiver of multicast traffic, such as in videoconferencing, Webex meetings, and group chat. When PIM bidirectional mode is used, the RP only creates the (*,G) entry for the shared tree. There is no (S,G) entry. This conserves resources on the RP because state tables for each (S,G) entry are not maintained.

In PIM sparse mode, traffic only flows down the shared tree. In PIM bidirectional mode, traffic flows up and down the shared tree.

PIM bidirectional mode also does not use the PIM register/register-stop mechanism to register sources to the RP. Each source can begin sending to the source at any time. When the multicast packets arrive at the RP, they are forwarded down the shared tree (if there are receivers) or dropped (when there are no receivers). However, there is no way for the RP to tell the source to stop sending multicast traffic.

Design-wise you must think about where to place the RP in your network because it should be somewhere in the middle between the sources and receivers in the network.

PIM bidirectional mode has no Reverse Path Forwarding (RPF) check. Instead it uses the concept of a Designated Forwarder (DF) to prevent loops. This DF is the only router on the segment that is allowed to send multicast traffic to the RP. If there is only one router per segment that forwards multicast traffic, there will be no loops. The DF is chosen using the following mechanism:

- The router with the lowest metric to the RP is the DF.
- If the metric is equal, then the router with the highest IP address becomes the DF.

PIM bootstrap router (BSR)

PIM Bootstrap Router (BSR) is a dynamic Rendezvous Point (RP) selection model that uses candidate routers for RP function and for relaying the RP information for a group.

The RP function includes RP discovery and provides a default route to the RP. It does this by configuring a set of devices as candidate BSRs (C-BSR) which participate in a BSR election process to choose a BSR amongst themselves. Once the BSR is chosen, devices that are configured as candidate Rendezvous Points (C-RP) start sending their group mapping to the elected BSR. The BSR then distributes the group-to-RP mapping information to all the other devices down the multicast tree through BSR messages that travel from PIM router to PIM router on a per-hop basis.

This feature allows networks to learn RPs dynamically. Dynamic RP discovery is essential in large, complex networks where an RP may occasionally go down and come up.

PIM bootstrap router (BSR) terminology

This reference provides definitions for key terminology used in PIM Bootstrap Router (BSR) configurations to help understand the roles and functions of different components in the BSR election and RP advertisement process.

These terms are frequently referenced in the PIM BSR configuration:

- Bootstrap Router (BSR) — A BSR advertises Rendezvous Point (RP) information to other routers with PIM on a hop-by-hop basis. Among multiple Candidate-BSRs, a single BSR is chosen after an election process. The primary purpose of this Bootstrap router is to collect all Candidate-RP (C-RP) announcements in to a database called the RP-set and to periodically send this out to all other routers in the network as BSR messages (every 60 seconds).
- Bootstrap Router (BSR) messages — BSR messages are multicast to the All-PIM-Routers group with a TTL of 1. All PIM neighbors that receive these messages retransmit them (again with a TTL of 1) out of all interfaces except the one in which the messages were received. BSR messages contain the RP-set and the IP address of the currently active BSR. This is how C-RPs know where to unicast their C-RP messages.
- Candidate Bootstrap Router (C-BSR) — A device that is configured as a candidate-BSR participates in the BSR election mechanism. A C-BSR with highest priority is elected as the BSR. The highest IP address of the C-BSR is used as a tiebreaker. The BSR election process is preemptive, for example if a new C-BSR with a higher priority comes up, it triggers a new election process.
- Candidate Rendezvous Point (C-RP) — An RP acts as a meeting place for sources and receivers of multicast data. A device that is configured as a C-RP periodically advertises the multicast group mapping information directly to the elected BSR through unicast. These messages contain the Group-range, C-RP address, and a hold time. The IP address of the current BSR is learned from the periodic BSR messages that are received by all routers in the network. In this way, the BSR learns about possible RPs that are currently up and reachable.



Note The Firewall Threat Defense device does not act as a C-RP, even though the C-RP is a mandatory requirement for BSR traffic. Only routers can act as a C-RP. So, for BSR testing functionality, you must add routers to the topology.

- BSR Election Mechanism — Each C-BSR originates Bootstrap messages (BSMs) that contain a BSR Priority field. Routers within the domain flood the BSMs throughout the domain. A C-BSR that hears about a higher-priority C-BSR than itself suppresses its sending of further BSMs for some period of time. The single remaining C-BSR becomes the elected BSR, and its BSMs inform all the other routers in the domain that it is the elected BSR.

Multicast group concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries. Hosts can be

located anywhere on the Internet. Hosts that want to receive data sent to a group must join the group using IGMP.

Group membership requirements

Hosts must be a member of the group to receive the data stream.

Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

Clustering

Multicast routing supports clustering. In Spanned EtherChannel clustering, the control unit sends all multicast routing packets and data packets until fast-path forwarding is established.

After fast-path forwarding is established, data units may forward multicast data packets. All data flows are full flows. Stub forwarding flows are also supported. Because only one unit receives multicast packets in Spanned EtherChannel clustering, redirection to the control unit is common.

Prerequisites for Multicast Routing

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

- Admin
- Network Admin

Guidelines for multicast routing

Table 71: System requirements

Item	Description
Context mode	Supported in single context mode.
Firewall mode	Supported only in routed firewall mode. Transparent firewall mode is not supported.

Item	Description
IPv6	IPv6 is not supported.
Multicast group	The range of addresses from 224.0.0.0 to 224.0.0.255 is reserved for routing protocols and other topology discovery or maintenance protocols, such as gateway discovery and group membership reporting. Internet multicast routing from the 224.0.0/24 address range is not supported. When multicast routing is enabled for reserved addresses, an IGMP group is not created.
Clustering	In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

Access control configuration

You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to multicast connections during initial connection validation.

Interface and protocol management

Ensure proper configuration management when working with PIM-enabled interfaces and multicast routing protocols.

- You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see Configure PIM protocol, on page 1149), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface.
- Multicast routing is not supported in ECMP.
- Do not configure Firewall Threat Defense to simultaneously be a Rendezvous Point (RP) and a First Hop Router.
- The HSRP standby IP address does not participate in PIM neighborship. If the RP router IP is routed through the HSRP standby IP address, multicast routing does not work in Firewall Threat Defense. To ensure multicast traffic passes through successfully, configure the route for the RP address to use an interface IP address rather than the HSRP standby IP address.
- For a device using virtual routing, you can configure multicast only for its global virtual router and not for its user-defined virtual router.

Configure IGMP features

Configure IGMP features to enable dynamic registration of individual hosts in multicast groups on a particular LAN and to manage multicast traffic efficiently.

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IP hosts use IGMP to report their group memberships to directly connected multicast routers. IGMP dynamically registers individual hosts in a multicast group on a specific LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

This section describes how to configure optional IGMP settings on a per-interface basis.

Procedure

Step 1 Enable multicast routing, on page 1144.
Step 2 Configure IGMP protocol, on page 1145.
Step 3 Configure IGMP access groups, on page 1146.
Step 4 Configure IGMP static groups, on page 1147.
Step 5 Configure IGMP join groups, on page 1148.

Enable multicast routing

Enable multicast routing to allow the device to forward multicast traffic using Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) protocols on all interfaces.

Enabling multicast routing on the Firewall Threat Defense device, enables IGMP and PIM on all interfaces by default. IGMP is used to learn whether members of a group are present on directly attached subnets. Hosts join multicast groups by sending IGMP report messages. PIM is used to maintain forwarding tables to forward multicast datagrams.

Note Only the UDP transport layer is supported for multicast routing.

These are the maximum number of entries for specific multicast tables. Any new entries are discarded when these limits are reached.

- Multicast Forwarding Information Base (MFIB): 30,000
- IGMP Groups: 30,000
- PIM Routes: 72,000

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
Step 2 Choose **Routing** > **Multicast Routing** > **IGMP**.
Step 3 Check the **Enable Multicast Routing** check box.

Checking this check box enables IP multicast routing on the device. Unchecking it disables IP multicast routing. By default, multicast is disabled. Enabling multicast routing enables multicast on all interfaces.

You can disable multicast on a per-interface basis. This is useful if you know that there are no multicast hosts on a specific interface and you want to prevent the Firewall Threat Defense device from sending host query messages on that interface.

Configure IGMP protocol

Use this task to configures IGMP parameters per-interface. These settings help manage multicast group membership on a Firewall Threat Defense device.

You can configure IGMP parameters per interface, such as the forward interface, query messages, and time intervals.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **IGMP**.

Step 3 Click the **Protocol** tab and click **Add**, or edit an interface.

In the **Add IGMP parameters** dialog box, configure new IGMP parameters to the Firewall Threat Defense device. Use the **Edit IGMP parameters** dialog box to modify the existing parameters.

Step 4 Configure these parameters:

- **Interface**: From the drop-down list, choose the interface for which you want to configure IGMP protocol.
- **Enable IGMP**: Check the check box to enable IGMP.



Note Disabling IGMP on specific interfaces is useful if you know that there are no multicast hosts on a specific interface and you want to prevent the device from sending host query messages on that interface.

- **Forward Interface**: From the drop-down list, choose the specific interface from which you want to forward IGMP messages.

  This configures the Secure Firewall Threat Defense device to act as an IGMP proxy agent and forward IGMP messages from hosts connected on one interface to an upstream multicast router on another interface.

- **Version**: Choose IGMP Version 1 or 2.

  By default, the Firewall Threat Defense device runs IGMP Version 2, which enables several additional features.

Note All multicast routers on a subnet must support the same version of IGMP. The Firewall Threat Defense device does not automatically detect Version 1 routers and switch to Version 1. However, you can have a mix of IGMP Version 1 and 2 hosts on the subnet; the Firewall Threat Defense device running IGMP Version 2 works correctly when IGMP Version 1 hosts are present.

- **Query Interval**: The interval in seconds at which the designated router sends IGMP host-query messages. The range is 1 to 3600. The default is 125.

Note If the Firewall Threat Defense device does not hear a query message on an interface for the specified timeout value, then the device becomes the designated router and starts sending the query messages.

- **Response Time**: The interval in seconds before the Firewall Threat Defense device deletes the group. The range is 1 to 25. The default is 10.

  If the Firewall Threat Defense device does not receive a response to a host query within this amount of time, it deletes the group.

- **Group Limit**: Maximum number of hosts that can join on an interface. The range is 1 to 500. The default is 500.

  You can limit the number of IGMP states resulting from IGMP membership reports on a per-interface basis. Membership reports that exceed the configured limits are not entered in the IGMP cache, and their traffic is not forwarded.

- **Query Timeout**: The period of time in seconds before which the Firewall Threat Defense device takes over as the requester for the interface after the previous requester has stopped. The range is 60 to 300. The default is 255.

Step 5 Click **OK** to save the IGMP protocol configuration.

Configure IGMP access groups

You can control access to multicast groups by using access control lists.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **Access Group**.

Step 3 On **Access Group**, click **Add** or **Edit**.

Use the **Add IGMP Access Group parameters** dialog box to add new IGMP access groups to the Access Group table. Use the **Edit IGMP Access Group parameters** dialog box to change the parameters of an existing access group.

Step 4 Configure the access group options:

a) From the **Interface** drop-down list, choose the interface associated with the access group. You cannot change the associated interface when you are editing an existing access group.

b) Click one of the following:

- **Standard Access List**: From the **Standard Access List** drop-down list, choose the standard ACL or click **Add** (+) to create a new standard ACL. For more information, refer to Configure a standard ACL object, on page 2355.
- **Extended Access List**: From the **Extended Access List** drop-down list, choose the extended ACL or click **Add** (+) to create a new extended ACL. For more information, refer to Configure an extended ACL object, on page 2351.

Step 5 Click **OK** to save the access group configuration.

Configure IGMP static groups

Configure a statically joined IGMP group to enable multicast traffic for that group to be sent to a network segment even when group members cannot report membership or no members exist on the segment.

Sometimes a group member cannot report its membership in the group or there may be no members of a group on the network segment, but you still want multicast traffic for that group to be sent to that network segment. You can have multicast traffic for that group sent to the segment by configuring a statically joined IGMP group. With this method, the Firewall Threat Defense device does not accept the packets itself, but only forwards them. Therefore, this method allows fast switching. The outgoing interface appears in the IGMP cache, but this interface is not a member of the multicast group.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **IGMP**.

Step 3 On **Static Group**, click **Add** or **Edit**.

Use the **Add IGMP Static Group parameters** dialog box to statically assign a multicast group to an interface. Use the **Edit IGMP Static Group parameters** dialog box to change existing static group assignments.

Note The IGMP Static Group enables PIM to send *Join* requests towards the sources or towards the Rendezvous Point (RP), provided, the firewall with this command is the PIM Designated Router (DR) on that interface where the command is applied.

Step 4 Configure the following options:

- From the **Interface** drop-down list, choose the interface to which you want to statically assign a multicast group. If you are editing an existing entry, you cannot change the value.
- From the **Multicast Group** drop-down list, choose the multicast group to which you want to assign the interface, or click **Add** (+) to create a new multicast group. Refer to Creating Network Objects for the procedure.

Step 5 Click **OK** to save the static group configuration.

Configure IGMP join groups

You can configure an interface to be a member of a multicast group.

Configuring the Firewall Threat Defense device to join a multicast group, upstream routers maintain multicast routing table information for that group and keep the group's paths active.

Note Refer to Configure IGMP static groups, on page 1147 if you want to forward multicast packets for a specific group to an interface without the Firewall Threat Defense device accepting those packets as part of the group.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **IGMP**.

Step 3 On **Join Group**, click **Add** or **Edit**.

Use the **Add IGMP Join Group parameters** dialog box to configure the Firewall Threat Defense device to be a member of a multicast group. Use the **Edit IGMP Join Group parameters** dialog box to change existing parameters.

Note The IGMP Join Group enables PIM to send *Join* requests to sources or to the Rendezvous Point (RP) if the firewall with this command is the PIM Designated Router (DR) on that interface.

Step 4 Configure the following options:

- From the **Interface** drop-down list, choose the interface you want to be a member of a multicast group. If you are editing an existing entry, you cannot change the value.
- From the **Join Group** drop-down list, choose the multicast group to which you want to assign the interface, or click **Plus** to create a new multicast group. Refer to Creating Network Objects for the procedure.

Configure PIM features

This section describes how to configure optional PIM settings.

Routers use PIM to maintain forwarding tables to use for forwarding multicast diagrams. Enable multicast routing on the Secure Firewall Threat Defense device, to automatically enable IGMP and PIM on all interfaces.

Note PIM is not supported with PAT. The PIM protocol does not use ports, and PAT only works with protocols that use ports.

Procedure

Step 1 Configure PIM protocol, on page 1149.
Step 2 Configure PIM neighbor filters, on page 1150.
Step 3 Configure PIM bidirectional neighbor filters, on page 1151.
Step 4 Configure PIM rendezvous points, on page 1152.
Step 5 Configure PIM route trees, on page 1153.
Step 6 Configure PIM request filters, on page 1154.
Step 7 Configure multicast boundary filters, on page 1156.

Configure PIM protocol

You can enable or disable PIM on a specific interface.

You can also configure the Designated Router (DR) priority. The DR is responsible for sending PIM register, join, and prune messages to the RP. When there is more than one multicast router on a network segment, the DR is chosen based on DR priority. If multiple devices share the same DR priority, the device with the highest IP address becomes the DR. By default, the Firewall Threat Defense device has a DR priority of 1.

Router query messages are used to choose the PIM DR. The PIM DR is responsible for sending router query messages. By default, router query messages are sent every 30 seconds. Additionally, every 60 seconds, the Firewall Threat Defense device sends PIM join or prune messages.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.
Step 3 Click the **Protocol** tab and click **Add**, or edit an interface.

In the **Add PIM parameters** dialog box, add new PIM parameters for the interface. Use the **Edit PIM parameters** dialog box to change existing parameters.

Step 4 Configure these options:

- **Interface**: From the drop-down list, select the interface for which you want to configure PIM protocol.
- **Enable PIM**: Check the check box to enable PIM.
- **DR Priority**: Set the DR priority value for the selected interface. The router with the highest DR priority on the subnet becomes the designated router.
- **Hello Interval(seconds)**: The interval in seconds at which the interface sends PIM hello messages. The range is 1 to 3600. The default is 30.
- **Join Prune Interval(seconds)**: The interval in seconds at which the interface sends PIM join and prune advertisements. The range is 10 to 600. The default is 60.

Step 5 Click **OK** to save the PIM protocol configuration.

Configure PIM neighbor filters

You can define and filter the routers that become Protocol Independent Multicast (PIM) neighbors.

PIM neighbor filters allow you to define and filter the routers that become Protocol Independent Multicast (PIM) neighbors to:

- Prevent unauthorized routers from becoming PIM neighbors.
- Prevent attached stub routers from participating in PIM.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.

Step 3 Click the **Neighbor Filter** tab and click **Add**, or edit an interface.

In the **Add PIM Neighbor Filter** dialog box, add new PIM neighbor filters to the interface. Use the **Edit PIM Neighbor Filter** dialog box to change existing parameters.

Step 4 Configure these options:

- From the **Interface** drop-down list, choose the interface to which you want to add a PIM neighbor filter.
- From the **Standard Access List** drop-down list, choose a standard ACL or click **Add** (+) to create a new standard ACL. Refer to Configure a standard ACL object, on page 2355 for the procedure.

Note Choosing **Allow** on the **Add Standard Access List Entry** dialog box lets the multicast group advertisements pass through the interface. Choosing **Block** prevents the specified multicast group advertisements from passing through the interface. When a multicast boundary is configured on an interface, all multicast traffic is prevented from passing through the interface unless permitted with a neighbor filter entry.

Step 5 Click **OK** to save the PIM neighbor filter configuration.

Configure PIM bidirectional neighbor filters

Configure PIM bidirectional neighbor filters to control which neighbor devices participate in the Designated Forwarder (DF) election for bidirectional multicast routing. This helps ensure proper multicast traffic forwarding in the network.

A PIM bidirectional neighbor filter is an ACL that defines the neighbor devices that can participate in the Designated Forwarder (DF) election. If you do not configure a PIM bidirectional neighbor filter for an interface, there are no restrictions. If you configure a PIM bidirectional neighbor filter, only neighbors permitted by the ACL can participate in the DF election process.

Bidirectional PIM allows multicast routers to keep reduced state information. All multicast routers in a segment must be bidirectionally enabled to elect a DF.

When a PIM bidirectional neighbor filter is enabled, the routers permitted by the ACL are considered to be bidirectionally capable. Therefore, the following is true:

- If a permitted neighbor does not support bidirectional mode, the DF election does not occur.
- If a denied neighbor supports bidirectional mode, the DF election does not occur.
- If a denied neighbor does not support bidirectional mode, the DF election can occur.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Multicast Routing** > **PIM**.

Step 3 On **Bidirectional Neighbor Filter**, click **Add** or **Edit**.

Use the **Add PIM Bidirectional Neighbor Filter** dialog box to create ACL entries for the PIM bidirectional neighbor filter ACL. Use the **Edit PIM Bidirectional Neighbor Filter** dialog box to change existing parameters.

Step 4 Configure these options:

- In the **Interface** drop-down list, select the interface for which you want to configure the PIM bidirectional neighbor filter ACL entry.

- From the **Standard Access List** drop-down list, select a standard ACL or click **Add** (+) to create a new standard ACL. Refer to Configure a standard ACL object, on page 2355 for the procedure.

Note Choosing **Allow** in the **Add Standard Access List Entry** dialog box lets the specified devices participate in the DR election process. Choosing **Block** prevents the specified devices from participating in the DR election process.

Step 5 Click **OK** to save the PIM bidirectional neighbor filter configuration.

Configure PIM rendezvous points

You can configure the Firewall Threat Defense device to serve as a RP to more than one group.

The group range specified in the ACL determines the PIM RP group mapping. If an ACL is not specified, then the RP for the group is applied to the entire multicast group range (224.0.0.0/4). Refer to Multicast Bidirectional PIM, on page 1140 for more information about bidirectional PIM.

These restrictions apply to RPs:

- You cannot use the same RP address twice.
- You cannot specify **All Groups** for more than one RP.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.

Step 3 On **Rendezvous Points**, click **Add** or **Edit**.

Use the **Add Rendezvous Point** dialog box to create a new entry in the Rendezvous Point table. Use the **Edit Rendezvous Point** dialog box to modify existing parameters.

Step 4 Configure these options:

- From the **Rendezvous Point IP address** drop-down list, choose the IP address that you want to add as an RP or click **Add** (+) to create a new network object. Refer to Creating Network Objects for the procedure.
- Check the **Use bi-directional forwarding** check box to enable bidirectional mode for the specified multicast groups. In this mode, if the Firewall Threat Defense device receives a multicast packet and has no directly connected members or PIM neighbors present, it sends a prune message back to the source.
- Click **Use this RP for all Multicast Groups** to use the specified RP for all multicast groups on the interface.
- Click **Use this RP for all Multicast Groups as specified below** to designate the multicast groups to use with the specified RP and then from the **Standard Access List** drop-down list, choose a standard ACL

or click **Add** (+) to create a new standard ACL. Refer to Configure a standard ACL object, on page 2355 for the procedure.

Step 5 Click **OK** to save the rendezvous point configuration.

Configure PIM route trees

Configure PIM route trees to control whether the Firewall Threat Defense device joins the shortest-path tree or uses the shared tree for multicast traffic routing.

By default, PIM leaf routers join the shortest-path tree immediately after the first packet arrives from a new source. This method reduces delay, but requires more memory than the shared tree. You can configure whether or not the Firewall Threat Defense device should join the shortest-path tree or use the shared tree, either for all multicast groups or only for specific multicast addresses.

The shortest-path tree is used for any group that is not specified in the Multicast Groups table. The Multicast Groups table displays the multicast groups to use with the shared tree. The table entries are processed from the top down. You can create an entry that includes a range of multicast groups, but excludes specific groups within that range by placing deny rules for the specific groups at the top of the table and the permit rule for the range of multicast groups below the deny statements.



Note This behavior is known as Shortest Path Switchover (SPT). We recommend that you always use the Shared Tree option.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.

Step 3 On **Route Tree**, select the path for the route tree:

- Click **Shortest Path** to use the shortest-path tree for all multicast groups.
- Click **Shared Tree** to use the shared tree for all multicast groups.
- Click **Shared tree for below mentioned group** to designate the groups specified in the Multicast Groups table, and then from the **Standard Access List** drop-down list, select a standard ACL or click **Add** (+) to create a new standard ACL. Refer to Configure a standard ACL object, on page 2355 for the procedure.

Step 4 Click **OK** to save the route tree configuration.

Configure PIM request filters

When the Firewall Threat Defense device is acting as an RP, you can restrict specific multicast sources from registering with it to prevent unauthorized sources from registering with the RP. You can define the multicast sources from which the Firewall Threat Defense device will accept PIM register messages.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.

Step 3 On **Request Filter**, define the multicast sources that are allowed to register with the Firewall Threat Defense device when it acts as an RP:

- From the **Filter PIM register messages using:** drop-down list select **None**, **RouteMap**, or **Access List**.
- If you choose **Access List** from the drop-down list, select an extended ACL or click **Add** (+) to create a new extended ACL. Refer to Configure an extended ACL object, on page 2351 for the procedure.

Note In the **Add Extended Access List Entry** dialog box, select **Allow** from the drop-down list to create a rule that allows the specified source of the specified multicast traffic to register with the Firewall Threat Defense device, or select **Block** to create a rule that prevents the specified source of the specified multicast traffic from registering with the device.

- If you choose **RouteMap**, select a route map from the **Route Map** drop-down list, or click **Add** (+) to create a new route map. Refer to Creating Network Objects for the procedure.

Step 4 Click **OK** to save the request filter configuration.

Configure the Firewall Threat Defense device as a candidate bootstrap router

You can configure the Firewall Threat Defense device as a candidate BSR.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **PIM**.

Step 3 On **Bootstrap Router**, check the **Configure this FTD as a Candidate Bootstrap Router (C-BSR)** check box to perform the C-BSR setup.

a) From the **Interface** drop-down list, select the interface in the Firewall Threat Defense device from which the BSR address is derived to make it a candidate.

This interface must be enabled with PIM.

b) In the **Hashmask Length** field, enter the length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to configure one RP for multiple groups. The range is 0 to 32.

c) In the **Priority** field, enter the priority of the candidate BSR. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The range is 0 to 255. The default value is 0.

Step 4 (Optional) Click **Add** (+) to select an interface on which no PIM BSR messages will be sent or received in the **Configure this FTD as a Border Bootstrap Router (BSR)** section.

- From the **Interface** drop-down list, select the interface on which no PIM BSR messages will be sent or received.

  RP or BSR advertisements are filtered effectively isolating two domains of RP information exchange.

- Check the **Enable Border BSR** check box to enable BSR.

Step 5 Click **OK** to save the bootstrap router configuration.

Configure multicast routes

Configure static multicast routes to separate multicast traffic from unicast traffic. For example, when a path between a source and destination does not support multicast routing, the solution is to configure two multicast devices with a GRE tunnel between them and to send the multicast packets over the tunnel.

When using PIM, the Firewall Threat Defense device expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.

Static multicast routes are not advertised or redistributed.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **Multicast Routes** > **Add or Edit**.

Use the **Add Multicast Route Configuration** dialog box to add a new multicast route to the Firewall Threat Defense device. Use the **Edit Multicast Route Configuration** dialog box to change an existing multicast route.

Step 3 Choose an existing network from the **Source Network** drop-down, or click **Add** (+) to add a new network.

Refer to Creating Network Objects for the procedure.

Step 4 To configure an interface to forward the route, click **Interface** and configure the following options:

- From the **Source Interface** drop-down list, choose the incoming interface for the multicast route.

- From the **Output Interface/Dense** drop-down list, choose the destination interface that the route is forwarded through.
- In the **Distance** field, enter the distance of the multicast route. The range is 0 to 255.

Step 5 To configure an RPF address to forward the route, click **Address** and configure the following options:

- In the **RPF Address** field, enter the IP address for the multicast route.
- Enter the multicast route distance in the **Distance** field. The value must be between 0 and 255.

Step 6 Click **OK** to save the multicast routes configuration.

Configure multicast boundary filters

Address scoping defines domain boundary filters so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.

You can set up an administratively scoped boundary filter on an interface for multicast group addresses. IANA has designated the multicast address range from 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. The addresses are considered local and are not globally unique.

A standard ACL defines the range of affected addresses. When a boundary filter is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary filter allows the same multicast group address to be reused in different administrative domains.

You can configure, examine, and filter Auto-RP discovery and announcement messages at the administratively scoped boundary. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL are removed. An Auto-RP group range announcement is permitted and passed by the boundary filter only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Choose **Routing** > **Multicast Routing** > **Multicast Boundary Filter**, and then click **Add** or **Edit**.

Use the **Add Multicast Boundary Filter** dialog box to add new multicast boundary filters to the device. Use the **Edit Multicast Boundary Filter** dialog box to change existing parameters.

You can configure a multicast boundary for administratively scoped multicast addresses. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains. When a multicast boundary is defined on an interface, only the multicast traffic permitted by the filter ACL passes through the interface.

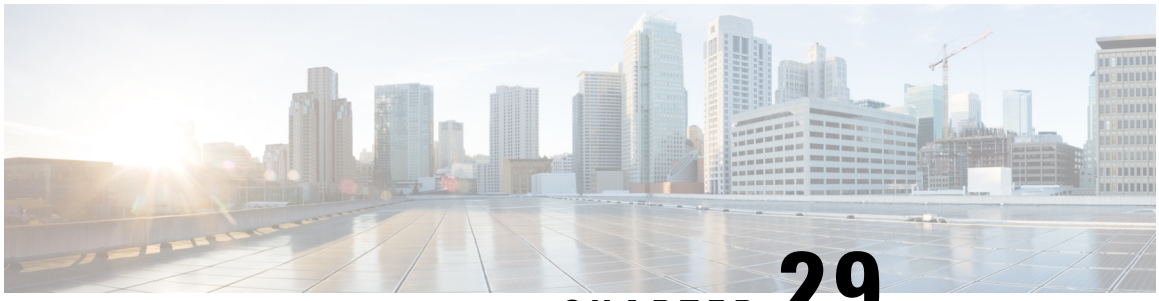
Step 3 From the **Interface** drop-down list, choose the interface for which you are configuring the multicast boundary filter ACL.

Step 4 From the **Standard Access List** drop-down list, choose the standard ACL you want to use, or click **Add** (+) to create a new standard ACL. Refer to Configure a standard ACL object, on page 2355 for the procedure.

Step 5 Check the **Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary** check box to filter Auto-RP messages from sources denied by the boundary ACL. If this check box is not checked, all Auto-RP messages are passed.

Step 6 Click **OK** to save the multicast boundary filter configuration.

The multicast boundary filter is configured on the selected interface with the specified standard ACL, restricting multicast traffic according to the filter rules and enabling address reuse across administrative domains.



CHAPTER 29

Policy-Based Routing

This chapter describes how to configure Firewall Threat Defense to support policy-based routing (PBR) through Firewall Management Center's policy-based routing page. The following sections describe policy based routing, guidelines for PBR, and configuration for PBR.

- About policy-based routing, on page 1159
- Licenses for policy-based routing, on page 1161
- Best practices for policy-based routing, on page 1161
- Path monitoring metrics for best path route determination, on page 1163
- Configure policy-based routing policy, on page 1166
- Configure policy-based routing, on page 1169
- Configure PBR with path monitoring, on page 1175
- Useful CLIs for monitoring PBR, on page 1177
- Troubleshoot PBR, on page 1179
- History for policy-based routing, on page 1182

About policy-based routing

Policy-based routing (PBR) extends traditional routing protocols to provide greater control over traffic flow. It enables routing decisions based on criteria beyond destination IP, such as source and destination ports, protocols, and applications. Furthermore, PBR facilitates secure, application-specific traffic breakout in large-scale network deployments.

Policy-based routing characteristics

In traditional routing, packets are routed based on the destination IP address. Changing the routing of specific traffic in a destination-based routing system is difficult. PBR extends and complements the mechanisms provided by routing protocols.

PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link. With PBR, you can define routing that is based on criteria other than destination network such as source port, destination address, destination port, protocol, applications, or a combination of these objects.

You can use PBR to classify the network traffic based on applications, username, group membership, and security group association. This routing method applies to scenarios involving numerous devices accessing applications and data in large network deployment. In large deployments, network traffic is typically backhauled to a hub as encrypted traffic in a route-based VPN. These topologies often result in issues such as packet

latency, reduced bandwidth, and packet drop. Resolving these issues requires costly, complex deployments and management.

PBR policy enables you to securely break out traffic for specified applications. You can configure PBR policy in the Secure Firewall Management Center user interface to allow the applications to be directly accessed.

Consider a company that has two links between locations: one a high-bandwidth, low-delay expensive link, and the other a low-bandwidth, higher-delay, less-expensive link. While using traditional routing protocols, the higher-bandwidth link gets most, if not all, of the traffic sent across it based on the metric savings obtained by the bandwidth, delay, or both (using EIGRP or OSPF) characteristics of the link. With PBR, you can route higher priority traffic over the high-bandwidth/low-delay link, while sending all other traffic over the low-bandwidth/high-delay link.

These scenarios demonstrate policy-based routing applications:

- **Direct internet access**: In this topology, application traffic from the branch office can be routed directly to the internet instead of through the VPN tunnel connecting to the headquarters. The branch Firewall Threat Defense is configured with an internet exit point. The PBR policy is applied on the ingress interface (*Inside 1*) to identify the traffic based on the applications, user identity (username and group membership), and Security Group Tag (security group association) defined in the ACL. Correspondingly, the traffic is forwarded through the egress interfaces directly to the internet or to the IPsec VPN tunnel.
- **Equal-access and source-sensitive routing**: In this topology, traffic from the HR and Mgmt networks can be configured to go through ISP1 and traffic from Eng network can be configured to go through ISP2. Thus, policy-based routing enables the network administrators to provide equal-access and source-sensitive routing, in this example.
- **Load sharing**: In addition to the dynamic load-sharing capabilities offered by ECMP load balancing, network administrators can now implement policies to distribute traffic among multiple paths based on the traffic characteristics. As an example, in the topology depicted in the Equal-Access Source Sensitive Routing scenario, an administrator can configure policy-based routing to route the traffic from HR network through ISP1 and traffic from Eng network through ISP2 and thus share the load.

Figure 361: Direct internet access scenario

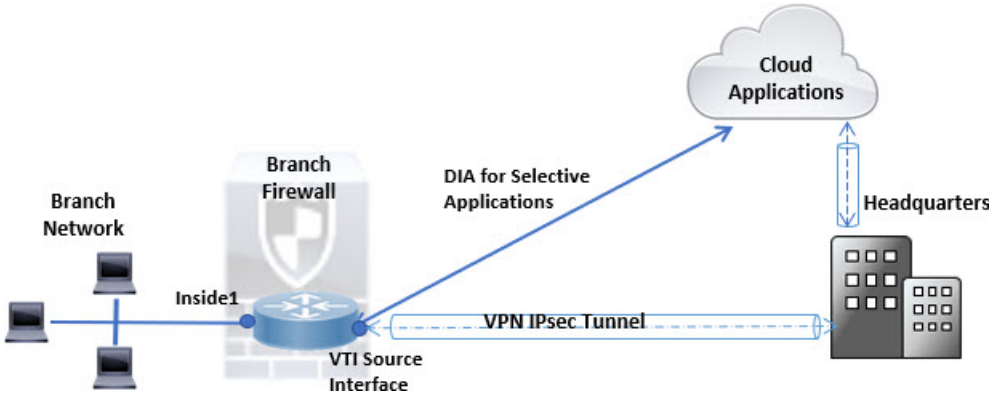
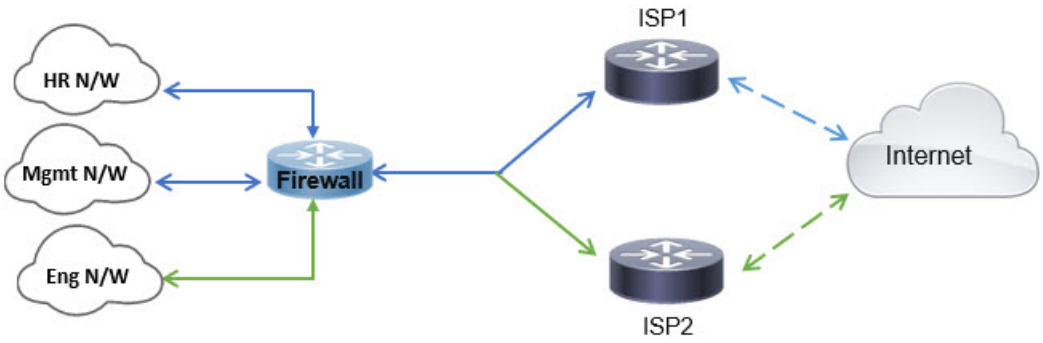


Figure 362: Equal access scenario



Licenses for policy-based routing

Policy-based routing (PBR) has specific licensing requirements depending on the features and services used in your configuration.

- All PBR policy features are supported with the Essentials Firewall Threat Defense smart license.
- Secure Client licensing is required if you are configuring PBR for routing traffic through RA VPN tunnel interface.
- Cisco ISE license is required for ISE usage in PBR policy.

Best practices for policy-based routing

Device guidelines

Ensure proper version compatibility and device-specific configurations when implementing PBR.

- PBR through Firewall Management Center's policy-based routing page is supported only from version 7.1 or later on both the Firewall Management Center and the Firewall Threat Defense device.
- When you upgrade Firewall Management Center or Firewall Threat Defense to version 7.1 or later, the PBR configuration in the device is removed. You must configure PBR again using the PBR page. If the managed device is earlier than version 7.1, you must configure PBR again using FlexConfig with deploy option set to "every time."
- On cluster devices, do not configure application, user identity, and Security Group Tag (SGT) based PBR policies, because they are not supported on cluster devices.

Interface guidelines

Configure appropriate interface types and settings for PBR policies.

- Configure only routed-mode interfaces and non management-only interfaces in the Global virtual router as ingress or egress interfaces for the PBR policy. You cannot configure user-defined virtual router interfaces for the policy.
- The interfaces that you want to define in the policy must have a logical name.

- Configure Static VTIs only as egress interfaces.
- Do not choose Dynamic VTIs for configuring the PBR egress interfaces.

You can apply PBR for managing both IPv4 and IPv6 traffic.

Application-based PBR and DNS configuration

Ensure proper DNS configuration for application-based PBR functionality.

- Application-based PBR uses DNS snooping for application detection. Application detection succeeds only if the DNS requests pass through Firewall Threat Defense in a clear-text format; the DNS traffic is not encrypted.
- You must configure trusted DNS servers for the application detection to succeed.

For more information on configuring DNS servers, refer to Configure DNS server settings, on page 852.

PBR policies not applied for output route look-up

PBR is an ingress-only feature; The system applies PBR only to the first packet of a new incoming connection, at which time the egress interface for the forward leg of the connection is selected. Note that PBR will not be triggered if the incoming packet belongs to an existing connection, or if NAT is applied and NAT chooses the egress interface.

PBR policies not applied for embryonic traffic

An embryonic connection is where the necessary handshake between source and destination has not been made. When a new internal interface is added and a new VPN policy is created using a unique address pool, PBR is applied to the outside interface matches the source of the new client pool. Thus, PBR sends traffic from the client to the next hop on the new interface. However, PBR does not process return traffic from a host until the new internal interface establishes a connection with the client. Thus, the return traffic from the host to the VPN client, specifically, the VPN client response is dropped as there is no valid route. To prevent the response from being dropped, configure a weighted static route with a higher metric on the internal interface.

HTTP-based path monitoring guidelines

Configure HTTP-based path monitoring with appropriate interface types and version considerations.

- Configure HTTP-based path monitoring only on physical, port-channel, subinterfaces, and static tunnel interfaces. Do not configure it on cluster devices.
- HTTP uses only IPv4 to ping applications. IPv4 metrics are applied for routing and forwarding both IPv4 and IPv6 traffic.
- HTTP-based application monitoring is enabled by default in Secure Firewall Management Center version 7.4 and higher. However, when you upgrade from previous versions, this option is not enabled by default. You must manually enable it.

Additional guidelines

Follow these additional configuration considerations for effective PBR implementation.

- All existing configuration restrictions and route map limitations remain in effect.
- When you define the ACL for the policy match criteria, you can select multiple predefined applications from a list to form an Access Control Entry (ACE). In Firewall Threat Defense, the predefined applications

are stored as Network Service objects and the group of applications as Network Service Groups (NSG). You can create a maximum of 1024 such NSGs. The application or network service group is detected through first-packet classification. Currently, you cannot add to or modify the predefined applications list.

- Unicast Reverse Path Forwarding (uRPF) validates the source IP address of packets received on an interface against the routing table and not against the PBR route map. When uRPF is enabled, packets received on an interface through PBR are dropped as they are without the specific route entry. Therefore, when using PBR, ensure you disable uRPF.

Path monitoring metrics for best path route determination

Path monitoring metrics for best path route determination is a dynamic routing method that uses various monitoring approaches, such as ICMP and HTTP, to collect performance metrics and determine the best path.

Path monitoring methods and operation

PBR uses either static cost or path monitoring (dynamic metrics) to route its traffic.

Path monitoring, when configured on interfaces, derive metrics such as round trip time (RTT), jitter, mean opinion score (MOS), and packet loss per interface. These metrics are used to determine the best path for routing PBR traffic.

ICMP-based path monitoring method

The metrics on the interfaces are collected dynamically using ICMP probe messages to the interface's default gateway or a specified remote peer.

HTTP-based path monitoring method

Path monitoring calculates dynamic metrics for each remote peer associated with an interface. HTTP is preferred over ICMP when monitoring multiple applications and determining the best path through a policy on a branch firewall, because:

- HTTP-ping can derive the performance metrics of the path up to the application layer of the server, where the application is hosted.
- Because the application domain is tracked instead of the IP address, you do not need to change the firewall configuration when the application server IP address changes.



Note You can configure both ICMP and HTTP on the same interface. If the destination in the policy matches to any of the domain IP, the corresponding metrics are used. If the destination does not match to any of the configured domains, the metrics from the ICMP are used by PBR to select the outgoing interface.

Default monitoring timers for metric collection

For metric collection and monitoring, the following timers are used:

- The interface monitor average interval is 30 seconds. This interval indicates the frequency to which the probes average.

- The interface monitor update interval is 30 seconds. This interval indicates the frequency at which the average of the collected values are calculated and made available for PBR to determine the best routing path.
- The interface monitor probe interval by ICMP is one second. This interval indicates the frequency at which an ICMP ping is sent.
- The application monitor probe interval by HTTP is 10 seconds. This interval indicates the frequency at which an HTTP ping is sent. Path monitoring uses the last 30 samples of HTTP ping for calculating the average metrics.

Note You cannot configure or modify the interval for any of these timers.

PBR and path monitoring integration

Typically, in PBR, traffic is forwarded through egress interfaces based on the priority value (interface cost) configured on them. From management center version 7.2, PBR uses IP-based path monitoring to collect the performance metrics (RTT, jitter, packet-lost, and MOS) of the egress interfaces. PBR uses the metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR about the monitored interface whose metric got changed. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path.

Path monitoring functions only with dynamic metrics, and only if the RTT, jitter, packet-lost, or MOS variables are set on the interfaces. Path monitoring does not function with static metrics—interface cost (cost set in interface).

You must enable path monitoring for the interface and configure the monitoring type. The PBR policy page allows you to specify the desired metric for path determination. See Configure policy-based routing policy, on page 1166.

PBR and HTTP-based path monitoring

From management center version 7.4, PBR can be configured to use HTTP-based path monitoring to collect the performance metrics of the application domains and not just one destination IP address. Path monitoring begins only after a DNS entry for a domain is detected; it does not start immediately when HTTP-based application monitoring is configured. After obtaining the resolved IP address for the domain, path monitoring sends an HTTP request and receives a response. If DNS resolves multiple IP addresses for a domain, path monitoring probes and monitors the application using the first resolved IP address. Path monitoring continues until the IP address changes or until HTTP-based monitoring is disabled.

Based on the HTTP request and response durations, path monitoring computes the performance metrics for the application. Path monitoring sends collected metrics to PBR at regular intervals so that PBR can make routing and forwarding decisions for traffic from the configured ingress interface. If traffic arrives before path monitoring sends metrics to PBR, the routing table determines the traffic flow. Once metrics are available, PBR uses them to make routing decisions for subsequent traffic.

Note Based on the Network Service Groups in the match ACL of the policy, you can apply PBR for multiple domains having multiple IP addresses.

The management center associates applications and NSGs with the egress interface only when the PBR configuration meets these criteria:

- The match ACL contains the monitored applications.
- The PBR policy is configured with any one of the interface ordering values (metric type):
  - Minimal Jitter
  - Maximum Mean Opinion Score
  - Minimal Round-Trip Time
  - Minimal Packet Loss

Configure path monitoring settings

Configure path monitoring to collect metrics such as RTT, jitter, MOS, and packet loss on specified interfaces for effective traffic management and routing optimization.

The PBR policy relies on flexible metrics, such as round-trip time (RTT), jitter, mean opinion score (MOS), and packet loss of the interfaces to identify the best routing path for its traffic. Path monitoring collects these metrics on the specified interfaces. On the **Interfaces** page, you can configure path monitoring settings on interfaces to send ICMP probes or HTTP pings to collect metrics.

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** ( ) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** ( ) for the interface you want to edit.

Step 3 Click the **Path Monitoring** tab.

Step 4 To configure ICMP based monitoring of the interface, click the **Enable IP based Monitoring** check box.

Step 5 From the **Monitoring Type** drop-down list, select the relevant option:

- **Auto**—Sends ICMP probes to the IPv4 default gateway of the interface. If the IPv4 gateway does not exist, path monitoring sends the probes to the IPv6 default gateway of the interface.
- **Peer IPv4**—Sends ICMP probes to the specified peer IPv4 address (next-hop IP) for monitoring. If you select this option, enter the IPv4 address in the **Peer IP To Monitor** field.
- **Peer IPv6**—Sends ICMP probes to the specified peer IPv6 address (next-hop IP) for monitoring. If you select this option, enter the IPv6 address in the **Peer IP To Monitor** field.
- **Auto IPv4**—Sends ICMP probes to the default IPv4 gateway of the interface.
- **Auto IPv6**—Send ICMP probes to the default IPv6 gateway of the interface.

Note

- The Auto options are not available for VTI interfaces. You must specify the peer address.
- Only one next-hop is monitored to a destination. That is, you cannot specify more than one peer address to monitor for an interface.

Step 6 By default, the **Enable HTTP based Application Monitoring** check box is selected. All applications selected for path monitoring in the match ACL of the PBR policy are listed, provided this interface is configured as the egress interface in the policy. To disable the HTTP-based monitoring of the interface, clear the check box.

Step 7 Click **Ok**.

Step 8 To save the settings, click **Save**.

Path monitoring is configured on the interface with the specified settings. The system will collect metrics using ICMP probes or HTTP pings based on your configuration to optimize routing paths.

Add path monitoring dashboard

Add the Path Monitoring Dashboard to enable viewing path monitoring metrics with customizable display options through predefined correlations and widget management.

Procedure

Step 1 Choose **System** ( ) > **Health** > **Monitor**.

Step 2 Select the device, and click **Add new dashboard** ( ).

Step 3 Enter a name for the custom dashboard.

Step 4 In the **Metrics** area, click the **Add from predefined correlations** button.

Step 5 From the list, click **Interface - Path metrics**.

By default, all four metrics and an additional metric field are selected to display as widgets in the dashboard.

To exclude any, click **Delete** ( ).

Step 6 Click **Add dashboard**.

Configure policy-based routing policy

This task enables you to configure Policy-Based Routing (PBR) to control traffic routing based on specific criteria rather than relying solely on the routing table.

You can configure the PBR policy on the Policy Based Routing page by specifying the ingress interfaces, match criteria (Extended Access Control List), and egress interfaces.

Before you begin

To use the path monitoring metrics for configuring the traffic forwarding priority over egress interfaces, you must configure the path monitoring settings for the interfaces. See Configure path monitoring settings, on page 1165.

Follow these steps to configure policy-based routing policy:

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Click **Routing**.

Step 3 Click **Policy Based Routing**.

On the Policy Based Routing page, you can view the configured policy. The grid shows ingress interfaces and the combination of the policy-based route access list and egress interfaces.

Step 4 To configure the policy, click **Add**.

Step 5 In the **Add Policy Based Route** dialog box, select the **Ingress Interface** from the drop-down list.

Note You can only select interfaces with logical names that belong to a global virtual router from the drop-down list. You cannot configure a VLAN interface with a logical name as the source (ingress) interface.

Step 6 To specify the match criteria and the forward action in the policy, click **Add**.

Step 7 In the **Add Forwarding Actions** dialog box, do the following:

a) From the **Match ACL** drop-down, choose the extended access control list object. You can predefine the ACL object (see Configure an extended ACL object, on page 2351) or click the **Add** (+) icon to create the object. In the **New Extended Access List Object** box, enter a name, click **Add** to open the **Add Extended Access List Entry** dialog box, where you can define the network, port, user identity, SGT, or application match criteria for the PBR policy.

Note You can either have destination address or application/user identity/SGT defined in an ACE.

To selectively apply PBR on the incoming interface, you can define *Block* criteria in the ACE. When the traffic matches the block rule of the ACE, the traffic is forwarded to the egress interface based on the routing table.

b) From the **Send To** drop-down list:

- To select the configured interfaces, choose **Egress Interfaces**.
- To specify the IPv4/IPv6 next hop addresses, choose **IP Address**. Proceed to Step 7.e, on page 1168

c) If you have selected **Egress Interfaces**, from the **Interface Ordering** drop-down, choose the relevant option:

- By **Interface Priority**—The traffic is forwarded based on the priority of the interfaces. Traffic is routed to the interface with the least priority value first. When the interface is not available, the traffic

is then forwarded to the interface with the next lowest priority value. For example, let us assume that interface1, interface2, and interface3 are configured with priority values *0*,*1*, and *2*, respectively. The traffic is forwarded to interface1. If interface1 becomes unavailable, the traffic is then forwarded to interface2.

Note To configure the priority for the interfaces, click **Configure Interface Priority** on the Policy Based Routing page. In the dialog box, provide the priority number against the interfaces, and then click **Save**. You can also configure the priority for an interface in the Interface Settings.

When the priority value is the same for all the interfaces, the traffic is balanced among the interfaces. By default, the interface priority for PBR is set to 0. Interfaces with the lowest priority value are preferred for traffic forwarding.

- By **Order**—The traffic is forwarded based on the sequence of the interfaces specified here. For example, let us assume that interface1, interface2, and interface3 are selected in this order, interface2, interface3, interface1. The traffic is forwarded first to interface2, then to interface3, regardless of their priority values.
- By **Minimal Jitter**—The traffic is forwarded to the interface that has the lowest jitter value. You need to enable Path Monitoring on the interfaces for PBR to obtain the jitter values.
- By **Maximum Mean Opinion Score**—The traffic is forwarded to the interface that has the maximum mean opinion score (MOS). You need to enable Path Monitoring on the interfaces for PBR to obtain the MOS values.
- By **Minimal Round Trip Time**—The traffic is forwarded to the interface that has the minimal round trip time (RTT). You need to enable Path Monitoring on the interfaces for PBR to obtain the RTT values.
- By **Minimal Packet Loss**—The traffic is forwarded to the interface that has the minimal packet loss. You need to enable Path Monitoring on the interfaces for PBR to obtain the packet loss values.

d) In the **Available Interfaces** box, all the interfaces with their priority values are listed. From the list of interfaces, click the **Add** (+) button to add to the selected egress interfaces. Proceed to Step 8.

Note The selected interface route must be present in the routing table.

e) If you have selected **IP Address**, enter the IP addresses separated by commas in the **IPv4 Addresses** or **IPv6 Addresses** fields. The traffic is forwarded as per the sequence of the specified IP addresses.

Note When multiple next-hop IP addresses are provided, the traffic is forwarded as per the sequence of the specified IP addresses until a valid routable next-hop IP address is found. The configured next-hops should be directly connected.

f) From the **Don't Fragment** drop-down list, select Yes, No, or None. If the DF (Don't Fragment) flag is set to *Yes*, the intermediate routers never perform fragmentation of a packet.To specify the current interface as the default for forwarding, check the **Default Interface** check box.

g) The **IPv4 Settings** and **IPv6 Settings** tabs enable you to specify the recursive and default settings:



Note For a route-map, you can only specify either IPv4 or IPv6 next-hop settings.

- **Recursive**—The route map configuration is applied only when the specified next-hop address and the default next-hop address are found on a directly connected subnet. However, you could use the recursive option, where the next-hop address need not be directly connected. Here, a recursive lookup is performed on the next-hop address, and matching traffic is forwarded to the next-hop used by that route entry according to the current routing path of the router.
- **Default**—If the normal route lookup fails to match traffic, the traffic is forwarded to this specified next-hop IP address.

h) Check the **Peer Address** check box to use the next-hop address as the peer address.



Note You cannot configure a route map with both default next-hop address and peer address.

i) For IPv4 settings, you can check whether the next IPv4 hops of a route map are available under **Verify Availability**—click the **Add** (+) button and add the next-hop IP address entries:

- **IP Address**—Enter the next hop IP address.
- **Sequence**—Entries are assessed in order using the sequence number. Ensure that no duplicate sequence numbers are entered. The valid range is 1 to 65535.
- **Track**—Enter a valid ID. The valid range is 1 to 255.

Step 8 To save the policy, click **Save** and **Deploy**.

The Firewall Threat Defense uses ACLs to match traffic and perform routing actions on the traffic. Typically, you configure a route map that specifies an ACL against which traffic is matched, and then you specify one or more actions for that traffic. With the use of path monitoring, PBR can now select the best egress interface for routing the traffic. Finally, you associate the route map with an interface on which you want to apply PBR on all incoming traffic.

Configure policy-based routing

Configure PBR to enable direct internet access for specific web-based applications, optimize traffic flow, and achieve load balancing between WAN and VTI interfaces.

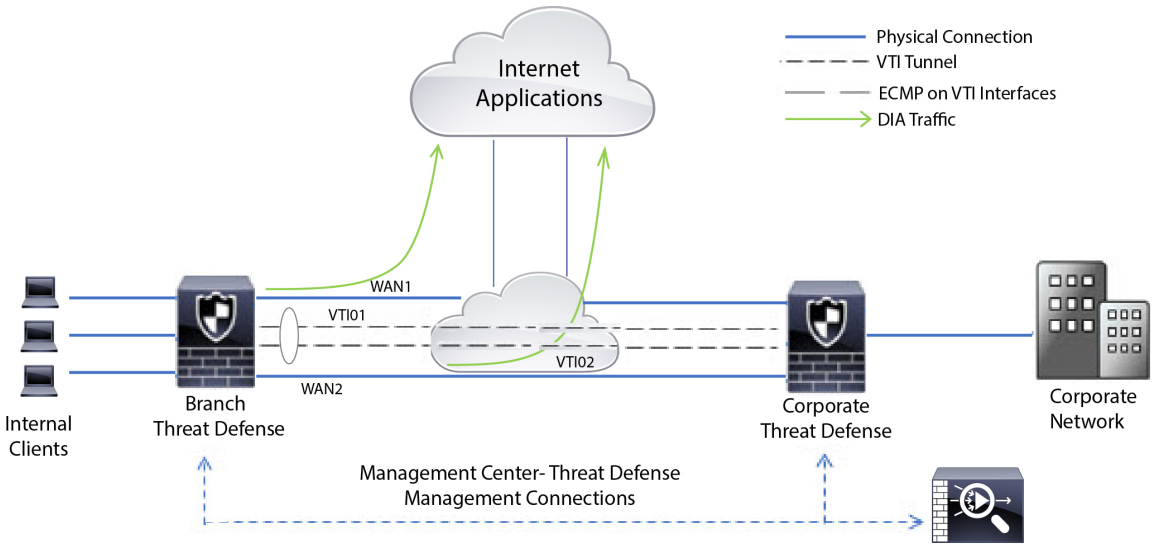
Consider a typical corporate network scenario where all the branch network traffic passes through a route-based VPN of the corporate network and diverges to the extranet, when required. Accessing web-based applications

through the corporate network to support daily operations may increase network size and maintenance costs. This example illustrates how to configure PBR for direct internet access.

The following figure depicts the topology of a corporate network. The branch network is connected to the corporate network through a route-based VPN. Traditionally, the corporate Firewall Threat Defense is configured to handle both the internal and external traffic of the branch office. With the PBR policy, the branch Firewall Threat Defense is configured with a policy that routes specific traffic to the WAN network instead of the virtual tunnels. The rest of the traffic flows through the route-based VPN, as usual.

This example also illustrates how to configure the WAN and VTI interfaces with ECMP zones to achieve load balancing.

Figure 363: Configuring policy-based routing on Branch Firewall Threat Defense in Firewall Management Center



Before you begin

This example assumes that you have already configured WAN and VTI interfaces for the branch Firewall Threat Defense in Firewall Management Center.

Procedure

Step 1 Configure policy-based routing for the branch Firewall Threat Defense, select the ingress interfaces:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

b) Choose **Routing** > **Policy Based Routing**, and on the **Policy Based Routing** page, click **Add**.

c) In the **Add Policy Based Route** dialog box, select the interfaces (say, *Inside 1*, and *Inside 2*) from the **Ingress Interface** drop-down list.

Step 2 Specify the match criteria:

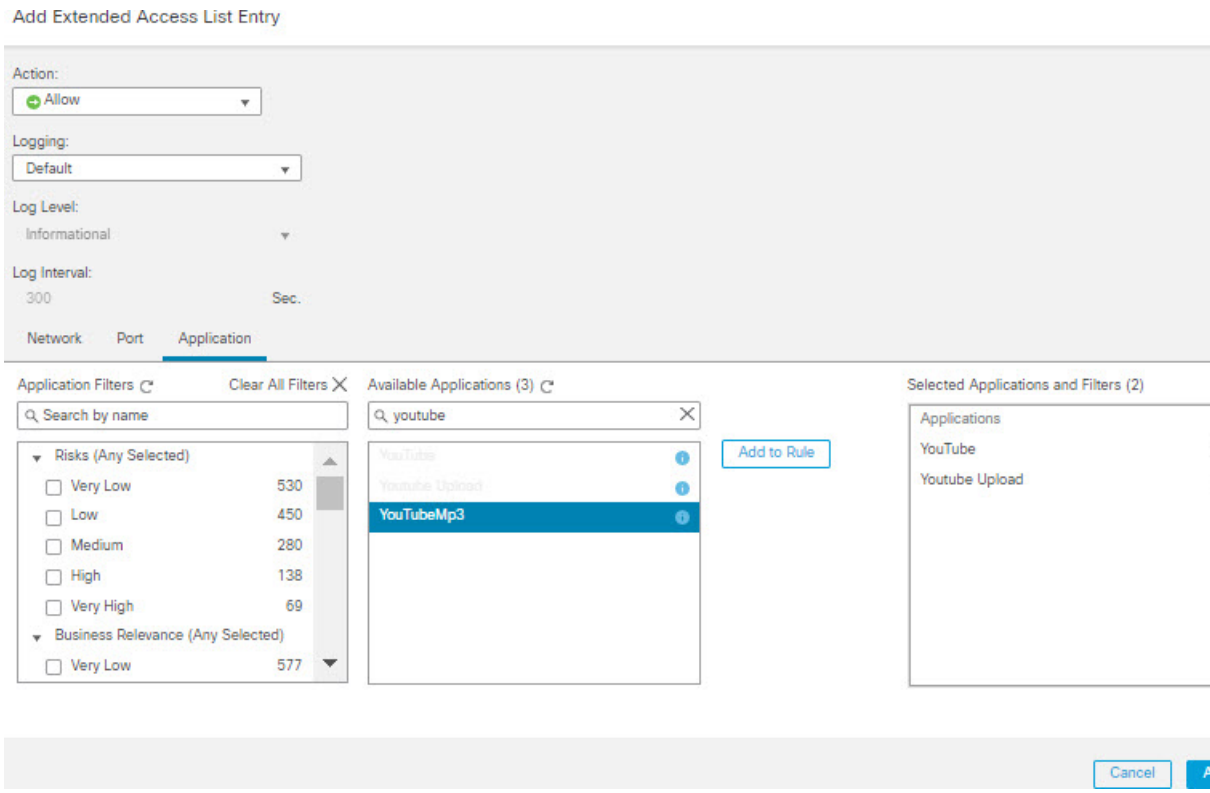
a) Click **Add**.

b) To define the match criteria, click the **Add** (+) button.

c) In **New Extended Access List Object**, enter the name for the ACL (say, *DIA-FTD-Branch*), and click **Add**.

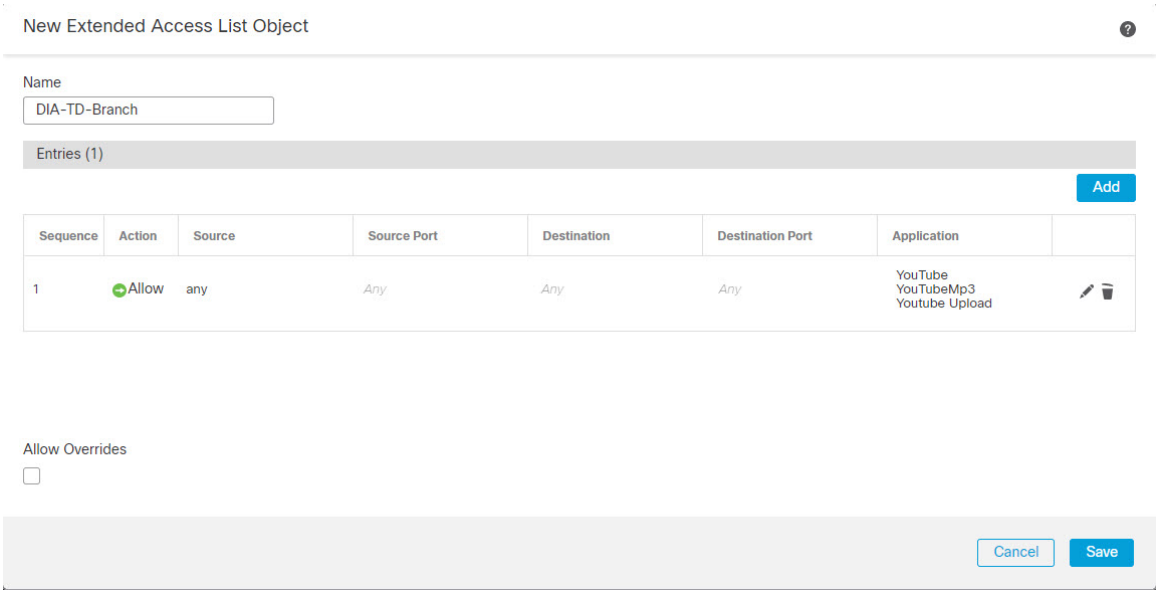
d) In the **Add Extended Access List Entry** dialog box, choose the required web-based applications from the **Application** tab:

Figure 364: Applications tab



On the Firewall Threat Defense, the application group in an ACL is configured as a network service group and each of the applications as a network service object.

Figure 365: Extended ACL



e) Click **Save**.

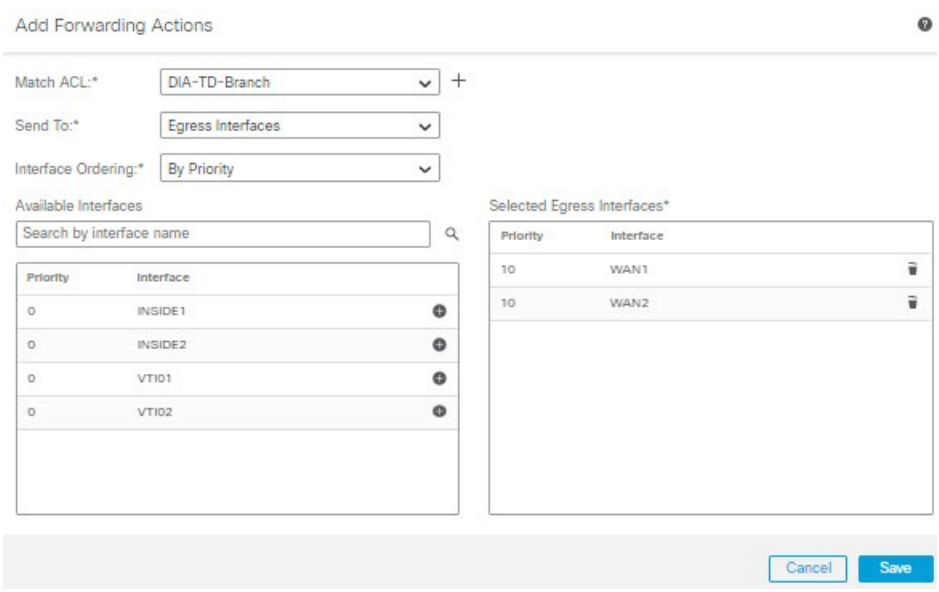
f) Select *DIA-FTD-Branch* from the **Match ACL** drop-down list.

Step 3 Specify the egress interfaces:

a) From the **Send To** and **Interface Ordering** drop-down lists, choose Egress Interfaces, and Interface Priority respectively.

b) Under **Available Interfaces**, click the ⊕ button against the respective interface names to add *WAN1* and *WAN2*:

Figure 366: Configuring policy-based routing



c) Click **Save**.

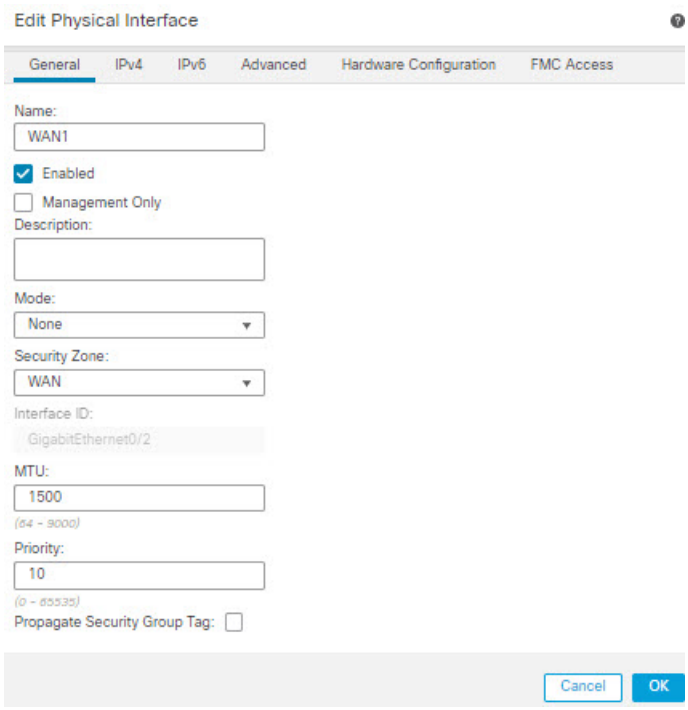
Step 4 Configure interface priority:

You can set the priority value for the interfaces either in the **Edit Physical Interface** page, or in the **Policy Based Routing** page (**Configure Interface Priority**). In this example, the Edit Physical Interface method is described.

a) Choose **Devices** > **Device Management**, and edit the branch Firewall Threat Defense.

b) Set the priority for the interfaces. Click **Edit** against the interface and enter the priority value:

Figure 367: Setting interface priority



c) Click **Ok** and **Save**.

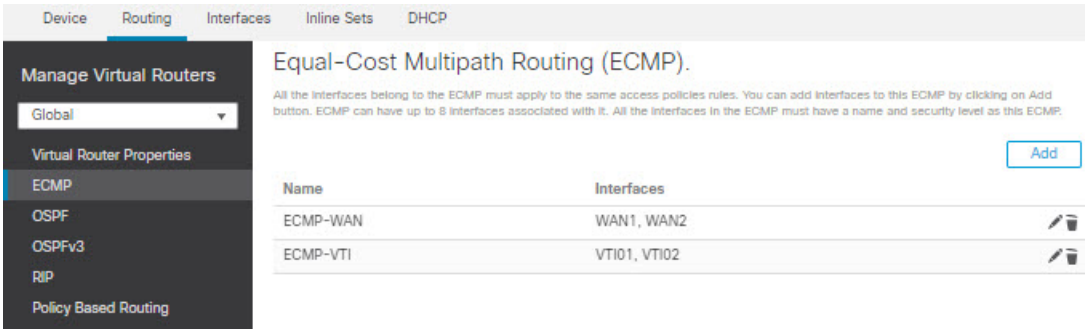
Step 5 Create ECMP zones for load balancing:

a) In the **Routing** page, click **ECMP**.

b) To associate interfaces to the ECMP zone, click **Add**.

c) Select *WAN1* and *WAN 2* and create an ECMP zone—*ECMP-WAN*. Similarly, add *VTI01* and *VTI02* and create an ECMP zone—*ECMP-VTI*:

Figure 368: Associating interfaces with ECMP zone

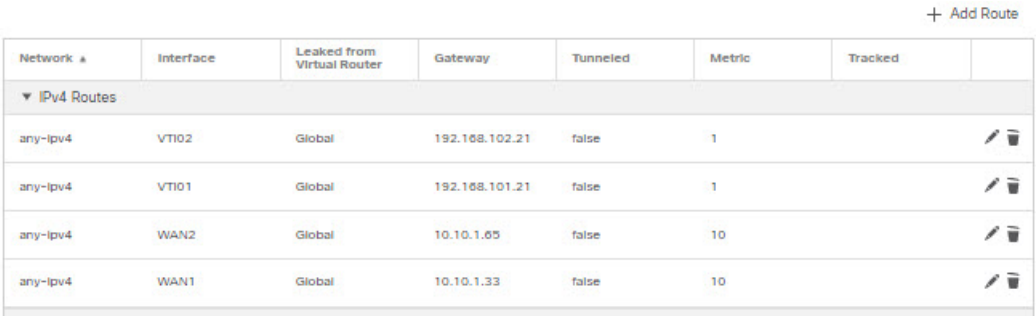


Step 6 Configure static routes for the zone interfaces for load balancing:

a) In the **Routing** page, click **Static Route**.

b) Click **Add** and specify the static routes for *WAN1*, *WAN2*, *VTI01*, and *VTI02*. Ensure that you specify the same metric value for the interfaces belonging to the same ECMP zones (Step 5):

Figure 369: Configuring static routes for ECMP zone interfaces



Note Ensure that the zone interfaces have the same destination address and metric, but different gateway addresses.

Step 7 Configure trusted DNS on the WAN objects of the branch Firewall Threat Defense to ensure secure flow of traffic to the internet:

a) Choose **Devices** > **Platform Settings**, and create a DNS policy on the branch Firewall Threat Defense.

b) To specify the trusted DNS, edit the policy and click **DNS**.

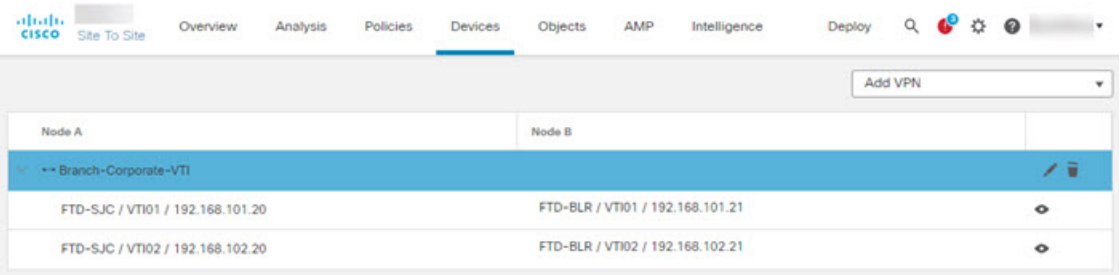
c) To specify the DNS servers for the DNS resolution to be used by WAN objects, in the **DNS Settings** tab, provide the DNS server group details and select WAN from the interface objects.

d) Use the **Trusted DNS Servers** tab to provide specific DNS servers that you trust for the DNS resolution.

Step 8 Click **Save**, and then click **Deploy**.

Any *YouTube* related access requests from the branch inside network *INSIDE1* or *INSIDE2* are routed to *WAN1* or *WAN2* as they would match the *DIA-FTD-Branch* ACL. Any other request, say *google.com*, are routed through *VTI01* or *VTI02* as configured in the Site to Site VPN Settings.

Figure 370: Site to site VPN settings



With the ECMP configured, the network traffic is seamlessly balanced.

Configure PBR with path monitoring

Configure PBR with path monitoring to optimize application traffic routing by dynamically selecting the best egress interface based on performance metrics such as jitter, round-trip time, and packet loss.

This example describes how to configure PBR with path monitoring for the following applications with flexible metrics:

- Audio or video sensitive applications (example, WebEx Meetings) with Jitter.
- Cloud-based application (example, Office365) with RTT.
- Network-based access control (with a specific source and destination) with packet loss.

Before you begin

1. This example assumes that you are aware of the basic configuration steps for PBR.
2. You have configured ingress and egress interfaces with logical names. In this example, the ingress interface is named *Inside1*, and egress interfaces are named *ISP01*, *ISP02*, and *ISP03*.

Follow these steps to configure PBR with path monitoring:

Procedure

Step 1 Path monitoring configuration on interfaces *ISP01*, *ISP02*, and *ISP03*:

For the metrics collection on the egress interfaces, you must enable and configure path monitoring on them.

a) Choose **Devices** > **Device Management**, and edit Firewall Threat Defense.
b) Under the **Interfaces** tab, edit the interface (in our example, *ISP01*)
c) Click the **Path Monitoring** tab, select the **Enable Path Monitoring** check box, and then specify the monitoring type (see Configure path monitoring settings, on page 1165).
d) Click **Ok** and **Save**.
e) Repeat these steps to configure the path monitoring settings for *ISP02* and *ISP03*.

Step 2 Configure policy-based routing for a branch in an organization Firewall Threat Defense, select the ingress interfaces:

a) Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.
b) Choose **Routing** > **Policy Based Routing**, and on the **Policy Based Routing** page, click **Add**.
c) In the **Add Policy Based Route** dialog box, select *Inside 1* from the **Ingress Interface** drop-down list.

Step 3 Specify the match criteria:

a) Click **Add**.
b) To define the match criteria, click the **Add** (+) button.
c) In **New Extended Access List Object**, enter the name for the ACL (example, *PBR-WebEx*), and click **Add**.
d) In the **Add Extended Access List Entry** dialog box, choose the necessary web-based applications, such as WebEx Meetings) from the **Application** tab.

Remember On Firewall Threat Defense, the application group in an ACL is configured as a network service group and each of the applications as a network service object.

e) Click **Save**.
f) Select *PBR-WebEx* from the **Match ACL** drop-down list.

Step 4 Specify the egress interfaces:

a) From the **Send To** drop-down list, choose Egress Interfaces.
b) From the **Interface Ordering** drop-down list, choose By Minimal Jitter.
c) Under **Available Interfaces**, click the **Right Arrow** (>)button against the respective interface names to add *ISP01*, *ISP02*, and *ISP03*.
d) Click **Save**.

Step 5 Repeat Step 2 and Step 3 to create PBRs for the *Inside1* interface to route Office365 and network-based access control traffic:

a) Create a match criteria object, example *PBR-Office365*, and select the Office365 application from the **Application** tab.
b) From the **Interface Ordering** drop-down list, choose By Minimal Round Trip Time.
c) Specify the egress interfaces *ISP01*, *ISP02*, and *ISP03*, and click **Save**.
d) Now, create a match criteria object, example *PBR-networks*, and specify the source and destination interface in the **Network** tab.
e) From the **Interface Ordering** drop-down list, choose By Minimal Packet Loss.
f) Specify the egress interfaces *ISP01*, *ISP02*, and *ISP03*, and click **Save**.

Step 6 Click **Save**, and then click **Deploy**.

Step 7 To view path monitoring metrics, Choose **Devices** > **Device Management**, and from **More** (⋮) click **Health Monitor**. To view the metric details for the interfaces of the device, you must add the path metrics dashboard. For details, see Add path monitoring dashboard, on page 1166.

The WebEx, Office365, and networks-based ACL traffic are forwarded through the best route derived from the metrics value collected on *ISP01*, *ISP02*, and *ISP03*.

Useful CLIs for monitoring PBR

Run the monitoring commands described in this topic from the Firewall Threat Defense device CLI.

Interface configurations

To view the interface configurations of the device, run the `show run interface` command:

```
> show run interface
!
interface Ethernetl/l
 description Outside ispl handoff
 nameif outside1
 security-level 0
 zone-member ECMP-WAN
 ip address dhcp setroute
 policy-route cost 10
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
interface Ethernet1/2
 description Outside isp2 handoff
 nameif outside2
 security-level 0
 zone-member ECMP-WAN
 ip address 192.133.243.240 255.255.255.192
 policy-route cost 20
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
```

DNS configurations

Application-based routing only uses trusted DNS servers to resolve domains. To view the DNS configurations of the device, run the `show run DNS` command:

```
> show run dns
DNS server-group DefaultDNS
dns trusted-source 10.100.0.5
dns trusted-source 10.200.0.5
```

Route map configurations

When you configure PBR on the device, the Management Center auto-generates the route-map and applies it to the specified ingress interface. To view the route maps of the device, run the `show run route-map` command:

```
> show run route-map
!
route-map FMC_VPN_CONNECTED_DIST_RMAP_1000 permit 10
 match interface inside-employee
 set community 1000
!
route-map FMC GENERATED PBR 1729024850865 permit 5
 match ip address Cloud-storage-apps-acl
  set adaptive-intertace cost outside1 outside2
```

```
!
route-map FMC_GENERATED PBR 1729024850865 permit 10
match ip address Social-media-apps-acl
set adaptive-interface rtt outside1 outside2

!
route-map FMC GENERATED PBR 1729024850865 permit 15
match ip address Conferencing-apps-acl
set adaptive-interface jitter outside1 outside2

!
route-map FMC_GENERATED_PBR_1729024850865 permit 20
match ip address Corp-internal-apps-acl
set adaptive-interface cost outside1_static_vti_1 outside2_static_vti_4
```

Access lists and network service groups configurations

The route-map applied to the ingress interface can reference an extended access control list. To view the details of an access list for PBR, run the `show run access list <access list_name>` command:

```
> show run access-list Cloud-storage-apps-acl
access-list Cloud-storage-apps-acl extended permit ip any object-group-network-service
FMC_NSG_4295470562
```

The network-service objects and object-groups are configured in extended access control lists and referenced in policy-based routing route maps and access control groups. To view the NSG configurations, run the `show object-group network-service <network-service-groups-name>` command. The *network-service-groups-name* is derived from the above show command for an access list.

```
> show object-group network-service FMC_NSG_4295470562
 object-group network-servire FMC_NSG_4295470562 (id=@xfdff0000)
 network-service-member "Box" dynamic
 description File storage and transfer site.
 app-id 1326
 domain box.com (bid=436735707) ip (hitcnt=0)
 domain boxcloud.com (bid=436924171) ip (hitcnt=0)
 domain box.net (bid=437080553) ip (hitcnt=0)
 domain box.org (bid=437174273) ip (hitcnt=0)
 domain boxcdn.net (bid=437272231) ip (hitcnt=0)
 domain boxrelay.com (bid=437481703) ip (hitcnt=0)
 domain boxenterprise.net (bid=437626005) ip {hitcnt=0)
 domain boxinvestorrelations.com (bid=437672765) ip (hitcnt=0)
 domain segment-box.com (bid=437886771) ip (hitcnt=0)
 domain box-corp.com (bid=437924995) ip (hitcnt=0)
 domain boxcn.net (bid=438072833) ip (hitcnt=0)
network-service-member "Dropbox" dynamic
 description Cloud based tile storage.
 app-id 125
 domain dropbox.com (bid=24259639) ip (hitcnt=0)
 domain cfl.dropboxstatic.com (bid=24495525) ip (hitcnt=0)
 domain dl.dropboxusercontent.com (bid=24596237) ip (hitcnt=0)
 domain dropboxapi.com (bid=24694467) ip (hitcnt=0)
 domain dropboxbusiness.com (bid=24859859) ip (hitcnt=0)
 domain dropboxcaptcha.com (bid=25008145) ip {hitcnt=0)
 domain dropbox-dns.com (bid=25087753) ip (hitcnt=0)
 domain dropboxer.net (bid=25236751) ip (hitcnt=0)
 domain dropboxusercontent.com (bid=25324335) ip (hitcnt=0)
 domain getdropbox.com (bid=25437501) ip (hitcnt=0)
 domain cloudon.com (bid=25580229) ip (hitcnt=0)
```

Path monitoring configurations

To view the path monitoring metrics collected on the egress interface, run the `show path-monitor` command:

```
> show path-monitor
Interface: outside2 (Ethernetl/2)
Remote peer: 8.8.8.8
    Remote peer reachable: Yes
    RTT average: 9138 microsecondes) Jitter: 1093 microsecond(s)
    Packet loss: 0% MOS: 4.39
    Last updated: 12 second(s) ago
Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470581
    Network Service: Facebook Domain name: fbsbx.com Remote peer reachable: Yes
    RTT average: 17460 microsecond(s) Jitter: 911 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago

    Network Service: Facebook
    Domain name: facebook.net
    Remote peer reachable: Yes
    RTT average: 17444 microsecondes)
    Jitter: 836 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago

    Network Service: Instagram
    Domain name: instagram.com Remote peer reachable: Yes
    RTT average: 17576 microsecondes)
    Jitter: 429 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 secondes) ago

Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470600
    Network Service: WebEx
    Domain name: webex.com Remote peer reachable: Yes RTT average: 18537 microsecond(s)
Jitter: 318 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
    Network Service: Zoom Domain name: zoom.com Remote peer reachable: Yes
    RTT average: 98196 microsecond(s) Jitter: 4120 microseconde)
    Packet loss: 0%
    MOS: 4.34
    Last updated: 12 second(s) ago
```

Troubleshoot PBR

This task helps you debug PBR configuration when packets get dropped by verifying routes, monitoring metrics, and validating interface selection.

When PBR is not working as intended, you need to systematically verify the configuration components including route maps, path monitoring, and interface selection to identify the root cause of packet drops.

Before you begin

Follow these steps to troubleshoot PBR configuration when packets get dropped:

Procedure

Step 1 Check that all essential routes for recursive resolution are present by using the show route or show ipv6 route commands in the appropriate tables.

Unless the route map for the interfaces participating in PBR is updated with correct routes, PBR will not work as intended.

Step 2 Display the remote address that path-monitoring uses to monitor metrics by using the **show running-config interface** command.

Example:

```
interface GigabitEthernet0/0
nameif outside_0
security-level 0
zone-member ecmp-zone
ip address 20.0.0.3 255.255.255.0 -> This is egress interface "show running-config" output,
 the monitored address and cost metric value is determined in this output.
policy-route cost 1
policy-route path-monitoring
20.0.0.4
!
int GigabitEthernet 0/3
!
interface GigabitEthernet0/3
nameif outside_3
security-level 0
ip address 11.1.1.2 255.255.255.0 -> This is ingress interface "show running-config" output,
 the specific route-map will be used by PBR to determine the next route.
policy-route route-map rtt-tes
```

This command shows the monitored address and cost metric values for path monitoring by sending ICMP packets or HTTP pings.

Step 3 Examine the **show path-monitoring** and **show run route-map** outputs for packet loss.

Example:

```
ciscoasa(config)# show path-monitoring
Interface: outside_0  -> The remote address used for ICMP monitoring
Remote peer: 20.0.0.4
Version: 6223
Remote peer reachable: Yes -> If this value turns "No", then the ICMPv4/v6 packet is not
reaching the required remote address.
RTT average: 1920 microsecond(s)
Jitter: 394 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago -> The data should be updated by path monitoring after every
 30 seconds. The 'show route-map' would show the
updated metric values.
Interface: outside_2
Remote peer: 40.0.0.4
Version: 6223
Remote peer reachable: Yes
RTT average: 1935 microsecond(s)
Jitter: 433 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago
```

Example:

```
ciscoasa(config)# show route-map
route-map rtt-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface rtt outside_0 (1920) outside_2 (1935) outside_1 (1971) -> Displays the
metric type (rtt) that is used by the policy route to select the adequate interface to send
 the packet. The interface list where cost of each interface is given. As the metric type
is "rtt" and considering the minimum rtt value, the "outside_0" interface route will be
selected by PBR.
route-map mos-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface mos outside_0 (378) outside_1 (390) outside_2 (440) - > As the metric
type is "mos", considering the maximum value of mos, the "outside_2" interface will be
selected by PBR.
```

The metric types (lost, rtt, jitter, cost) should select the interface with the minimum metric value for routing.

The metric type "mos" should select the interface with the maximum metric value for routing.

Step 4 Use **packet-tracer** command to validate the interface selection based on the metric type defined in the PBR.

Example:

```
packet-tracer input <interface> icmp <src ip address> 8 0 <dst ip
address> detailed
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 60656 ns
Config:
route-map rtt-test permit 10
match ip address allow_101_1_1_2
set adaptive-interface rtt outside_0 outside_2
Additional Information:
Matched route-map rtt-test, sequence 10, permit
Found next-hop 40.0.0.4 using egress ifc outside_2 -> PBR selects the adequate interface
from adaptiveinterface list given in "rtt-test" route-map.
```

Step 5 Use the **packet-tracer** command similar to the **debug policy-route** command.

When PBR successfully selects the route, the packet tracer output looks like this:

```
pbr: policy based route lookup called for 101.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 20.0.0.4
```

When PBR is not able to find the adequate route, it falls back to normal route lookup, and the packet tracer output looks like this:

```
pbr: policy based route lookup called for 100.1.1.1/0 to 100.1.1.2/0 proto 1 sub_proto 8
received on interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map mos-test, sequence 10, permit; proceed with policy routing
pbr: no route to 100.1.1.2 on adaptive-interface outside_2
pbr: no route to 100.1.1.2 on adaptive-interface outside_1
pbr: no route to 100.1.1.2 on adaptive-interface outside_0
pbr: policy based routing could not be applied; proceeding with normal route lookup
```

When a monitored remote address goes down, and path monitoring marks **Remote peer reachable** as **No** for that address, the PBR displays the a log that excludes the interface from adaptive-interface list.

```
pbr: policy based route lookup called for 100.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: Path Monitoring Ifc Down : adaptive-interface outside_1 Excluded from PBR routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 40.0.0.4
```

Note The interface becomes eligible for adaptive PBR routing when the interface is reported as reachable in the path monitoring module.

History for policy-based routing

This reference provides a comprehensive history table that summarizes the introduction and evolution of policy-based routing features in Cisco Secure Firewall Management Center across releases, enabling quick tracking of feature availability and changes.

Table 72: History table

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Identity and SGT based PBR Policy	7.4.0	7.4.0	You can now classify the network traffic based on users and user groups, and SGTs in PBR policies. You can select the identity and SGT objects while defining the extended ACLs for the PBR policies. New/modified screens: New tabs added in the extended access list object for configuring the policy-based routing policy: **Objects** > **Object Management** > **Access Control Lists** > **Add Extended** page, **Users** and **Security Group Tag**.
HTTP based Path Monitoring	7.4.0	7.2.0	PBR can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and desired metric type for path determination. New/modified screens: New option in Interfaces page for enabling path monitoring: **Devices** > **Device Management** > **Edit Interfaces** > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box.

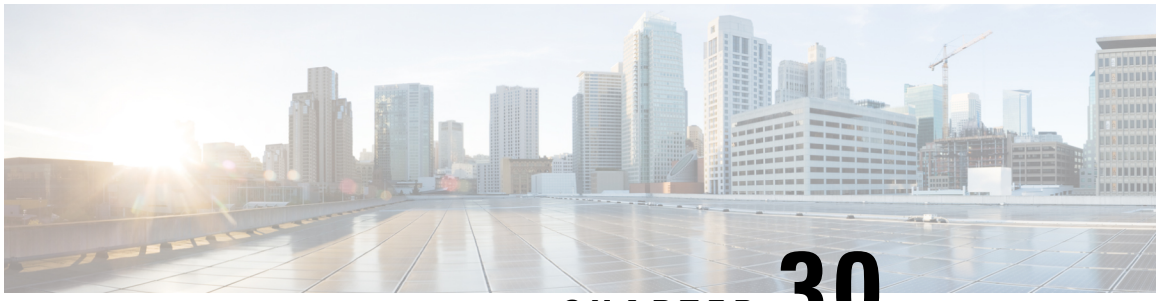
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dual WAN/ISP Threat Defense Management Support	7.3.0	7.3.0	On a dual WAN-enabled threat defense, a single data interface was configured to communicate with the management center. Now, support to configure a secondary data interface is provided so that the communication channel is sustained when the primary data interface fails. The management center automatically configures PBR to route the SF-Tunnel traffic from the *tapnlp* (internal) interface to one of the available data interfaces based on the priority and SLA metric.
Next-hop settings for PBR route map	7.3.0	7.1.0	You can configure the next-hops for the PBR route-map while enabling packet forwarding actions. New/modified screens: New fields in Add/Edit Forwarding Actions page for configuring egress interfaces: **Device Management** > **Routing** > **Policy Based Routing** > **Add Forwarding Actions** page.
PBR and Path Monitoring	7.2.0	7.2.0	PBR uses path monitoring to collect the performance metrics (RTT, jitter, packet-lost, and MOS) of the egress interfaces. You must enable path monitoring for the interface and configure the monitoring type. You can configure a PBR policy with the desired metric for path determination. New/modified screens: New tab in Interfaces page for enabling path monitoring: **Devices** > **Device Management** > **Edit Interfaces** > **Path Monitoring** tab.
Configure policy based routing from the FMC web interface.	7.1.0	7.1.0	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now configure policy based routing (PBR) from the FMC web interface. This allows you to classify network traffic based on applications and to implement direct internet access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy. This feature requires Version 7.1+ on both the FMC and the device. When you upgrade the FMC to Version 7.1+, existing policy based routing FlexConfigs are removed. After you upgrade your devices to Version 7.1+, redo your policy based routing configurations in the FMC web interface. For devices that you do not upgrade to Version 7.1+, redo the FlexConfigs and configure them to deploy "every time." New/modified screens: **Devices** > **Device Management** > **Routing** > **Policy Based Routing**



PART V

Network Policies

- Network Address Translation, on page 1187
- Quality of Service, on page 1313



CHAPTER 30

Network Address Translation

The following topics explain Network Address Translation (NAT) and how to configure it on Firewall Threat Defense devices.

- NAT functions, on page 1187
- NAT basics, on page 1188
- Requirements and prerequisites for NAT policies, on page 1197
- Guidelines for NAT, on page 1197
- Manage NAT policies, on page 1203
- Configure NAT for threat defense, on page 1205
- Translating IPv6 networks, on page 1245
- Monitoring NAT, on page 1258
- Examples for NAT, on page 1259
- History for Firewall Threat Defense NAT, on page 1310

NAT functions

NAT enables private IP networks to connect to the Internet by replacing private IP addresses with public IP addresses. It conserves public addresses by advertising at minimum only one public address for the entire network to the outside world.

Private IP address ranges

Most devices within an IP network are assigned private IP addresses, which are not routable outside the company network due to the shortage of public IPv4 addresses. RFC 1918 defines the private IP address ranges that should not be advertised externally:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the primary functions of NAT is to enable private IP networks to access the Internet by translating private IP addresses into legal, routable public addresses. This approach conserves public IP addresses since NAT can be configured to advertise only a single public address for the entire network.

Other functions of NAT include:

- Security: Hides internal IP addresses, discouraging direct attacks.
- IP routing solutions: Handles overlapping IP addresses without conflict.
- Flexibility: Allows internal IP addressing schemes to change without affecting externally visible public addresses.
- Translating between IPv4 and IPv6 (Routed mode only): Supports translating between IPv4 and IPv6, enabling interoperability between different network types.

Note NAT is optional. If NAT is not configured for specific traffic, that traffic will not be translated but will still be subject to normal security policies.

NAT basics

The following topics explain some of the basics of NAT.

NAT terminology

This document uses the following terminology:

- Real address/host/network/interface—The real address is the address that is defined on the host, before it is translated. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the inside network would be the “real” network. Note that you can translate any network connected to the device, not just an inside network. Therefore if you configure NAT to translate outside addresses, “real” can refer to the outside network when it accesses the inside network.
- Mapped address/host/network/interface—The mapped address is the address that the real address is translated to. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the outside network would be the “mapped” network.

Note During address translation, IP addresses configured for the device interfaces are not translated.

- Bidirectional initiation—Static NAT allows connections to be initiated *bidirectionally*, meaning both to the host and from the host.
- Source and destination NAT—For any given packet, both the source and destination IP addresses are compared to the NAT rules, and one or both can be translated/untranslated. For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address.

NAT types

You can implement NAT using the following methods:

- Dynamic NAT—A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses, on a first come, first served basis. Only the real host can initiate traffic. See Dynamic NAT, on page 1210.
- Dynamic Port Address Translation (PAT)—A group of real IP addresses are mapped to a single IP address using a unique source port of that IP address. See Dynamic PAT, on page 1216.
- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See Static NAT, on page 1226.
- Identity NAT—A real address is statically translated to itself, essentially bypassing NAT. You might want to configure NAT this way when you want to translate a large group of addresses, but then want to exempt a smaller subset of addresses. See Identity NAT, on page 1235.

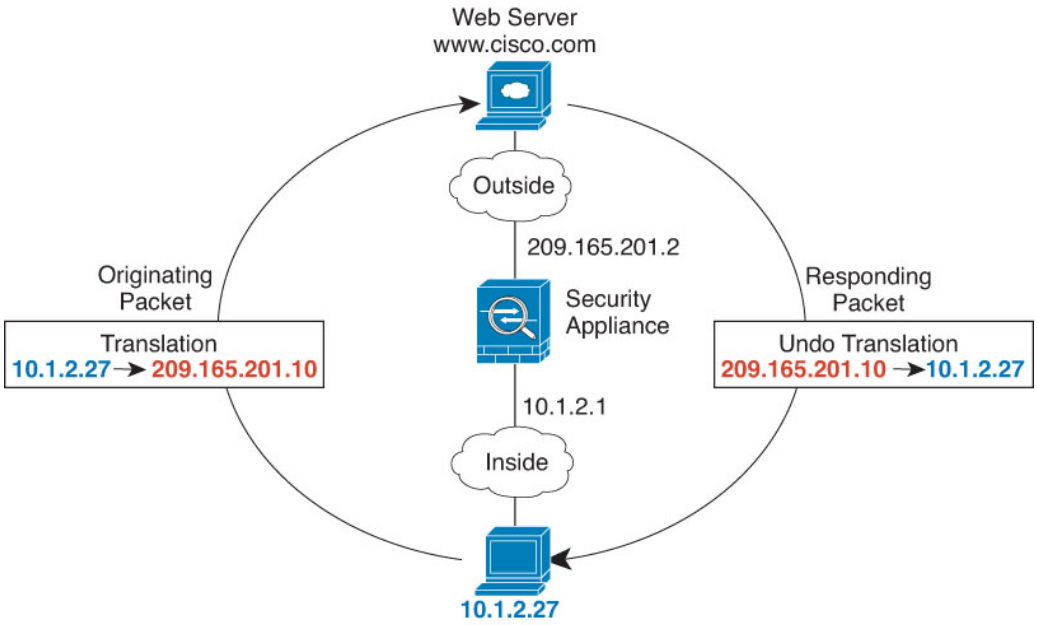
NAT in routed and transparent mode

You can configure NAT in both routed and transparent firewall mode. You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes. The following sections describe typical usage for each firewall mode.

NAT in routed mode

The following figure shows a typical NAT example in routed mode, with a private network on the inside.

Figure 371: NAT Example: Routed Mode



1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is translated to a mapped address, 209.165.201.10.
2. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the Firewall Threat Defense receives the packet because the Firewall Threat Defense performs proxy ARP to claim the packet.

3. The Firewall Threat Defense then changes the translation of the mapped address, 209.165.201.10, back to the real address, 10.1.2.27, before sending it to the host.

NAT in transparent mode or within a bridge group

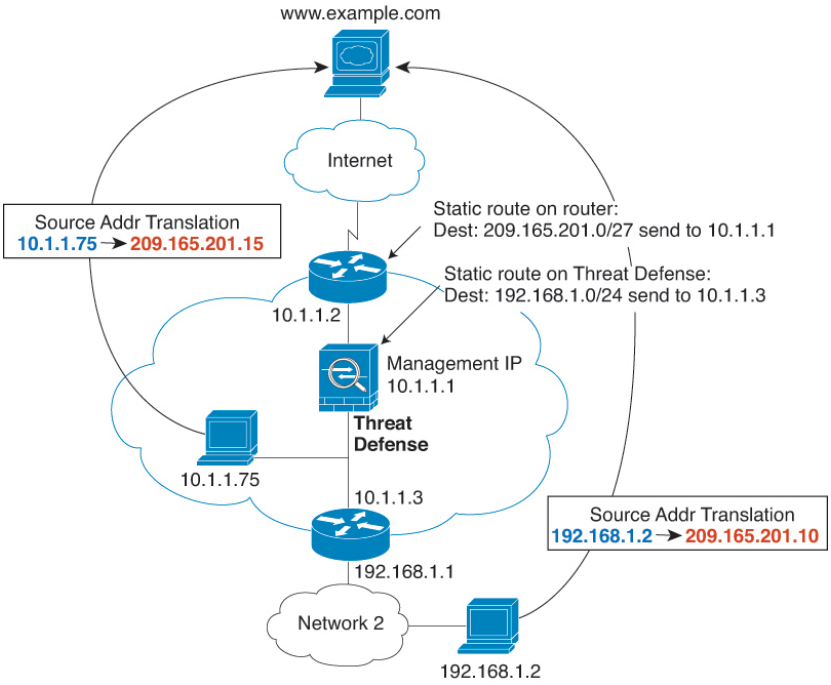
Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks. It can perform a similar function within a bridge group in routed mode.

NAT in transparent mode, or in routed mode between members of the same bridge group, has the following requirements and limitations:

- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the Firewall Threat Defense sends an ARP request to a host on the other side of the Firewall Threat Defense, and the initiating host real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.
- Translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

The following figure shows a typical NAT scenario in transparent mode, with the same network on the inside and outside interfaces. The transparent firewall in this scenario is performing the NAT service so that the upstream router does not have to perform NAT.

Figure 372: NAT Example: Transparent Mode



1. When the inside host at 10.1.1.75 sends a packet to a web server, the real source address of the packet, 10.1.1.75, is changed to a mapped address, 209.165.201.15.

2. When the server responds, it sends the response to the mapped address, 209.165.201.15, and the Firewall Threat Defense receives the packet because the upstream router includes this mapped network in a static route directed to the Firewall Threat Defense management IP address.
3. The Firewall Threat Defense then undoes the translation of the mapped address, 209.165.201.15, back to the real address, 10.1.1.1.75. Because the real address is directly-connected, the Firewall Threat Defense sends it directly to the host.
4. For host 192.168.1.2, the same process occurs, except for returning traffic, the Firewall Threat Defense looks up the route in its routing table and sends the packet to the downstream router at 10.1.1.3 based on the Firewall Threat Defense static route for 192.168.1.0/24.

Auto NAT and Manual NAT

You can implement address translation in two ways: *auto NAT* and *manual NAT*.

We recommend using auto NAT unless you need the extra features that manual NAT provides. It is easier to configure auto NAT, and it might be more reliable for applications such as Voice over IP (VoIP). (For VoIP, you might see a failure in the translation of indirect addresses that do not belong to either of the objects used in the rule.)

Auto NAT

All NAT rules that are configured as a parameter of a network object are considered to be *auto NAT* rules. This is a quick and easy way to configure NAT for a network object. You cannot create these rules for a group object, however.

Although these rules are configured as part of the object itself, you cannot see the NAT configuration in the object definition through the object manager.

When a packet enters an interface, both the source and destination IP addresses are checked against the auto NAT rules. The source and destination address in the packet can be translated by separate rules if separate matches are made. These rules are not tied to each other; different combinations of rules can be used depending on the traffic.

Because the rules are never paired, you cannot specify that sourceA/destinationA should have a different translation than sourceA/destinationB. Use manual NAT for that kind of functionality, where you can identify the source and destination address in a single rule.

Manual NAT

Manual NAT lets you identify both the source and destination address in a single rule. Specifying both the source and destination addresses lets you specify that sourceA/destinationA can have a different translation than sourceA/destinationB.

Note For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address. For example, if you configure static NAT with port address translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then you must specify the *source* ports to be translated (real: 23, mapped: 2323). You specify the source ports because you specified the Telnet server address as the source address.

The destination address is optional. If you specify the destination address, you can either map it to itself (identity NAT), or you can map it to a different address. The destination mapping is always a static mapping.

Comparing Auto NAT and Manual NAT

The main differences between these two NAT types are:

- How you define the real address.
  - Auto NAT—The NAT rule becomes a parameter for a network object. The network object IP address serves as the original (real) address.
  - Manual NAT—You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network object; the network object or group is a parameter of the NAT configuration. The ability to use a network object *group* for the real address means that manual NAT is more scalable.
- How source and destination NAT is implemented.
  - Auto NAT— Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.
  - Manual NAT—A single rule translates both the source and destination. A packet matches one rule only, and further rules are not checked. Even if you do not configure the optional destination address, a matching packet still matches one manual NAT rule only. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different translation than sourceA/destinationB.
- Order of NAT Rules.
  - Auto NAT—Automatically ordered in the NAT table.
  - Manual NAT—Manually ordered in the NAT table (before or after auto NAT rules).

NAT rule order

Auto NAT and manual NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.



Note There is also a Section 0, which contains any NAT rules that the system creates for its own use. These rules have priority over all others. The system automatically creates these rules and clears xlates as needed. You cannot add, edit, or modify rules in Section 0.

Table 73: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Manual NAT	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, manual NAT rules are added to section 1. By "specific rules first," we mean: • Static rules should come before dynamic rules. • Rules that include destination translation should come before rules with source translation only. If you cannot eliminate overlapping rules, where more than one rule might apply based on the source or destination address, be especially careful to follow these recommendations. If you do not follow the above recommendation, ensure that accurate routes are configured for the mapped addresses to match the correct NAT rule.
Section 2	Auto NAT	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.
Section 3	Manual NAT	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)

- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object def)
- 172.16.1.0/24 (dynamic) (object abc)

The resultant ordering would be:

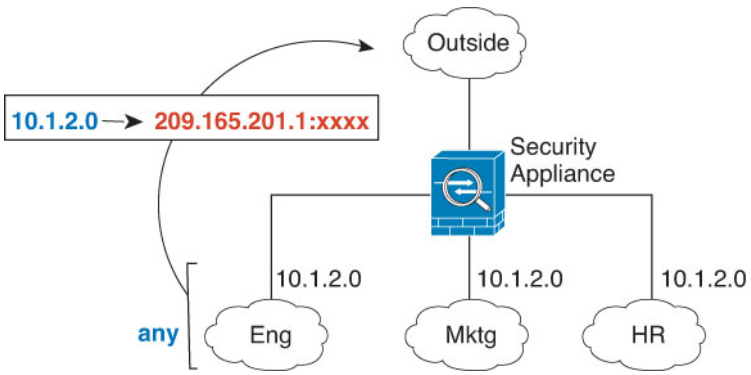
- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object abc)
- 172.16.1.0/24 (dynamic) (object def)
- 192.168.1.0/24 (dynamic)

NAT interfaces

Except for bridge group member interfaces, you can configure a NAT rule to apply to any interface (in other words, all interfaces), or you can identify specific real and mapped interfaces. You can also specify any interface for the real address, and a specific interface for the mapped address, or vice versa.

For example, you might want to specify any interface for the real address and specify the outside interface for the mapped address if you use the same private addresses on multiple interfaces, and you want to translate them all to the same global pool when accessing the outside.

Figure 373: Specifying Any Interface



However, the concept of "any" interface does not apply to bridge group member interfaces. When you specify "any" interface, all bridge group member interfaces are excluded. Thus, to apply NAT to bridge group members, you must specify the member interface. This could result in many similar rules where only one interface is different. You cannot configure NAT for the Bridge Virtual Interface (BVI) itself, you can configure NAT for member interfaces only.

Note You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes. When specifying interfaces, you do so indirectly by selecting the interface object that contains the interface.

NAT exemption

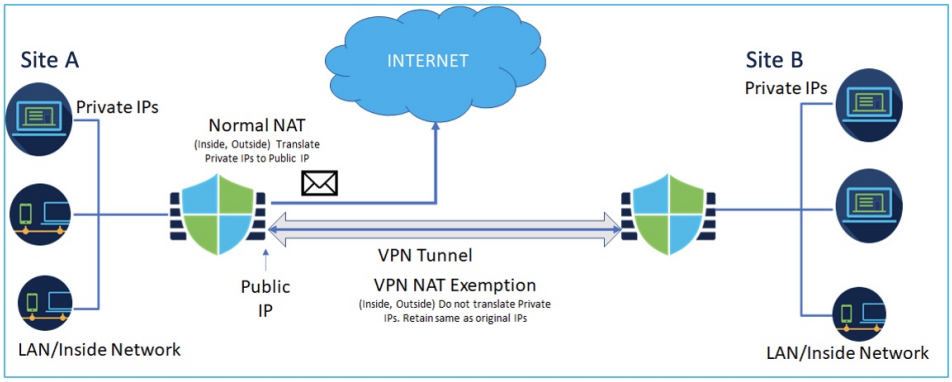
When internet edge devices have a site-to-site VPN configured on an interface and also have NAT rules for that interface, you must exempt the VPN traffic from the NAT rules. If you do not exempt the VPN traffic from NAT translation, the traffic gets dropped or is not routed through the VPN tunnel to the remote peer.

NAT exemption allows you to exclude traffic from being translated by NAT rules. When you create a policy-based site-to-site VPN using the Firewall Management Center VPN wizard, you can select the **NAT Exempt** option to create the rules automatically (**Devices** > **VPN** > **Site to Site**). By default, this option is enabled. You can view the NAT exemptions for a device in the NAT policy page (**Devices** > **NAT**, and then click **NAT Exemptions**).

The Firewall Management Center supports NAT exemption for all policy-based site-to-site VPN topology types. For more information, see Configure a policy-based site-to-site VPN, on page 1351.

Consider the following example, which shows a site-to-site VPN tunnel connecting Site A and Site B. For traffic that must go to the Internet, NAT translates the private IPs to a public IP address to access the Internet. For traffic that must go over the VPN tunnel, you must configure NAT exemption for the device in the VPN wizard.

Figure 374: Site-to-site VPN Topology with NAT Exemption



Note that when you upgrade from versions earlier than 7.4, if you have enabled NAT exemption, Firewall Management Center will disable this option. You must enable this option in the policy-based site-to-site VPN wizard.

Configuring routing for NAT

The Firewall Threat Defense device needs to be the destination for any packets sent to the translated (mapped) address.

When sending packets, the device uses the destination interface if you specify one, or a routing table lookup if you do not, to determine the egress interface. For identity NAT, you have the option to use a route lookup even if you specify a destination interface.

The type of routing configuration needed depends on the type of mapped address, as explained in the following topics.

Addresses on the same network as the mapped interface

If you use addresses on the same network as the destination (mapped) interface, the Firewall Threat Defense uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the Firewall Threat Defense does not have to be the gateway for any additional networks. This solution is ideal if the outside network contains an adequate number of free addresses, a consideration if you are using a 1:1 translation like dynamic NAT or static NAT. Dynamic PAT greatly extends the number of translations you can use with a small number of addresses, so even if the available addresses on the outside network is small, this method can be used. For PAT, you can even use the IP address of the mapped interface.



Note If you configure the mapped interface to be any interface, and you specify a mapped address on the same network as one of the mapped interfaces, then if an ARP request for that mapped address comes in on a *different* interface, then you need to manually configure an ARP entry for that network on the ingress interface, specifying its MAC address. Typically, if you specify any interface for the mapped interface, then you use a unique network for the mapped addresses, so this situation would not occur. Configure the ARP table in the ingress interface's **Advanced** settings.

Addresses on a unique network

If you need more addresses than are available on the destination (mapped) interface network, you can identify addresses on a different subnet. The upstream router needs a static route for the mapped addresses that points to the Firewall Threat Defense.

Alternatively for routed mode, you can configure a static route on the Firewall Threat Defense for the mapped addresses using any IP address on the destination network as the gateway, and then redistribute the route using your routing protocol. For example, if you use NAT for the inside network (10.1.1.0/24) and use the mapped IP address 209.165.201.5, then you can configure a static route for 209.165.201.5 255.255.255.255 (host address) to the 10.1.1.99 gateway that can be redistributed.

For transparent mode, if the real host is directly-connected, configure the static route on the upstream router to point to the Firewall Threat Defense: specify the bridge group IP address. For remote hosts in transparent mode, in the static route on the upstream router, you can alternatively specify the downstream router IP address.

The same address as the real address (identity NAT)

The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. You can also disable proxy ARP for regular static NAT if desired, in which case you need to be sure to have proper routes on the upstream router.

Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues. For example, if you configure a broad identity NAT rule for “any” IP address, then leaving proxy ARP enabled can cause problems for hosts on the network directly connected to the mapped interface. In this case, when a host on the mapped network wants to communicate with another host on the same network, then the address in the ARP request matches the NAT rule (which matches “any” address). The Firewall Threat Defense will then proxy ARP for the address, even though the packet is not actually destined for the Firewall Threat Defense. (Note that this problem occurs even if you have a manual NAT rule; although the NAT rule must match both the source and destination addresses, the proxy ARP decision is made only on the “source” address). If the

Firewall Threat Defense ARP response is received before the actual host ARP response, then traffic will be mistakenly sent to the Firewall Threat Defense.

Requirements and prerequisites for NAT policies

Ensure you meet these requirements for configuring NAT policies:

Supported domains

Any

User roles

You must have one of these user privileges to configure and use NAT policies:

- Admin
- Access Admin
- Network Admin

Guidelines for NAT

The following topics provide detailed guidelines for implementing NAT.

Firewall mode guidelines for NAT

NAT is supported in routed and transparent firewall mode.

However, configuring NAT on bridge group member interfaces (interfaces that are part of a Bridge Group Virtual Interface, or BVI) has the following restrictions:

- When configuring NAT for the members of a bridge group, you specify the member interface. You cannot configure NAT for the bridge group interface (BVI) itself.
- When doing NAT between bridge group member interfaces, you must specify the real and mapped addresses. You cannot specify “any” as the interface.
- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.
- You cannot translate between IPv4 and IPv6 networks (NAT64/46) when the source and destination interfaces are members of the same bridge group. Static NAT/PAT 44/66, dynamic NAT44/66, and dynamic PAT44 are the only allowed methods; dynamic PAT66 is not supported. However, you can do NAT64/46 between members of different bridge groups, or between a bridge group member (source) and standard routed interface (destination).

Note You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes.

IPv6 NAT guidelines

NAT supports IPv6 with the following guidelines and restrictions.

- For standard routed mode interfaces, you can also translate between IPv4 and IPv6.
- You cannot translate between IPv4 and IPv6 for interfaces that are members of the same bridge group. You can translate between two IPv6 or two IPv4 networks only. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.
- You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.
- For static NAT, you can specify an IPv6 subnet up to /64. Larger subnets are not supported.
- When using FTP with NAT46, when an IPv4 FTP client connects to an IPv6 FTP server, the client must use either the extended passive mode (EPSV) or extended port mode (EPRT); PASV and PORT commands are not supported with IPv6.

IPv6 NAT best practices

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices:

- NAT66 (IPv6-to-IPv6)—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only).
- NAT46 (IPv4-to-IPv6)—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is by default an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.4 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address. You can also optionally translate the addresses net-to-net, where the first IPv4 address maps to the first IPv6 address, the second to the second, and so on.
- NAT64 (IPv6-to-IPv4)—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

NAT support for inspected protocols

Some application layer protocols that open secondary connections, or that embedded IP addresses in packets, are inspected to provide the following services:

- Pinhole creation—Some application protocols open secondary TCP or UDP connections either on standard or negotiated ports. Inspection opens pinholes for these secondary ports so that you do not need to create access control rules to allow them.

- NAT rewrite— Protocols such as FTP embed IP addresses and ports for the secondary connections in packet data as part of the protocol. If there is NAT translation involved for either of the endpoints, the inspection engines rewrite the packet data to reflect the NAT translation of the embedded addresses and ports. The secondary connections would not work without NAT rewrite.
- Protocol enforcement—Some inspections enforce some degree of conformance to the RFCs for the inspected protocol.

The following table lists the inspected protocols that apply NAT rewrite and their NAT limitations. Keep these limitations in mind when writing NAT rules that include these protocols. Inspected protocols not listed here do not apply NAT rewrite. These inspections include GTP, HTTP, IMAP, POP, SMTP, SSH, and SSL.

Note NAT rewrite is supported on the listed ports only. For some of these protocols, you can extend inspection to other ports using Network Analysis Policies, but NAT rewrite is not extended to those ports. This includes DCERPC, DNS, FTP, and Sun RPC inspection. If you use these protocols on non-standard ports, do not use NAT on the connections.

Table 74: NAT Supported Application Inspection

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
DCERPC	TCP/135	No NAT64.	Yes
DNS over UDP	UDP/53	No NAT support is available for name resolution through WINS.	No
ESMTP	TCP/25	No NAT64.	No
FTP	TCP/21	(Clustering) No static PAT.	Yes
H.323 H.225 (Call signaling) H.323 RAS	TCP/1720 UDP/1718 For RAS, UDP/1718-1719	(Clustering) No static PAT. No extended PAT. No NAT64.	Yes
ICMP ICMP Error	ICMP (ICMP traffic directed to a device interface is never inspected.)	No limitations.	No
IP Options	RSVP	No NAT64.	No
NetBIOS Name Server over IP	UDP/137, 138 (Source ports)	No extended PAT. No NAT64.	No
RSH	TCP/514	No PAT. No NAT64. (Clustering) No static PAT.	Yes

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
RTSP	TCP/554 (No handling for HTTP cloaking.)	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes
SIP	TCP/5060 UDP/5060	No extended PAT. No NAT64 or NAT46. (Clustering) No static PAT.	Yes
Skinny (SCCP)	TCP/2000	No extended PAT. No NAT64, NAT46, or NAT66. (Clustering) No static PAT.	Yes
SQL*Net (versions 1, 2)	TCP/1521	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes
Sun RPC	TCP/111 UDP/111	No extended PAT. No NAT64.	Yes
TFTP	UDP/69	No NAT64. (Clustering) No static PAT. Payload IP addresses are not translated.	Yes
XDMCP	UDP/177	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes

FQDN destination guidelines

You can specify the translated (mapped) destination in a manual NAT rule using a fully-qualified domain name (FQDN) network object instead of an IP address. For example, you can create a rule based on traffic that is destined for the www.example.com web server.

When using an FQDN, the system obtains the DNS resolution and writes the NAT rule based on the returned address. If you are using multiple DNS server groups, the filter domains are honored and the address is requested from the appropriate group based on the filters. If more than one address is obtained from the DNS server, the address used is based on the following:

- If there is an address on the same subnet as the specified interface, that address is used. If there isn't one on the same subnet, the first address returned is used.
- The IP type for the translated source and translated destination must match. For example, if the translated source address is IPv6, the FQDN object must specify IPv6 as the address type. If the translated source is IPv4, the FQDN object can specify IPv4 or both IPv4 and IPv6. In this case, an IPv4 address is selected.

You cannot include an FQDN object in a network group that is used for manual NAT destination. In NAT, an FQDN object must be used alone, as only a single destination host makes sense for this type of NAT rule.

If the FQDN cannot be resolved to an IP address, the rule is not functional until a DNS resolution is obtained.

Additional guidelines for NAT

- NAT rules apply to through the device traffic only, they do not apply to traffic initiated by the device, such as a RADIUS authentication.
- For interfaces that are members of a bridge group, you write NAT rules for the member interfaces. You cannot write NAT rules for the Bridge Virtual Interface (BVI) itself.
- You cannot write NAT rules for a Virtual Tunnel Interface (VTI), which are used in site-to-site VPN. Writing rules for the VTI's source interface will not apply NAT to the VPN tunnel. To write NAT rules that will apply to VPN traffic tunneled on a VTI, you must use "any" as the interface; you cannot explicitly specify interface names.
- (Auto NAT only.) You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules for an object, you need to create multiple objects with different names that specify the same IP address.
- If a VPN is defined on an interface, inbound ESP traffic on the interface is not subject to the NAT rules. The system allows the ESP traffic for established VPN tunnels only, dropping traffic not associated with an existing tunnel. This restriction applies to ESP and UDP ports 500 and 4500.
- If you define a site-to-site VPN on a device that is behind a device that is applying dynamic PAT, so that UDP ports 500 and 4500 are not the ones actually used, you must initiate the connection from the device that is behind the PAT device. The responder cannot initiate the security association (SA) because it does not know the correct port numbers.
- If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT configuration is used, you can clear the translation table using the **clear xlate** command in the device CLI. However, clearing the translation table disconnects all current connections that use translations.

  If you create a new NAT rule that should apply to an existing connection (such as a VPN tunnel), you need to use **clear conn** to end the connection. Then, the attempt to re-establish the connection should hit the NAT rule and the connection should be NAT'ed correctly.



Note If you remove a dynamic NAT or PAT rule, and then add a new rule with mapped addresses that overlap the addresses in the removed rule, then the new rule will not be used until all connections associated with the removed rule time out or are cleared using the **clear xlate** or **clear conn** commands. This safeguard ensures that the same address is not assigned to multiple hosts.

- You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
- A network object used in NAT cannot include more than 131,838 IP addresses, either explicitly or implied in a range of addresses or a subnet. Break up the address space into smaller ranges and write separate rules for the smaller objects.

- (Manual NAT only.) When using **any** as the source address in a NAT rule, the definition of "any" traffic (IPv4 vs. IPv6) depends on the rule. Before the Firewall Threat Defense performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the Firewall Threat Defense can determine the value of **any** in a NAT rule. For example, if you configure a rule from "any" to an IPv6 server, and that server was mapped from an IPv4 address, then **any** means "any IPv6 traffic." If you configure a rule from "any" to "any," and you map the source to the interface IPv4 address, then **any** means "any IPv4 traffic" because the mapped interface address implies that the destination is also IPv4.
- You can use the same mapped object or group in multiple NAT rules.
- The mapped IP address pool cannot include:
  - The mapped interface IP address. If you specify "any" interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), specify the interface name instead of the interface address.
  - The failover interface IP address.
  - (Transparent mode.) The management IP address.
  - (Dynamic NAT.) The standby interface IP address when VPN is enabled.
- Avoid using overlapping addresses in static and dynamic NAT policies. For example, with overlapping addresses, a PPTP connection can fail to get established if the secondary connection for PPTP hits the static instead of dynamic xlate.
- You cannot use overlapping addresses in the source address of a NAT rule and a remote access VPN address pool.
- If you specify a destination interface in a rule, then that interface is used as the egress interface rather than looking up the route in the routing table. However, for identity NAT, you have the option to use a route lookup instead.
- If you use PAT on Sun RPC traffic, which is used to connect to NFS servers, be aware that the NFS server might reject connections if the PAT'ed port is above 1024. The default configuration of NFS servers is to reject connections from ports higher than 1024. The error is typically "Permission Denied." Mapping ports above 1024 happens if you do not select the option to include the reserved ports (1-1023) in the port range of a PAT pool. You can avoid this problem by changing the NFS server configuration to allow all port numbers.
- NAT applies to through traffic only. Traffic generated by the system is not subject to NAT.
- Do not name a network object or group pat-pool, using any combination of upper- or lower-case letters.
- The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.
- You cannot use NAT on the internal payload of Protocol Independent Multicast (PIM) registers.
- (Manual NAT) When writing NAT rules for a dual ISP interface setup (primary and backup interfaces using service level agreements in the routing configuration), do not specify destination criteria in the rule. Ensure the rule for the primary interface comes before the rule for the backup interface. This allows the device to choose the correct NAT destination interface based on the current routing state when the primary ISP is unavailable. If you specify destination objects, the NAT rule will always select the primary interface for the otherwise duplicate rules.

- If you get the ASP drop reason nat-no-xlate-to-pat-pool for traffic that should not match the NAT rules defined for the interface, configure identity NAT rules for the affected traffic so the traffic can pass untranslated.
- If you configure NAT for GRE tunnel endpoints, you must disable keepalives on the endpoints or the tunnel cannot be established. The endpoints send keepalives to the original addresses.
- DHCP and BOOTP share ports UDP/67-68. Because BOOTP is obsolete, writing NAT rules for the bootps port can cause port allocation problems when also running DHCP. Consider using DHCP relay instead for transmitting DHCP requests between network segments.
- In rare cases, return traffic (server to client) with an existing translation (xlate) might be logged as a new flow in Connection Events. This can occur when the client has already terminated the connection and the server sends another packet that reaches the device during the brief interval between connection closure and xlate removal, often due to application behavior or TCP stack cleanup. Because the device removes the xlate only after deleting the connection, a server packet can arrive while the xlate still exists. If no valid connection entry is found, the device logs a separate connection event based on the matched Access Control Policy rule.

Manage NAT policies

NAT converts the IP address of an incoming packet to a different address in the outgoing packet. One of the main functions of NAT is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into routable addresses that can be used on the public Internet. NAT keeps track of the translations, also known as xlates, to ensure that return traffic is directed to the correct untranslated host address.

Procedure

Step 1 Choose **Devices** > **NAT**.

Step 2 Manage your NAT policies:

- Create—Click **New Policy** and select **Threat Defense NAT**. Refer to Create NAT policies, on page 1204.
- Copy—Click **Copy** ( ) next to the policy you want to copy. You are prompted to give the copy a new, unique name. The copy includes all policy rules and configurations, but does not include device assignments.
- Report—Click **Report** ( ) for the policy. You are prompted to save the PDF report, which includes policy attributes, device assignments, rules, and object usage information.
- Edit—Click **Edit** ( ) next to the policy you want to edit. Refer to Configure NAT for threat defense, on page 1205.
- Delete—Click **Delete** ( ) next to the policy you want to delete, then click **OK**. When prompted whether to continue, you are also informed if another user has unsaved changes in the policy.

Caution After you have deployed a NAT policy to a managed device, you cannot delete the policy from the device. Instead, you must deploy a NAT policy with no rules to remove the NAT rules already present on the managed device. You also cannot delete a policy that is the last deployed policy on any of its target devices, even if it is out of date. Before you can delete the policy completely, you must deploy a different policy to those targets.

Create NAT policies

Create a NAT policy to define how network addresses are translated between different network segments.

When you create a new NAT policy you must, at minimum, give it a unique name. Although you are not required to identify policy targets at policy creation time, you must perform this step before you can deploy the policy. If you apply a NAT policy with no rules to a device, the system removes all NAT rules from that device.

Procedure

Step 1 Choose **Devices** > **NAT**.

Step 2 Click **New Policy** and from the drop-down list, choose **Threat Defense NAT** for Firewall Threat Defense devices.

Firepower NAT is for older devices that are not covered in this document.

Step 3 Enter a unique **Name**.

Step 4 (Optional) Enter a **Description**.

Step 5 Choose the devices where you want to deploy the policy:

- Choose a device in the **Available Devices** list, and then click **Add to Policy**.

  Alternatively, click and drag a device from the **Available Devices** list to the **Selected Devices** list.

- Remove a device from the **Selected Devices** list by clicking **Delete** ( ) next to the device.

Step 6 Click **Save**.

Configure NAT policy targets

Identify the managed devices that you want to target with your policy while creating or editing a policy and assign NAT policies to identified devices to control NAT behavior. You can search a list of available devices and high-availability pairs, and add them to a list of selected devices.

Procedure

Step 1 Choose **Devices** > **NAT**.

Step 2 Click **Edit** ( ) next to the NAT policy you want to modify.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click **Policy Assignments**.

Step 4 Do any of the following:

- To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add to Policy**. Alternatively, you can also drag and drop selected devices.
- To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** list.

Step 5 Click **OK**.

Configure NAT for threat defense

The NAT policy is a shared policy. Assign it to devices that need similar NAT rules.

Each rule applies to a device if its interface objects (security zones or interface groups) include an interface for that device. When the interface objects include one or more interface for the device, the rule is deployed to the device. You can target subsets of devices within a shared policy by designing interface objects accordingly. Rules using the "any" interface object apply to all devices.

If you change an interface type to one not valid for NAT on an assigned device, the policy marks the interface as deleted. Click **Save** in the NAT policy to automatically remove the interface from the policy.

You can configure multiple NAT policies if groups of your devices require significantly different rules.

Procedure

Step 1 Select **Devices** > **NAT**.

- Click **New Policy** > **Threat Defense NAT** to create a new policy. Give the policy a name, optionally assign devices to it, and click **Save**.

  You can change device assignments later by editing the policy and clicking **Policy Assignments**.

- Click **Edit** ( ) to edit an existing threat defense NAT policy. Note that the page also shows Firepower NAT policies, which are not used by Firewall Threat Defense devices.

  If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Decide what kinds of rules you need.

You can create dynamic NAT, dynamic PAT, static NAT, and identity NAT rules. For an overview, refer to NAT types, on page 1188.

Step 3 Decide which rules should be implemented as manual or auto NAT.

For a comparison of these two implementation options, refer to Auto NAT and Manual NAT, on page 1191.

Step 4 Decide which rules should be custom per device.

Because you can assign a NAT policy to multiple devices, you can configure a single rule on many devices. However, you might have rules that should be interpreted differently by each device, or some rules that should apply to a subset of devices only.

Use interface objects to control on which devices a rule is configured. Then, use object overrides on network objects to customize the addresses used per device.

For detailed information, refer to Customize NAT rules for multiple devices, on page 1207.

Step 5 Create the rules as explained in these sections.

- Dynamic NAT, on page 1210
- Dynamic PAT, on page 1216
- Static NAT, on page 1226
- Identity NAT, on page 1235

Step 6 Do these to manage your NAT policy:

- To edit the policy name or description, click in those fields, type in your changes, and click outside the fields.
- To view only those rules that apply to a specific device, click **Filter by Device** and select the desired device. A rule applies to a device if it uses an interface object that includes an interface on the device.
- To view any warnings or errors in the policy, click **Show Warnings**, then choose a **Device**. Warnings and errors mark configurations that could adversely affect traffic flow or prevent the policy from deploying.
- To change the devices to which the policy is assigned, click the **Policy Assignments** link and modify the selected devices list as desired.
- To change the number of rules displayed on the page, use the **Rows Per Page** drop-down list.

Step 7 Do these to manage your NAT rules:

- To add a rule, click the **Add Rule** button.
- To edit a rule, click the **Edit** ( ) icon next to the rule.
- To delete a rule, click the **Delete** ( ) icon next to the rule.
- To enable or disable a rule, right-click the rule and choose **Enable** or **Disable** from the **State** menu. You can temporarily disable a rule without deleting it using these controls.
- To select more than one rule to enable, disable, or delete, click the checkbox for the rules, or the checkbox in the header, then perform the action.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Customize NAT rules for multiple devices

Because the NAT policy is shared, you can assign a given policy to more than one device. However, you can configure at most one auto NAT rule for a given object. Thus, if you want to configure different translations for an object based on the specific device doing the translation, you need to carefully configure the interface objects (security zones or interface groups) and define network object overrides for the translated address. The interface objects determine on which devices a rule gets configured. The network object overrides determine what IP addresses are used by a given device for that object.

Consider the following scenario:

- FTD-A and FTD-B have inside networks 192.168.1.0/24 attached to the interface named “inside.”
- On FTD-A, you want to translate all 192.168.1.0/24 addresses to a NAT pool in the 10.100.10.10 - 10.100.10.200 range when going to the “outside” interface.
- On FTD-B, you want to translate all 192.168.1.0/24 addresses to a NAT pool in the 10.200.10.10 - 10.200.10.200 range when going to the “outside” interface.

Do these steps to accomplish the above scenario. Although this example rule is for dynamic auto NAT, you can generalize the technique for any type of NAT rule.

Procedure

Step 1 Create the security zones for the inside and outside interfaces.

a) Choose **Objects** > **Object Management**.
b) Select **Interface** from the table of contents and click **Add** > **Security Zone**.

You can use interface groups instead of zones.

c) Configure the inside zone properties.

- **Name**—Enter a name, for example, **inside-zone**.
- **Type**—Select **Routed** for routed-mode devices, **Switched** for transparent mode.
- **Selected Interfaces**—Add the FTD-A/inside and FTD-B/inside interfaces to the selected list.

d) Click **Save**.
e) Click **Add** > **Security Zone** and define the outside zone properties.

- **Name**—Enter a name, for example, **outside-zone**.
- **Interface Type**—Select **Routed** for routed-mode devices, **Switched** for transparent mode.
- **Selected Interfaces**—Add the FTD-A/outside and FTD-B/outside interfaces to the selected list.

f) Click **Save**.

Step 2 Create the network object for the original inside network on the Object Management page.

a) Select **Network** from the table of contents and click **Add Network** > **Add Object**.

b) Configure the inside network properties.

- **Name**—Enter a name, for example, **inside-network**.
- **Network**—Enter the network address, for example, **192.168.1.0/24**.

c) Click **Save**.

Step 3 Create the network object for the translated NAT pool and define overrides.

a) Click **Add Network** > **Add Object**.

b) Configure the NAT pool properties for FTD-A.

- **Name**—Enter a name, for example, **NAT-pool**.
- **Network**—Enter the range of addresses to include in the pool for FTD-A, for example, **10.100.10.10-10.100.10.200**.

c) Select **Allow Overrides**.

d) Click the **Overrides** heading to open the list of object overrides.

e) Click **Add** to open the Add Object Override dialog box.

f) Select FTD-B and **Add** it to the **Selected Devices** list.

g) Click **Override** and change **Network** to **10.200.10.10-10.200.10.200**.

h) Click **Add** to add the override to the device.

By defining an override for FTD-B, whenever the system configures this object on FTD-B, it will use the override value instead of the value defined in the original object.

i) Click **Save**.

Step 4 Configure the NAT rule.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamic.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside-zone.
- **Destination Interface Objects** = outside-zone.



Note The interface objects control on which devices the rule is configured. Because in this example the zones contain interfaces for FTD-A and FTD-B only, even if the NAT policy were assigned to additional devices, the rule would be deployed to those 2 devices only.

e) On **Translation**, configure the following:

- **Original Source** = inside-network object.
- **Translated Source** > **Address**= NAT-pool object.

f) Click **Save**.

You now have a single rule that will be interpreted differently for FTD-A and FTD-B, providing unique translations for the inside networks protected by each firewall.

Search and filter the NAT rule table

You can search and filter the NAT rule table to help you find rules that you need to modify or view. When you filter the table, only matching rules are shown. Note that although the rule numbers change to be sequentially 1, 2, and so forth, filtering does not change the actual rule number or the rule's location in the table relative to hidden rules. Filtering simply changes what you can see to help you locate rules that interest you.

When editing the NAT policy, you can use the fields above the table to do these types of search or filter:

- **Filter by Device**—Click **Filter by Device**, then select the devices whose rules you want to see and click **OK**. Whether a rule applies to a device is determined by the rule's interface constraints. If you specify a security zone or interface group for either the source or destination interface, the rule applies to a device if at least one interface for the device is in the zone or group. If a NAT rule applies to any source and any destination interface, then it applies to all devices.

  If you also do a text or multiple-attribute search, the results are constrained to the selected devices.

  To remove this filter, click **Filter by Device** and deselect the devices, or select **All**, and click **OK**.

- **Simple Text Search**—In the **Filter** box, type a string and press Enter. The string is compared to all values in the rules. For example, if you enter "network-object-1," which is the name of a network object, you would get rules that use the object in source, destination, and PAT pool attributes.

  For network and port objects, the string is also compared to the contents of the objects used in the rule. For example, if a PAT pool object includes the range 10.100.10.3-10.100.10.100, searching on either 10.100.10.3 or 10.100.10.100 (or a partial 10.100.10) will include rules that use that PAT pool object. However, the match must be exact: searching on 10.100.10.5 will not match this PAT pool object, even though the IP address is within the object's IP address range.

  To remove the filter, click the **x** on the right side of the Filter box.

- **Multiple-Attribute Search**—If a simple text search gives you too many hits, you can configure multiple values for the search. Click in the **Filter** box to open the list of attributes, then select or enter strings for the attributes you intend to search and click the **Filter** button. These attributes are the same as the ones you would configure within a NAT rule. The attributes are and'ed, so filtered results include only those rules that match all attributes you configured.

  - For binary attributes, such as the rule state (enabled/disabled), whether a PAT pool is configured (enabled/disabled), the direction of the rule (uni/bi), or rule type (static/dynamic), simply check or uncheck the boxes as appropriate. Select both boxes if you do not care about the attribute value. If you deselect both boxes, no rules will match the filter.

- For string attributes, type a full or partial string relevant to that attribute. These will be object names, either for security zones/interface groups, network objects, or port objects. It can also be the network or port object contents, which are matched the same way they are for simple text searches.

To remove the filter, click the **x** on the right side of the Filter box, or click in the Filter box to open the drop-down list, and click the Clear button.

Enable, disable, or delete multiple rules

You can enable or disable manual NAT rules, or delete any NAT rule, one by one. You can also select multiple rules and apply changes to all of them at once. Because enable/disable applies to manual NAT only, if you select a mix of rule types, you can delete them only. Note that when you enable or disable rules, it does not matter if you select some rules that were already enabled or disabled. For example, enabling an already enabled rule simply leaves the rule enabled.

Procedure

Step 1 Select **Devices** > **NAT**, and edit a threat defense NAT policy.

Step 2 (Optional) Filter the NAT rules to locate the ones you want to change.

Filtering is especially useful if you have a large NAT policy. For example, you could search on disabled rules to find ones that need to be enabled.

Step 3 Select the rules you want to change.

- Click the checkbox in the left column of the rule to select (or deselect) individual rules.
- Click the checkbox in the table header to select all the rules on the currently displayed page.

Your selection is preserved as you go from page to page. However, in practice, it makes most sense to perform your actions on the rules selected on a page before going to the next page.

Step 4 Perform the desired action. When selecting multiple rules, you are asked to confirm the action.

Note that these actions are also available on the right-click menu.

- To enable all rules, click **Select Bulk Action** > **Enable**.
- To disable all rules, click **Select Bulk Action** > **Disable**.
- To delete all rules, click **Select Bulk Action** > **Delete**.

Dynamic NAT

The following topics explain dynamic NAT and how to configure it.

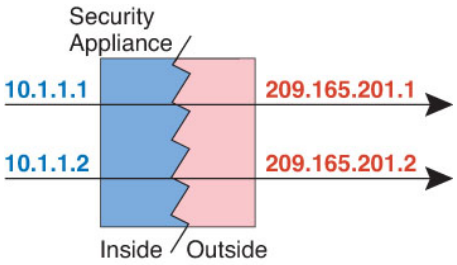
About dynamic NAT

Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool typically includes fewer addresses than the real group. When a host you want to translate accesses the destination network, NAT assigns the host an IP address from the mapped pool. The translation is created only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, even if the connection is allowed by an access rule.

Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule. A successful connection from a remote host can reset the idle timer for the connection.

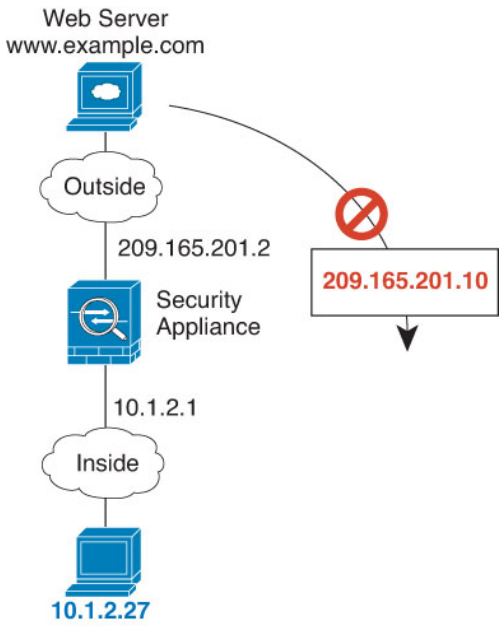
The following figure shows a typical dynamic NAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back.

Figure 375: Dynamic NAT



The following figure shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the packet is dropped.

Figure 376: Remote Host Attempts to Initiate a Connection to a Mapped Address



Dynamic NAT disadvantages and advantages

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

  Use PAT or a PAT fall-back method if this event occurs often because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool, and routable addresses may not be available in large quantities.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.
- Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

Configure dynamic auto NAT

Use dynamic auto NAT rules to translate addresses to different IP addresses that are routable on the destination network.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host, range, or subnet.

- **Translated Source**—This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** (✎) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **NAT Rule**—Select **Auto NAT Rule**.
- **Type**—Select **Dynamic**.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 On **Translation**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—The network object or group that contains the mapped addresses.

Step 6 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see DNS query and response rewriting using NAT, on page 1296.
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 7 Click **Save** to add the rule.

Step 8 Click **Save** on the NAT page to save your changes.

Configure dynamic manual NAT

Use dynamic manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic NAT translates addresses to different IP addresses that are routable on the destination network.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—This can be a network object or group, but it cannot include a subnet. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.

You can also create network objects or groups for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule.

For dynamic NAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** () to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

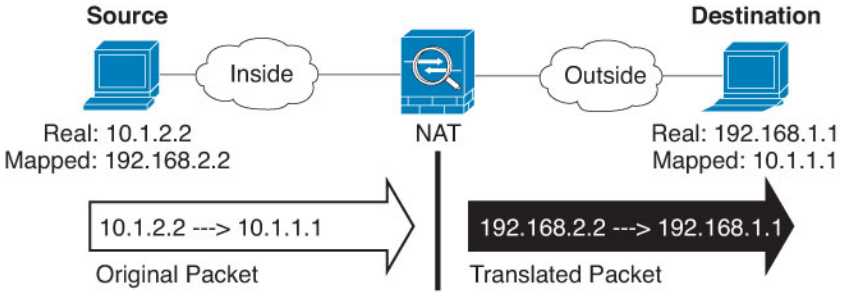
- **NAT Rule**—Select **Manual NAT Rule**.
- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 (On the **Translation** page.) Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object or group that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Source Interface IP** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—The network object or group that contains the mapped addresses.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the destination service ports for service translation: **Original Destination Port**, **Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 8 (Optional.) On **Advanced**, select the desired options:

- (For source translation only.) **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see DNS query and response rewriting using NAT, on page 1296.
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 9 Click **Save** to add the rule.

Step 10 Click **Save** on the NAT page to save your changes.

Dynamic PAT

The following topics describe dynamic PAT.

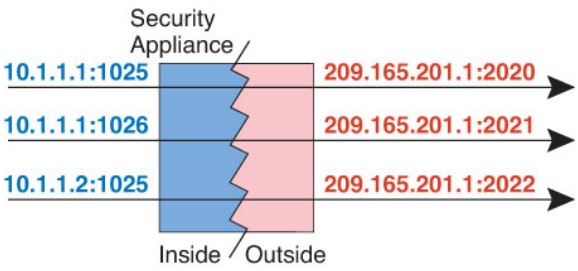
About dynamic PAT

Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port.

Each connection requires a separate translation session because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The following figure shows a typical dynamic PAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back. The mapped address is the same for each translation, but the port is dynamically assigned.

Figure 377: Dynamic PAT



For the duration of the translation, a remote host on the destination network can initiate a connection to the translated host if an access rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

After the connection expires, the port translation also expires.

Note We recommend that you use different PAT pools for each interface. If you use the same pool for multiple interfaces, especially if you use it for "any" interface, the pool can be quickly exhausted, with no ports available for new translations.

Dynamic PAT disadvantages and advantages

Dynamic PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the Firewall Threat Defense interface IP address as the PAT address.

You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group. This restriction does not apply when the interfaces are members of different bridge groups, or between a bridge group member and a standard routed interface.

Dynamic PAT does not work with some multimedia applications that have a data stream that is different from the control path. For more information, see NAT support for inspected protocols, on page 1198.

Dynamic PAT might also create a large number of connections appearing to come from a single IP address, and servers might interpret the traffic as a DoS attack. You can configure a PAT pool of addresses and use a round-robin assignment of PAT addresses to mitigate this situation.

PAT pool object guidelines

When creating network objects for a PAT pool, follow these guidelines.

For a PAT pool

- Ports are mapped to an available port in the 1024 to 65535 range. You can optionally include the reserved ports, those below 1024, to make the entire port range available for translations.

  When operating in a cluster, blocks of 512 ports per address are allocated to the members of the cluster, and mappings are made within these port blocks. If you also enable block allocation, the ports are distributed according to the block allocation size, whose default is also 512. If you change the cluster unit limit (the size of the cluster), ensure that you clear xlates or reboot the devices so that PAT pools can be appropriately reallocated to the cluster units.

- If you enable block allocation for a PAT pool, port blocks are allocated in the 1024-65535 range only. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host.

- If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT, then the other rule must also specify extended PAT.

- If a host has an existing connection, then subsequent connections from that host use the same PAT IP address. If no ports are available, this can prevent the connection. Use the round robin option to avoid this problem.

- For best performance, limit the number of IP addresses within a PAT pool to 10,000.

For extended PAT for a PAT pool

- Many application inspections do not support extended PAT.
- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT with port translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.
- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.
- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.
- You cannot use extended PAT on units in a cluster.
- Extended PAT increases memory usage on the device.

For round robin for a PAT pool

- If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. However, this "stickiness" does not survive a failover. If the device fails over, then subsequent connections from a host might not use the initial IP address.
- IP address "stickiness" is also impacted if you mix PAT pool/round robin rules with interface PAT rules on the same interface. For any given interface, choose either a PAT pool or interface PAT; do not create competing PAT rules.
- Round robin, especially when combined with extended PAT, can consume a large amount of memory. Because NAT pools are created for every mapped protocol/IP address/port range, round robin results in a large number of concurrent NAT pools, which use memory. Extended PAT results in an even larger number of concurrent NAT pools.

Configure dynamic auto PAT

Use dynamic auto PAT rules to translate addresses to unique IP address/port combinations, rather than to multiple IP addresses only. You can translate to a single address (either the destination interface's address or another address), or use a PAT pool of addresses to provide a larger number of possible translations.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host, range, or subnet.
- **Translated Source**—You have the following options to specify the PAT address:
  - **Destination Interface**—To use the destination interface address, you do not need a network object.
  - **Single PAT address**—Create a network object containing a single host.
  - **PAT pool**—Create a network object that includes a range, or create a network object group that contains hosts, ranges, or both. You cannot include subnets. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** ( ) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **NAT Rule**—Select **Auto NAT Rule**.
- **Type**—Select **Dynamic**.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 On **Translation**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—One of the following:
  - (Interface PAT.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Skip the step for configuring a PAT pool.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose. Skip the step for configuring a PAT pool.
  - To use a PAT pool, leave **Translated Source** empty. Do not select the destination interface IP or a single address as the **Translated Source**.

Step 6 If you are using a PAT pool, select the **PAT Pool** page and do the following:

a) Select **Enable PAT pool**.

b) Select the network object group that contains the addresses for the pool in the **PAT** > **Address** field.

You can alternatively select **Destination Interface IP**, which is another way to implement interface PAT.

c) (Optional) Select the following options as needed:

- **Use Round Robin Allocation**—To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

- **Extended PAT Table**—To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.
- **Flat Port Range**, **Include Reserved Ports**—To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. (Pre-6.7) When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option. For the Firewall Threat Defense devices running version 6.7 or higher, the flat port range is always configured, whether you select the option or not. You can still select the **Include Reserved Ports** option for these systems, and that setting is honored.
- **Block Allocation**—To enable port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with round robin, but you cannot use it with the extended PAT or flat port range options. You also cannot use interface PAT fallback.

Step 7 (Optional.) On **Advanced**, select the desired options:

- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option. You cannot select this option if you already configured interface PAT as the translated address or PAT pool.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 8 Click **Save** to add the rule.

Step 9 Click **Save** on the NAT page to save your changes.

Configure dynamic manual PAT

Use dynamic manual PAT rules when auto PAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic PAT translates addresses to unique IP address/port combinations, rather than to multiple IP addresses only. You can translate to a single address (either the destination interface's address or another address), or use a PAT pool of addresses to provide a larger number of possible translations.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—You have the following options to specify the PAT address:
  - **Destination Interface**—To use the destination interface address, you do not need a network object.
  - **Single PAT address**—Create a network object containing a single host.
  - **PAT pool**—Create a network object that includes a range, or create a network object group that contains hosts, ranges, or both. You cannot include subnets.

You can also create network objects or groups for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule.

For dynamic NAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** ( ) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

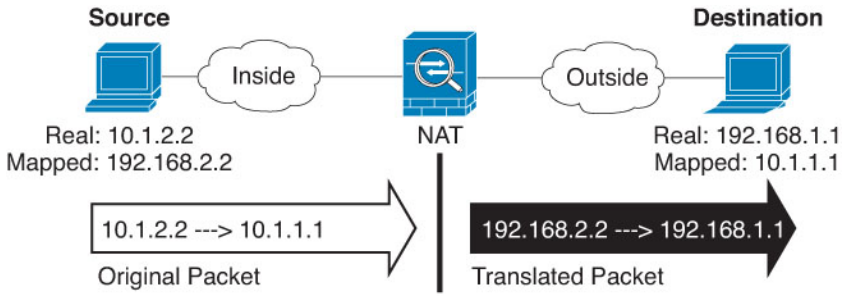
- **NAT Rule**—Select **Manual NAT Rule**.
- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 (On the **Translation** page.) Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object or group that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Source Interface IP** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—One of the following:
  - (Interface PAT.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Skip the step for configuring a PAT pool.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose. Skip the step for configuring a PAT pool.
  - To use a PAT pool, leave **Translated Source** empty. Do not select the destination interface IP or a single address as the **Translated Source**.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the destination service ports for service translation: **Original Destination Port**, **Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 8 If you are using a PAT pool, select the **PAT Pool** page and do the following:

a) Select **Enable PAT pool**.

b) Select the network object group that contains the addresses for the pool in the **PAT** > **Address** field.

You can alternatively select **Destination Interface IP**, which is another way to implement interface PAT.

c) (Optional) Select the following options as needed:

- **Use Round Robin Allocation**—To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
- **Extended PAT Table**—To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.
- **Flat Port Range**, **Include Reserved Ports**—To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. (Pre-6.7) When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option. For the Firewall Threat Defense devices running version 6.7 or higher, the flat port range is always configured, whether you select the option or not. You can still select the **Include Reserved Ports** option for these systems, and that setting is honored.
- **Block Allocation**—To enable port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with round robin, but you cannot use it with the extended PAT or flat port range options. You also cannot use interface PAT fallback.

Step 9 (Optional.) On **Advanced**, select the desired options:

- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 10 Click **Save** to add the rule.

Step 11 Click **Save** on the NAT page to save your changes.

Configure PAT with port block allocation

For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). If you allocate a block of ports, subsequent connections from the host use new randomly-selected ports within the block. If necessary, additional blocks are allocated

if the host has active connections for all ports in the original block. Blocks are freed when the last xlate that uses a port in the block is removed.

The main reason for allocating port blocks is reduced logging. The port block allocation is logged, connections are logged, but xlates created within the port block are not logged. On the other hand, this makes log analysis more difficult.

Port blocks are allocated in the 1024-65535 range only. There are separate blocks for TCP, UDP, and ICMP connections, and these blocks can overlap. Thus, if an application requires a low port number (1-1023), it might not work. For example, an application requesting port 22 (SSH) will get a mapped port within the range of 1024-65535 and within the block allocated to the host. You can create a separate NAT rule that does not use block allocation for applications that use low port numbers; for twice NAT, ensure the rule comes before the block allocation rule.

Before you begin

Usage notes for NAT rules:

- You can include the **Use Round Robin Allocation** option, but you cannot include the options for extending PAT uniqueness, using a flat range, including the reserved ports, or falling through to interface PAT. Other source/destination address and port information is also allowed.
- As with all NAT changes, if you replace an existing rule, you must clear xlates related to the replaced rule to have the new rule take effect. You can clear them explicitly or simply wait for them to time out. However, when operating in a cluster, you must reload the cluster so that the units can distribute blocks correctly.



Note If you are switching between a regular PAT and block allocation PAT rule, for object NAT, you must first delete the rule, then clear xlates. You can then create the new object NAT rule. Otherwise, you will see pat-port-block-state-mismatch drops in the **show asp drop** output.

- When you form a cluster while the device that will become the control node has an existing NAT policy that uses PAT pools, PAT port block distribution might not initialize correctly. The control node does not own or distribute the port blocks, and the **show nat pool cluster summary** command might show all port blocks as *RESERVED* on every cluster node.
  - Before forming a cluster, remove any existing NAT policy that uses PAT pools from the device that will become the control node. After cluster formation is complete, reconfigure and deploy the NAT policy.
  - If the cluster is already formed and all port blocks appear as *RESERVED*, delete the affected NAT policy and deploy the change. Then re-create and deploy the policy. Use the **show nat pool cluster summary** command to verify that the port blocks are distributed correctly across the cluster nodes.
- For a given PAT pool, you must specify (or not specify) block allocation for all rules that use the pool. You cannot allocate blocks in one rule and not in another. PAT pools that overlap also cannot mix block allocation settings. You also cannot overlap static NAT with port translation rules with the pool.

Procedure

Step 1 (Optional.) Configure global PAT port block allocation settings.

There are a few global settings that control port block allocation. If you want to change the defaults for these options, you must configure a FlexConfig object and add it to your FlexConfig policy.

a) Select **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** and create a new object.

b) Configure the block allocation size, which is the number of ports in each block.

xlate block-allocation size *value*

The range is 32-4096. The default is 512. Use the "no" form to return to the default.

If you do not use the default, ensure that the size you choose divides evenly into 64,512 (the number of ports in the 1024-65535 range). Otherwise, there will be ports that cannot be used. For example, if you specify 100, there will be 12 unused ports.

Using the default block-allocation size, a single PAT IP can serve 126 unique, simultaneous users (number of ports 64,512 divided by 512).

c) Configure the maximum blocks that can be allocated per host.

xlate block-allocation maximum-per-host *number*

The limit is per protocol, so a limit of 4 means at most 4 UDP blocks, 4 TCP blocks, and 4 ICMP blocks per host. The range is 1-8, the default is 4. Use the "no" form to return to the default.

d) (Optional.) Enable interim syslog generation.

xlate block-allocation pba-interim-logging *seconds*

By default, the system generates syslog messages during port block creation and deletion. If you enable interim logging, the system generates the following message at the interval you specify. The messages report all active port blocks allocated at that time, including the protocol (ICMP, TCP, UDP) and source and destination interface and IP address, and the port block. You can specify an interval from 21600-604800 seconds (6 hours to 7 days).

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num*-*end_port_num*

Example:

The following example sets the block allocation size to 64, the per-host maximum to 8, and enables interim logging every 6 hours.

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) Select the following options in the FlexConfig object:

- **Deployment** = **Everytime**
- **Type** = **Append**

f) Click **Save** to create the FlexConfig object.

g) Select **Devices** > **FlexConfig**, and create or edit the FlexConfig policy that is assigned to the devices that need to have these settings adjusted.
h) Select your object in the available objects list and click > to move it to the selected objects list.
i) Click **Save**.

You can click **Preview Config**, select one of the target devices, and verify that the xlate commands appear correctly.

Step 2 Add NAT rules that use PAT pool port block allocation.

a) Select **Devices** > **NAT** and add or edit the threat defense NAT policy.
b) Add or edit a NAT rule and configure at least the following options.

- **Type** = **Dynamic**
- In **Translation** > **Original Source**, select the object that defines the source address.
- On **PAT Pool**, configure the following options:
  - Select **Enable PAT Pool**
  - In **PAT** > **Address**, select a network object or group that defines the pat pool.
  - Select the **Block Allocation** option.

c) Save your changes to the rule and to the NAT policy.

Static NAT

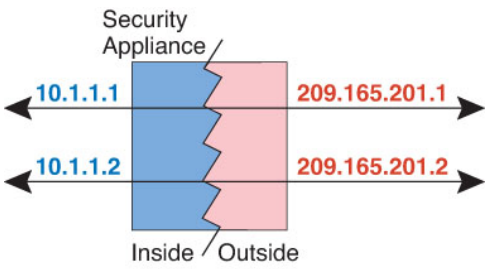
The following topics explain static NAT and how to implement it.

About static NAT

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an access rule exists that allows it). With dynamic NAT and PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

The following figure shows a typical static NAT scenario. The translation is always active so both real and remote hosts can initiate connections.

Figure 378: Static NAT



Note You can disable bidirectionality if desired.

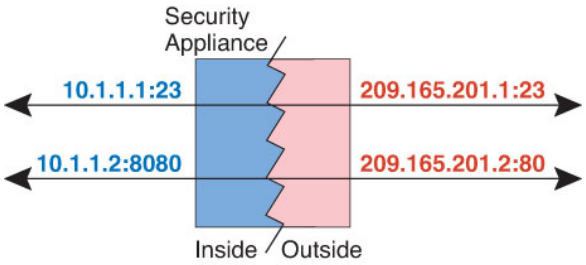
Static NAT with port translation

Static NAT with port translation lets you specify a real and mapped protocol and port.

When you specify the port with static NAT, you can choose to map the port and/or the IP address to the same value or to a different value.

The following figure shows a typical static NAT with port translation scenario showing both a port that is mapped to itself and a port that is mapped to a different value; the IP address is mapped to a different value in both cases. The translation is always active so both translated and remote hosts can initiate connections.

Figure 379: Typical Static NAT with Port Translation Scenario



Static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. In addition, for manual NAT, traffic that does not match the source IP address of the NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, you must add additional rules for all other traffic allowed to the destination IP address. For example, you can configure a static NAT rule for the IP address, without port specification, and place it after the port translation rule.

Note For applications that require application inspection for secondary channels (for example, FTP and VoIP), NAT automatically translates the secondary ports.

Following are some other uses of static NAT with port translation.

Static NAT with Identity Port Translation

You can simplify external access to internal resources. For example, if you have three separate servers that provide services on different ports (such as FTP, HTTP, and SMTP), you can give external users a single IP address to access those services. You can then configure static NAT with identity port translation to map the single external IP address to the correct IP addresses of the real servers based on the port they are trying to access. You do not need to change the port, because the servers are using the standard ones (21, 80, and 25 respectively).

Static NAT with Port Translation for Non-Standard Ports

You can also use static NAT with port translation to translate a well-known port to a non-standard port or vice versa. For example, if inside web servers use port 8080, you can allow outside users to connect

to port 80, and then undo translation to the original port 8080. Similarly, to provide extra security, you can tell web users to connect to non-standard port 6785, and then undo translation to port 80.

Static Interface NAT with Port Translation

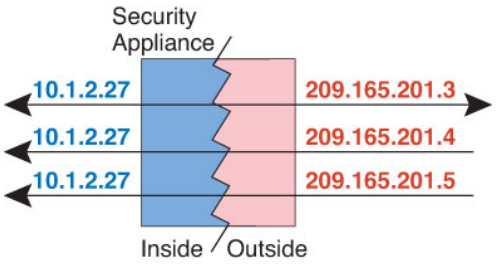
You can configure static NAT to map a real address to an interface address/port combination. For example, if you want to redirect Telnet access for the device's outside interface to an inside host, then you can map the inside host IP address/port 23 to the outside interface address/port 23.

One-to-many static NAT

Typically, you configure static NAT with a one-to-one mapping. However, in some cases, you might want to configure a single real address to several mapped addresses (one-to-many). When you configure one-to-many static NAT, when the real host initiates traffic, it always uses the first mapped address. However, for traffic initiated to the host, you can initiate traffic to any of the mapped addresses, and they will be untranslated to the single real address.

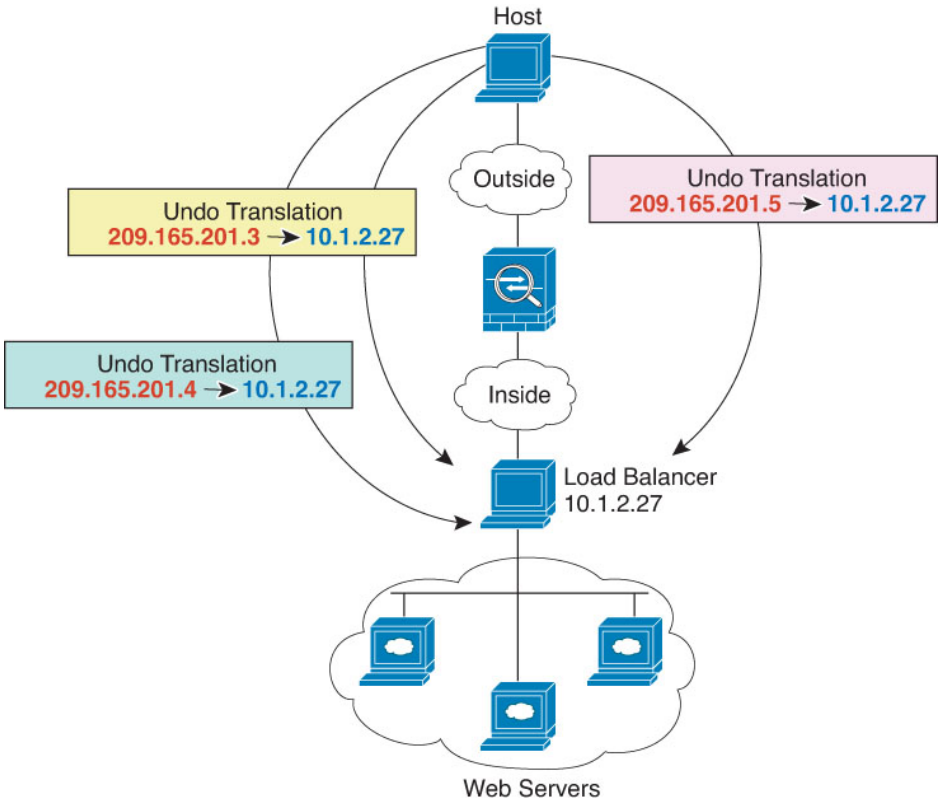
The following figure shows a typical one-to-many static NAT scenario. Because initiation by the real host always uses the first mapped address, the translation of real host IP/first mapped IP is technically the only bidirectional translation.

Figure 380: One-to-Many Static NAT



For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server.

Figure 381: One-to-Many Static NAT Example



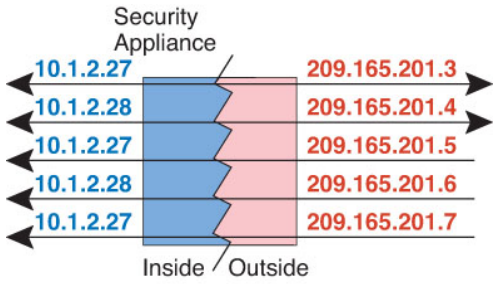
Other mapping scenarios (not recommended)

NAT has the flexibility to allow any kind of static mapping scenario: one-to-one, one-to-many, but also few-to-many, many-to-few, and many-to-one mappings. We recommend using only one-to-one or one-to-many mappings. These other mapping options might result in unintended consequences.

Functionally, few-to-many is the same as one-to-many; but because the configuration is more complicated and the actual mappings may not be obvious at a glance, we recommend creating a one-to-many configuration for each real address that requires it. For example, for a few-to-many scenario, the few real addresses are mapped to the many mapped addresses in order (A to 1, B to 2, C to 3). When all real addresses are mapped, the next mapped address is mapped to the first real address, and so on until all mapped addresses are mapped (A to 4, B to 5, C to 6). This results in multiple mapped addresses for each real address. Just like a one-to-many configuration, only the first mappings are bidirectional; subsequent mappings allow traffic to be initiated *to* the real host, but all traffic *from* the real host uses only the first mapped address for the source.

The following figure shows a typical few-to-many static NAT scenario.

Figure 382: Few-to-Many Static NAT

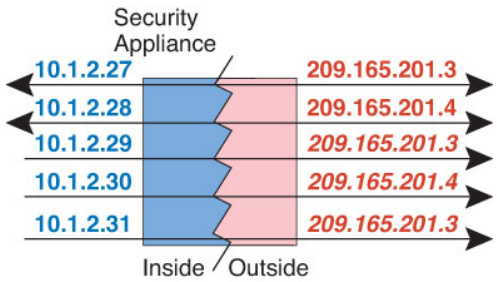


For a many-to-few or many-to-one configuration, where you have more real addresses than mapped addresses, you run out of mapped addresses before you run out of real addresses. Only the mappings between the lowest real IP addresses and the mapped pool result in bidirectional initiation. The remaining higher real addresses can initiate traffic, but traffic cannot be initiated to them (returning traffic for a connection is directed to the correct real address because of the unique 5-tuple (source IP, destination IP, source port, destination port, protocol) for the connection).

Note Many-to-few or many-to-one NAT is not PAT. If two real hosts use the same source port number and go to the same outside server and the same TCP destination port, and both hosts are translated to the same IP address, then both connections will be reset because of an address conflict (the 5-tuple is not unique).

The following figure shows a typical many-to-few static NAT scenario.

Figure 383: Many-to-Few Static NAT



Instead of using a static rule this way, we suggest that you create a one-to-one rule for the traffic that needs bidirectional initiation, and then create a dynamic rule for the rest of your addresses.

Configure static auto NAT

Use static auto NAT rules to translate addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host, range, or subnet.

- **Translated Source**—You have the following options to specify the translated address:
  - **Destination Interface**—To use the destination interface address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
  - **Address**—Create a network object or group containing hosts, ranges, or subnets. A group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** ( ) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **NAT Rule**—Select **Auto NAT Rule**.
- **Type**—Select **Static**.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 On **Translation**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—One of the following:
  - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.

- (Optional.) **Original Port**, **Translated Port**—If you need to translate a TCP or UDP port, select the protocol in **Original Port**, and type the original and translated port numbers. For example, you can translate TCP/80 to 8080 if necessary.

Step 6 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see DNS query and response rewriting using NAT, on page 1296. This option is not available if you are doing port translation.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Net to Net Mapping**—For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Step 7 Click **Save** to add the rule.

Step 8 Click **Save** on the NAT page to save your changes.

Configure static manual NAT

Use static manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Static NAT translates addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—You have the following options to specify the translated address:
  - **Destination Interface**—To use the destination interface address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.

- **Address**—Create a network object or group containing hosts, range, or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.

You can also create network objects or groups for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** (✎) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

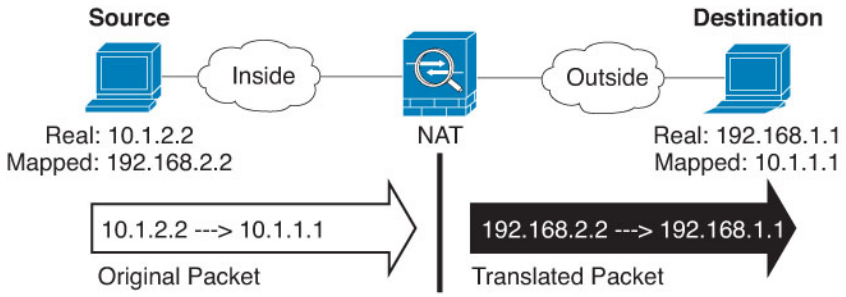
- **NAT Rule**—Select **Manual NAT Rule**.
- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 (On the **Translation** page.) Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object or group that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Source Interface IP** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—One of the following:
  - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port**, **Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port**, **Translated Destination Port**—Defines a port translation for the destination address.

Step 8 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see DNS query and response rewriting using NAT, on page 1296. This option is not available if you are doing port translation.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Net to Net Mapping**—For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Unidirectional**—Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

Step 9 Click **Save** to add the rule.

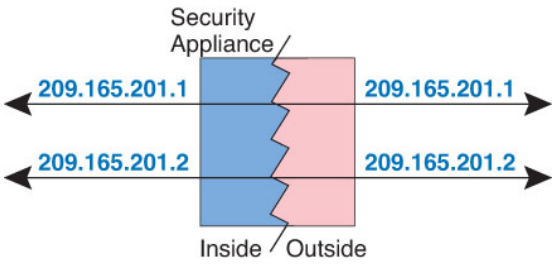
Step 10 Click **Save** on the NAT page to save your changes.

Identity NAT

You might have a NAT configuration in which you need to translate an IP address to itself. For example, if you create a broad rule that applies NAT to every network, but want to exclude one network from NAT, you can create a static NAT rule to translate that network to itself.

The following figure shows a typical identity NAT scenario.

Figure 384: Identity NAT



The following topics explain how to configure identity NAT.

Configure identity auto NAT

Use static identity auto NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host, range, or subnet.
- **Translated Source**—A network object or group with the exact same contents as the original source object. You can use the same object.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** ( ) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **NAT Rule**—Select **Auto NAT Rule**.
- **Type**—Select **Static**.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 On **Translation**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Do not configure the **Original Port** and **Translated Port** options for identity NAT.

Step 6 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **IPv6**—Do not configure this option for identity NAT.
- **Net to Net Mapping**—Do not configure this option for identity NAT.

- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Perform Route Lookup for Destination Interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Step 7 Click **Save** to add the rule.

Step 8 Click **Save** on the NAT page to save your changes.

Configure identity manual NAT

Use static identity manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Use static identity NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin

Select **Objects** > **Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—The same object or group as the original source. Optionally, you can select a different object that has the exact same contents.

You can also create network objects or groups for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports. You can use the same object for identity NAT.

Procedure

Step 1 Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

Step 2 Do one of the following:

- Click the **Add Rule** button to create a new rule.
- Click **Edit** (✎) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

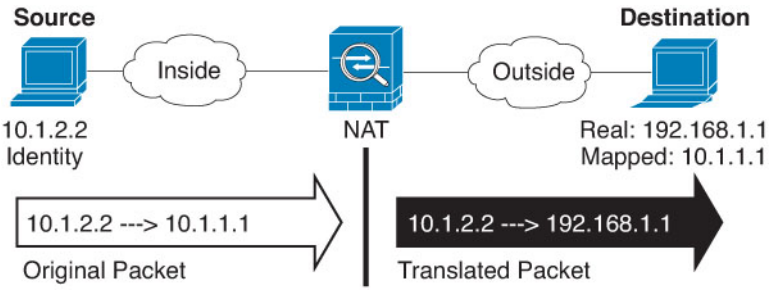
- **NAT Rule**—Select **Manual NAT Rule**.
- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Step 4 On **Interface Objects**, configure the following options:

- **Source Interface Objects**, **Destination Interface Objects**—(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 5 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet where you perform identity NAT on the inside host but translate the outside host.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object or group that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

  You can select **Interface Object** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 6 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—The same object or group as the original source. Optionally, you can select a different object that has the exact same contents.

- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 7 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port**, **Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port**, **Translated Destination Port**—Defines a port translation for the destination address.

Step 8 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Perform Route Lookup for Destination Interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.
- **Unidirectional**—Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

Step 9 Click **Save** to add the rule.

Step 10 Click **Save** on the NAT page to save your changes.

NAT rule properties for Firewall Threat Defense

Use network address translation (NAT) rules to translate IP addresses to other IP addresses. You would typically use NAT rules to convert private addresses to publicly routable addresses. The translation can be from one address to another, or you can use port address translation (PAT) to translate many addresses to one or a few addresses, using port numbers to distinguish among the source addresses.

NAT rules include the following basic properties. The properties are the same for auto NAT and manual NAT rules except where indicated.

NAT Type

Whether you want to configure a **Manual NAT Rule** or an **Auto NAT Rule**. Auto NAT translates the source address only, and you cannot make different translations based on the destination address. Because auto NAT is more simple to configure, use it unless you need the added features of manual NAT. For more information on the differences, see Auto NAT and Manual NAT, on page 1191.

Type

Whether the translation rule is **Dynamic** or **Static**. Dynamic translation automatically chooses the mapped address from a pool of addresses, or an address/port combination when implementing PAT. Use static translation if you want to precisely define the mapped address/port.

Enable (Manual NAT only.)

Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page. You cannot disable auto NAT rules.

Insert (Manual NAT only.)

Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Description (Optional. Manual NAT only.)

A description of the purpose of the rule.

The following topics describe the tabs for the NAT rules properties.

Interface objects NAT properties

Interface objects (security zones or interface groups) define the interfaces to which a NAT rule applies. In routed mode, you can use the default "any" for both source and destination to apply to all interfaces of all assigned devices. However, you typically want to select specific source and destination interfaces.

Notes

- The concept of “any” interface does not apply to bridge group member interfaces. When you specify “any” interface, all bridge group member interfaces are excluded. Thus, to apply NAT to bridge group members, you must specify the member interface. You cannot configure NAT for the bridge virtual interface (BVI) itself, you can configure NAT for member interfaces only.

  If you select interface objects, a NAT rule will be configured on an assigned device only if the device has interfaces included in all selected objects. For example, if you select both source and destination security zones, both zones must contain one or more interface for a given device.

- If more than one interface in an interface object exists on a given device, identical rules are created for each interface. This can become an issue for static NAT rules that include destination translation. Because NAT rules are applied based on first hit rule, only the rule created for the first interface configured for the object matches traffic. When configuring static NAT with destination translation, use interface objects that include at most one interface per device assigned to the NAT policy to ensure you are getting the desired results.

Source Interface Objects, Destination Interface Objects

(Required for bridge group member interfaces.) The interface objects (security zones or interface groups) that identify the interfaces where this NAT rule applies. **Source** is the object containing the real interface, the one through which the traffic enters the device. **Destination** is the object containing the mapped

interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Translation properties for auto NAT

Use the **Translation** options to define the source addresses and the mapped translated addresses. The following properties apply to auto NAT only.

Original Source (Always required.)

The network object that contains the addresses you are translating. This must be a network object (not a group), and it can be a host, range, or subnet.

You cannot create auto NAT rules for the system-defined any-ipv4 or any-ipv6 objects.

Translated Source (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.
- **Dynamic PAT**—One of the following:
  - (Interface PAT.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Do not configure a PAT pool.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose. Do not configure a PAT pool.
  - To use a PAT pool, leave **Translated Source** empty. Select the PAT pool object on **PAT Pool**.
- **Static NAT**—One of the following:
  - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. The object or group can contain hosts, ranges, or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on the **Advanced** tab. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Port, Translated Port (Static NAT only.)

If you need to translate a TCP or UDP port, select the protocol in **Original Port**, and type the original and translated port numbers. For example, you can translate TCP/80 to 8080 if necessary. Do not configure these options for identity NAT.

Translation properties for manual NAT

Use the **Translation** options to define the source addresses and the mapped translated addresses. The following properties apply to manual NAT only. All are optional except as indicated.

Original Source (Always required.)

The network object or group that contains the addresses you are translating. This can be a network object or group, and it can contain a host, range, or subnet. If you want to translate all original source traffic, you can specify **Any** in the rule.

Translated Source (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. If a group contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback. If the object contains one host address only, it is used for PAT.
- **Dynamic PAT**—One of the following:
  - (Interface PAT.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Do not configure a PAT pool.
  - To use a single address other than the destination interface address, select the host network object you created for this purpose. Do not configure a PAT pool.
  - To use a PAT pool, leave **Translated Source** empty. Select the PAT pool object on **PAT Pool**.
- **Static NAT**—One of the following:
  - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. The object or group can contain hosts, ranges, or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
  - (Static interface NAT with port translation.) To use the address of the destination interface, select **Destination Interface IP**. You must also select a specific destination interface object. To use the IPv6 address of the interface, you must also select the **IPv6** option on the **Advanced** tab. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Destination

The network object or group that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Source Interface IP** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Translated Destination

The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

You can use a network object that specifies a fully-qualified domain name as the translated destination; for more information, see FQDN destination guidelines, on page 1200.

Original Source Port, Translated Source Port, Original Destination Port, Translated Destination Port

The port objects that define the source and destination services for the original and translated packets. You can translate the ports, or select the same object to make the rule sensitive to the service without translating the ports. Keep the following rules in mind when configuring services:

- (Dynamic NAT or PAT.) You cannot do translation on the **Original Source Port** and **Translated Source Port**. You can do translation on the destination port only.
- NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

PAT pool NAT properties

When you configure dynamic NAT, you can define a pool of addresses to use for port address translation using the properties on the **PAT Pool** tab.

Enable PAT Pool

Select this option to configure a pool of addresses for PAT.

PAT

The addresses to use for the PAT pool, one of the following:

- **Address**—The object that defines the PAT pool addresses, either a network object that includes a range, or a network object group that contains hosts, ranges, or both. You cannot include subnets. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
- **Destination Interface IP**—Indicates that you want to use the destination interface as the PAT address. For this option, you must select a specific **Destination Interface Object**; you cannot use **Any** as the destination interface. This is another way to implement interface PAT.

Round Robin

To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one

address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

Extended PAT Table

To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.

Flat Port Range; Include Reserved Ports

To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. (Pre-6.7) When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option. For the Firewall Threat Defense devices running version 6.7 or higher, the flat port range is always configured, whether you select the option or not. You can still select the **Include Reserved Ports** option for these systems, and that setting is honored.

Block Allocation

To enable port block allocation. For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time. If you allocate a block of ports, subsequent connections from the host use new randomly selected ports within the block. If necessary, additional blocks are allocated if the host has active connections for all ports in the original block. Port blocks are allocated in the 1024-65535 range only. Port block allocation is compatible with round robin, but you cannot use it with the extended PAT or flat port range options. You also cannot use interface PAT fallback.

Advanced NAT properties

When you configure NAT, you can configure properties that provide specialized services in the **Advanced** options. All of these properties are optional: configure them only if you need the service.

Translate DNS replies that match this rule

Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. For more information, see DNS query and response rewriting using NAT, on page 1296. This option is not available if you are doing port translation in a static NAT rule.

Fallthrough to Interface PAT (Destination Interface) (Dynamic NAT only.)

Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option. You cannot select this option if you already configured interface PAT as the translated address. You also cannot select the option if you configure a PAT pool.

IPv6

Whether to use the IPv6 address of the destination interface for interface PAT.

Net to Net Mapping (Static NAT only.)

For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.

Do not proxy ARP on Destination Interface (Static NAT only.)

Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Perform Route Lookup for Destination Interface (Static Identity NAT only. Routed mode only.)

If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Unidirectional (Manual NAT only, static NAT only.)

Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

Translating IPv6 networks

In cases where you need to pass traffic between IPv6-only and IPv4-only networks, you need to use NAT to convert between the address types. Even with two IPv6 networks, you might want to hide internal addresses from the outside network.

You can use the following translation types with IPv6 networks:

- NAT64, NAT46—Translates IPv6 packets into IPv4 and vice versa. You need to define two policies, one for the IPv6 to IPv4 translation, and one for the IPv4 to IPv6 translation. Although you can accomplish this with a single manual NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a manual NAT rule when you specify a destination, creating two auto NAT rules is the better solution.



Note NAT46 supports static mappings only.

- NAT66—Translates IPv6 packets to a different IPv6 address. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.

Note NAT64 and NAT 46 are possible on standard routed interfaces only. NAT66 is possible on both routed and bridge group member interfaces.

NAT64/46: translating IPv6 addresses to IPv4

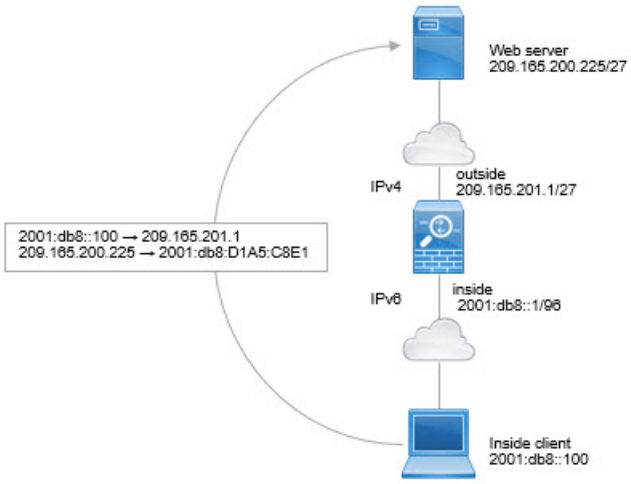
When traffic goes from an IPv6 network to an IPv4-only network, you need to convert the IPv6 address to IPv4, and return traffic from IPv4 to IPv6. You need to define two address pools, an IPv4 address pool to bind IPv6 addresses in the IPv4 network, and an IPv6 address pool to bind IPv4 addresses in the IPv6 network.

- The IPv4 address pool for the NAT64 rule is normally small and typically might not have enough addresses to map one-to-one with the IPv6 client addresses. Dynamic PAT might more easily meet the possible large number of IPv6 client addresses compared to dynamic or static NAT.
- The IPv6 address pool for the NAT46 rule can be equal to or larger than the number of IPv4 addresses to be mapped. This allows each IPv4 address to be mapped to a different IPv6 address. NAT46 supports static mappings only, so you cannot use dynamic PAT.

You need to define two policies, one for the source IPv6 network, and one for the destination IPv4 network. Although you can accomplish this with a single manual NAT rule, if the DNS server is on the external network, you probably need to rewrite the DNS response. Because you cannot enable DNS rewrite on a manual NAT rule when you specify a destination, creating two auto NAT rules is the better solution.

NAT64/46 example: inside IPv6 network with outside IPv4 internet

Following is a straight-forward example where you have an inside IPv6-only network, and you want to convert to IPv4 for traffic sent to the Internet. This example assumes you do not need DNS translation, so you can perform both the NAT64 and NAT46 translations in a single manual NAT rule.



In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network.

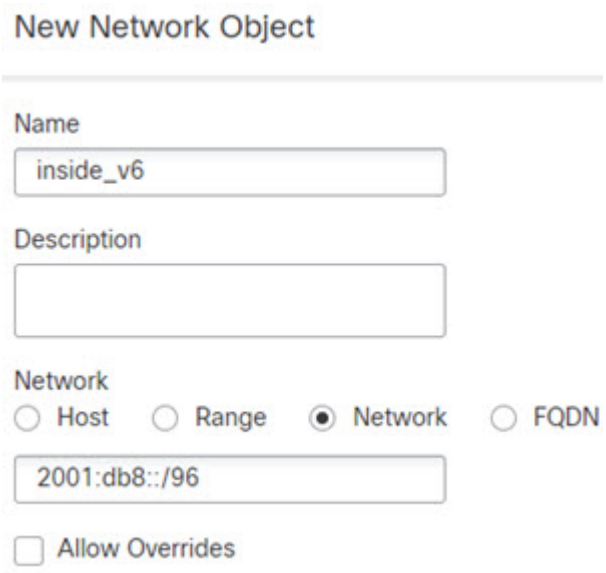
Procedure

Step 1 Create the network object that defines the inside IPv6 network.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the inside IPv6 network.

Name the network object (for example, inside_v6) and enter the network address, 2001:db8::/96.



c) Click **Save**.

Step 2 Create the manual NAT rule to translate the IPv6 network to IPv4 and back again.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

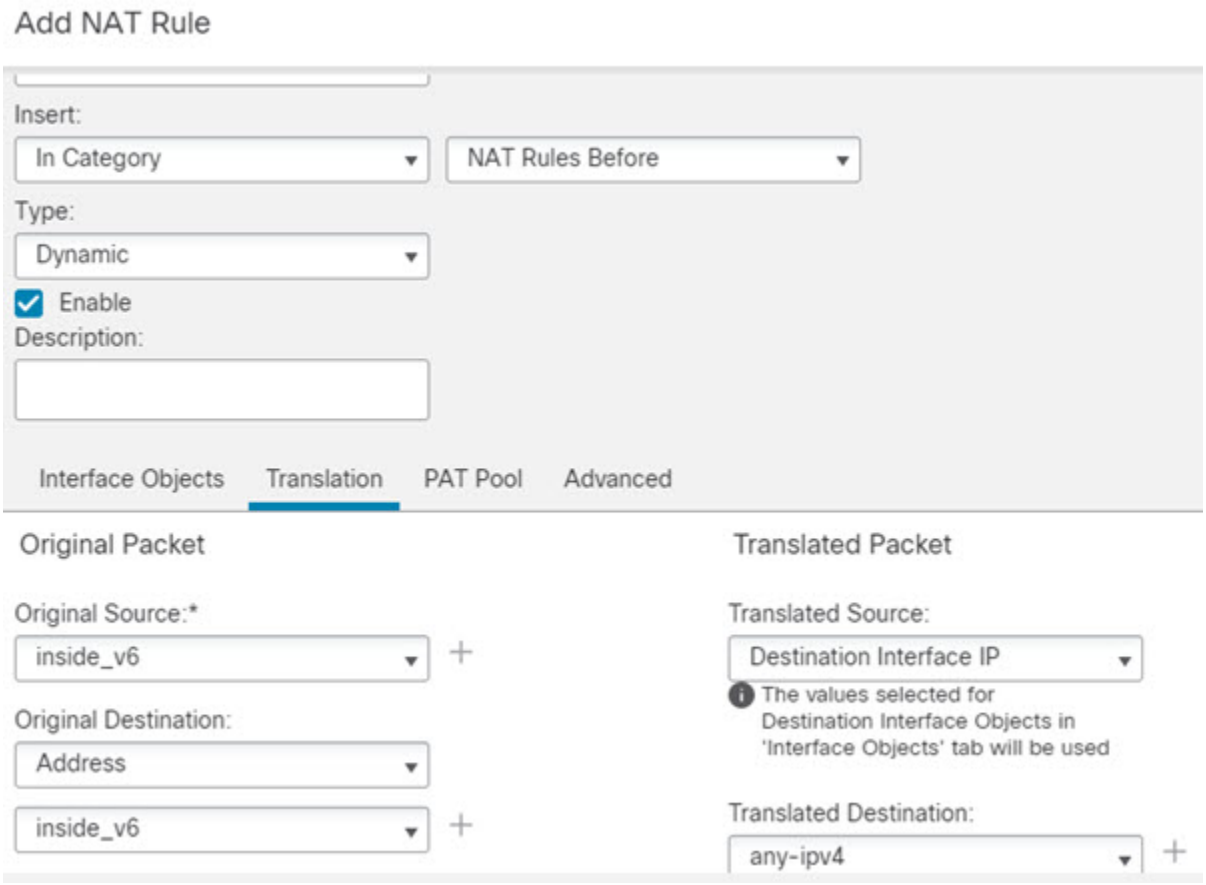
- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = inside_v6 network object.
- **Translated Source** = **Destination Interface IP**.
- **Original Destination** = inside_v6 network object.
- **Translated Destination** = any-ipv4 network object.



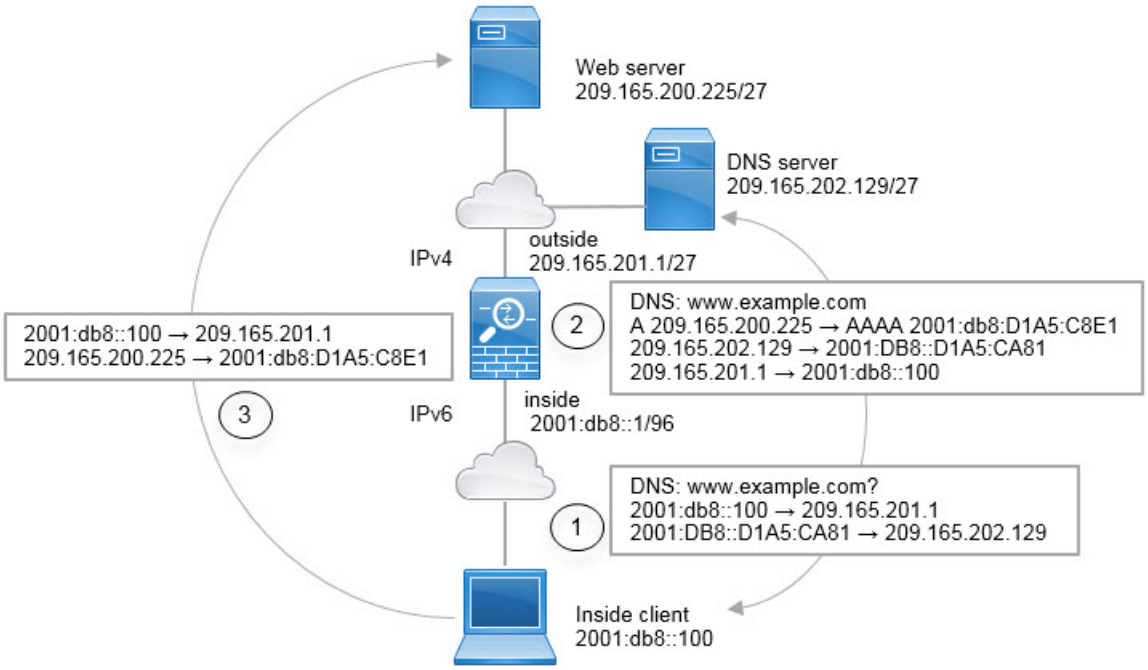
f) Click **OK**.

With this rule, any traffic from the 2001:db8::/96 subnet on the inside interface going to the outside interface gets a NAT64 PAT translation using the IPv4 address of the outside interface. Conversely, any IPv4 address on the outside network coming to the inside interface is translated to an address on the 2001:db8::/96 network using the embedded IPv4 address method.

g) Click **Save** on the NAT rules page.

NAT64/46 example: inside IPv6 network with outside IPv4 internet and DNS translation

Following is a typical example where you have an inside IPv6-only network, but there are some IPv4-only services on the outside Internet that internal users need.



In this example, you translate the inside IPv6 network to IPv4 using dynamic interface PAT with the IP address of the outside interface. Outside IPv4 traffic is statically translated to addresses on the 2001:db8::/96 network, allowing transmission on the inside network. You enable DNS rewrite on the NAT46 rule, so that replies from the external DNS server can be converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

Following is a typical sequence for a web request where a client at 2001:DB8::100 on the internal IPv6 network tries to open www.example.com.

1. The client's computer sends a DNS request to the DNS server at 2001:DB8::D1A5:CA81. The NAT rules make the following translations to the source and destination in the DNS request:
   - 2001:DB8::100 to a unique port on 209.165.201.1 (The NAT64 interface PAT rule.)
   - 2001:DB8::D1A5:CA81 to 209.165.202.129 (The NAT46 rule. D1A5:CA81 is the IPv6 equivalent of 209.165.202.129.)
2. The DNS server responds with an A record indicating that www.example.com is at 209.165.200.225. The NAT46 rule, with DNS rewrite enabled, converts the A record to the IPv6-equivalent AAAA record, and translates 209.165.200.225 to 2001:db8:D1A5:C8E1in the AAAA record. In addition, the source and destination addresses in the DNS response are untranslated:
   - 209.165.202.129 to 2001:DB8::D1A5:CA81
   - 209.165.201.1 to 2001:db8::100
3. The IPv6 client now has the IP address of the web server, and makes an HTTP request to www.example.com at 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) The source and destination of the HTTP request are translated:
   - 2001:DB8::100 to a unique port on 209.156.101.54 (The NAT64 interface PAT rule.)
   - 2001:db8:D1A5:C8E1 to 209.165.200.225 (The NAT46 rule.)

The following procedure explains how to configure this example.

Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

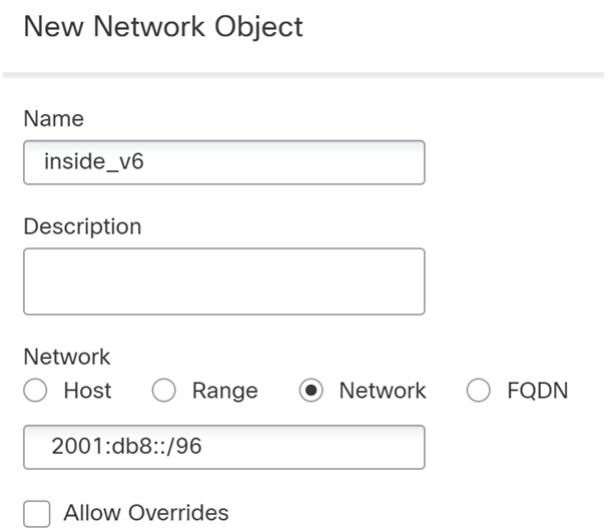
Procedure

Step 1 Create the network objects that define the inside IPv6 and outside IPv4 networks.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the inside IPv6 network.

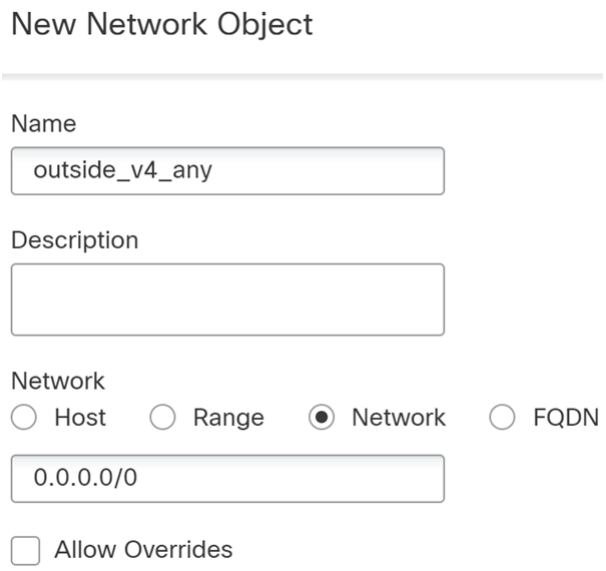
Name the network object (for example, inside_v6) and enter the network address, 2001:db8::/96.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the outside IPv4 network.

Name the network object (for example, outside_v4_any) and enter the network address 0.0.0.0/0.



e) Click **Save**.

Step 2 Configure the NAT64 dynamic PAT rule for the inside IPv6 network.

Step 3 Configure the static NAT46 rule for the outside IPv4 network.

a) Click **Add Rule**.

b) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

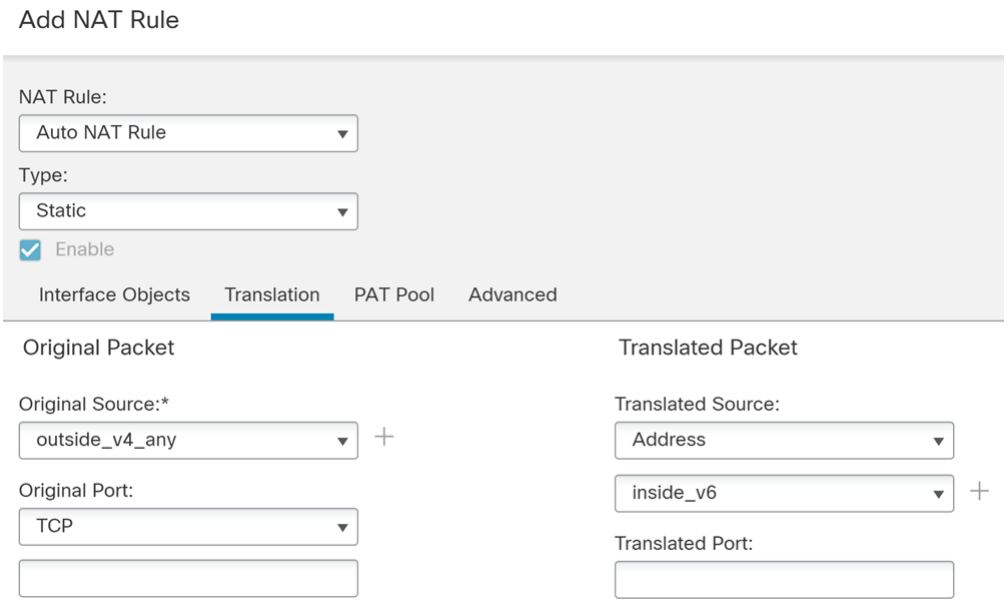
c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) On **Translation**, configure the following:

- **Original Source** = outside_v4_any network object.
- **Translated Source** > **Address** = inside_v6 network object.

e) On **Advanced**, select **Translate DNS replies that match this rule**.



f) Click **OK**.

With this rule, any IPv4 address on the outside network coming to the inside interface is translated to an address on the 2001:db8::/96 network using the embedded IPv4 address method. In addition, DNS responses are converted from A (IPv4) to AAAA (IPv6) records, and the addresses converted from IPv4 to IPv6.

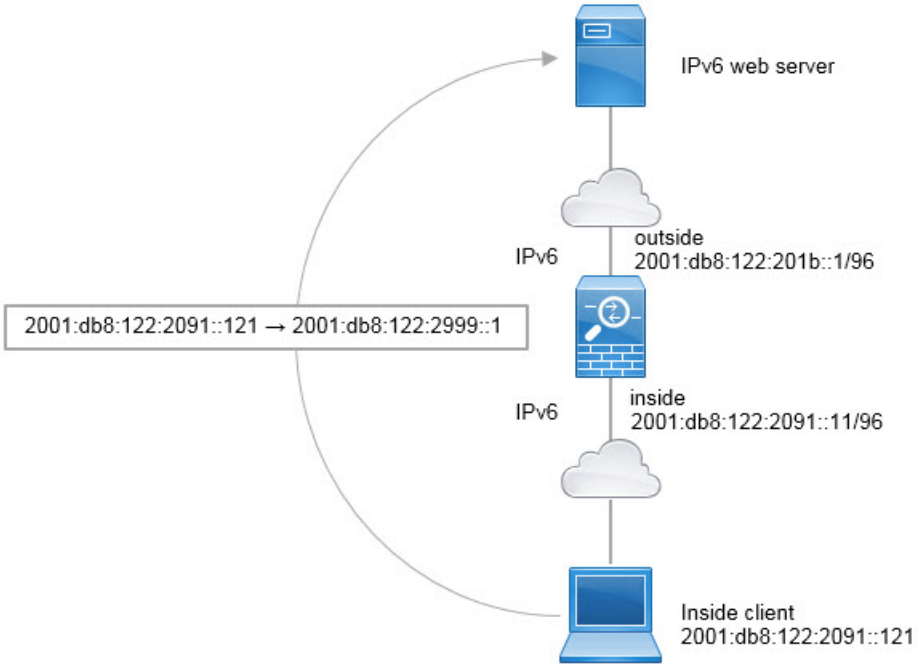
NAT66: translating IPv6 addresses to different IPv6 addresses

When going from an IPv6 network to another IPv6 network, you can translate the addresses to different IPv6 addresses on the outside network. We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT.

Because you are not translating between different address types, you need a single rule for NAT66 translations. You can easily model these rules using auto NAT. However, if you do not want to allow returning traffic, you can make the static NAT rule unidirectional using manual NAT only.

NAT66 example, static translation between networks

You can configure a static translation between IPv6 address pools using auto NAT. The following example explains how to convert inside addresses on the 2001:db8:122:2091::/96 network to outside addresses on the 2001:db8:122:2999::/96 network.



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

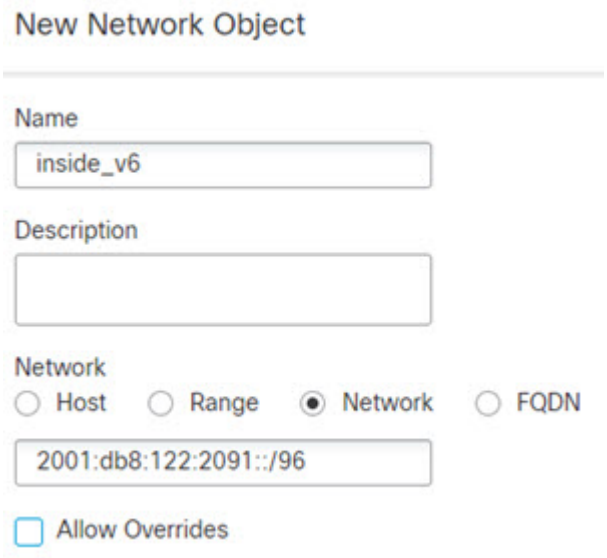
Procedure

Step 1 Create the network objects that define the inside IPv6 and outside IPv6 NAT networks.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the inside IPv6 network.

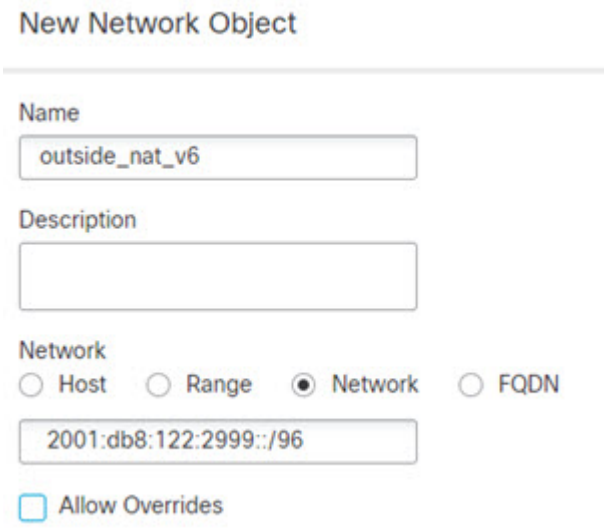
Name the network object (for example, inside_v6) and enter the network address, 2001:db8:122:2091::/96.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the outside IPv6 NAT network.

Name the network object (for example, outside_nat_v6) and enter the network address 2001:db8:122:2999::/96.



e) Click **Save**.

Step 2 Configure the static NAT rule for the inside IPv6 network.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

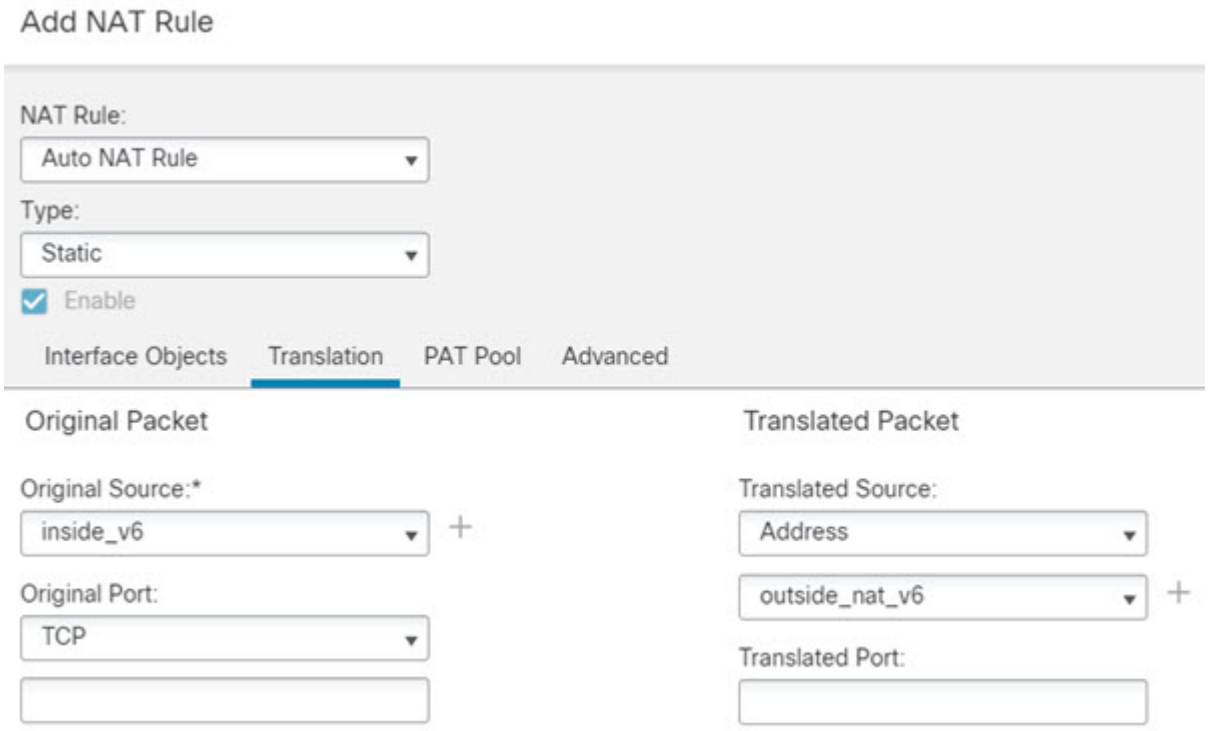
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = inside_v6 network object.
- **Translated Source** > **Address** = outside_nat_v6 network object.



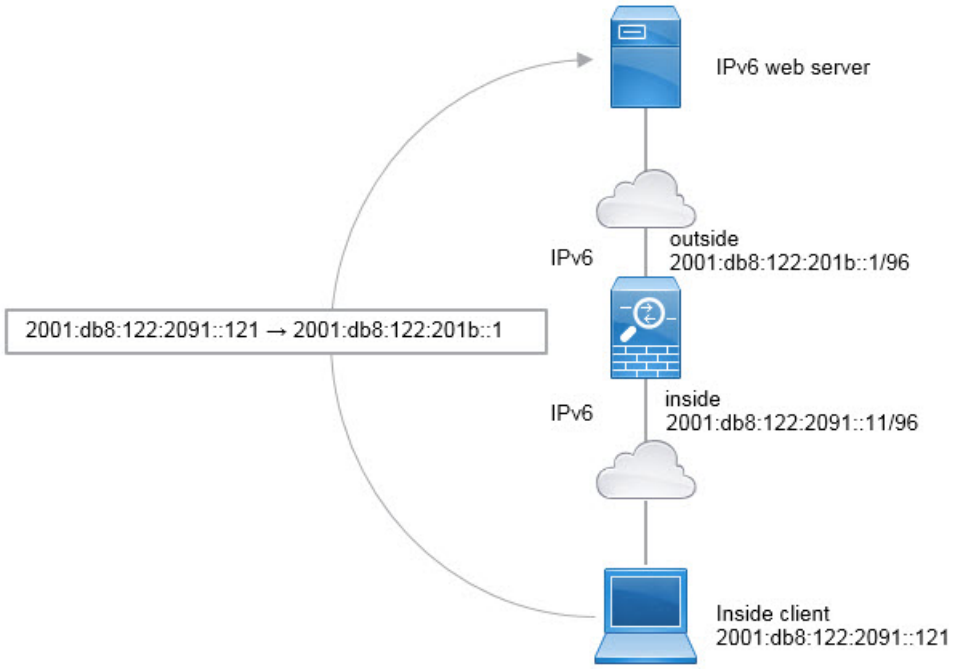
f) Click **OK**.

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a static NAT66 translation to an address on the 2001:db8:122:2999::/96 network.

NAT66 example, simple IPv6 interface PAT

A simple approach for implementing NAT66 is to dynamically assign internal addresses to different ports on the outside interface IPv6 address.

When you configure an interface PAT rule for NAT66, all the global addresses that are configured on that interface are used for PAT mapping. Link-local or site-local addresses for the interface are not used for PAT.



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

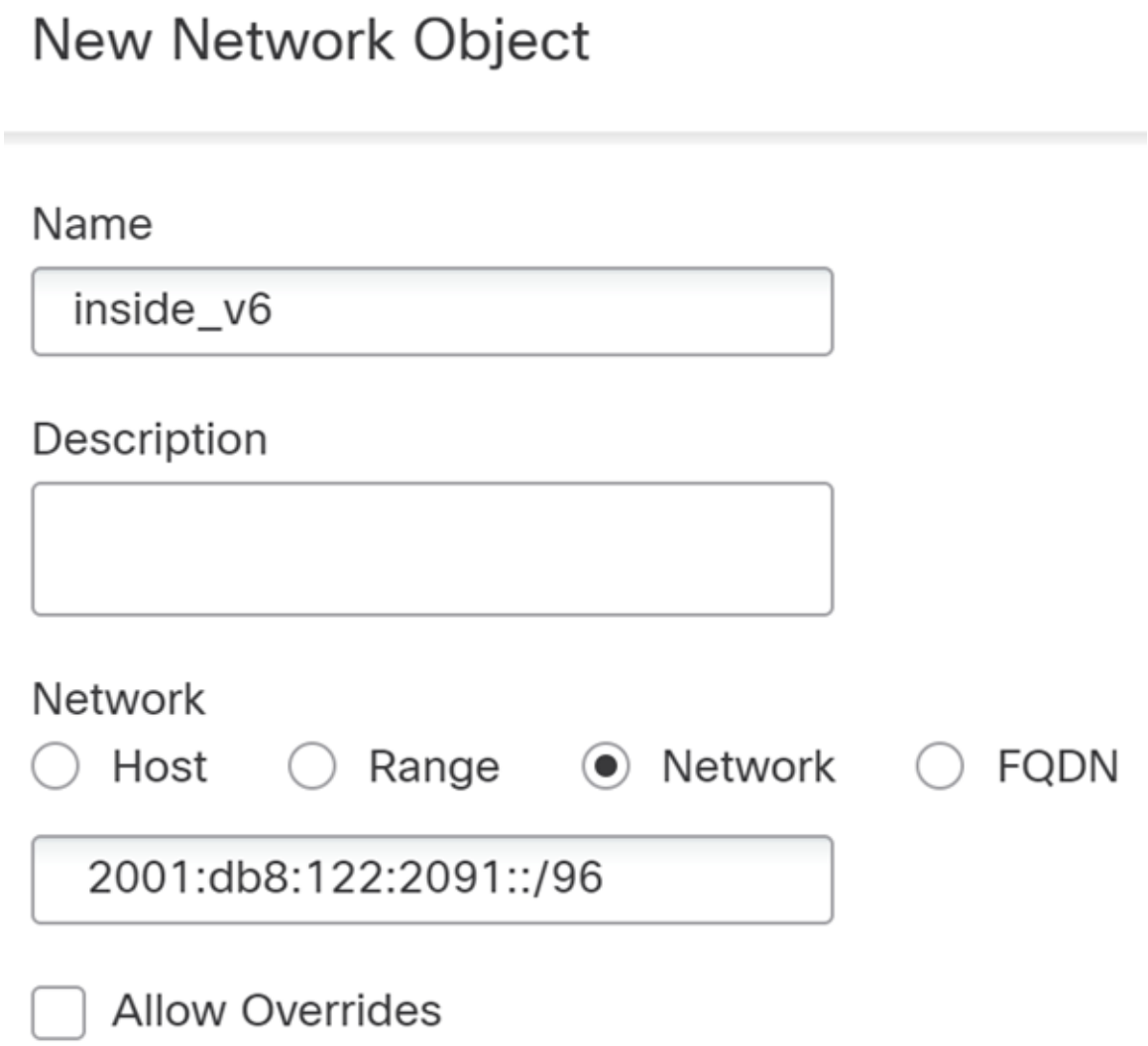
Procedure

Step 1 Create the network object that defines the inside IPv6 network.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the inside IPv6 network.

Name the network object (for example, inside_v6) and enter the network address, 2001:db8:122:2091::/96.



c) Click **Save**.

Step 2 Configure the dynamic PAT rule for the inside IPv6 network.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamic.

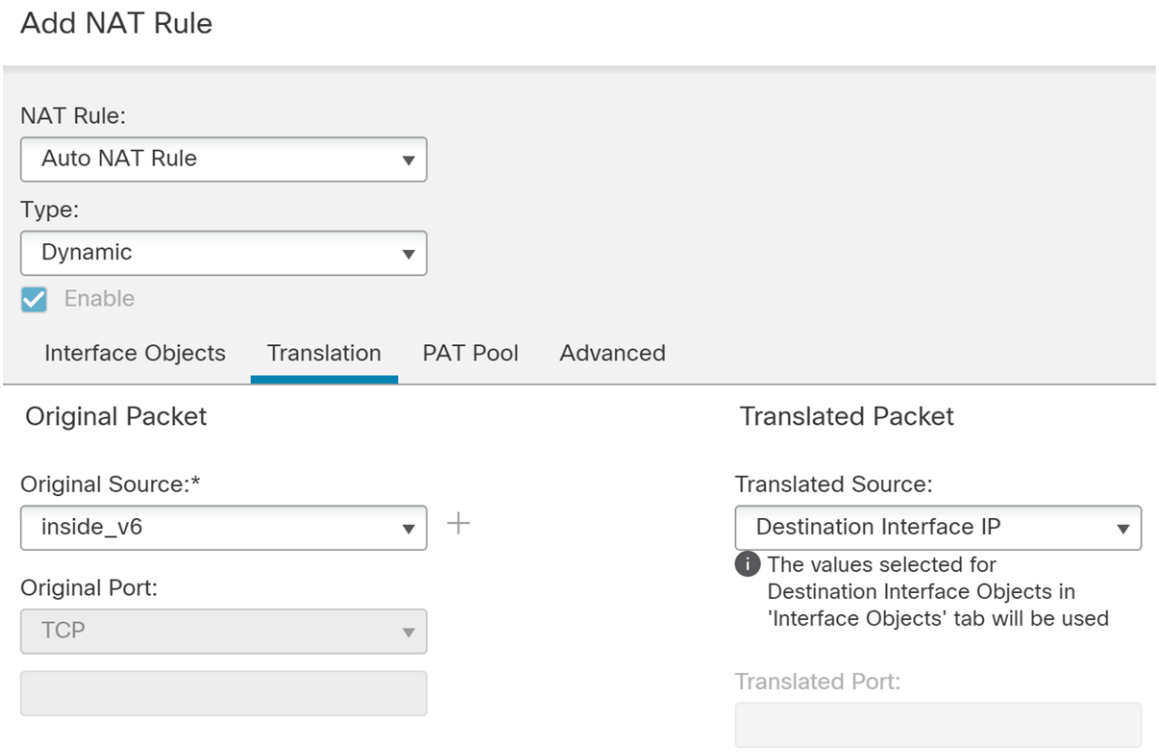
d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = inside_v6 network object.
- **Translated Source** = **Destination Interface IP**.

f) On **Advanced**, select **IPv6**, which indicates that the IPv6 address of the destination interface should be used.



g) Click **OK**.

With this rule, any traffic from the 2001:db8:122:2091::/96 subnet on the inside interface going to the outside interface gets a NAT66 PAT translation to one of the IPv6 global addresses configured for the outside interface.

Monitoring NAT

To monitor and troubleshoot NAT connections, log into the device CLI and use the following commands.

- **show nat** displays the NAT rules and per-rule hit counts. There are additional keywords to show other aspects of NAT.
- **show xlate** displays the actual NAT translations that are currently active.
- **clear xlate** lets you remove an active NAT translation. You might need to remove active translations if you alter NAT rules, because existing connections continue to use the old translation slot until the

connection ends. Clearing a translation allows the system to build a new translation for a client on the client's next connection attempt based on your new rules.

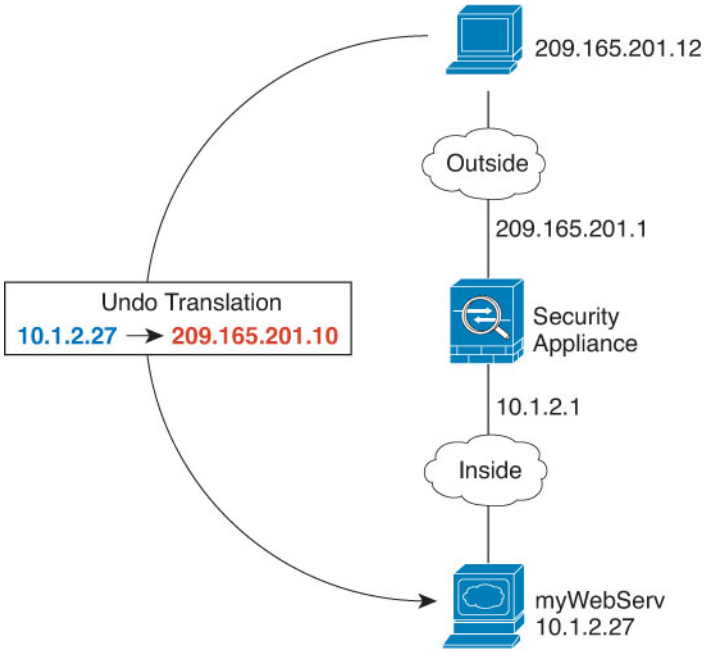
Examples for NAT

The following topics provide examples for configuring NAT.

Providing access to an inside web server (static auto NAT)

This example performs static NAT for an inside web server. The real address is on a private network, so a public address is required. Static NAT is necessary so hosts can initiate traffic to the web server at a fixed address.

Figure 385: Static NAT for an inside web server



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the web server. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

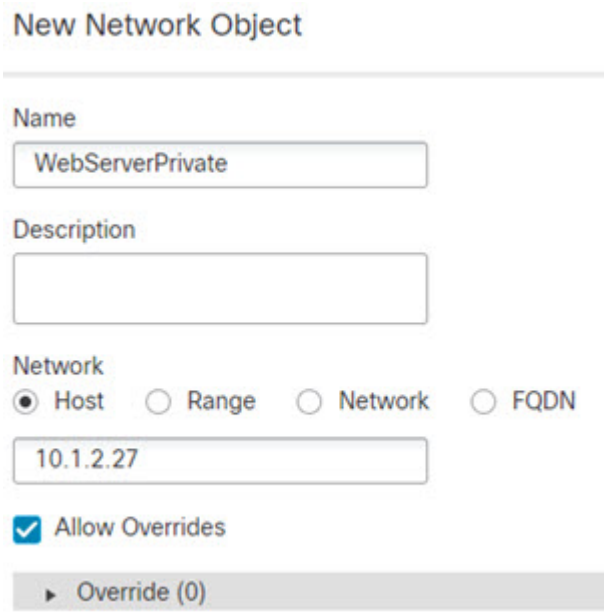
Procedure

Step 1 Create the network objects that define the server's private and public host addresses.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the web server's private address.

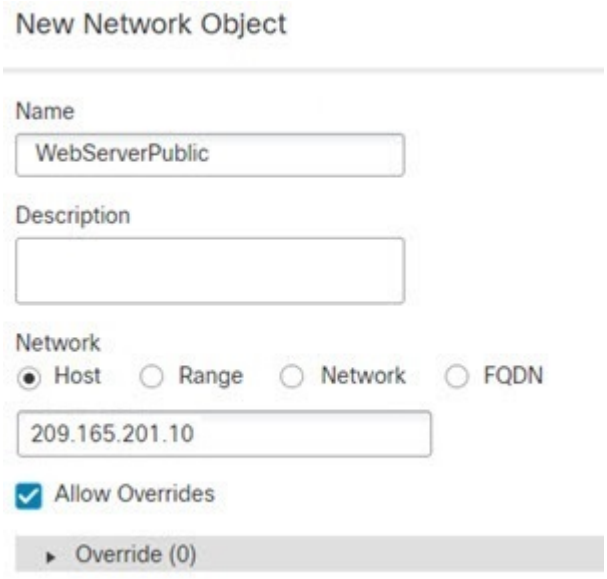
Name the network object (for example, WebServerPrivate) and enter the real host IP address, 10.1.2.27.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the public address.

Name the network object (for example, WebServerPublic) and enter the host address 209.165.201.10.



e) Click **Save**.

Step 2 Configure static NAT for the object.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

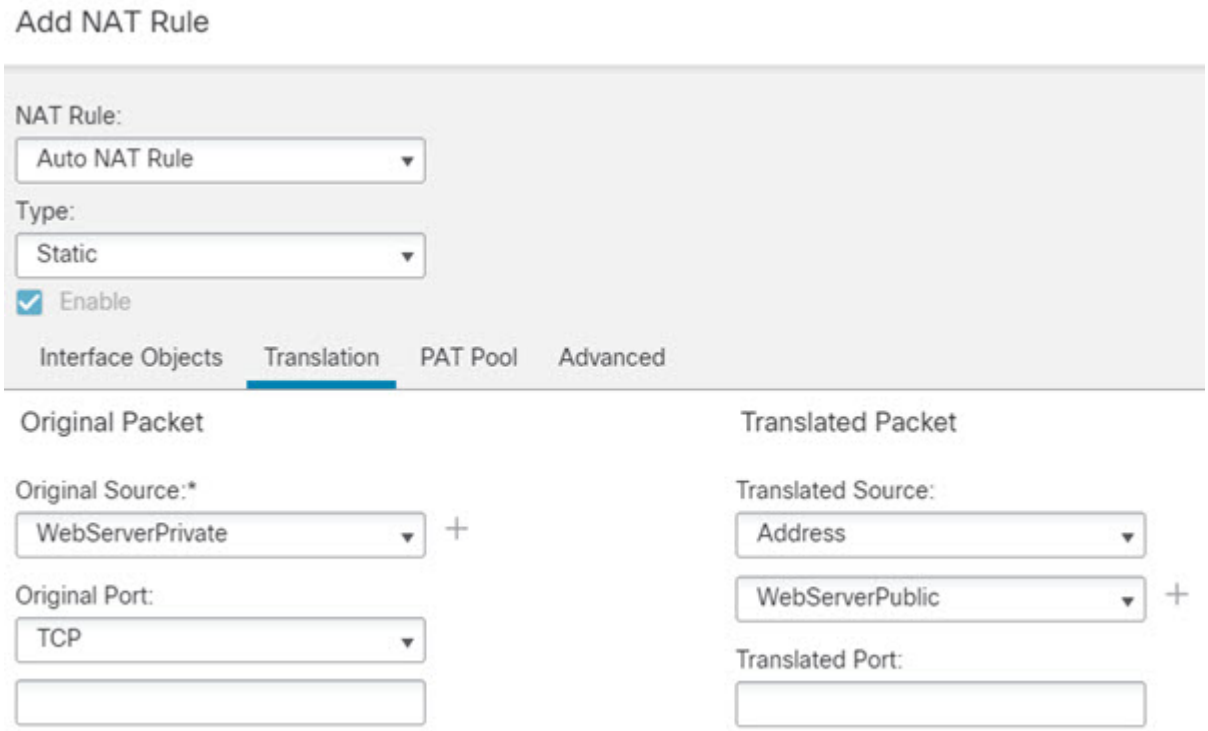
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = WebServerPrivate network object.
- **Translated Source** > **Address** = WebServerPublic network object.



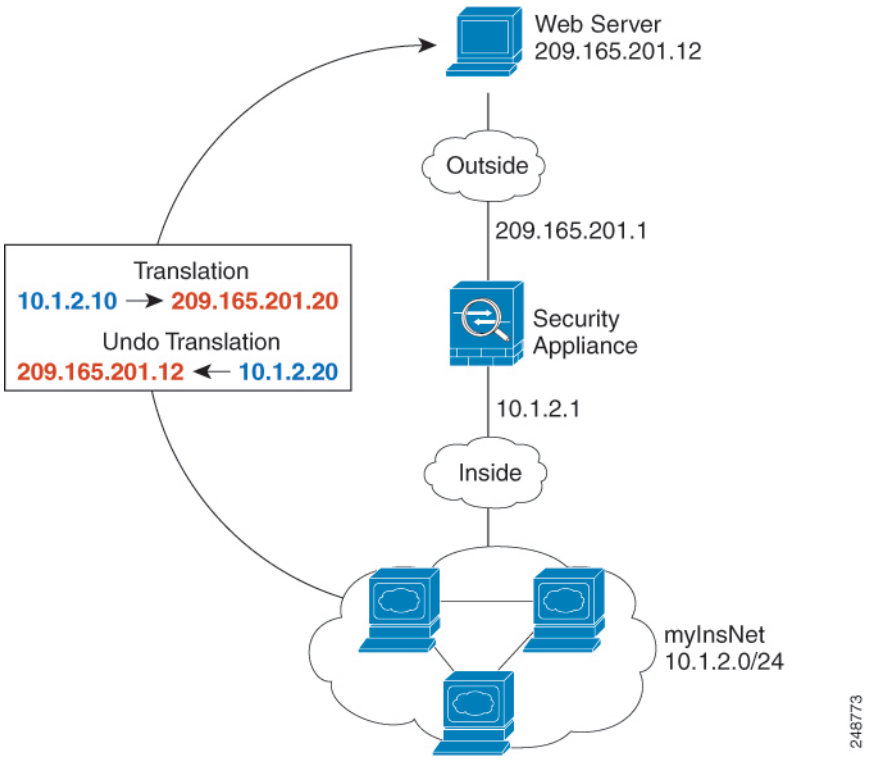
f) Click **Save**.

Step 3 Click **Save** on the NAT rule page.

Dynamic auto NAT for inside hosts and static NAT for an outside web server

The following example configures dynamic NAT for inside users on a private network when they access the outside. Also, when inside users connect to an outside web server, that web server address is translated to an address that appears to be on the inside network.

Figure 386: Dynamic NAT for Inside, Static NAT for Outside Web Server



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the web server. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select and click **Add Network** > **Add ObjectObjects** > **Object Management** > **Interface**.

Procedure

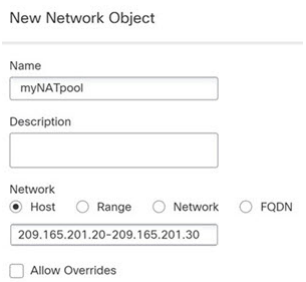
Step 1 Create a network object for the dynamic NAT pool to which you want to translate the inside addresses.

a) Choose **Objects** > **Object Management**.

b) Select **Network** from the table of contents and click **Add Network** > **Add Object**.

c) Define the dynamic NAT pool.

Name the network object (for example, myNATpool) and enter the network range 209.165.201.20-209.165.201.30.

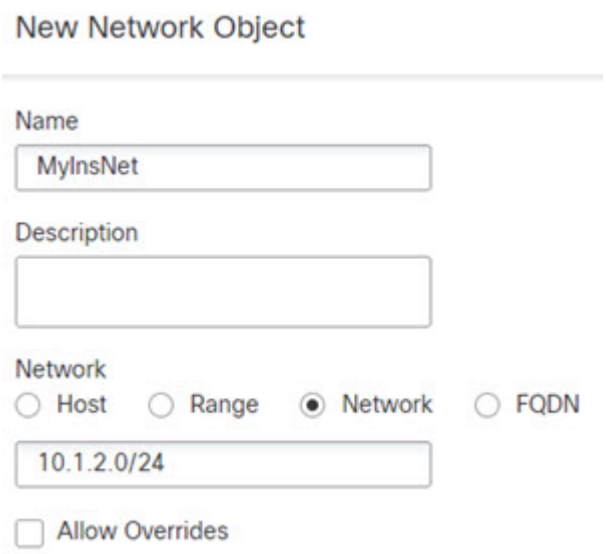


d) Click **Save**.

Step 2 Create a network object for the inside network.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, MyInsNet) and enter the network address 10.1.2.0/24.

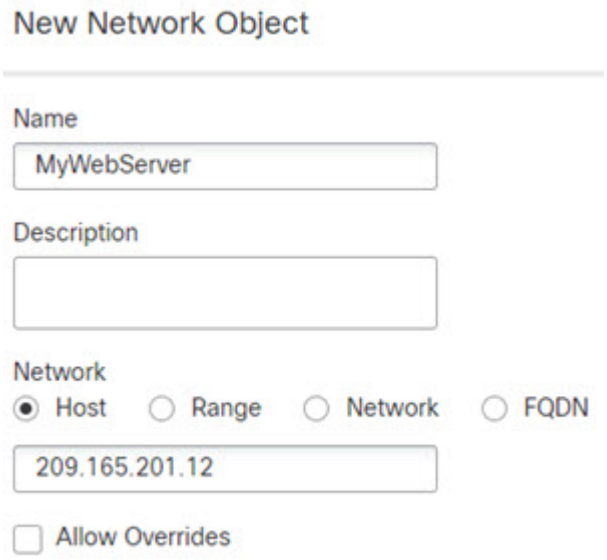


c) Click **Save**.

Step 3 Create a network object for the outside web server.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, MyWebServer) and enter the host address 209.165.201.12.

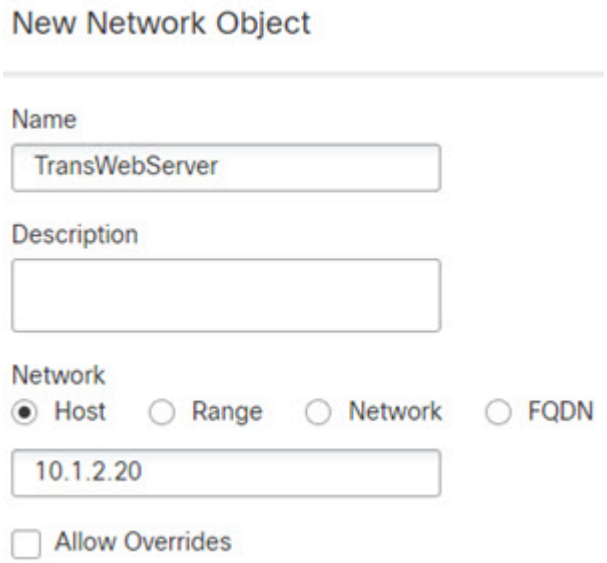


c) Click **Save**.

Step 4 Create a network object for the translated web server address.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, TransWebServer) and enter the host address 10.1.2.20.



c) Click **Save**.

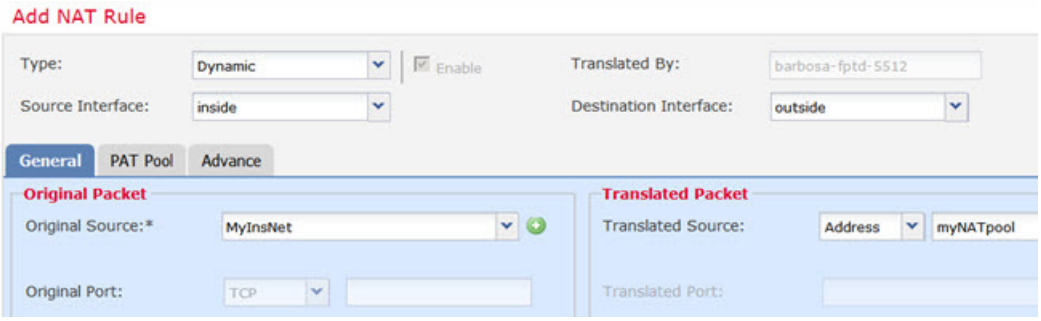
Step 5 Configure dynamic NAT for the inside network using the dynamic NAT pool object.

a) Select **Devices** > **Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

b) Click **Add NAT Rule** > **Add Auto NAT**.
c) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Source** = myInsNet network object.
- **Translated Source** > **Address**= myNATpool network group.



d) Click **Save**.

Step 6 Configure dynamic NAT for the inside network using the dynamic NAT pool object.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

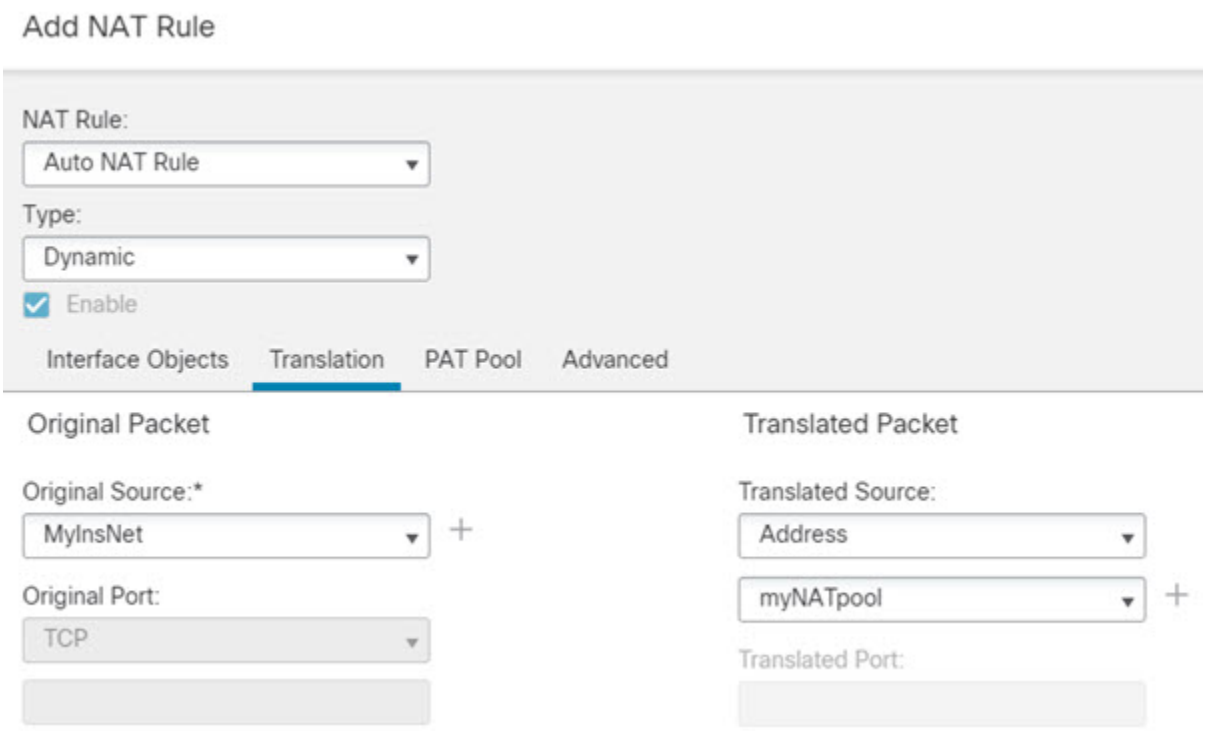
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamic.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = myInsNet network object.
- **Translated Source** > **Address**= myNATpool network group.



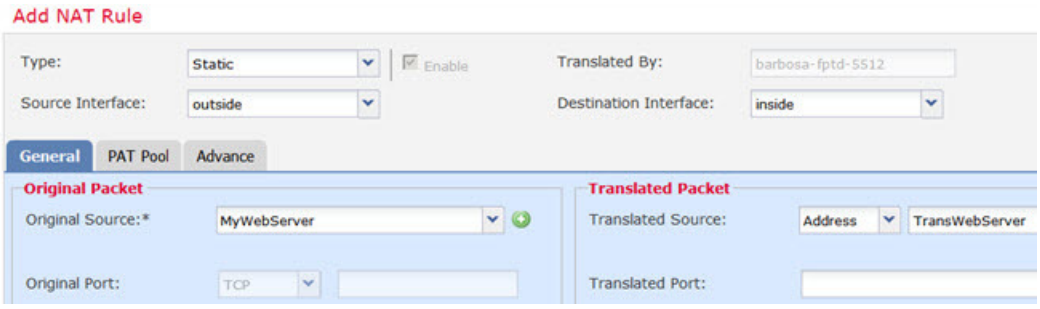
f) Click **Save**.

Step 7 Configure static NAT for the web server.

a) Click **Add NAT Rule** > **Add Auto NAT**.

b) Configure the following properties:

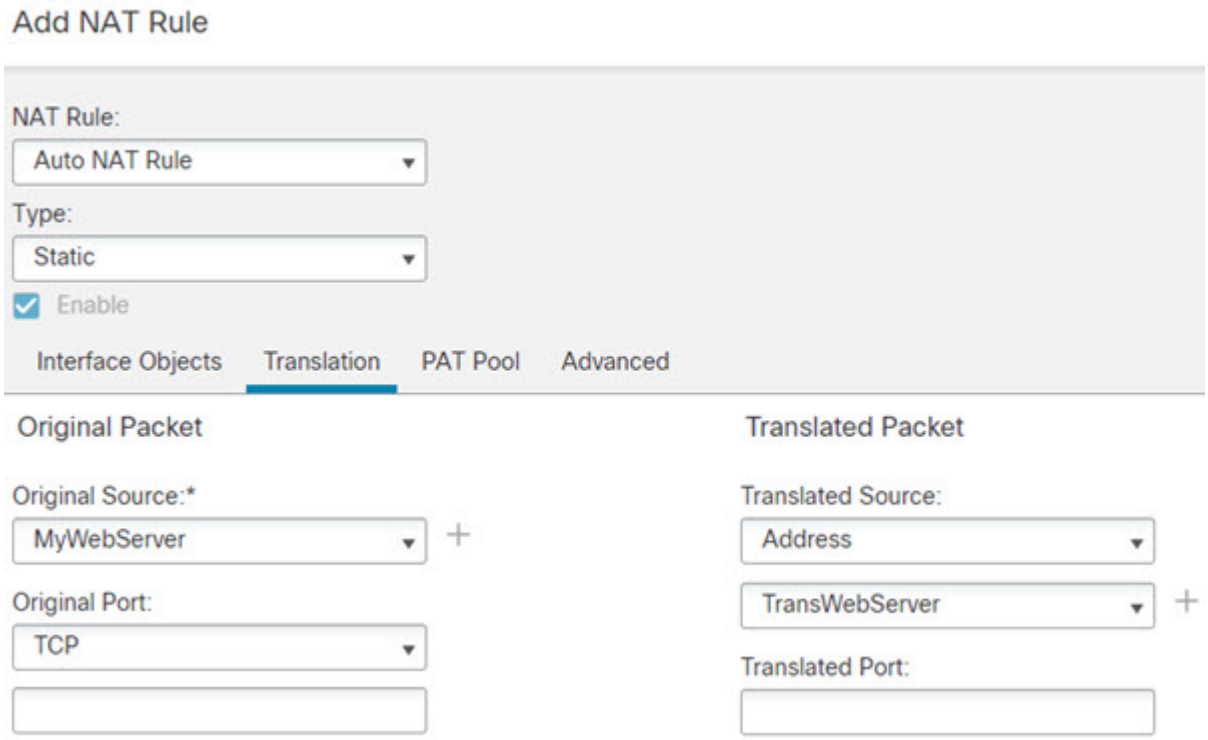
- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.
- **Original Source** = myWebServer network object.
- **Translated Source** > **Address**= TransWebServer network object.



c) Click **Save**.

Step 8 Configure static NAT for the web server.

a) Click **Add Rule**.
b) Configure the following properties:
   - **NAT Rule** = Auto NAT Rule.
   - **Type** = Static.
c) On **Interface Objects**, configure the following:
   - **Source Interface Objects** = outside.
   - **Destination Interface Objects** = inside.
d) On **Translation**, configure the following:
   - **Original Source** = myWebServer network object.
   - **Translated Source** > **Address**= TransWebServer network object.



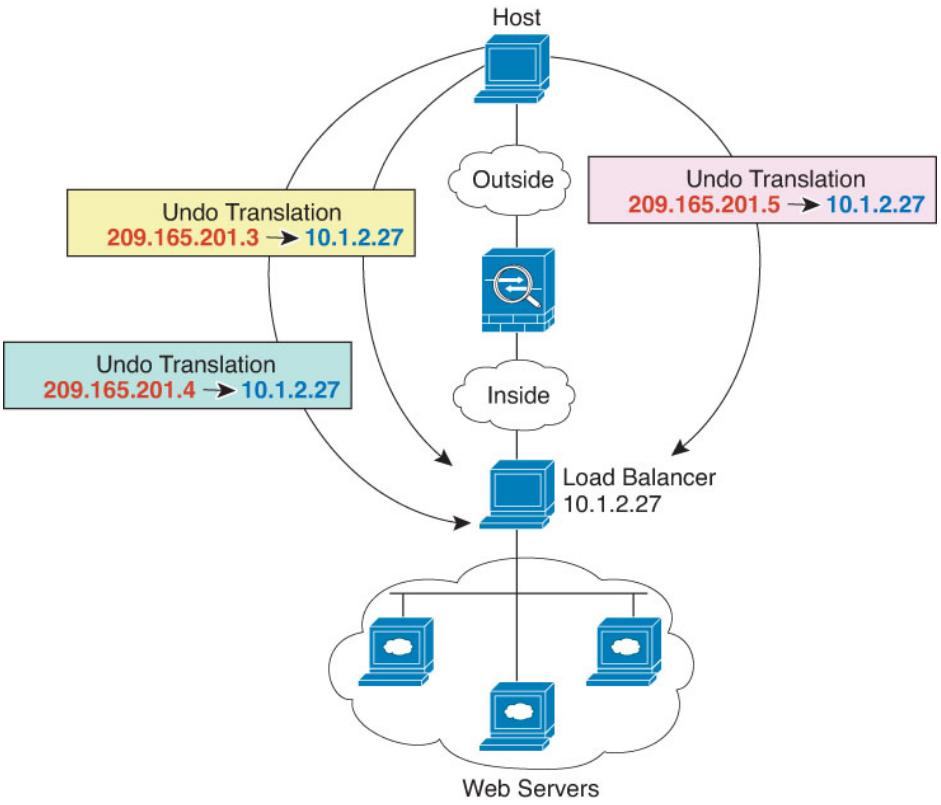
e) Click **Save**.

Step 9 Click **Save** on the NAT rule page.

Configure inside load balancer with multiple mapped addresses

The following example shows an inside load balancer that is translated to multiple IP addresses. When an outside host accesses one of the mapped IP addresses, it is untranslated to the single load balancer address. Depending on the URL requested, it redirects traffic to the correct web server.

Figure 387: Static NAT with One-to-Many for an Inside Load Balancer



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the web server. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

Procedure

Step 1 Create a network object for the addresses to which you want to map the load balancer.

a) Choose **Objects** > **Object Management**.

b) Select **Network** from the table of contents and click **Add Network** > **Add Object**.

c) Define the addresses.

Name the network object (for example, myPublicIPs) and enter the network range 209.165.201.3-209.165.201.5.

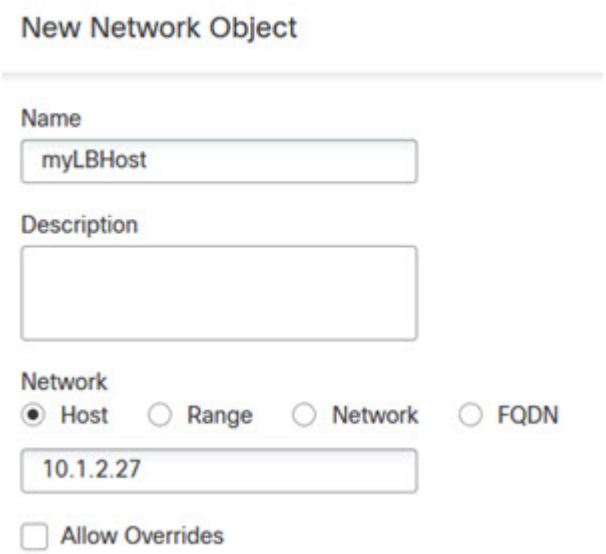


d) Click **Save**.

Step 2 Create a network object for the load balancer.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, myLBHost), enter the host address 10.1.2.27.



c) Click **Save**.

Step 3 Configure static NAT for the load balancer.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

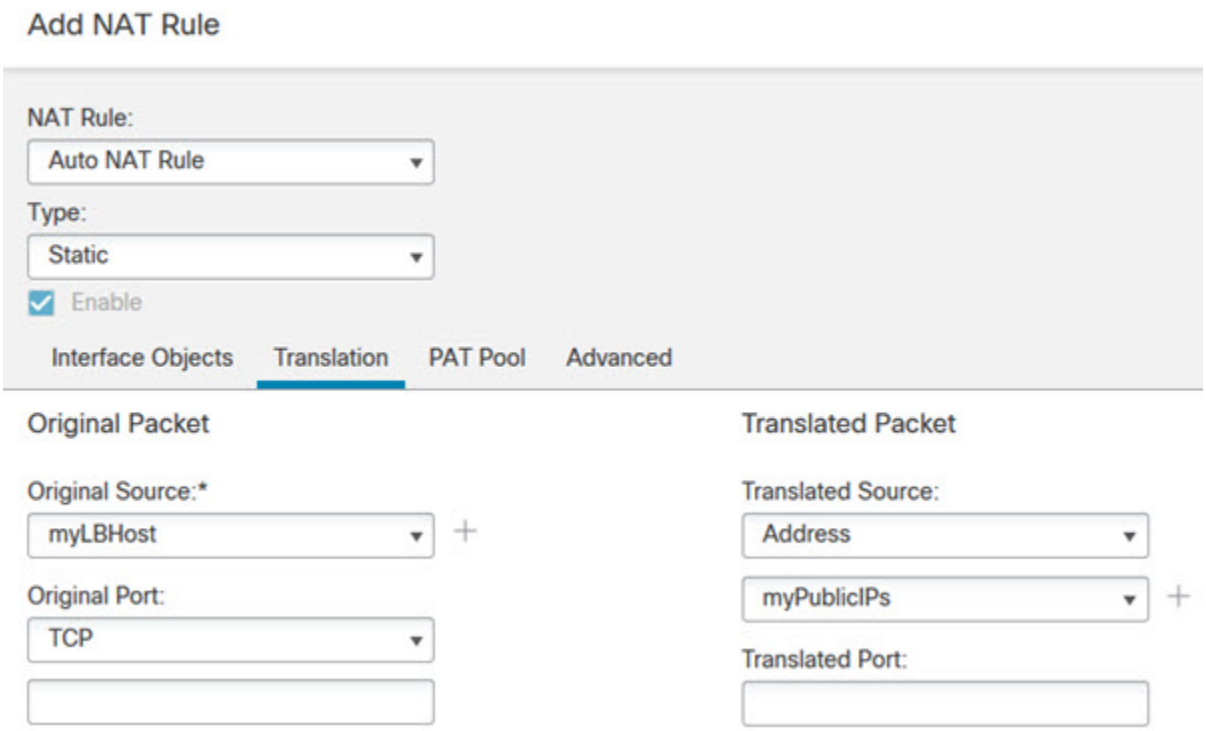
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = myLBHost network object.
- **Translated Source** > **Address** = myPublicIPs network group.



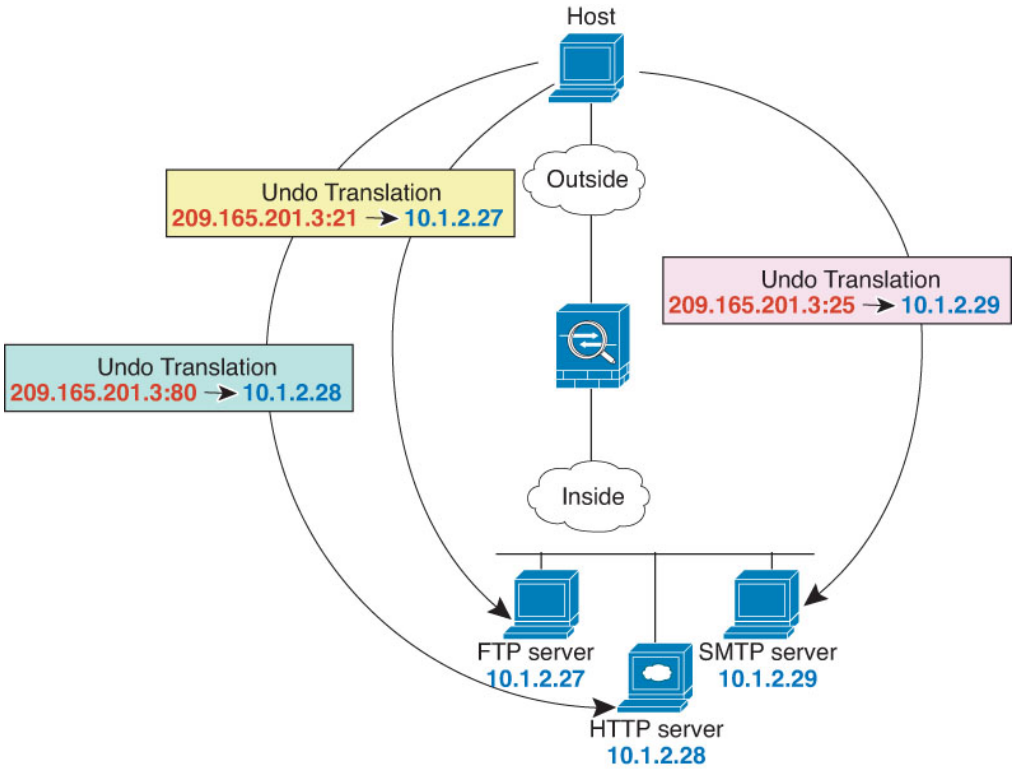
f) Click **Save**.

Step 4 Click **Save** on the NAT rule page.

Single address for FTP, HTTP, and SMTP (static auto NAT with port translation)

The following static NAT-with-port-translation example provides a single address for remote users to access FTP, HTTP, and SMTP. These servers are actually different devices on the real network, but for each server, you can specify static NAT-with-port-translation rules that use the same mapped IP address, but different ports.

Figure 388: Static NAT-with-Port-Translation



Before you begin

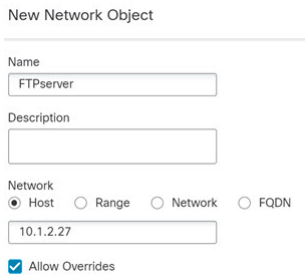
Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the servers. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select and click **Add Network** > **Add GroupObjects** > **Object Management** > **Interface**.

Procedure

Step 1 Create a network object for the FTP server.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Name the network object (for example, FTPserver), and enter the real IP address for the FTP server, 10.1.2.27.

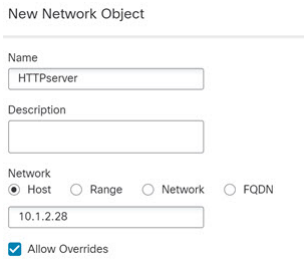


c) Click **Save**.

Step 2 Create a network object for the HTTP server.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, HTTPserver), enter the host address 10.1.2.28.

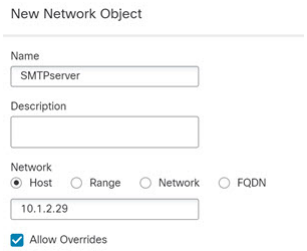


c) Click **Save**.

Step 3 Create a network object for the SMTP server.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, SMTPserver), enter the host address 10.1.2.29.

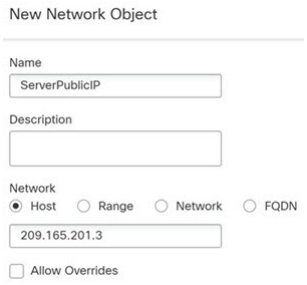


c) Click **Save**.

Step 4 Create a network object for the public IP address used for the three servers.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, ServerPublicIP) and enter the host address 209.165.201.3.



c) Click **Save**.

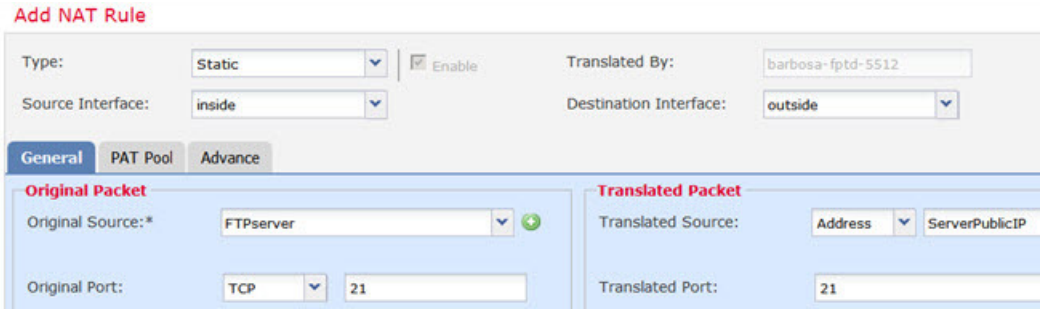
Step 5 Configure static NAT with port translation for the FTP server, mapping the FTP port to itself.

a) Select **Devices** > **Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

b) Click **Add NAT Rule** > **Add Auto NAT**.
c) Configure the following properties:

- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Source** = FTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 21.
- **Translated Port** = 21.



d) Click **Save**.

Step 6 Configure static NAT with port translation for the FTP server, mapping the FTP port to itself.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

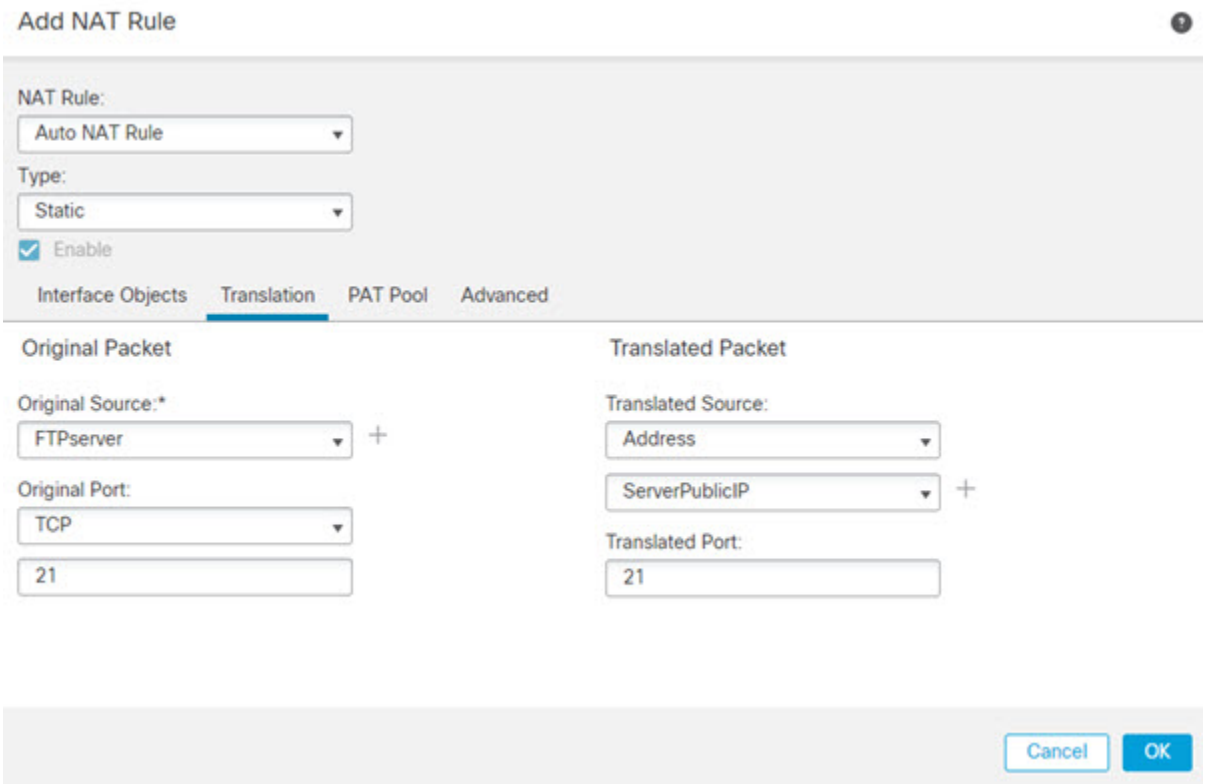
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = FTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 21.
- **Translated Port** = 21.



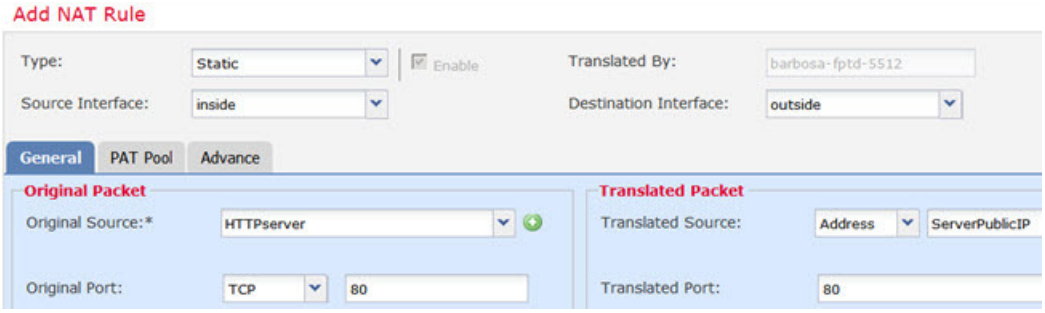
f) Click **Save**.

Step 7 Configure static NAT with port translation for the HTTP server, mapping the HTTP port to itself.

a) Click **Add NAT Rule** > **Add Auto NAT**.

b) Configure the following properties:

- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Source** = HTTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 80.
- **Translated Port** = 80.



c) Click **Save**.

Step 8 Configure static NAT with port translation for the HTTP server, mapping the HTTP port to itself.

a) Click **Add Rule**.

b) Configure the following properties:

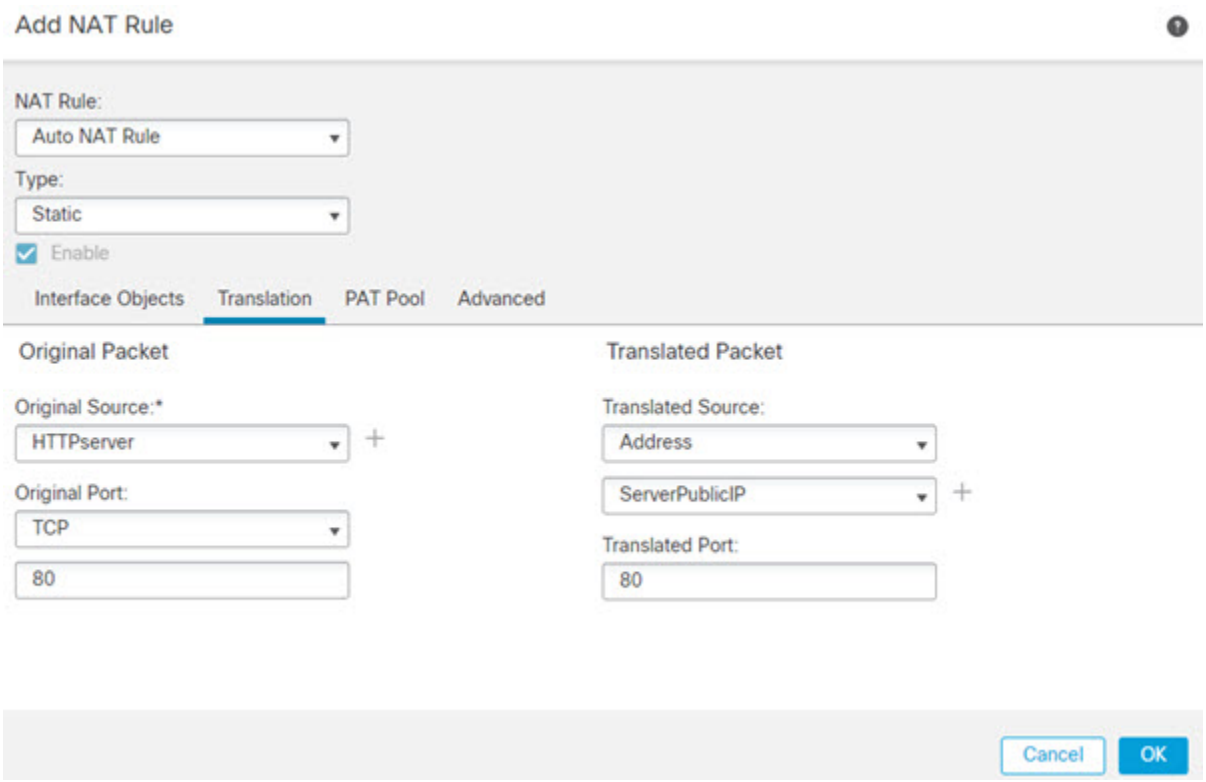
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) On **Translation**, configure the following:

- **Original Source** = HTTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 80.
- **Translated Port** = 80.



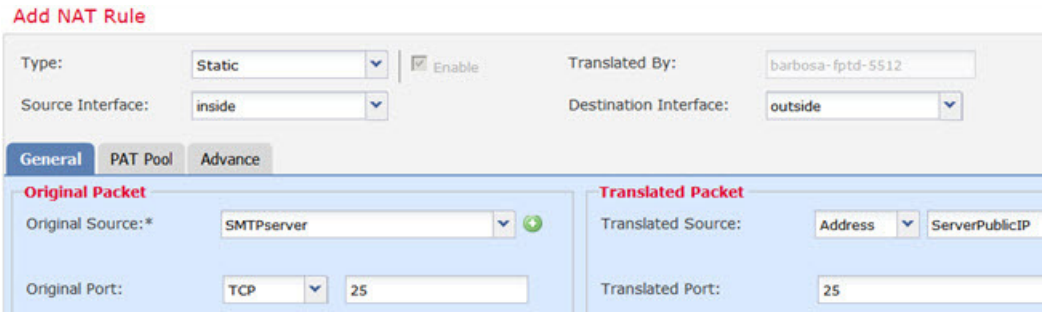
e) Click **Save**.

Step 9 Configure static NAT with port translation for the SMTP server, mapping the SMTP port to itself.

a) Click **Add NAT Rule** > **Add Auto NAT**.

b) Configure the following properties:

- **Type** = Static.
- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Source** = SMTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 25.
- **Translated Port** = 25.



c) Click **Save**.

Step 10 Configure static NAT with port translation for the SMTP server, mapping the SMTP port to itself.

a) Click **Add Rule**.

b) Configure the following properties:

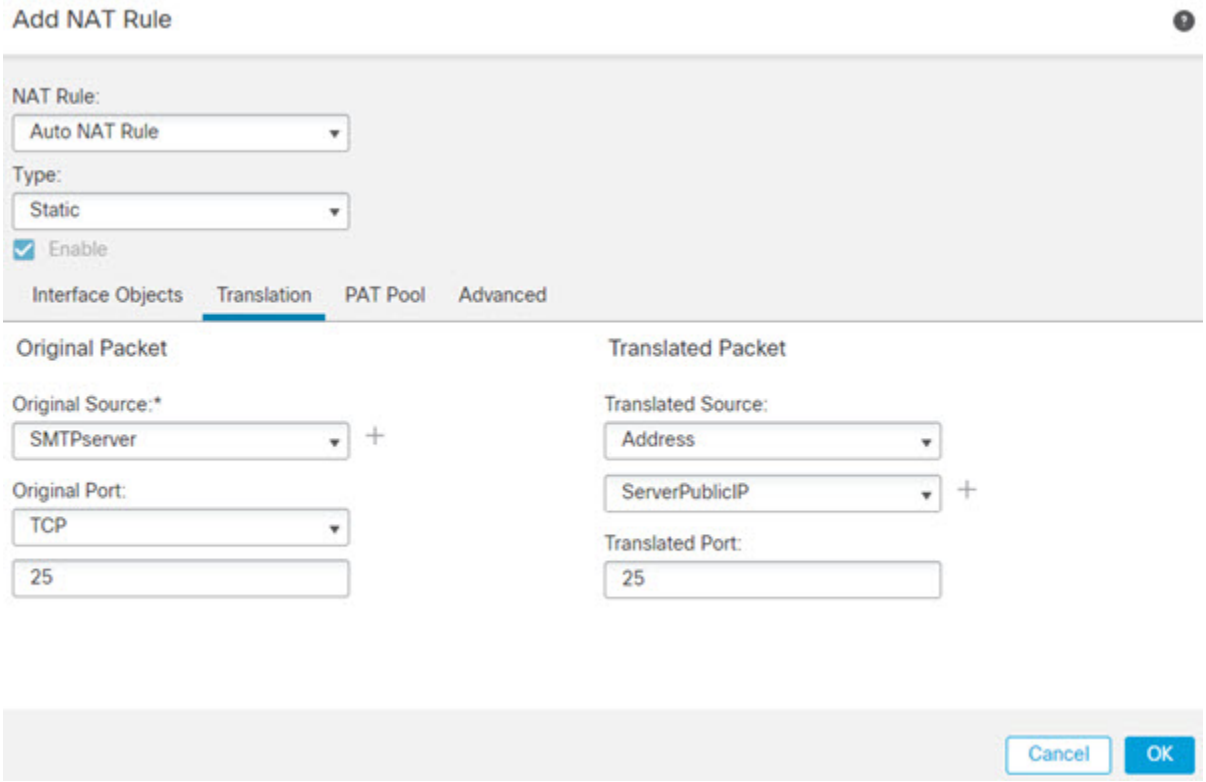
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

d) On **Translation**, configure the following:

- **Original Source** = SMTPserver network object.
- **Translated Source** > **Address**= ServerPublicIP network object.
- **Original Port** > **TCP** = 25.
- **Translated Port** = 25.



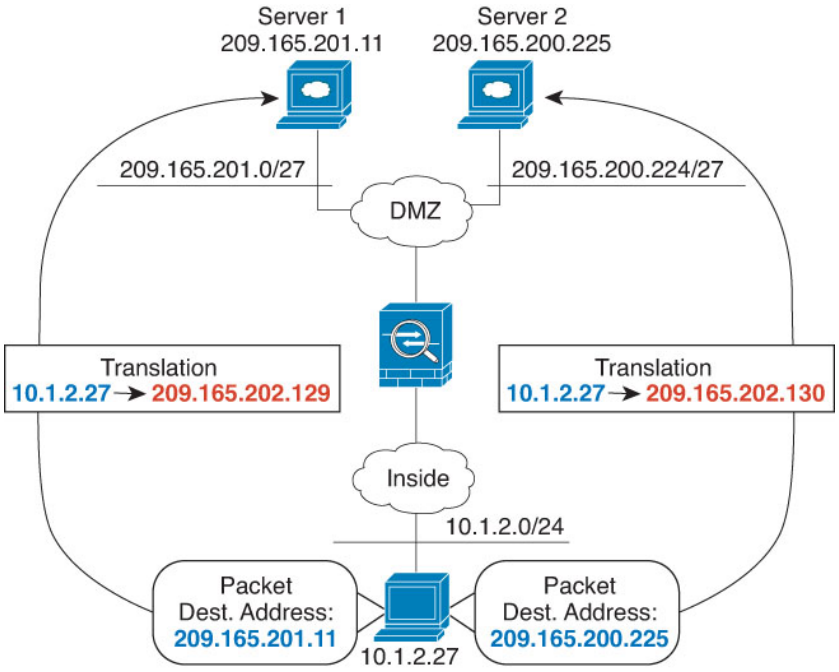
e) Click **Save**.

Step 11 Click **Save** on the NAT rule page.

Different translation depending on the destination (dynamic manual PAT)

The following figure shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129:*port*. When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130:*port*.

Figure 389: Manual NAT with Different Destination Addresses



Before you begin

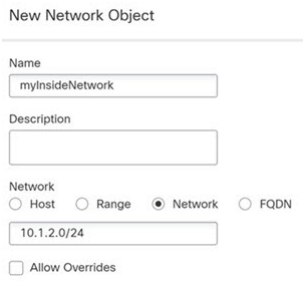
Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the servers. In this example, we will assume the interface objects are security zones named **inside** and **dmz**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

Procedure

Step 1 Create a network object for the inside network.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Name the network object (for example, myInsideNetwork), and enter the real network address, 10.1.2.0/24.



c) Click **Save**.

Step 2 Create a network object for the DMZ network 1.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, DMZnetwork1) and enter the network address 209.165.201.0/27 (subnet mask of 255.255.255.224).

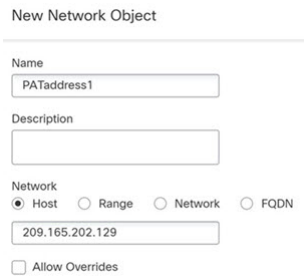


c) Click **Save**.

Step 3 Create a network object for the PAT address for DMZ network 1.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, PATaddress1) and enter the host address 209.165.202.129.

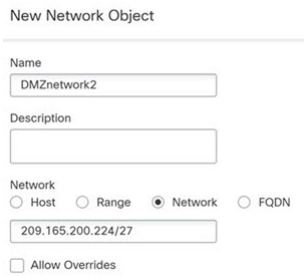


c) Click **Save**.

Step 4 Create a network object for the DMZ network 2.

a) Click **Add Network** > **Add Object**.

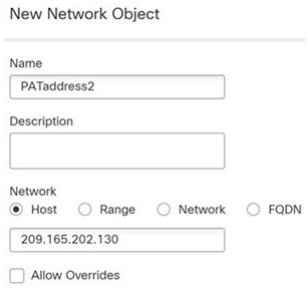
b) Name the network object (for example, DMZnetwork2) and enter the network address 209.165.200.224/27 (subnet mask of 255.255.255.224).



c) Click **Save**.

Step 5 Create a network object for the PAT address for DMZ network 2.

a) Click **Add Network** > **Add Object**.
b) Name the network object (for example, PATaddress2) and enter the host address 209.165.202.130.



c) Click **Save**.

Step 6 Configure dynamic manual PAT for DMZ network 1.

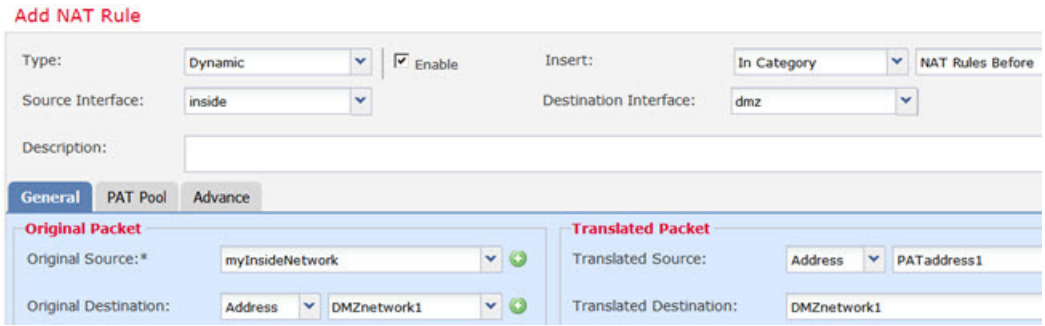
a) Select **Devices** > **Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

b) Click **Add NAT Rule** > **Add Manual NAT**.
c) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address**= PATaddress1 network object.
- **Original Destination** > **Address** = DMZnetwork1 network object.
- **Translated Destination** = DMZnetwork1 network object.

Note Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank.



d) Click **Save**.

Step 7 Configure dynamic manual PAT for DMZ network 1.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.

d) On **Interface Objects**, configure the following:

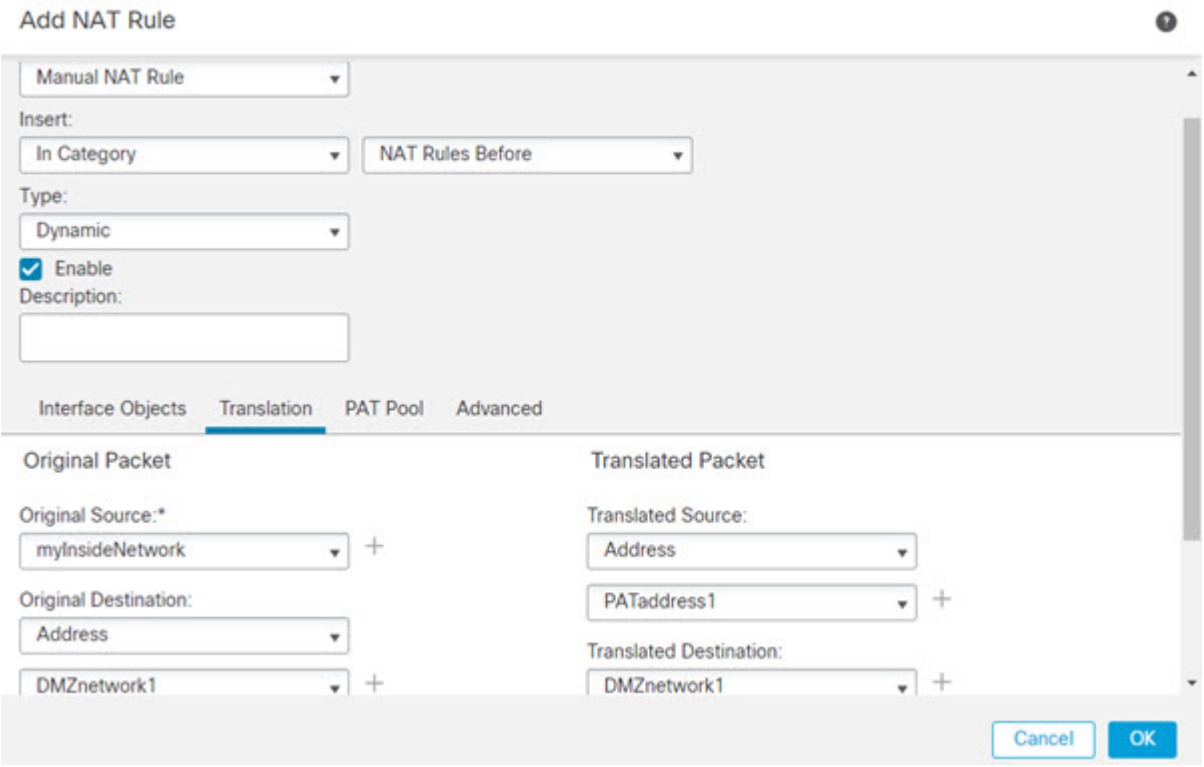
- **Source Interface Objects** = inside.
- **Destination Interface Objects** = dmz.

e) On **Translation**, configure the following:

- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address**= PATaddress1 network object.
- **Original Destination** > **Address** = DMZnetwork1 network object.
- **Translated Destination** = DMZnetwork1 network object.



Note Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank.



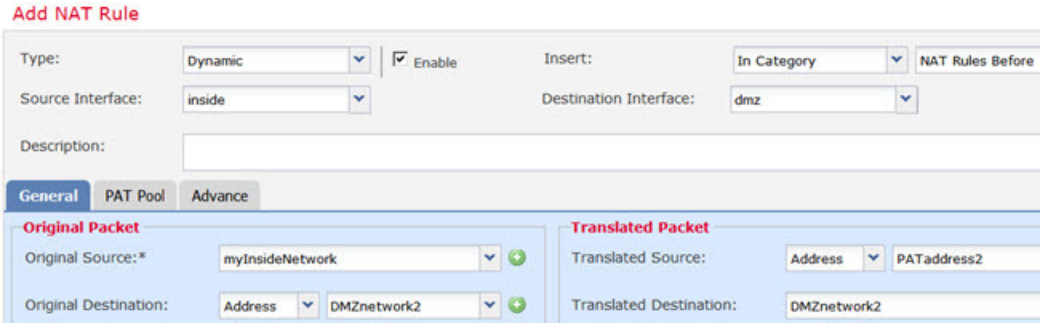
f) Click **Save**.

Step 8 Configure dynamic manual PAT for DMZ network 2.

a) Click **Add NAT Rule** > **Add Manual NAT**.

b) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address**= PATaddress2 network object.
- **Original Destination** > **Address** = DMZnetwork2 network object.
- **Translated Destination** = DMZnetwork2 network object.



c) Click **Save**.

Step 9 Configure dynamic manual PAT for DMZ network 2.

a) Click **Add Rule**.

b) Configure the following properties:

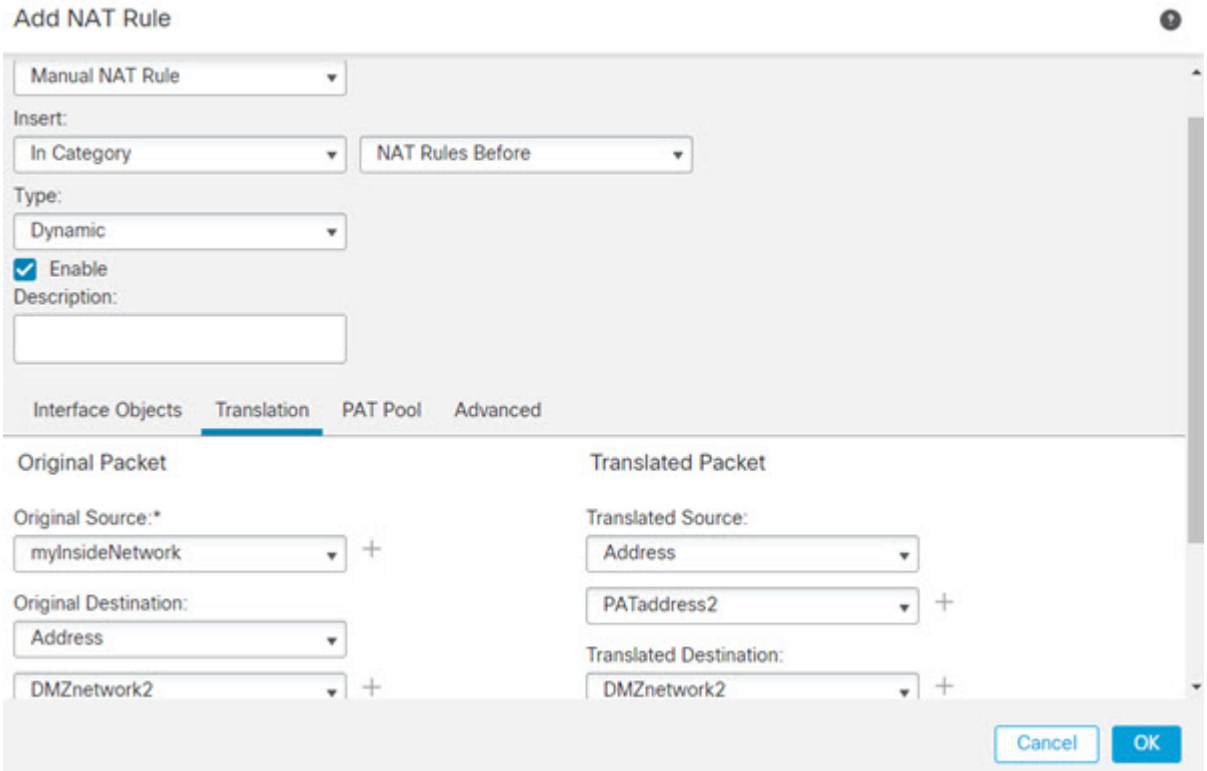
- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.

c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = dmz.

d) On **Translation**, configure the following:

- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address**= PATaddress2 network object.
- **Original Destination** > **Address** = DMZnetwork2 network object.
- **Translated Destination** = DMZnetwork2 network object.



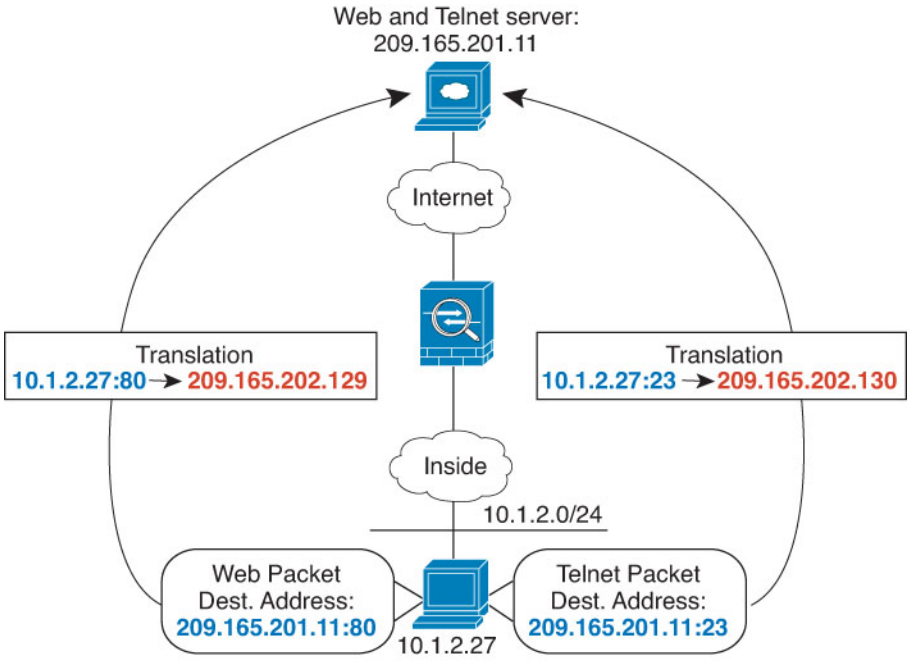
e) Click **Save**.

Step 10 Click **Save** on the NAT rule page.

Configure dynamic manual PAT with different destination ports

This illustration displays the use of source and destination ports. The host on the 10.1.2.0/24 network accesses a single host for both web services and Telnet services. When the host accesses the server for Telnet services, the real address is translated to 209.165.202.129: *port*. When the host accesses the same server for web services, the real address is translated to 209.165.202.130: *port*.

Figure 390: Manual NAT with Different Destination Ports



Before you begin

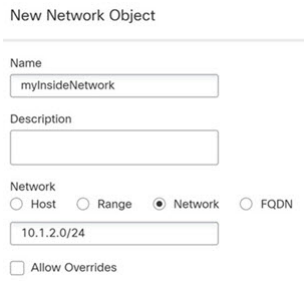
Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device that protects the servers. In this example, we will assume the interface objects are security zones named **inside** and **dmz**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

Procedure

Step 1 Create a network object for the inside network.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Name the network object (for example, myInsideNetwork) and enter the real network address, 10.1.2.0/24.



c) Click **Save**.

Step 2 Create a network object for the Telnet/Web server.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, TelnetWebServer) and enter the host address 209.165.201.11.

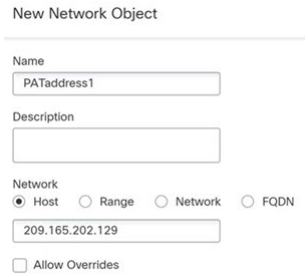


c) Click **Save**.

Step 3 Create a network object for the PAT address when using Telnet.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, PATaddress1) and enter the host address 209.165.202.129.

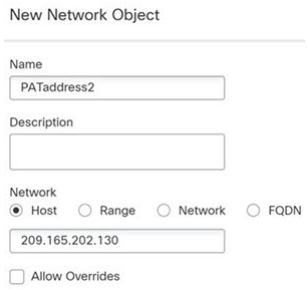


c) Click **Save**.

Step 4 Create a network object for the PAT address when using HTTP.

a) Click **Add Network** > **Add Object**.

b) Name the network object (for example, PATaddress2) and enter the host address 209.165.202.130.



c) Click **Save**.

Step 5 Configure dynamic manual PAT for Telnet access.

a) Select **Devices** > **Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

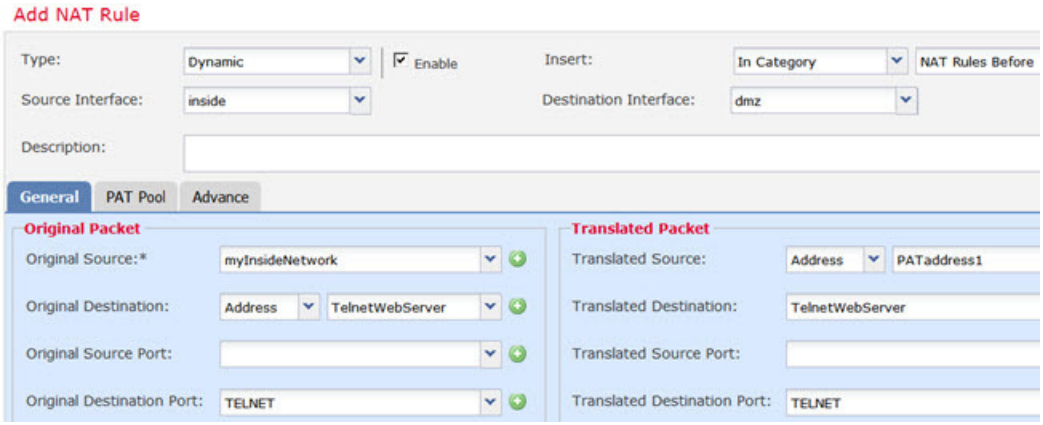
b) Click **Add NAT Rule** > **Add Manual NAT**.

c) Configure the following properties:

- **Type** = Dynamic.

- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address** = PATaddress1 network object.
- **Original Destination** > **Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = TELNET port object (system-defined).
- **Translated Destination Port** = TELNET port object (system-defined).

Note Because you do not want to translate the destination address or port, you need to configure identity NAT for them by specifying the same address for the original and translated destination addresses, and the same port for the original and translated port.



d) Click **Save**.

Step 6 Configure dynamic manual PAT for Telnet access.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.

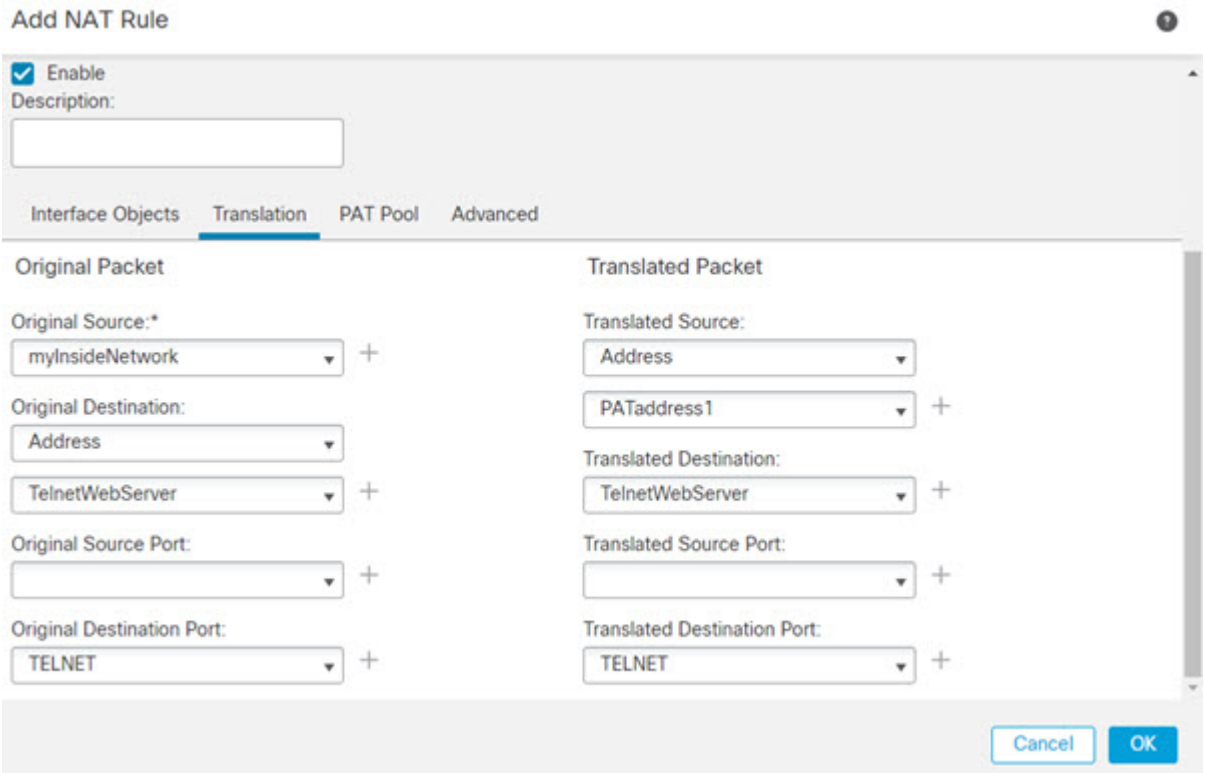
d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = dmz.

e) On **Translation**, configure the following:

- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address** = PATaddress1 network object.
- **Original Destination** > **Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = TELNET port object (system-defined).
- **Translated Destination Port** = TELNET port object (system-defined).

Note Because you do not want to translate the destination address or port, you need to configure identity NAT for them by specifying the same address for the original and translated destination addresses, and the same port for the original and translated port.



f) Click **Save**.

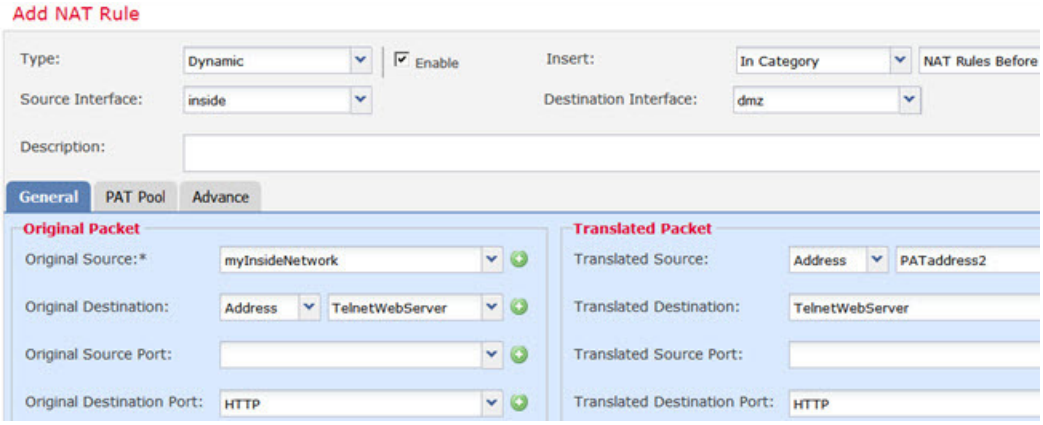
Step 7 Configure dynamic manual PAT for web access.

a) Click **Add NAT Rule** > **Add Manual NAT**.

b) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.

- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address** = PATaddress2 network object.
- **Original Destination** > **Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = HTTP port object (system-defined).
- **Translated Destination Port** = HTTP port object (system-defined).



c) Click **Save**.

Step 8 Configure dynamic manual PAT for web access.

a) Click **Add Rule**.

b) Configure the following properties:

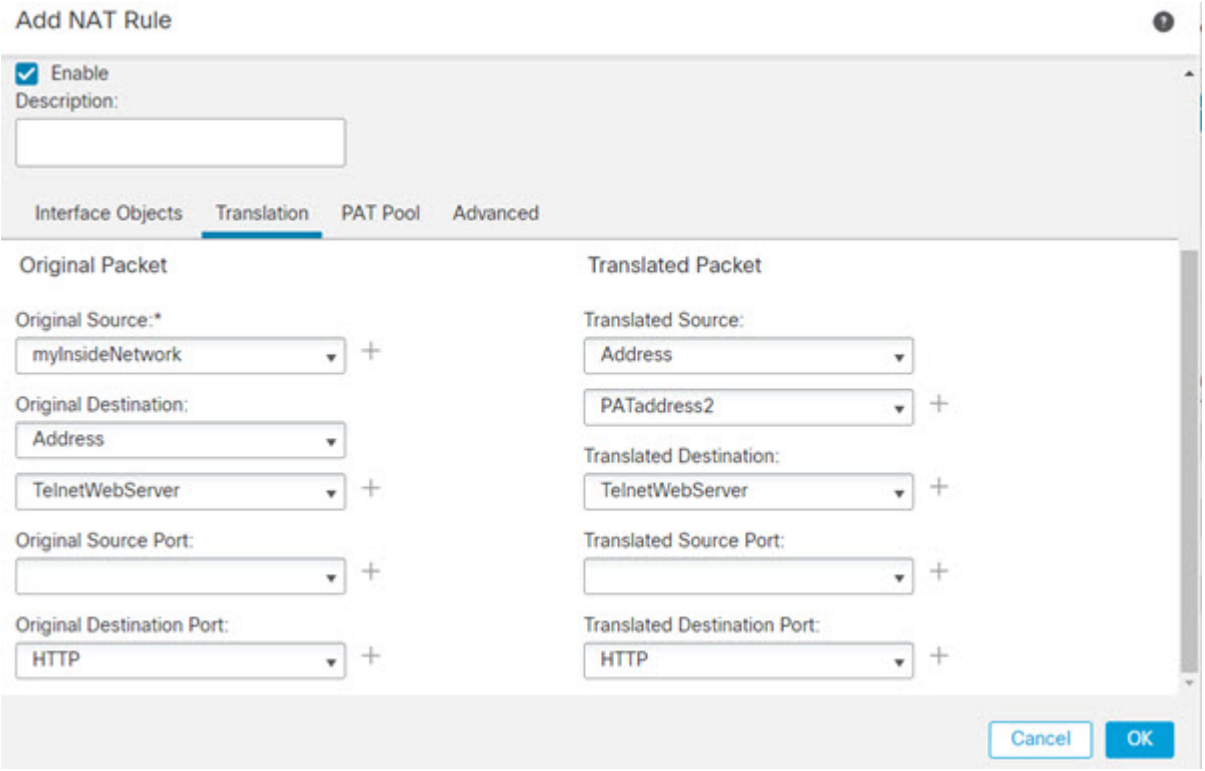
- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.

c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = dmz.

d) On **Translation**, configure the following:

- **Original Source** = myInsideNetwork network object.
- **Translated Source** > **Address** = PATaddress2 network object.
- **Original Destination** > **Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = HTTP port object (system-defined).
- **Translated Destination Port** = HTTP port object (system-defined).



e) Click **Save**.

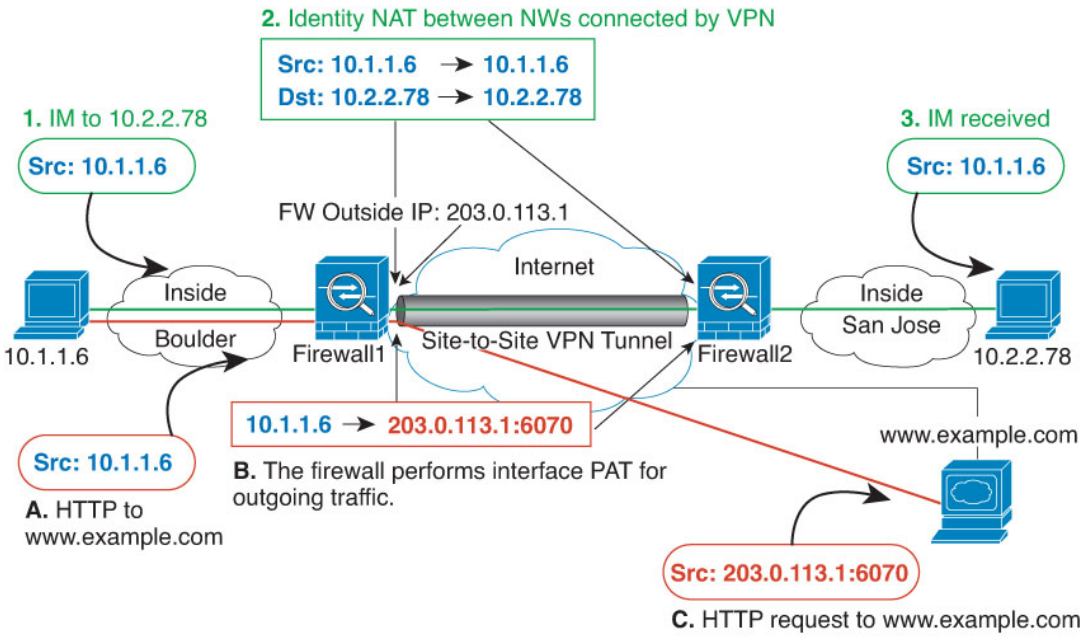
Step 9 Click **Save** on the NAT rule page.

NAT and site-to-site VPN

When you create a policy-based site-to-site VPN using the management center VPN wizard (**Device > Site To Site**), you can select the NAT Exempt option to create the rules automatically. You can view the NAT exemptions for a device in the NAT policy page (**Device > NAT > NAT Exemptions**). If you do not want to configure NAT Exempt in the VPN wizard, you can use the following procedure for NAT exemption.

The following figure shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface PAT rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT simply translates an address to the same address.

Figure 391: Interface PAT and Identity NAT for Site-to-Site VPN



This example explains the configuration for Firewall1 (Boulder).

Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the devices in the VPN. In this example, we will assume the interface objects are security zones named **inside-boulder** and **outside-boulder** for the Firewall1 (Boulder) interfaces. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

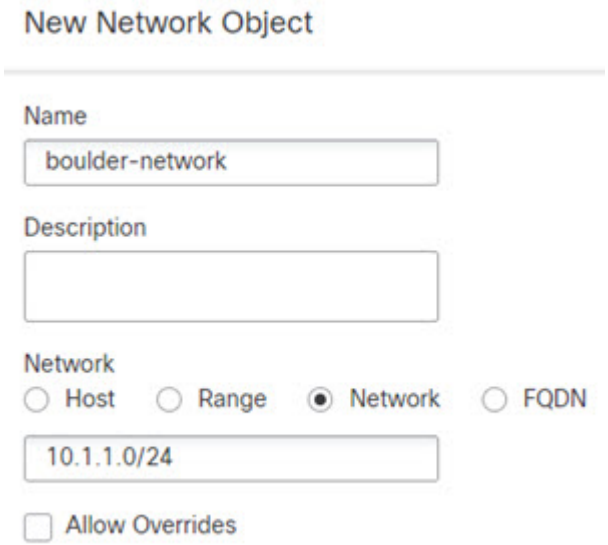
Procedure

Step 1 Create the objects to define the various networks.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Identify the Boulder inside network.

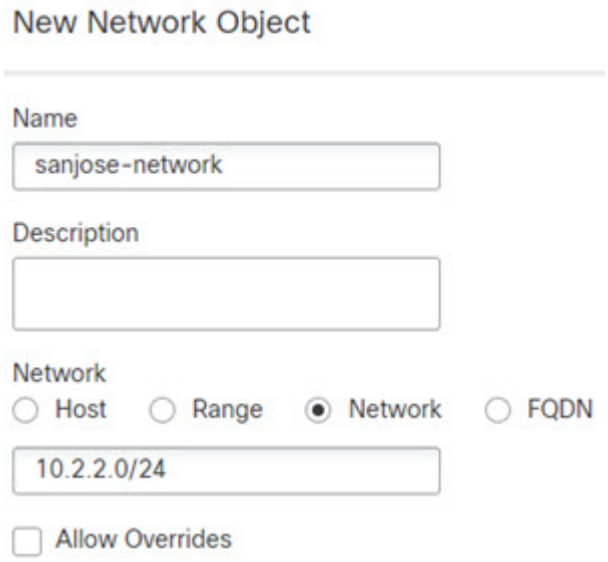
Name the network object (for example, boulder-network) and enter the network address, 10.1.1.0/24.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the inside San Jose network.

Name the network object (for example, sanjose-network) and enter the network address 10.2.2.0/24.



e) Click **Save**.

Step 2 Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

- **NAT Rule** = Manual NAT Rule.

- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside-boulder.
- **Destination Interface Objects** = outside-boulder.

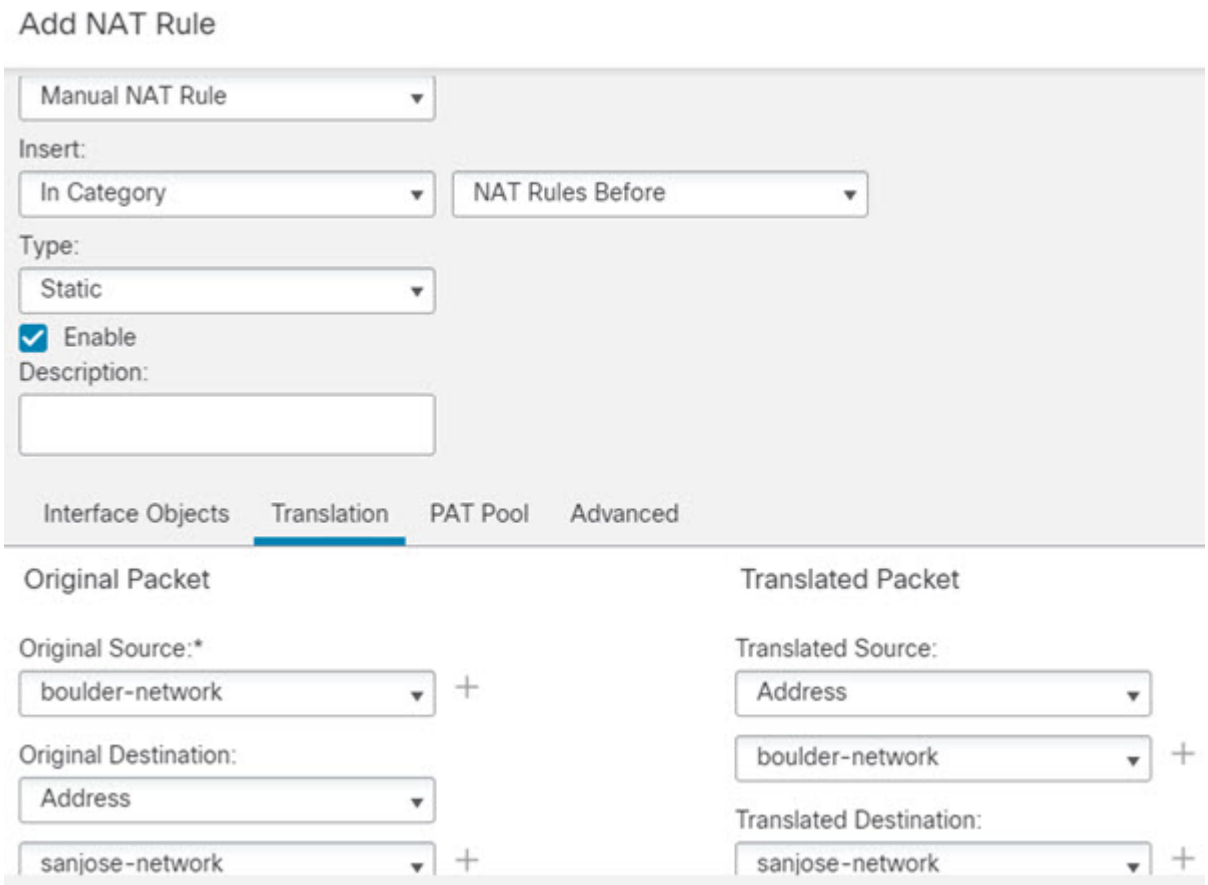
e) On **Translation**, configure the following:

- **Original Source** = boulder-network object.
- **Translated Source** > **Address** = boulder-network object.
- **Original Destination** > **Address** = sanjose-network object.
- **Translated Destination** = sanjose-network object.



Note Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.

f) On **Advanced**, select **Do not proxy ARP on Destination interface**.



g) Click **Save**.

Step 3 Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder).

a) Click **Add Rule**.

b) Configure the following properties:

- **NAT Rule** = Manual NAT Rule.
- **Type** = Dynamic.
- **Insert Rule** = any position after the first rule. Because this rule will apply to any destination address, the rule that uses sanjose-network as the destination must come before this rule, or the sanjose-network rule will never be matched. The default is to place new manual NAT rules at the end of the "NAT Rules Before Auto NAT" section.

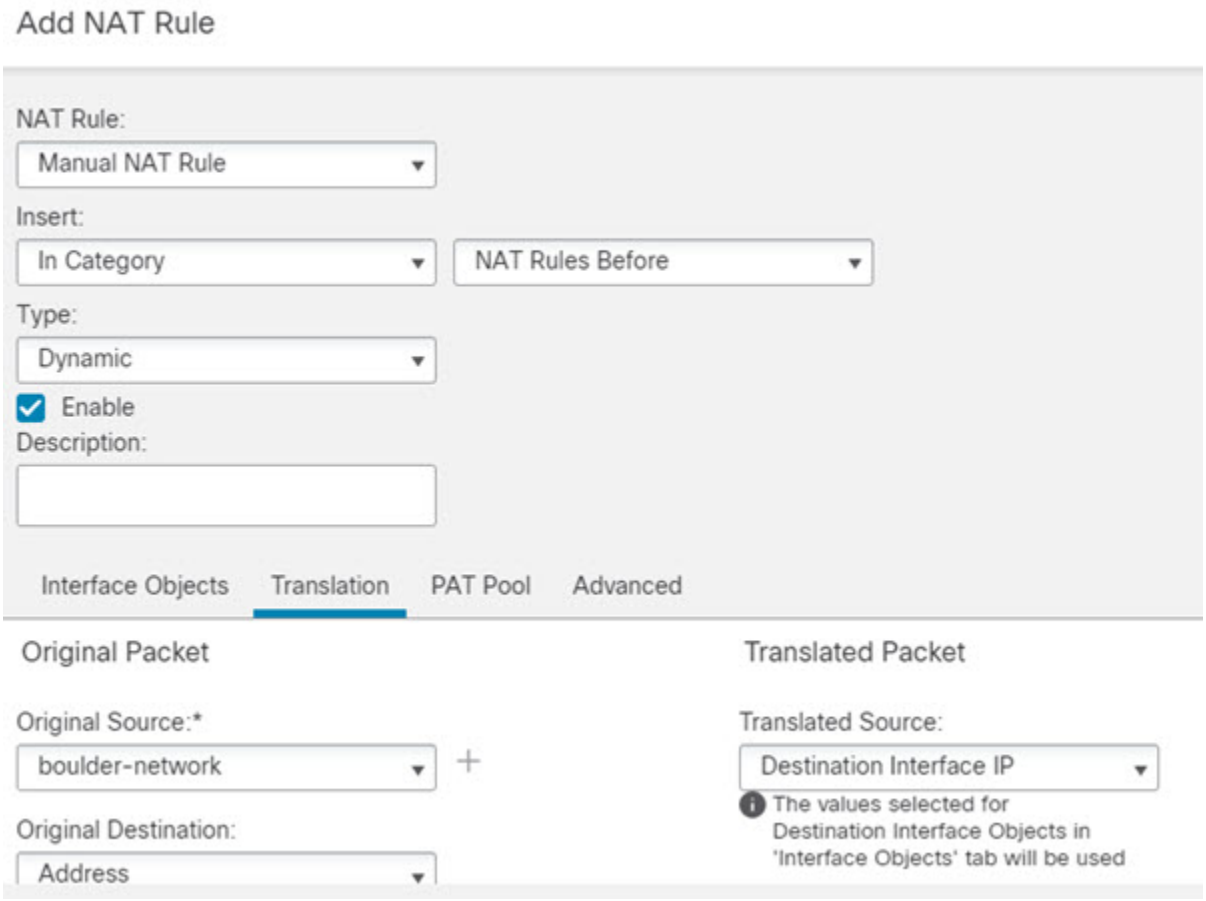
c) On **Interface Objects** , configure the following:

- **Source Interface Objects** = inside-boulder.
- **Destination Interface Objects** = outside-boulder.

d) On **Translation** , configure the following:

- **Original Source** = boulder-network object.

- **Translated Source** = **Destination Interface IP**. This option configures interface PAT using the interface contained in the destination interface object.
- **Original Destination** > **Address** = any (leave blank).
- **Translated Destination** = any (leave blank).



e) Click **Save**.

Step 4 If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.

- The manual identity NAT rule would be for sanjose-network when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
- The manual dynamic interface PAT rule would be for sanjose-network when the destination is "any."

DNS query and response rewriting using NAT

DNS rewrite is the process of modifying DNS replies so that the IP address returned in the DNS response is replaced with an address that matches the NAT configuration. It is used when a translated address must be

returned to the requester instead of the original address in the DNS record. This function is also known as DNS doctoring.

This feature rewrites the address in DNS queries and replies that match a NAT rule (for example, the A record for IPv4, the AAAA record for IPv6, or the PTR record for reverse DNS queries). For DNS replies traversing from a mapped interface to any other interface, the record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the record is rewritten from the real value to the mapped value. This feature works with NAT44,NAT 66, NAT46, and NAT64.

The main circumstances when you would need to configure DNS rewrite on a NAT rule are:

- The rule is NAT64 or NAT46, and the DNS server is on the outside network. You need DNS rewrite to convert between DNS A records (for IPv4) and AAAA records (for IPv6).
- The DNS server is on the outside, clients are on the inside, and some of the fully-qualified domain names that the clients use resolve to other inside hosts.
- The DNS server is on the inside and responds with private IP addresses, clients are on the outside, and the clients access fully-qualified domain names that point to servers that are hosted on the inside.

DNS rewrite has the following limitations:

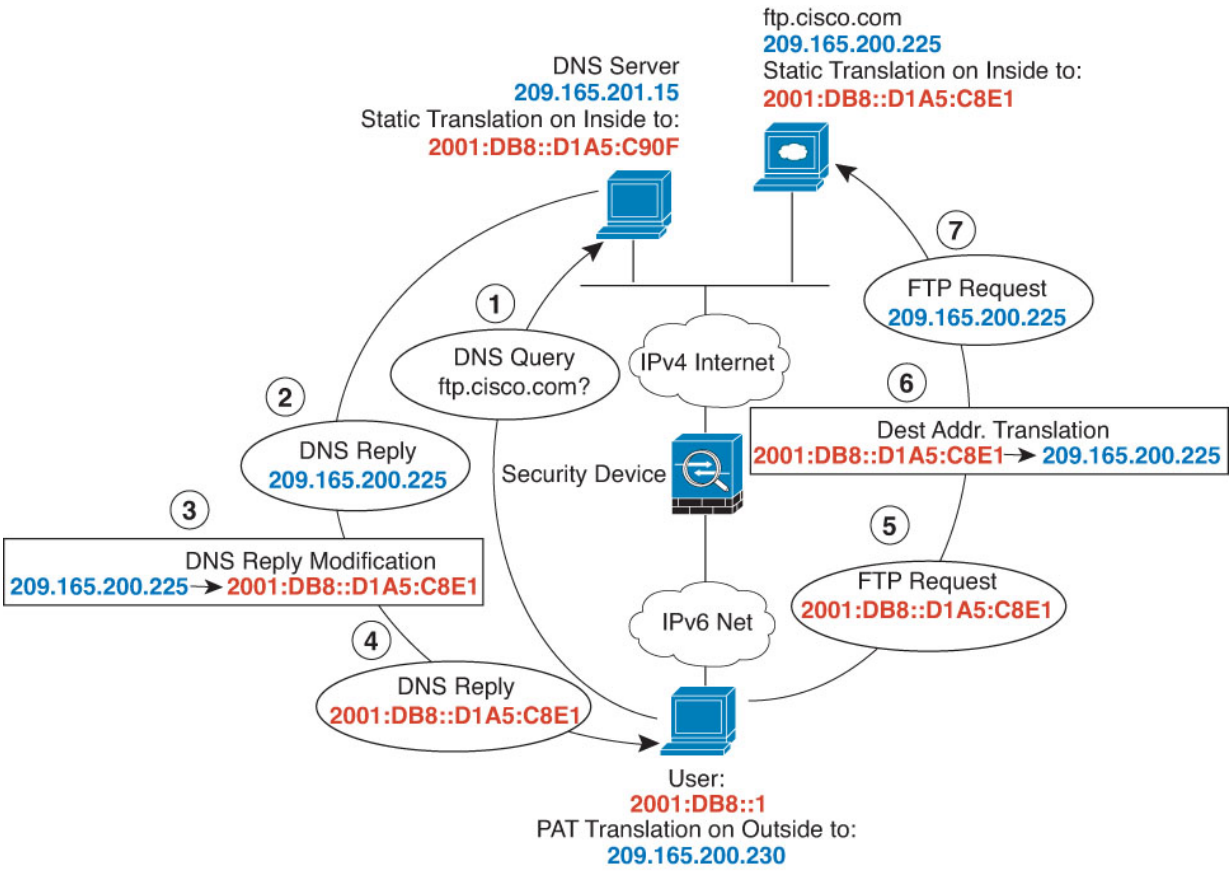
- DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A or AAAA record, and the PAT rule to use is ambiguous.
- If you configure a manual NAT rule, you cannot configure DNS modification if you specify the destination address as well as the source address. These kinds of rules can potentially have a different translation for a single address when going to A vs. B. Therefore, the can not accurately match the IP address inside the DNS reply to the correct twice NAT rule; the DNS reply does not contain information about which source/destination address combination was in the packet that prompted the DNS request.
- You must enable DNS application inspection with DNS NAT rewrite enabled for NAT rules to rewrite DNS queries and responses. By default, DNS inspection with DNS NAT rewrite enabled is globally applied, so you probably do not need to change the inspection configuration.
- DNS rewrite is actually done on the xlate entry, not the NAT rule. Thus, if there is no xlate for a dynamic rule, rewrite cannot be done correctly. The same problem does not occur for static NAT.
- DNS rewrite does not rewrite DNS Dynamic Update messages (opcode 5).

These topics provide examples of DNS rewrite in NAT rules.

DNS64 reply modification

The following figure shows an FTP server and DNS server on the outside IPv4 network. The system has a static translation for the outside server. In this case, when an inside IPv6 user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.200.225.

Because you want inside users to use the mapped address for ftp.cisco.com (2001:DB8::D1A5:C8E1, where D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225) you need to configure DNS reply modification for the static translation. This example also includes a static NAT translation for the DNS server, and a PAT rule for the inside IPv6 hosts.



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

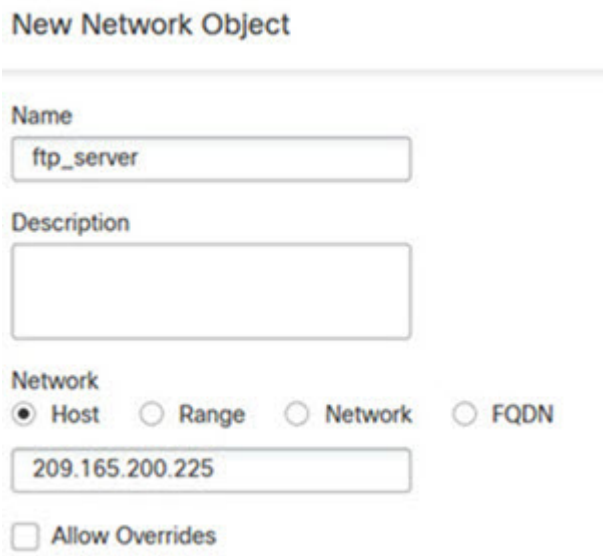
Procedure

Step 1 Create the network objects for the FTP server.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the real FTP server address.

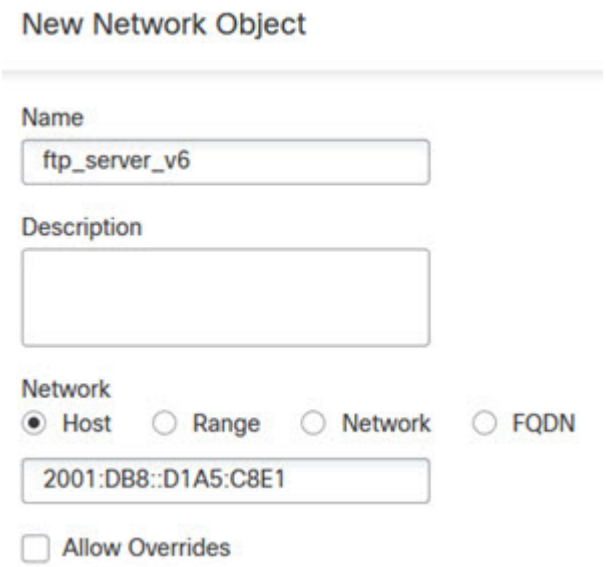
Name the network object (for example, ftp_server) and enter the host address, 209.165.200.225.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the FTP server's translated IPv6 address.

Name the network object (for example, ftp_server_v6) and enter the host address, 2001:DB8::D1A5:C8E1.

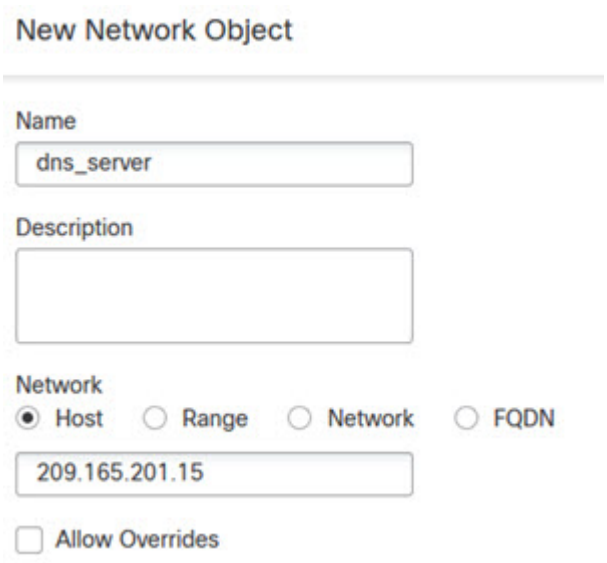


e) Click **Save**.

Step 2 Create the network objects for the DNS server.

a) Click **Add Network** > **Add Object** and define the DNS server's real address.

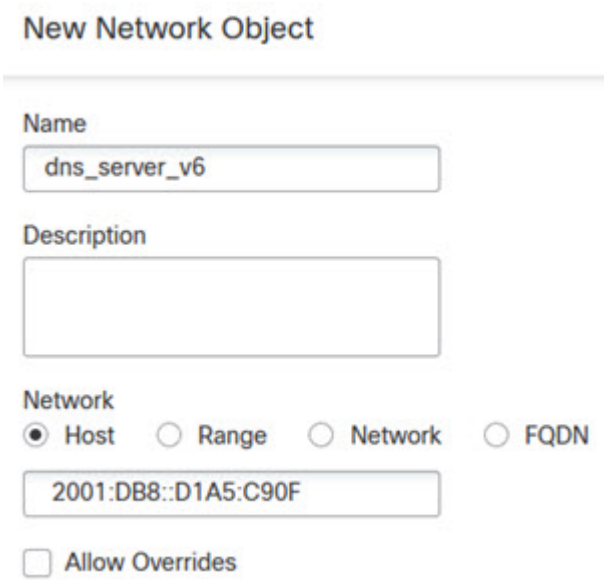
Name the network object (for example, dns_server) and enter the host address, 209.165.201.15.



b) Click **Save**.

c) Click **Add Network** > **Add Object** and define the DNS server's translated IPv6 address.

Name the network object (for example, dns_server_v6) and enter the host address, 2001:DB8::D1A5:C90F (where D1A5:C90F is the IPv6 equivalent of 209.165.201.15).

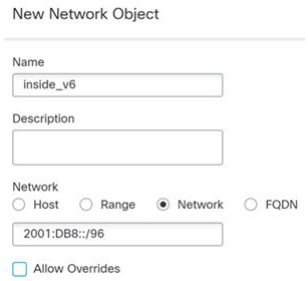


d) Click **Save**.

Step 3 Create the network objects for the inside network.

a) Click **Add Network** > **Add Object** and define the inside IPv6 network.

Name the network object (for example, inside_v6) and enter the network address, 2001:DB8::/96.

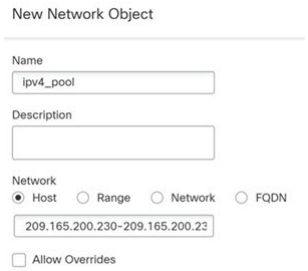


b) Click **Save**.

Step 4 Create the network objects for the PAT pool.

a) Click **Add Network** > **Add Object** and define the IPv4 PAT pool for the inside IPv6 network.

Name the network object (for example, ipv4_pool) and enter the range 209.165.200.230-209.165.200.235.



b) Click **Save**.

Step 5 Configure the static NAT rule with DNS modification for the FTP server.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

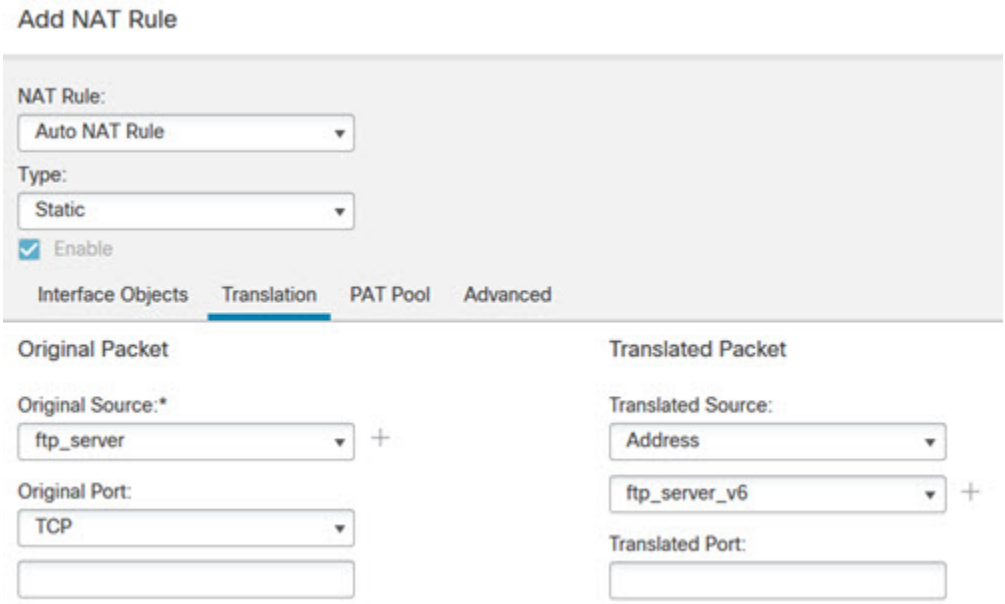
- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

e) On **Translation**, configure the following:

- **Original Source** = ftp_server network object.
- **Translated Source** > **Address** = ftp_server_v6 network object.



f) On **Advanced**, select the following options:

- **Translate DNS replies that match this rule**.
- **Net to Net Mapping**, because this is a one-to-one NAT46 translation.

g) Click **OK**.

Step 6 Configure the static NAT rule for the DNS server.

a) Click **Add Rule**.

b) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

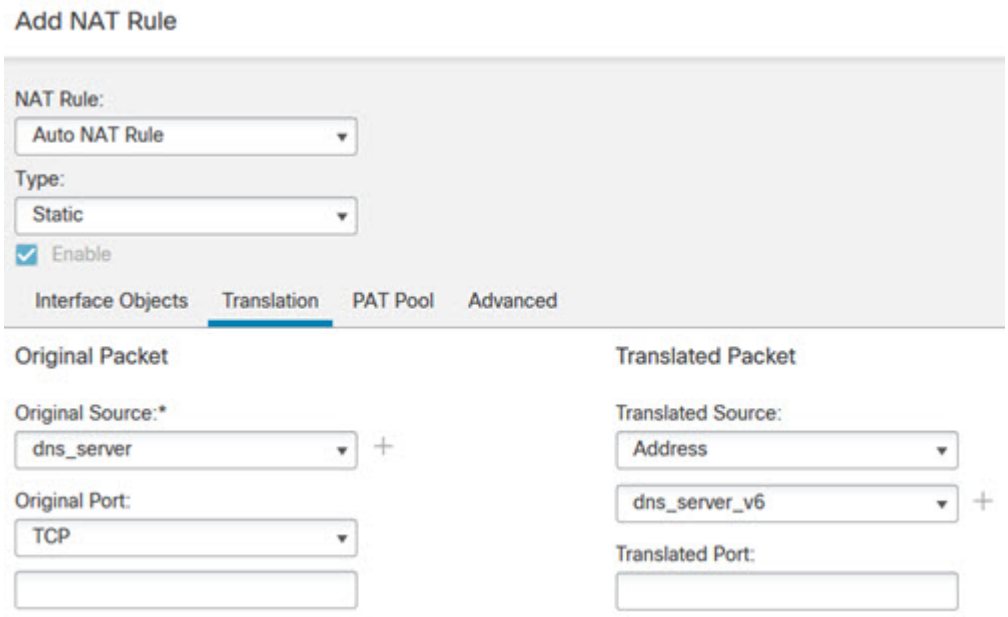
c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

d) On **Translation**, configure the following:

- **Original Source** = dns_server network object.
- **Translated Source** > **Address** = dns_server_v6 network object.

e) On **Advanced**, select **Net to Net Mapping**, because this is a one-to-one NAT46 translation.



f) Click **OK**.

Step 7 Configure the dynamic NAT with a PAT pool rule for the inside IPv6 network.

a) Click **Add Rule**.

b) Configure the following properties:

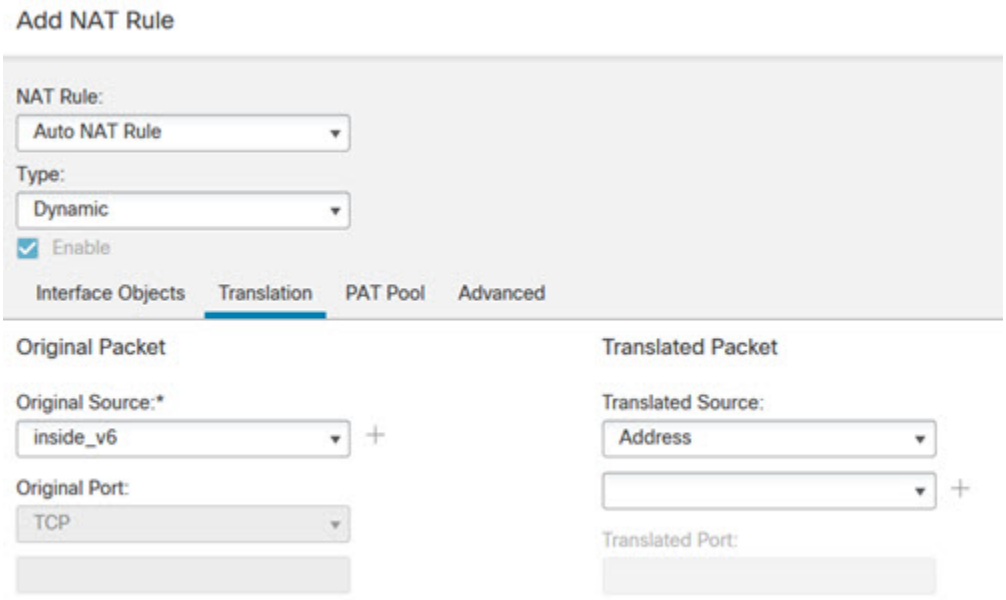
- **NAT Rule** = Auto NAT Rule.
- **Type** = Dynamic.

c) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

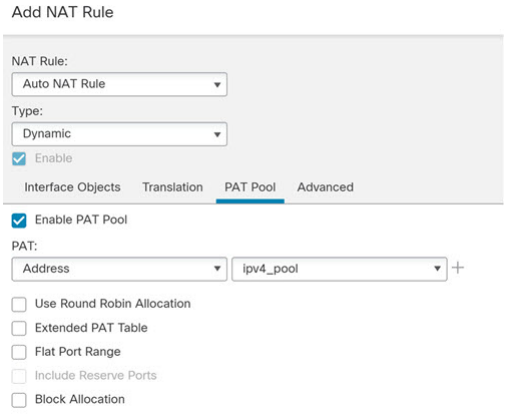
d) On **Translation**, configure the following:

- **Original Source** = inside_v6 network object.
- **Translated Source** > **Address** = leave this field empty.



e) On **PAT Pool**, configure the following:

- **Enable PAT Pool** = select this option.
- **Translated Source** > **Address** = ipv4_pool network object.



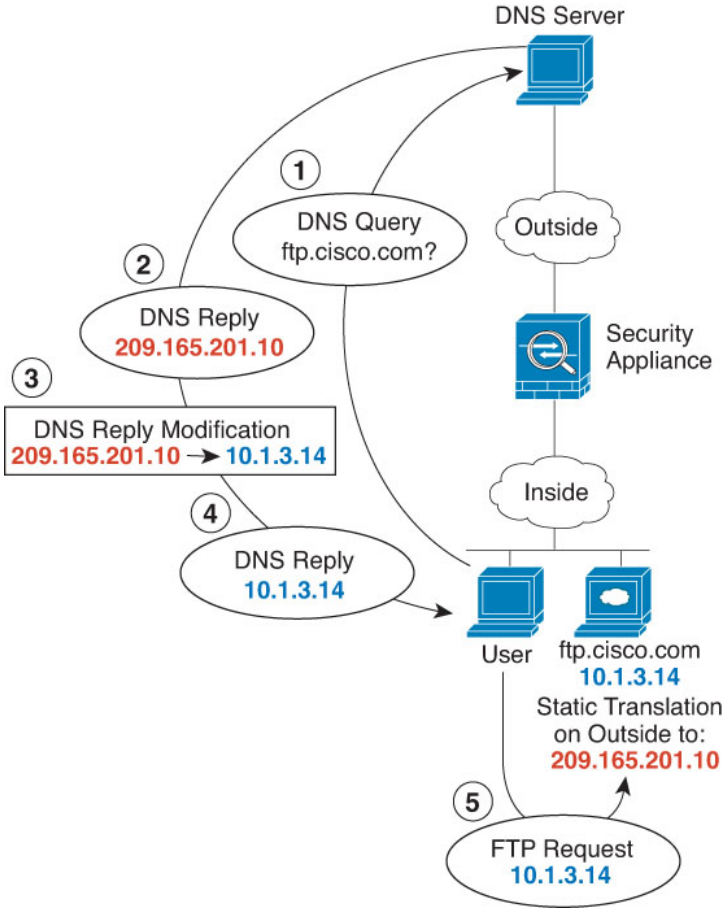
f) Click **OK**.

Create DNS reply modification with DNS server on outside

The following figure shows a DNS server that is accessible from the outside interface. A server, ftp.cisco.com, is on the inside interface. You configure NAT to statically translate the ftp.cisco.com real address (10.1.3.14) to a mapped address (209.165.201.10) that is visible on the outside network.

In this case, you want to enable DNS reply modification on this static rule so that inside users who have access to ftp.cisco.com using the real address receive the real address from the DNS server, and not the mapped address.

When an inside host sends a DNS request for the address of ftp.cisco.com, the DNS server replies with the mapped address (209.165.201.10). The system refers to the static rule for the inside server and translates the address inside the DNS reply to 10.1.3.14. If you do not enable DNS reply modification, then the inside host attempts to send traffic to 209.165.201.10 instead of accessing ftp.cisco.com directly.



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

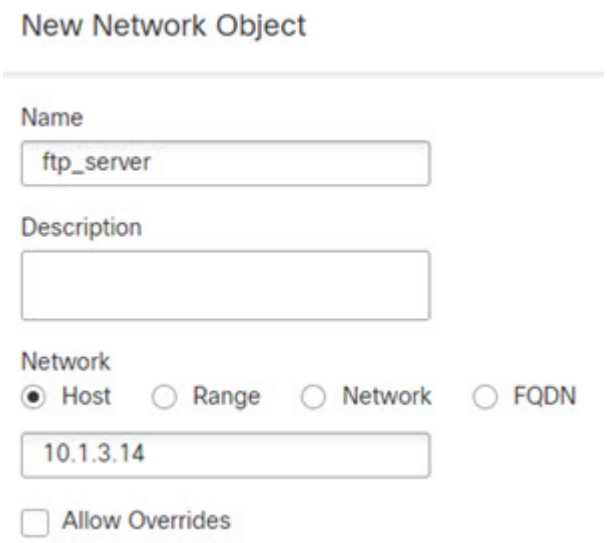
Procedure

Step 1 Create the network objects for the FTP server.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

b) Define the real FTP server address.

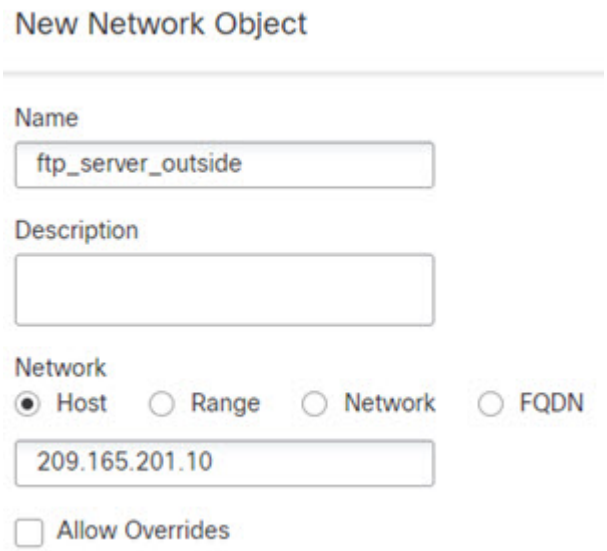
Name the network object (for example, ftp_server) and enter the host address, 10.1.3.14.



c) Click **Save**.

d) Click **Add Network** > **Add Object** and define the FTP server's translated address.

Name the network object (for example, ftp_server_outside) and enter the host address, 209.165.201.10.



e) Click **Save**.

Step 2 Configure the static NAT rule with DNS modification for the FTP server.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.

b) Click **Add Rule**.

c) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

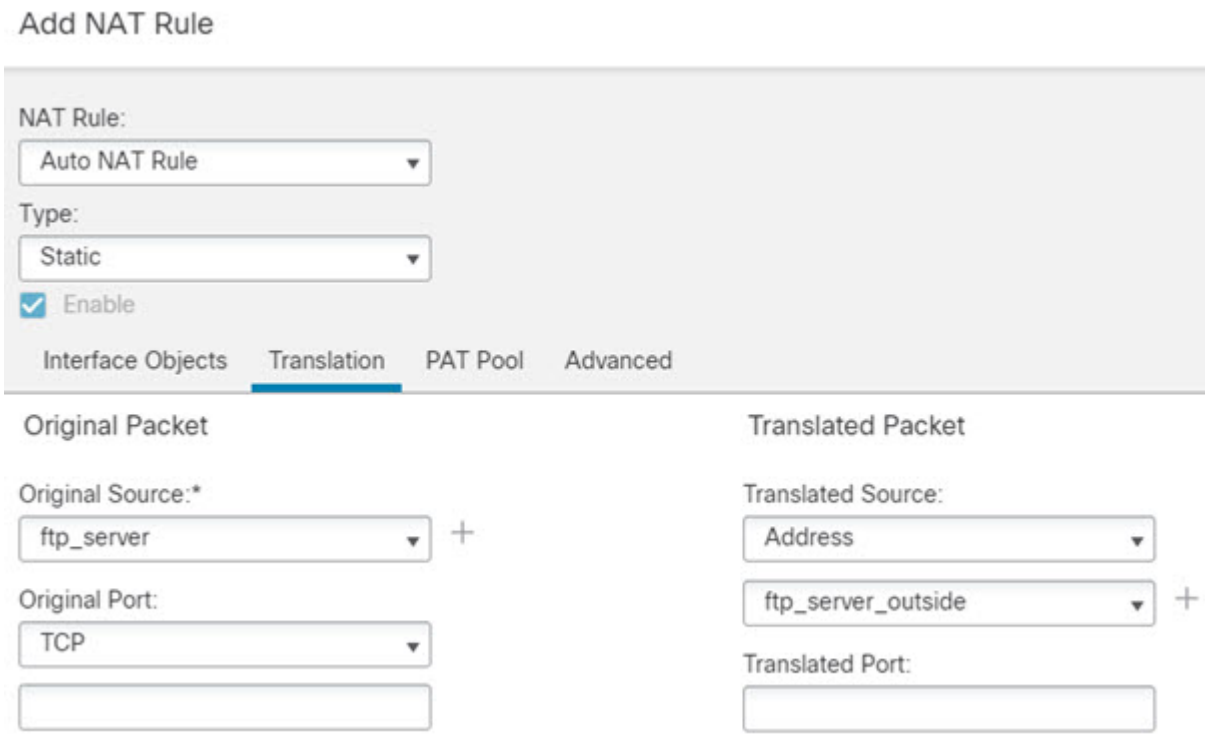
d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = inside.
- **Destination Interface Objects** = outside.

e) On **Translation**, configure the following:

- **Original Source** = ftp_server network object.
- **Translated Source** > **Address** = ftp_server_outside network object.

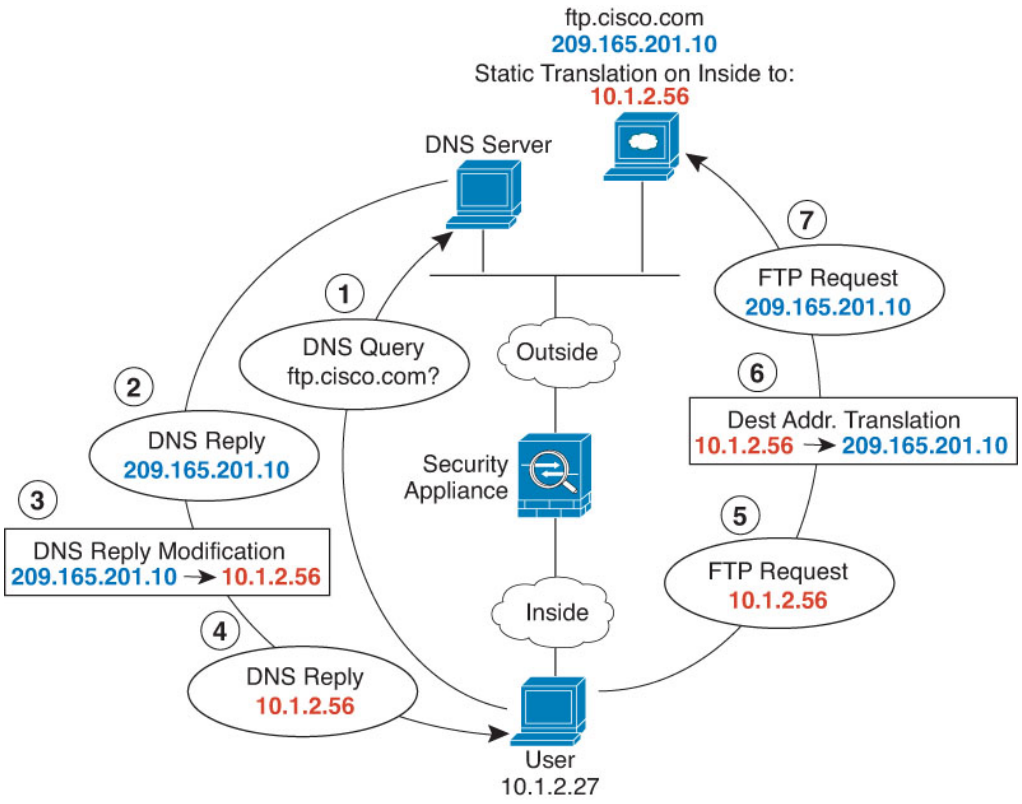
f) On **Advanced**, select **Translate DNS replies that match this rule**.



g) Click **OK**.

Configure DNS reply modification with DNS server on host network

The following figure shows an FTP server and DNS server on the outside. The system has a static translation for the outside server. In this case, when an inside user requests the address for ftp.cisco.com from the DNS server, the DNS server responds with the real address, 209.165.20.10. Because you want inside users to use the mapped address for ftp.cisco.com (10.1.2.56) you need to configure DNS reply modification for the static translation.



Before you begin

Ensure that you have interface objects (security zones or interface groups) that contain the interfaces for the device. In this example, we will assume the interface objects are security zones named **inside** and **outside**. To configure interface objects, select **Objects** > **Object Management** > **Interface**.

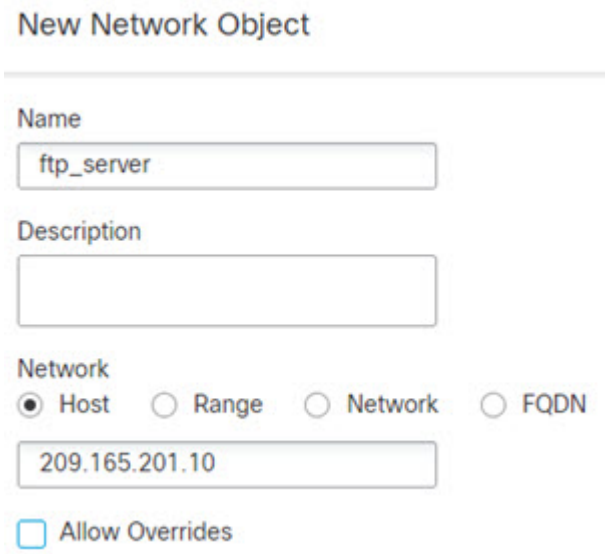
Procedure

Step 1 Create the network objects for the FTP server.

a) Choose **Objects** > **Object Management** > **Network** and click **Add Network** > **Add Object**.

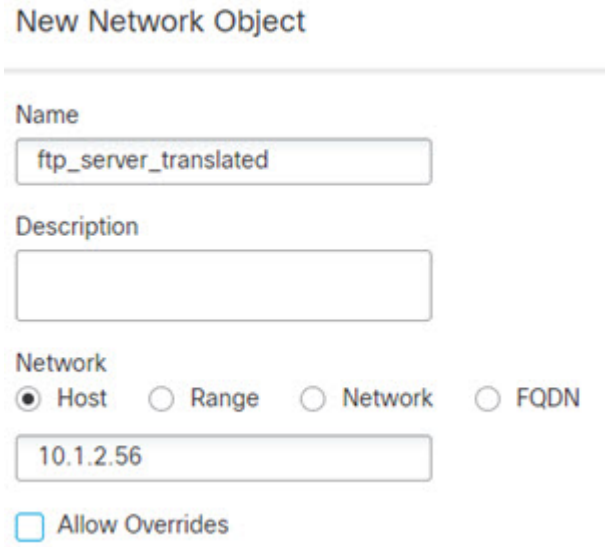
b) Define the real FTP server address.

Name the network object (for example, ftp_server) and enter the host address, 209.165.201.10.



c) Click **Save**.
d) Click **Add Network** > **Add Object** and define the FTP server's translated address.

Name the network object (for example, ftp_server_translated) and enter the host address, 10.1.2.56.



e) Click **Save**.

Step 2 Configure the static NAT rule with DNS modification for the FTP server.

a) Select **Devices** > **NAT** and create or edit the Firewall Threat Defense NAT policy.
b) Click **Add Rule**.
c) Configure the following properties:

- **NAT Rule** = Auto NAT Rule.
- **Type** = Static.

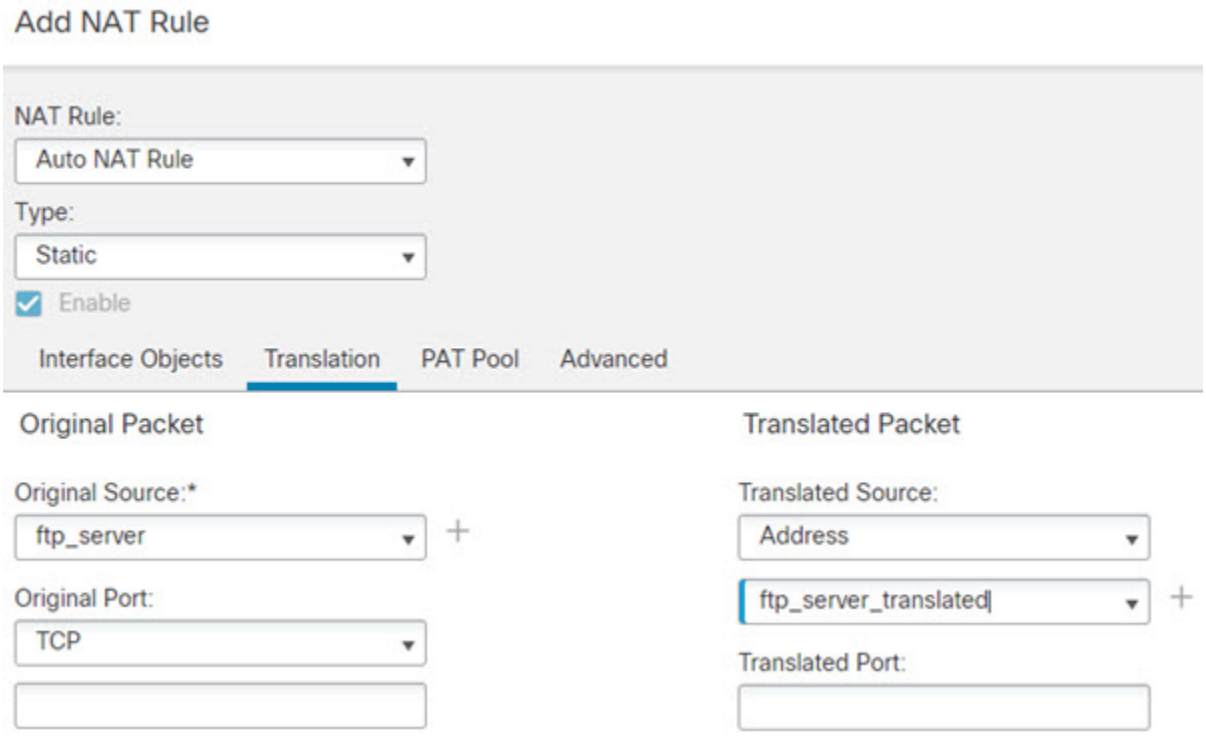
d) On **Interface Objects**, configure the following:

- **Source Interface Objects** = outside.
- **Destination Interface Objects** = inside.

e) On **Translation**, configure the following:

- **Original Source** = ftp_server network object.
- **Translated Source** > **Address** = ftp_server_translated network object.

f) On **Advanced**, select **Translate DNS replies that match this rule**.



g) Click **OK**.

History for Firewall Threat Defense NAT

This table provides a chronological summary of feature changes and enhancements for the network address translation policy across different software releases.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Creation of network groups while editing NAT rules.	7.2.6 7.4.1	Any	You can create network groups in addition to network objects when you are editing a NAT rule. This feature is not supported in Version 7.3.x or 7.4.0.
Ability to enable, disable, or delete more than one NAT rule at a time.	7.2	Any	You can select multiple NAT rules and enable, disable, or delete them all at the same time. Enable and disable apply to manual NAT rules only, whereas delete applies to any NAT rule.
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	7.1	Any	You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.
Changes to PAT address allocation in clustering. The PAT pool **Flat Port Range** option is now enabled by default and it is not configurable.	6.7	Any	The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the control unit instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally included the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address. As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1023 - 65535. Previously, you could optionally use a flat range by including the **Flat Port Range** option in a PAT pool rule. The **Flat Port Range** option is now ignored: the PAT pool is now always flat. You can optionally select the **Include Reserved Ports** option to include the 1 - 1023 port range within the PAT pool. Note that if you configure port block allocation (the **Block Allocation** PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster.
Ability to search and filter the Firewall Threat Defense NAT rule table.	6.7	Any	You can now search for rules in Firewall Threat Defense NAT policies to help you find rules based on IP addresses, ports, object names, and so forth. Search results include partial matches. Searching on criteria filters the rule table so only matching rules are displayed. We added a search field above the rule table when you edit Firewall Threat Defense NAT policies.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Carrier grade NAT enhancements.	6.5	Any	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). New/modified screens: We added the **Block Allocation** option to the NAT PAT Pool tab for Firewall Threat Defense NAT rules.
Support for network range objects in NAT for Firewall Threat Defense.	6.1.0	Any	You can now use network range objects in Firewall Threat Defense NAT rules where appropriate.
Network Address Translation (NAT) for Firewall Threat Defense.	6.0.1	Any	The NAT policy for Firewall Threat Defense was added. New/modified screens: Threat Defense was added as a type of NAT policy to the **Devices** > **NAT** page.



CHAPTER 31

Quality of Service

Quality of Service is a network management feature that:

- enables the policing of network traffic on Firewall Threat Defense devices.
- assists administrators in managing network traffic,
- provides guidelines for rate limiting.

- QoS, on page 1313
- QoS policies, on page 1314
- Requirements and prerequisites for QoS, on page 1314
- Guidelines and limitations for QoS policies, on page 1315
- Rate limiting with QoS policies, on page 1315
- History for QoS, on page 1326

QoS

QoS is a traffic management mechanism that

- rate limits (polices) network traffic that is allowed or trusted by access control
- does not rate limit traffic that was fastpathed and
- is supported only on the routed interfaces of Firewall Threat Defense devices.

QoS interface limitations

QoS is supported only on the routed interfaces of Firewall Threat Defense devices. However, it does not support site-to-site VPN and VTI interfaces.

Logging Rate-Limited Connections

You cannot configure logging for QoS. A connection can be rate limited without being logged. Conversely, a logged connection may not be rate-limited. To view QoS details, you must separately log connection ends in your Firewall Management Center database. See *Other Connections You Can Log* in the *Cisco Secure Firewall Management Center Administration Guide* for more information.

Connection events for rate-limited connections show how much traffic was dropped and the specific QoS configurations that applied. You can view this information in event views (workflows), dashboards, and reports.

QoS policies

A QoS policy is a configuration mechanism that

- governs rate limiting on managed devices
- can target multiple devices with each device having one deployed QoS policy at a time, and
- contains up to 63 QoS rules that handle network traffic in specified order.

QoS policy characteristics

QoS policies have these key characteristics:

-
- The system matches traffic to QoS rules in the order specified. The system rate limits traffic according to the first rule where all rule conditions match the traffic. Traffic not matching any of the rules is not rate limited.
- QoS rules can be limited by source or destination (routed) interfaces. The system enforces rate limiting *independently* on *each* of those interfaces and does not support an aggregate rate limit for a set of interfaces.
-
- You can independently rate limit download and upload traffic based on the connection initiator.



Note A device can have no more than 255 rules, including QoS rules. Exceeding this number causes a deployment warning necessitating a reduction in the number of rules..



Note QoS operates independently and is not subordinate to a main access control configuration. However, the access control and QoS policies deployed to the same device share identity configurations. For more infomration, see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Requirements and prerequisites for QoS

This reference provides the requirements and prerequisites for implementing QoS, including supported models, domains, and user roles.

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

Access Admin

Network Admin

Guidelines and limitations for QoS policies

QoS rules and service policy rules (in the access control policy) are translated into firewall commands. There can be only one policy map per interface as the system combines QoS and service policy configurations automatically.

However, you can also create policy maps manually using FlexConfig. For lower-end firewalls, such as the Secure Firewall 3100, you can create up to 64 policy maps using FlexConfig. For more powerful firewalls, such as the Firepower 4100, you can create up to 128 policy maps. Ensure not to exceed this limit to prevent deployment failures. You can check the device configuration using the CLI or the deployment transcript to see how rules are translated into commands.

Rate limiting with QoS policies

To perform policy-based rate limiting, configure and deploy QoS policies to managed devices. Each QoS policy can target multiple devices; each device can have one deployed QoS policy at a time.

Only one person should edit a policy at a time, using a single browser window. If multiple users save the same policy, the last saved changes are retained. For your convenience, the system displays information on who (if anyone) is currently editing each policy. To protect the privacy of your session, a warning appears after 30 minutes of inactivity on the policy editor. After 60 minutes, the system discards your changes.

Procedure

Step 1 Choose **Devices** > **QoS**.

Step 2 Click **New Policy** to create a new QoS policy and, optionally assign target devices; see Create a QoS policy, on page 1316.

You can also **Copy** ( ) or **Edit** ( ) an existing policy.

Step 3 Configure QoS rules; see Configuring QoS rules, on page 1318 and QoS rule conditions, on page 1320.

The QoS policy editor lists each rule in evaluation order and displays a summary of the rule conditions and rate limiting configurations. Use the right-click menu to manage rules, including moving, enabling, and disabling them.

This feature is helpful in larger deployments. You can **Filter by Device** to display only the rules that affect a specific device or group of devices. You can also search for rules, and the system matches text entered in the **Search Rules** field to rule names and condition values, including objects and object groups.

Note Properly creating and ordering rules is a complex but essential to effective deployment. Careful planning is necessary to prevent rules from preempting each other, requiring additional licenses, or containing invalid configurations. Icons in the interface represent comments, warnings, and errors. If issues exist, click **Show Warnings** to display a list. For more information, see Best practices for access control rules, on page 1625.

Step 4 Click **Policy Assignments** to identify which managed devices the policy targets; see Set target devices for a QoS policy , on page 1317.

Verify your choices, if you identified target devices during policy creation.

Step 5 Save the QoS policy.

Step 6 Since this feature must allow some packets to pass, configure your system to examine those packets.

Step 7 Deploy configuration changes; see Deploy configuration changes, on page 135.

The QoS policy is configured and deployed to the target devices, enabling policy-based rate limiting for network traffic.

Create a QoS policy

Create a QoS policy to establish the foundation for implementing rate limiting and traffic management rules on network devices.

The new QoS policy you create will not perform any rate limiting unless rules are added.

Procedure

Step 1 Choose **Devices** > **QoS**.

Step 2 Click **New Policy**.

Step 3 Enter a **Name** and, optionally, a **Description**.

Step 4 (Optional) Choose the **Available Devices** where you want to deploy the policy, then click **Add to Policy**, or drag and drop to the **Selected Devices**. To narrow the devices that appear, type a search string in the **Search** field.

Devices must be assigned before policy deployment.

Step 5 Click **Save**.

A new QoS policy is created and ready for configuration with rate limiting rules.

What to do next

- Configure and deploy the QoS policy; see Rate limiting with QoS policies, on page 1315.

Set target devices for a QoS policy

Before you begin

Ensure you are logged into the QoS policy editor and have the necessary access rights to configure system policies.

A QoS policy can target multiple devices, but each device can have one deployed QoS policy at a time.

Procedure

Step 1 In the QoS policy editor, click **Policy Assignments**.

Step 2 Build your target list:

- Add—Choose one or more **Available Devices**, then either click **Add to Policy** or drag and drop into the list of **Selected Devices**.
- Delete—Click **Delete** ( ) next to a single device, or choose multiple devices, right-click, then choose **Delete Selected**.
- Search—Enter a search string in the search field. Click **Clear** ( ) to clear the search.

Step 3 Click **OK** to save policy assignments.

Step 4 Click **Save** to save the policy.

The QoS policy is successfully configured with assigned target devices and is ready for deployment.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Filter QoS rules by device

You can filter the list of QoS policy rules based on the device to which the rules apply. A rule's interface constraints determine if the rule affects a device.

Tip Hover your pointer over a rule criterion to see its value. If the criterion represents an object with device-specific overrides, the system displays the override value when you filter the rules list by that device. If the criterion represents an object with domain-specific overrides, the system displays the override value when you filter the rules list by devices in that domain.

Procedure

Step 1 In the policy editor, click **Rules**, then click **Filter by Device**.
A list of targeted devices and device groups appears.

Step 2 Check one or more check boxes to display only the rules that apply to those devices or groups. Or, check **All** to reset and display all of the rules.

Step 3 Click **OK**.

A message appears next to the button showing the filter used. To remove the filter, click the X in the message. Alternatively, select **All** in the Filter by device dialog box.

The QoS rules list displays only the rules that apply to the selected devices or device groups. It simplifies the process of reviewing and managing device-specific QoS policies.

Configuring QoS rules

QoS rules enable you to control and rate limit network traffic on specific interfaces by configuring rule properties, conditions, and traffic limits.

When you create or edit a rule, use the upper portion of the rule editor to configure general rule properties. Use the lower portion of the rule editor to configure rule conditions and comments.

Procedure

Step 1 On Rules of the QoS policy editor:

- Add Rule—Click **Add Rule**.
- Edit Rule—Click **Edit** ( ).

Step 2 Enter a **Name**.

Step 3 Configure rule components:

- Enabled—Specify whether the rule is **Enabled**.
- Apply QoS On—Select the interfaces you want to rate limit, either **Interfaces in Destination Interface Objects** or **Interfaces in Source Interface Objects**. Your choice must correspond with a populated interface constraint (not **any**).
- Traffic Limit Per Interface—Enter a **Download Limit** and an **Upload Limit** in Mbits/sec. The default value of **Unlimited** prevent matching traffic from being rate limited in that direction.
- Conditions—Click the corresponding condition you want to add. You must configure a source or destination interface condition, corresponding to your choice for **Apply QoS On**.
- Comments—Click **Comments**. To add a comment click **New Comment**, enter a comment, and click **OK**. You can edit or delete this comment until you save the rule.

For detailed information on rule components, see QoS rule components, on page 1319.

Step 4 Save the rule.

Step 5 In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste.

Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

Step 6 Click **Save** to save the policy.

The QoS rule you created or modified is saved to the policy and configured with your set traffic limits and conditions.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Related Topics

Best practices for access control rules, on page 1625

QoS rule components

QoS rules consist of several key components that control traffic rate limiting and filtering behavior. Understanding these components helps you configure effective quality of service policies.

QoS rules include these main components:

- State (Enabled/Disabled): Controls whether the rule is active and enforced by the system.
- Interfaces (Apply QoS On): Specifies which interfaces the rate limiting applies to.
- Traffic Limit Per Interface: Sets the rate limiting values for matching traffic.
- Conditions: Defines the traffic criteria that must be matched for the rule to apply.
- Comments: Provides documentation and change tracking for the rule.

State (Enabled/Disabled)

By default, rules are enabled. If you disable a rule, the system does not use it and stops generating warnings and errors for that rule.

Interfaces (apply QoS on)

You cannot save a QoS rule that rate limits all traffic. For each QoS rule, apply QoS on one of the options:

- Interfaces in Source Interface Objects—Rate limits traffic through the rule's source interfaces. If you choose this option, you must add at least one source interface constraint (cannot be **any**).
- Interfaces in Destination Interface Objects—Rate limits traffic through the rule's destination interfaces. If you choose this option, you must add at least one destination interface constraint (cannot be **any**).

Traffic limit per interface

A QoS rule enforces rate limiting *independently* on *each* interface specified with the Apply QoS On option. Aggregate rate limits cannot be applied to a group of interfaces.

You can rate limit traffic by Mbits per second. The default value of **Unlimited** prevents matching traffic from being rate limited.

You can independently rate limit download and upload traffic. The system determines download and upload directions based on the connection initiator.

If you specify a limit greater than the interface's maximum throughput, the system does not rate limit matching traffic. Maximum throughput may be affected by an interface's hardware configuration, which you specify in each device's properties (**Devices** > **Device Management**).

Conditions

Conditions specify the specific traffic that the rule handles. You can configure each rule with multiple conditions. Traffic must meet all conditions to match the rule. Each condition type has its own tab in the rule editor. For more information, see QoS rule conditions, on page 1320.

Comments

Each time you save changes to a rule, add comments. You might summarize the overall configuration for users, or note any changes made and the reasons.

In the policy editor, the system displays how many comments a rule has. In the rule editor, use the Comments tab to view existing comments and add new ones.

QoS rule conditions

Conditions specify the traffic the rule handles. You can configure each rule with multiple conditions. All conditions must be met for traffic to match the rule. Each condition type has its own tab in the rule editor. You can rate limit traffic using these conditions.

Related Topics

Interface rule conditions, on page 1320
Network rule conditions, on page 1321
User rule conditions, on page 1321
Application rule conditions, on page 1322
Best practice: use application-based rules over port-based rules, on page 1323
Recommendation: use URL conditions for website access control, on page 1324
Custom SGT rule conditions, on page 1325

Interface rule conditions

An interface rule condition is a network traffic control that

- controls traffic by its source and destination interfaces,
- uses predefined interface objects called security zones or interface groups to build interface conditions, and
- improves system performance by constraining rules to specific interfaces.

Interface rule condition characteristics

Interface objects segment your network by grouping interfaces across multiple devices to manage and classify traffic flow. For more information, refer to Interfaces, on page 2383.

QoS rules can be applied only on routed interfaces.

Note Constraining rules by interface is one of the best ways to improve system performance. If a rule excludes all of a device's interfaces, that rule does not affect that device's performance.

Network rule conditions

A network condition is a traffic matching criterion that

- controls or decrypts traffic based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Note You *cannot* use FDQN network objects in identity rules.

User rule conditions

A user rule condition is a traffic matching mechanism that

- matches traffic based on whether the user initiating the connection or the group to which they belong
- can be configured for users in Microsoft Active Directory realms only, and
- enables policy enforcement based on user identity and group membership.

Special identities users

In addition to configuring users and groups for configured realms, you can set policies for the special identities users:

- Failed Authentication: User who failed authentication with the captive portal.
- Guest: Users configured as guest users in the captive portal.
- No Authentication Required: Users that match an identity **No Authentication Required** rule action.
- Unknown: Users that cannot be identified such as users who are not downloaded by a configured realm.

For access control rules only, you must first associate an identity policy with the access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

User rule condition example

Configure a Block rule to prohibit anyone in the Finance group from accessing a network resource.

Application rule conditions

Application rule conditions are application awareness and control mechanisms that

- identify and classify applications through IP traffic analysis
- enable control with organized filters
- require one enabled detector for each condition.

Application filters and control benefits

System-provided *application filters* help perform control by organizing applications according to basic characteristics, such as type, risk, business relevance, category, and tags. You can also create reuseable, user-defined filters using combinations of system-provided filters, or custom combinations of applications.

At least one detector must be enabled for each application rule condition in the policy. If no detector is enabled, the system automatically enables all available system-provided detectors, or the most recently modified user-defined detector. For more information about application detectors, see Application detectors, on page 2284.

You can utilize both application filters and individually specified applications to ensure complete coverage. Understand the application's requirements to effectively order access control rules.

Application filters help you to quickly configure application control effectively. For example, you can easily use system-provided filters to create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the system blocks the session.

Using application filters simplifies policy creation and administration. It assures you that the system controls application traffic as expected. Because Cisco frequently updates and adds application detectors via system and vulnerability database (VDB) updates, you can ensure that the system uses up-to-date detectors to monitor application traffic. You can also create your own detectors and assign characteristics to the applications they detect, automatically adding them to existing filters.

The system characterizes detected applications using several criteria which form effective filters.

Table 75: Application characteristics

Characteristic	Description	Example
Type	Application protocols represent communications between hosts. Clients represent software running on a host. Web applications represent the content or requested URL for HTTP traffic.	HTTP and SSH are application protocols. Web browsers and email applications are clients. MPEG video and Facebook are web applications.

Characteristic	Description	Example
Risk	The likelihood that the application is being used for purposes that might be against your organization's security policy.	Peer-to-peer applications tend to have a very high risk.
Business Relevance	The likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally.	Gaming applications tend to have a very low business relevance.
Category	A general classification for the application that describes its most essential function. Each application belongs to at least one category.	Facebook is in the social networking category.
Tag	Additional information about the application. Applications can have any number of tags, including none.	Video streaming web applications often are tagged `high bandwidth` and `displays ads`.

Best practice: use application-based rules over port-based rules

Use application filtering criteria instead of port filtering to target traffic. Applications can be configured to use unique ports to bypass access control blocks.

Port conditions allow you to control traffic by its source and destination ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

The traditional method targets applications by using port specifications, but applications can manipulate unique ports to bypass these controls

Application filtering is recommended for applications to avoid blocking legitimate applications, like Firewall Threat Defense, that dynamically open separate channels for control and data flow. Port-based access control rules could block such applications, impacting desirable operations.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP).

- For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).
- If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

Port, protocol, and ICMP code rule conditions (concept)

A port, protocol, and ICMP code rule condition is a traffic matching criterion that

- matches traffic based on source and destination ports
- supports TCP, UDP, ICMP, and other protocols that do not use ports, and
- controls traffic flow in access control and other policy rules.

Port condition types

Port conditions match traffic based on the source and destination ports. Depending on the rule type, "port" can represent any of these types:

- TCP and UDP—Control TCP and UDP traffic based on the port. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP (6) /22.
- ICMP—Control ICMP and ICMPv6 (IPv6-ICMP) traffic based on its internet layer protocol plus an optional type and code. For example: ICMP(1):3:3.
- Protocol—Control traffic using other protocols that do not use ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Best practices for port-based rules

Specifying ports is the traditional method used to target applications. However, applications can be configured to use unique ports to bypass access control blocks. Use application filtering criteria when possible; however, note that application filtering is unavailable in prefilter rules.

Use application filtering for FTP and similar applications that open separate channels for control and data flow. Using port-based access control rules can prevent these kinds of applications from performing correctly and could result in blocking desirable connections.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as destination port conditions in a single access control rule.

Matching non-TCP traffic with port conditions

You can match non-port-based protocols. By default, if you do not specify a port condition, you are matching IP traffic. Although configuring port conditions can match non-TCP traffic, restrictions apply:

- Access control rules—For Classic devices, match GRE-encapsulated traffic with an access control rule by using the GRE (47) protocol as a destination port condition. To a GRE-constrained rule, add only network-based conditions: zone, IP address, port, and VLAN tag. The system uses outer headers to match **all** traffic in access control policies with GRE-constrained rules. For Firewall Threat Defense devices, use tunnel rules in the prefilter policy to control GRE-encapsulated traffic.
- Decryption rules—These rules support only TCP port conditions.
- IMCP echo—A destination ICMP port with the type set to 0 or a destination ICMPv6 port with the type set to 129 only matches unsolicited echo replies. ICMP echo replies, sent in response to ICMP echo requests, are ignored. To match any ICMP echo, use ICMP type 8 or ICMPv6 type 128.

Recommendation: use URL conditions for website access control

Use URL conditions to control the websites that users on your network can access.

For complete information, see URL filtering with category and reputation, on page 1652.

Custom SGT rule conditions

A custom SGT rule condition is a traffic filtering mechanism that

- Use manually created SGT objects to filter traffic. Do not rely on ISE SGTs from a server.
- Correspond to the SGT attributes on the traffic to be controlled.
- Exclude user control considerations when using custom SGT traffic.

SGT traffic control without ISE configuration

If you do not configure ISE or ISE-PIC as an identity source, you can control traffic using Security Group Tags (SGTs) that were **not** assigned by ISE. SGTs specify traffic source privileges in a trusted network.

ISE SGT versus custom SGT rule conditions

Certain rules allow you to control traffic based on assigned SGT. The rule type and identity source configuration determine whether ISE-assigned SGTs or custom SGTs are used to match traffic with assigned SGT attributes.

Condition Type	Requires	SGTs Listed in Rule Editor
ISE SGT	ISE identity source	SGTs obtained by querying the ISE server, automatically updated metadata
Custom SGT	No ISE or ISE-PIC identity source	Static SGT objects you create

Note If using ISE SGTs to match traffic, any packet will match an ISE SGT rule if the SGT associated with the packet source IP address is recognized in ISE, even without an assigned SGT attribute.

Autotransition from custom Security Group Tags to ISE Security Group Tags

An autotransition from custom Security Group Tags (SGTs) to ISE Security Group Tags is a system process that automatically adjusts rule configuration when you configure ISE/ISE-PIC as an identity source after creating rules with custom Security Group Tags.

System behavior during autotransition

If you create rules that match custom SGTs, then configure ISE or ISE-PIC as an identity source, the system will:

- Disable **Security Group Tag** options: The system retains existing SGT objects, but you cannot modify them or add new ones.
- Retain existing rules: Existing rules with custom SGT conditions remain, but they do not match traffic, and you cannot add more custom SGT conditions.

If you configure ISE, it is recommended to delete or disable existing rules with custom Security Group Tag conditions and use ISE attribute conditions to match traffic with Security Group Tag attributes.

History for QoS

This reference provides a chronological history of QoS feature updates, including version information and implementation details.

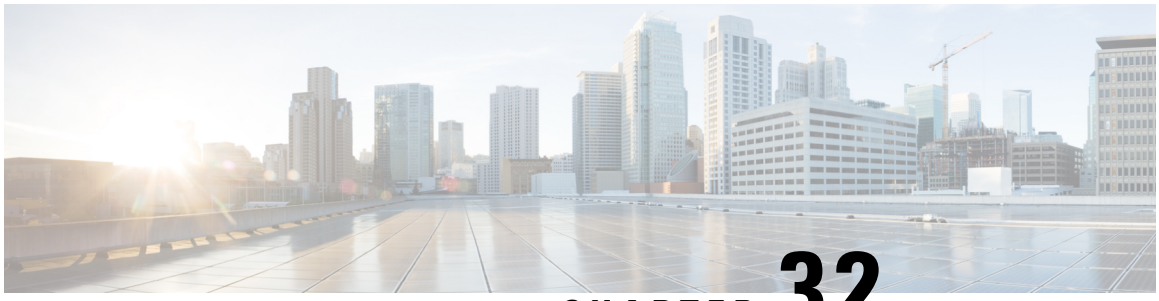
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Deprecated: priority-queue with FlexConfig.	7.2.5	7.2.5	FlexConfig was used to configurethe priority-queue in threat defense. This command was removed.
Ability to specify handling of URLs having unknown reputation.	6.7.0	Any	For details, see History for URL filtering, on page 1678. New/modified screens: QoS rule editor
Rate limit increased.	6.2.1	Any	Raised the maximum rate limit from 1,000 Mbps to 100,000 Mbps. New/modified screens: QoS rule editor
Custom SGT and original client network filtering.	6.2.1	Any	Rate limit traffic using custom Security Group Tags (SGTs) and original client network information (XFF, True-Client-IP, or custom-defined HTTP headers). New/modified screens: QoS Rule Editor
QoS (rate limiting) introduced.	6.1.0	Any	FTD can rate limit (police) network traffic that is either allowed or trusted by access control. New/modified screens: **Devices** > **QoS**



PART VI

Secure Connections

- Secure Connections Overview, on page 1329
- Site-to-Site VPN, on page 1345
- SD-WAN, on page 1405
- Remote Access VPN, on page 1415
- Dynamic Access Policies , on page 1531



CHAPTER 32

Secure Connections Overview

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

This chapter applies to Remote Access and Site-to-site VPNs on Secure Firewall Threat Defense devices. It describes the Internet Protocol Security (IPsec), the Internet Security Association and Key Management Protocol (ISAKMP, or IKE) and SSL standards that are used to build site-to-site and remote access VPNs.

- VPN types, on page 1329
- VPN basics, on page 1330
- VPN packet flow, on page 1333
- IPsec flow offload, on page 1333
- VPN licensing, on page 1334
- VPN encryption and performance, on page 1334
- Deprecated hash algorithms, encryption algorithms, and Diffie-Hellman modulus groups, on page 1339
- VPN topologies, on page 1340

VPN types

VPN types are network connection categories that

- provide secure, encrypted connections between remote locations and private networks
- support deployment models including remote access and site-to-site configurations, and
- use various protocols including SSL and IPsec for establishing secure tunnels.

Supported VPN connection types

The Firewall Management Center supports these types of VPN connections:

- Remote Access VPNs in Firewall Threat Defense devices.

  Remote access VPNs provide secure, encrypted connections, or tunnels, between remote users and your company's private network. These connection use two devices: a VPN endpoint device, which is a workstation or mobile device with VPN client capabilities, and a VPN headend device, or secure gateway, at the edge of the corporate private network.

  Secure Firewall Threat Defense devices can be configured to support Remote Access VPNs over SSL or IPsec IKEv2 by the Firewall Management Center. When acting as secure gateways, these devices

authenticate remote users, authorize access, and encrypt data to provide secure connections to your network. Only these devices support remote access VPN connections, managed by the Firewall Management Center.

Secure Firewall Threat Defense secure gateways support the Secure Client full tunnel client. This client is required to provide secure SSL IPsec IKEv2 connections for remote users. This client automatically installs when a connection is established, so network administrators do not need to manually install or configure it on remote computers. It is the only client supported on endpoint devices.

- Site-to-site VPNs in Firewall Threat Defense devices.

  A site-to-site VPN connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices, and between managed devices and other Cisco or third-party peers. These peers can use either IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and IKEv1 or IKEv2. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

VPN basics

A VPN is a secure networking technology that

- uses tunneling to create secure connections between remote users and private corporate networks over public TCP/IP networks such as the Internet
- employs IPsec-based technologies with ISAKMP (IKE) and IPsec tunneling standards to build and manage tunnels, and
- enables bidirectional data transfer through tunnel endpoints that encapsulate and unencapsulate packets.

VPN tunnel management capabilities

ISAKMP and IPsec accomplish these tunnel management functions:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

A device in a VPN functions as a bidirectional tunnel endpoint. It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

After the site-to-site VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. A connection consists of the IP addresses

and hostnames of the two gateways, the subnets behind them, and the method the two gateways use to authenticate to each other.

VPN deployments use two primary device types:

- Hubs: Devices that enable secure VPN connectivity to and from one or more remote branch devices or spokes. Hubs also act as a gateway for spokes to communicate with each other.
- Spokes: Devices that connect over VPN to a hub to securely access the corporate resources behind the hub. Spokes communicate with each other through the hub.

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is a key management protocol that

- authenticates IPsec peers
- negotiates and distributes IPsec encryption keys, and
- automatically establishes IPsec security associations (SAs).

IKE negotiation phases and policies

The IKE negotiation comprises two phases:

- Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2.
- During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec.

Each phase uses proposals to negotiate a connection.

An IKE policy is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins when each peer agrees on a common IKE policy. This policy defines security parameters to protect subsequent IKE negotiations. IKEv1 policies contain a single set of algorithms and a modulus group. In an IKEv2 policy, you can select multiple algorithms and modulus groups for peers to choose from during the Phase 1 negotiation. You may create a single IKE policy, or create multiple policies to give higher priority to preferred options. For site-to-site VPNs, you can create an IKE policy. IKEv1 and IKEv2 each support a maximum of 20 IKE policies, each with a different set of values. Assign a unique priority to each policy that you create. A lower priority number indocates a higher priority for the policy.

To define an IKE policy, specify:

- A unique priority (1 to 65,543, with 1 being the highest priority).
- An encryption method for the IKE negotiation to protect the data and ensure privacy.
- A Hashed Message Authentication Codes (HMAC) method (called integrity algorithm in IKEv2) to verify the sender's identity, and to confirm that the message is unchanged during transit.
- For IKEv2, a separate pseudorandom function (PRF) used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. The options are the same as those used for the hash algorithm.
- A Diffie-Hellman group to determine the strength of the encryption key determination algorithm. The device uses this algorithm to derive the encryption and hash keys.

- An authentication method, to ensure the identity of the peers.
- A limit to the time the device uses an encryption key before replacing it.

When IKE negotiation begins, the initiating peer sends all its policies to the remote peer. The remote peer searches for a match with its own policies, in priority order. IKE policies match if both peers use the same encryption, hash (integrity and PRF for IKEv2), authentication, and Diffie-Hellman values. The SA lifetime must be less than or equal to the lifetime in the policy sent. If the lifetimes are not identical, the shorter value from the remote peer policy applies. By default, the Secure Firewall Management Center deploys an IKEv1 policy with the lowest priority for all VPN endpoints to ensure a successful negotiation.

IPsec

IPsec is a secure method for setting up a VPN that:

- provides data encryption at the IP packet level,
- transmits data over a public network through tunnels, which are secure, logical communication paths between two peers, and
- secures traffic that enters an IPsec tunnel by a combination of security protocols and algorithms.

With IPsec, data is transmitted over a public network through tunnels.

IPsec proposal policy components

An IPsec proposal policy defines the settings for IPsec tunnels. An IPsec proposal includes one or more crypto maps that are applied to the VPN interfaces in the devices. A crypto map combines all the components required to set up IPsec security associations, including:

- A proposal (or transform set) combines security protocols and algorithms that secure traffic in an IPsec tunnel. During the IPsec security association (SA) negotiation, peers search for a matching proposal. Apply the selected proposal to create an SA that protects data flows in the crypto map's access list and secures VPN traffic. There are separate IPsec proposals for IKEv1 and IKEv2. In IKEv1 proposals (or transform sets), you set one value for each parameter. In IKEv2 proposals, you can configure multiple encryption and integration algorithms for a single proposal.
- A crypto map combines all components required to set up IPsec security associations (SA), including IPsec rules, proposals, remote peers, and other parameters that are necessary to define an IPsec SA. When two peers try to establish an SA, they must each have at least one compatible crypto map entry.

  Dynamic crypto map policies are used in site-to-site VPNs when an unknown remote peer tries to start an IPsec security association with the local hub. The hub does not initiate the security association negotiation. Dynamic crypto policies allow remote peers to exchange IPsec traffic with a local hub, even if the hub does not know the remote peer's identity. A dynamic crypto map policy creates a crypto map entry before configuring all parameters. IPsec negotiation then dynamically configures the missing parameters to match a remote peer's requirements.

  Dynamic crypto map policies are applicable to both hub-and-spoke and point-to-point VPN topologies. To apply dynamic crypto map policies, specify a dynamic IP address for one of the peers in the topology and ensure that the dynamic crypto-map is enabled on this topology. In a full mesh VPN topology, you can apply only static crypto map policies.

Note Simultaneous IKEv2 dynamic crypto map is not supported for the same interface for both remote access and site-to-site VPNs in a Firewall Threat Defense device.

VPN packet flow

VPN packet flow is a security process that

- requires explicit permission through access control before allowing traffic to pass through,
- decrypts incoming tunnel packets before sending them to the Snort process,
- processes outgoing packets through Snort before encryption, and
- blocks tunnel traffic to the public source when the tunnel is down.

Access control requirements

Access control identifies the protected networks for each endpoint node of a VPN tunnel and determines which traffic is allowed to pass through the Firewall Threat Defense device and reach the endpoints. For remote access VPN traffic, a group policy filter or an access control rule must be configured to permit VPN traffic flow.

IPsec flow offload

IPsec flow offload is a performance optimization feature that

- offloads IPsec connections to field-programmable gate array (FPGA) or specialized hardware components after initial setup
- improves device performance by handling pre-decryption, decryption, pre-encryption, and encryption processing in hardware, and
- is enabled by default on supporting device models while allowing system software to handle inner flow security policies.

IPsec flow offload characteristics

After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device. This process improves device performance.

Offloaded operations include pre-decryption and decryption processing on ingress and egress. The system software applies your security policies for traffic within the inner flow.

IPsec flow offload applies to these device types:

- Secure Firewall 3100
- Secure Firewall 4200

IPsec flow offload is also used when the device's VTI loopback interface is enabled.

By default, the system enables IPsec flow offload on supported device models. To change the configuration, use FlexConfig to implement the **flow-offload-ipsec** command. For more information, refer to the ASA command reference.

VPN licensing

You do not need any specific license to enable VPN on a Firewall Threat Defense device, it is available by default.

The Firewall Management Center determines whether to allow or block the usage of strong encryption in the Firewall Threat Defense device based on the export-controlled functionality in the device. You can enable this functionality when you register with the Cisco Smart License Manager. If you are using the evaluation license, or you did not enable export-controlled functionality, you cannot use strong encryption. Choose **System** (⚙) > **Licenses** > **Smart Licenses** to verify this functionality in Firewall Management Center.

If you created your VPN configurations with an evaluation license and later upgraded your license to a smart license with export-controlled functionality, check and update your encryption algorithms to use stronger encryption so that the VPNs function properly. Do not use DES-based encryption, as it is not supported.

VPN encryption and performance

When you configure VPN tunnel encryption, provide sufficient protection and maintain efficiency by balancing security and performance.

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques with IKE policies and IPsec proposals. Using stronger tunnel encryption may lower system performance.

If your device license allows strong encryption, you can choose from a range of encryption and hash algorithms and Diffie-Hellman groups. This document does not provide specific guidance on which options you should choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

Comply with security certification requirements

Review your certification requirements and the available options to plan your VPN configuration. Many VPN settings have options that allow you to comply with various security certification standards.

Decide encryption algorithms for VPN policies

When deciding which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

- For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order.
- For IKEv1, you can select a single option only.

- For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-.

If your device license qualifies for strong encryption, you can choose from the available encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

Strong encryption license considerations



Note If you are qualified for strong encryption, before upgrading from the evaluation license to a smart license, check and update your encryption algorithms for stronger encryption so that the VPN configuration works properly. Choose AES-based algorithms. DES is not supported if you are registered using an account that supports strong encryption. After registration, you cannot deploy changes until you remove all uses of DES.

Available encryption algorithms

- AES-GCM—(IKEv2 only) Advanced Encryption Standard in Galois or Counter Mode is a block cipher mode that provides confidentiality and data-origin authentication. It offers greater security than AES.

  AES-GCM offers three different key strengths: 128-bit, 192-bit, and 256-bit keys. Longer keys increase security but reduce performance. NSA Suite B, a set of cryptographic algorithms that devices must support to meet federal cryptographic strength standards, requires GCM.

- AES—Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-bit, 192-bit, and 256-bit keys. Longer keys increase security but reduce performance.

- DES—Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option.

- Null, ESP-Null—A null encryption algorithm provides authentication without encryption. This method is not secure; use at your own discretion.

Decide which hash algorithms to use

In IKE policies, the hash algorithm creates a message digest to ensure your messages remain secure. In IKEv2, you can choose one hash algorithm for integrity and another for the pseudo-random function (PRF).

In IPsec proposals, the Encapsulating Security Protocol (ESP) uses the hash algorithm for authentication. In IKEv2 IPsec proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name has the ESP- prefix and an -HMAC suffix.

The system arranges your settings from the most secure to the least secure and negotiates with the peer in that order. For IKEv1, select only one option.

Select a hash algorithm that meets your security and performance needs:

- SHA (Secure Hash Algorithm)—The standard SHA (SHA1) produces a 160-bit digest.

  These SHA-2 options provide increased security and are available for IKEv2 configurations. Choose one if you require NSA Suite B cryptography compliance.

- SHA256—Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
- SHA384—Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
- SHA512—Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

- Null or None (NULL, ESP-NONE)—(IPsec Proposals only) AUse a null hash algorithm only for testing purposes. If you select one of the AES-GCM options as the encryption algorithm, choose the null integrity algorithm. For these encryption standards, the integrity hash is ignored even if you choose a non-null option.

Decide which Diffie-Hellman modulus group to use

You can use Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus increases security but requires more processing time. You must have a matching modulus group on both peers.

For AES encryption, use Diffie-Hellman (DH) Group 5 or higher to support the large key sizes required by AES. IKEv1 policies do not support all of the groups.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curve Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use a 2048-bit modulus reduce exposure to attacks such as Logjam.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure, then negotiates with the peer using that order. For IKEv1, you can select only a single option.

- 14—Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 15—Diffie-Hellman Group 15: 3072-bit MODP group.
- 16—Diffie-Hellman Group 16: 4096-bit MODP group.
- 19—Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20—Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21—Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 31—Diffie-Hellman Group 31: Curve25519 256-bit EC Group.

Decide VPN authentication methods

A VPN authentication method is a security mechanism that

- validates the identity of peers in a VPN connection
- enables secure communication between network devices, and
- ensures that only authorized devices can establish VPN connections.

Available authentication methods

VPNs support two primary authentication methods:

- **Preshared keys**: A secret key shared between two peers and used by IKE during the authentication phase. The same shared key must be configured at each peer or the IKE SA cannot be established.
- **Digital certificates**: Use RSA key pairs to sign and encrypt IKE key management messages. Certificates provide proof of communication between two peers.

VPN type support varies by authentication method.

Table 76: VPN authentication method support

VPN Type	Preshared Keys	Digital Certificates
Site-to-site IKEv1 and IKEv2	Supported	Supported
Remote Access (SSL and IPsec IKEv2)	Not supported	Supported

When you use digital certificate authentication, you need a Public Key Infrastructure (PKI) defined for peers to obtain digital certificates from a Certification Authority (CA). CAs manage certificate requests and issue certificates to participating network devices, providing centralized key management for all participating devices.

Preshared keys are difficult to manage for large networks. CAs make it easier to manage and scale your IPsec network. With a CA, you do not need to configure keys between all encrypting devices. Register each device with the CA to request its certificate. Devices with their own certificates and the CA's public key can authenticate other devices within the CA's domain.

Pre-shared keys

A pre-shared key is a secret key that

- enables you to share authentication credentials between two peers
- is used by IKE in the authentication phase, and
- must be configured identically on each peer or the IKE SA cannot be established.

Key configuration options

To configure pre-shared keys, select either a manual key or an automatically generated key. Specify this key in the IKEv1 or IKEv2 options. When you deploy your configuration, the key is configured on all devices in the topology.

PKI infrastructure and digital certificates

A PKI infrastructure is a centralized key management system that

- provides defined policies, procedures, and roles supporting public key cryptography
- generates, verifies, and revokes public key certificates, commonly known as digital certificates, and
- manages key pairs consisting of public and private keys for VPN endpoints to sign and encrypt messages.

Public key cryptography and certificate components

In public key cryptography, each endpoint of a connection has a key pair consisting of both a public and a private key. The key pairs are used by the VPN endpoints to sign and encrypt messages. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other, securing the data flowing over the connection.

Generate a general-purpose RSA, ECDSA, or EDDSA key pair for signing and encryption. Alternatively, generate separate key pairs for each purpose. Separate signing and encryption keys help to reduce key exposure. SSL uses a key for encryption, while IKE uses a key for signing. Separate keys for each purpose minimize exposure.

Certificates also ensure non-repudiation by providing proof that communication between two peers occurred.

You can obtain CA certificates by:

- Using the Simple Certificate Enrollment Protocol (SCEP) or Enrollment over Secure Transport (EST) to retrieve the CA's certificate from the CA server
- Manually copying the CA's certificate from another participating device

Trustpoints represent the object representation of a CA and associated certificates. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

A PKCS#12, or PFX, file holds the server certificate, any intermediate certificates, and the private key in one encrypted file. This type of file may be imported directly into a device to create a trustpoint.

A CA may also revoke certificates for peers that no longer participate in your network. Revoked certificates are either managed by an Online Certificate Status Protocol (OCSP) server or are listed in a certificate revocation list (CRL) stored on an LDAP server. A peer may check these before accepting a certificate from another peer.

Digital certificates or identity certificates

When you use digital certificates as the authentication method for VPN connections, peers are configured to obtain digital certificates from a Certificate Authority (CA). CAs are trusted authorities that sign certificates to verify their authenticity, thereby guaranteeing the identity of the device or user.

Digital certificates contain these components:

- The digital identification of the owner for authentication, such as name, serial number, company, department, or IP address.
- A public key needed to send and receive encrypted data to the certificate owner.
- The secure digital signature of a CA.

The certificate enrollment process includes these steps:

1. CA servers manage public CA certificate requests and issue certificates to participating network devices as part of a PKI.
2. Each participating device enrolls individually with a CA server, which validates identities and creates an identity certificate.
3. Each participating peer sends their identity certificate to the other peer to validate their identities and establish encrypted sessions with the public keys contained in the certificates.

Certificate enrollment

Using a PKI improves the manageability and scalability of your VPN because you do not have to configure preshared keys between all encrypting devices. Instead, enroll each participating device with a CA server, which validates identities and creates an identity certificate for the device. After completing enrollment, each participating peer sends its identity certificate to the other peer to validate their identities and establish encrypted sessions with the public keys contained in the certificates. For more information about enrolling Firewall Threat Defense device certificates, refer to Certificate enrollment objects, on page 2400.

Certificate authority certificates

In order to validate a peer's certificate, each participating device must retrieve the CA's certificate from the server. A CA certificate is used to sign other certificates. It is self-signed and called a root certificate. This certificate contains the CA's public key, which you use to decrypt and validate the CA's digital signature and the contents of the received peer's certificate.

To obtain the CA certificate:

- Use the Simple Certificate Enrollment Protocol (SCEP) or Enrollment over Secure Transport (EST) to retrieve the CA's certificate from the CA server
- Manually copy the CA's certificate from another participating device

Trustpoints

Once enrollment is complete, a trustpoint is created in the managed device. It is the object representation of a CA and associated certificates. A trustpoint includes the identity of the CA, CA-specific parameters, and one enrolled identity certificate.

PKCS#12 file

A PKCS#12 file, or PFX file holds the server certificate, intermediate certificates, and the private key in one encrypted file. This type of file may be imported directly into a device to create a trustpoint.

Revocation checking

A CA may also revoke certificates for peers that no longer participate in your network. Revoked certificates are either managed by an Online Certificate Status Protocol (OCSP) server or are listed in a certificate revocation list (CRL) stored on an LDAP server. A peer may check these before accepting a certificate from another peer.

Deprecated hash algorithms, encryption algorithms, and Diffie-Hellman modulus groups

Update your VPN configuration to use supported DH and encryption algorithms before upgrading to Firewall Threat Defense 6.70 or later.

- Update your IKE proposals and IPSec policies to match the ones supported in Firewall Threat Defense 6.70 or later.
- Deploy the configuration changes after updating to supported algorithms.

Support has been removed for these less secure ciphers from Firewall Threat Defense Version 6.70:

- **Diffie-Hellman GROUP 5** is deprecated for IKEv1 and IKEv2.
- Diffie-Hellman groups 2 and 24 have been removed.
- **Encryption algorithms**: 3DES, AES-GMAC, AES-GMAC-192, and AES-GMAC-256 have been removed.

Note **DES** continues to be supported in evaluation mode or for users who do not satisfy export controls for strong encryption.

NULL is removed in IKEv2 policy, but supported in both IKEv1 and IKEv2 IPsec transform-sets.

VPN topologies

When you create a new VPN topology you must give it a unique name, specify a topology type, and select the IKE version. You can select from three types of topologies, each containing a group of VPN tunnels:

- Point-to-point (PTP) topologies establish a VPN tunnel between two endpoints.
- Hub and spoke topologies establish a group of VPN tunnels connecting a hub endpoint to a group of spoke endpoints.
- Full mesh topologies establish a group of VPN tunnels among a set of endpoints.

There is no default pre-shared key for VPN authentication. You must define a pre-shared key manually or let the system generate it automatically. When choosing automatic, the Secure Firewall Management Center generates a pre-shared key and assigns it to all the nodes in the topology.

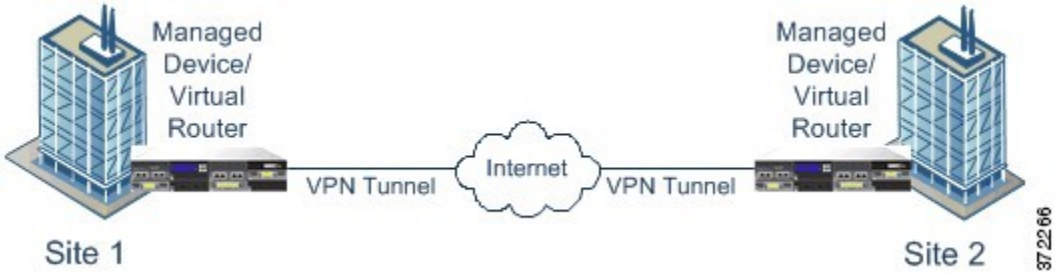
Point-to-point VPN topologies

A point-to-point VPN topology is a network configuration that

- enables two endpoints to communicate directly with each other
- allows you to configure the two endpoints as peer devices, and
- permits either device to start the secured connection.

This diagram displays a typical point-to-point VPN topology.

Figure 392: Point-to-point VPN topology



Hub and spoke VPN topology

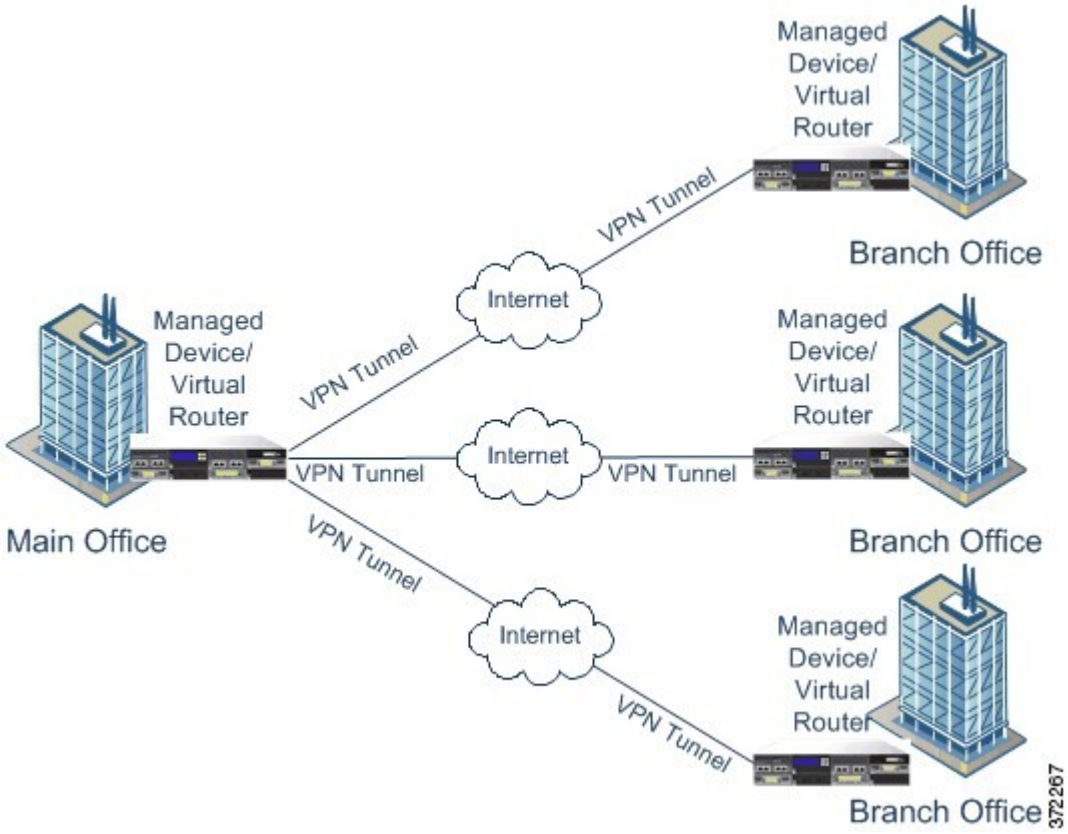
A hub and spoke VPN topology is a network architecture that

- connects a central endpoint (hub node) with multiple remote endpoints (spoke nodes)
- establishes each connection between the hub node and an individual spoke endpoint as a separate VPN tunnel, and
- enables hosts behind any of the spoke nodes to communicate with each other through the hub node.

The hub and spoke topology commonly represent a VPN that connects an organization's main and branch office locations using secure connections over the Internet or other third-party network. These deployments provide all employees with controlled access to the organization's network. Typically, the hub node is located at the main office. Spoke nodes are located at branch offices and start most of the traffic.

This diagram displays a typical hub and spoke VPN topology.

Figure 393: Hub and spoke VPN topology diagram



Full mesh VPN topology

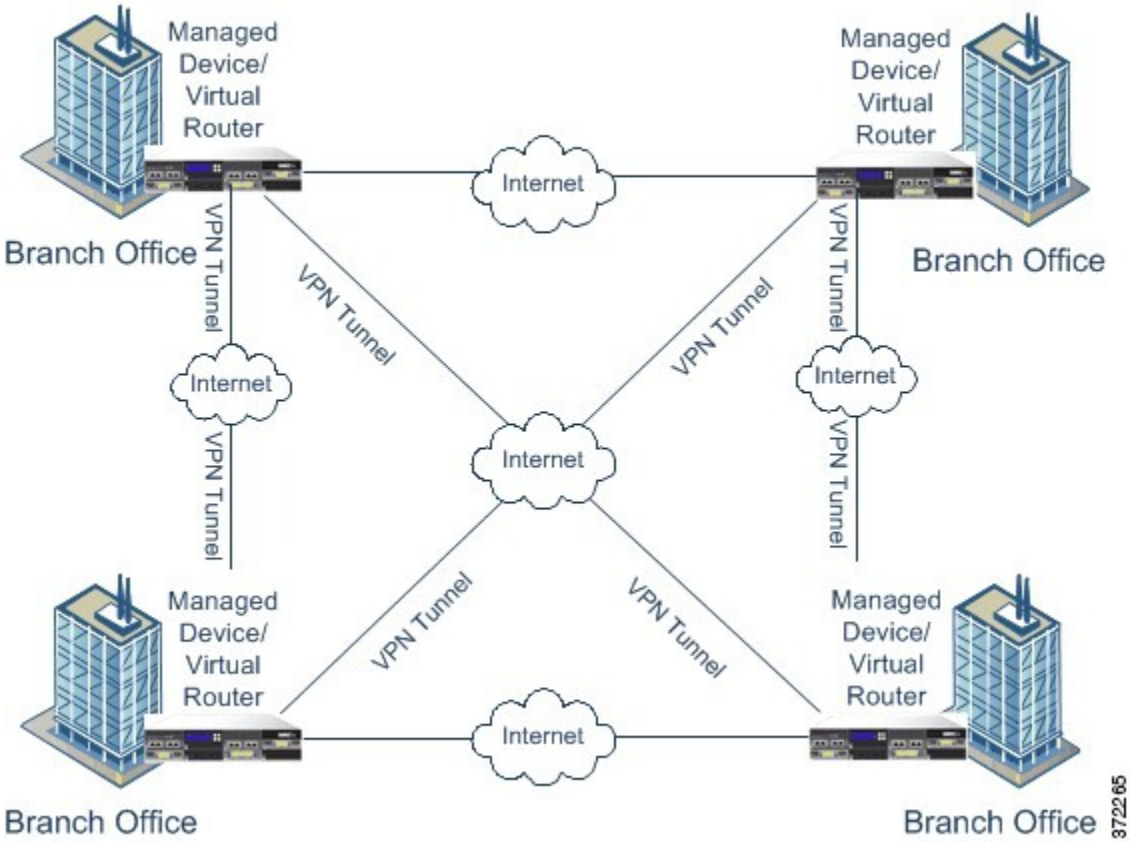
A full mesh VPN topology is a network configuration that

- allows all endpoints to communicate with every other endpoint by an individual VPN tunnel
- offers redundancy so that when one endpoint fails, the remaining endpoints can still communicate with each other, and
- commonly represents a VPN that connects a group of decentralized branch office locations.

The number of VPN-enabled managed devices you deploy in this configuration depends on the level of redundancy you require.

This diagram displays a typical full mesh VPN topology.

Figure 394: Full mesh VPN topology



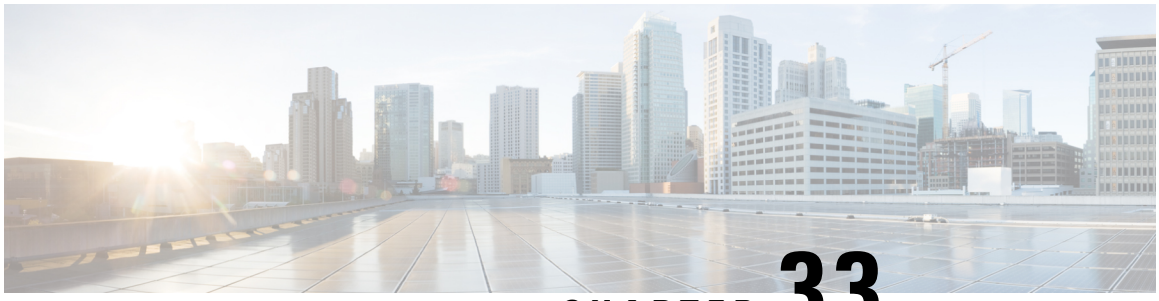
Implicit topologies

Implicit topologies are complex VPN network configurations that

- combine elements from the three main VPN topologies (full mesh, hub-and-spoke, and point-to-point)
- create more advanced network architectures than individual topology types, and
- provide customized connectivity solutions for specific network requirements.

Types of implicit topologies

- **Partial mesh**: A network where some devices use a full mesh topology, while others form either hub-and-spoke or point-to-point connections with some fully meshed devices. The partial mesh does not offer the redundancy found in a full mesh but costs less to implement. Peripheral networks use partial mesh topologies to connect to a fully meshed backbone.
- **Tiered hub-and-spoke**: A network of hub-and-spoke topologies where devices act as a hub in some topologies and as a spoke in others. Spoke groups can send traffic to their closest hub.
- **Joined hub-and-spoke**: A combination of two topologies (hub-and-spoke, point-to-point, or full mesh) that connect to form a point-to-point tunnel. For example, a joined hub-and-spoke topology could comprise two hub-and-spoke topologies, with the hubs acting as peer devices in a point-to-point topology.



CHAPTER 33

Site-to-Site VPN

- Site-to-site VPN, on page 1345
- Types of site-to-site VPN topologies, on page 1348
- License requirements for site-to-site VPN, on page 1348
- Prerequisites for site-to-site VPN, on page 1349
- Manage site-to-site VPNs, on page 1349
- Configure a policy-based site-to-site VPN, on page 1351
- Configure virtual tunnel interfaces, on page 1364
- Deploy a SASE tunnel on Umbrella, on page 1388
- Monitor site-to-site topologies, on page 1395
- History for site-to-site VPN, on page 1400

Site-to-site VPN

A site-to-site VPN is a secure, encrypted VPN tunnel between two networks in different geographic locations. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. You can create site-to-site IPsec connections between managed devices, and between managed devices and other Cisco or third-party peers.

Site-to-site VPN features

Secure Firewall Threat Defense site-to-site VPN supports these features:

- IPsec IKEv1 & IKEv2 protocols.
- Certificates and automatic or manual preshared keys for authentication.
- IPv4 & IPv6 addresses. All combinations of inside and outside are supported.
- Static and dynamic interfaces.
- HA environments for both Firewall Management Center and Firewall Threat Defense.
- VPN alerts when the tunnel goes down and tunnel statistics.
- IKEv1 and IKEv2 back-up peer configuration for point-to-point extranet and hub-and-spoke VPNs.
- Extranet device as hub in 'Hub and Spokes' deployments.

- Dynamic IP address for a managed endpoint pairing with extranet device in 'Point to Point' deployments and for extranet device as an endpoint.

VPN topologies

VPN topology configuration requires specifying a unique name, a topology type, IKE version selection, and authentication method. The Secure Firewall Management Center configures site-to-site VPNs on Firewall Threat Defense devices only.

You can select from three types of topologies, containing one or more VPN tunnels:

- Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.
- Hub and Spoke deployments establish a group of VPN tunnels connecting a hub endpoint to a group of spoke nodes.
- Full Mesh deployments establish a group of VPN tunnels among a set of endpoints.

In the Secure Firewall Management Center, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

For authentication of VPN connections, configure a preshared key in the topology, or a trustpoint on each device. Preshared keys allow for a secret key, used during the IKE authentication phase, to be shared between two peers. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

IPsec and IKE

In the Secure Firewall Management Center, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication

For authentication of VPN connections, configure a preshared key in the topology, or a trustpoint on each device. Preshared keys allow for a secret key, used during the IKE authentication phase, to be shared between two peers. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

Extranet Devices

Each topology type can include extranet devices, devices that you don't manage in Firewall Management Center. These include:

- Cisco devices that Secure Firewall Management Center supports, but for which your organization isn't responsible. Such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.
- Non-Cisco devices. You can't use Secure Firewall Management Center to create and deploy configurations to non-Cisco devices.

Add non-Cisco devices, or Cisco devices not managed by the Secure Firewall Management Center, to a VPN topology as "Extranet" devices. Also specify the IP address of each remote device.

Guidelines for configuring site-to-site VPN in Secure Firewall Threat Defense devices

General guidelines

- Site-to-site VPN supports ECMP zone interfaces.
- Configure all nodes in a topology with either crypto ACL or a protected network. You cannot configure a topology with crypto ACL on one node and protected network on another.
- Configure a VPN connection across domains by using an extranet peer for the endpoint not in the current domain.
- You can backup Firewall Threat Defense VPNs using the Firewall Management Center backup.
- Configure unique local IKE identity for all tunnels across all your VPN topologies.
- Ensure that IKE ports 500 and 4500 are not already in use and that no active PAT translations exist on those ports before configuring a site-to-site VPN. Configuring a site-to-site VPN on ports that are already in use will cause the service to fail to start.
- When configuring a site-to-site VPN between two devices managed by the same Firewall Management Center, do not configure the devices as backup peers. Instead, configure one of the peer devices in the topology as an extranet device.
- If a spoke is part of multiple topologies with the same hub, for the Local Tunnel (IKE) Identity, we recommend that you use Key ID instead of an IP address.

  If the spoke uses an IP address as its local identity, the hub creates only one tunnel group. The spoke is then mapped to a specific virtual template interface, so the connection works with only one topology.

Limitations for configuring site-to-site VPN in Threat Defense devices

General limitations

- IKEv1 does not support CC/UCAPL-compliant devices. IKEv2 is recommended for these devices.
- VPN does not support network objects with a 'range' option.
- Firewall Threat Defense VPNs do not support PDF export and policy comparison.
- Tunnel status is not updated realtime, but at an interval of five minutes in the Firewall Management Center.
- You cannot use the double quote character (") in pre-shared keys, replace it if already in use.

Crypto ACL limitations

- Firewall Management Center supports only point-to-point VPN with crypto ACL and does not support tunnel health events.

- Firewall Management Center does not verify the device interface address verification for transport mode when you select a crypto ACL.
- There is no support for automatic mirror ACE generation. Mirror ACE generation for the peer is a manual process on either side.

Topology management limitations

- You cannot move a VPN topology between domains.
- There is no per-tunnel or per-device edit option for Firewall Threat Defense VPNs, you can edit only the whole topology.

Types of site-to-site VPN topologies

This table provides an overview of the different site-to-site VPN topology options available for secure network connectivity configuration.

Site-to-Site VPN Topology	Description	More Information
Route-Based VPN	Configure secure traffic dynamically between peers in a network based on routing over Virtual Tunnel Interfaces (VTIs).	Create a route-based site-to-site VPN, on page 1373
Policy-Based VPN	Configure secure traffic between peers in a network based on a static policy using protected networks.	Configure a policy-based site-to-site VPN, on page 1351
SASE Topology	Configure an IPsec IKEv2 tunnel from a Firewall Threat Defense device to an Umbrella Secure Internet Gateway (SIG). This tunnel forwards all internet-bound traffic to Umbrella SIG for inspection and filtering.	Configure a SASE tunnel for Umbrella, on page 1392

License requirements for site-to-site VPN

This topic lists the license requirements for setting up various types of site-to-site VPN connections.

License requirements for policy-based and route-based VPN

With the Essentials license, you can set up policy-based and route-based VPNs on your Firewall Threat Defense devices.

Depending on whether export-controlled functionality is enabled in your Smart License account, Firewall Management Center determines whether to allow or block the usage of strong crypto on devices. To verify if export-controlled functionality is enabled for your Smart License account, choose **System** (⚙) > **Licenses** > **Smart Licenses**.

Note If you use an evaluation license, or if you have not enabled the export-controlled functionality, you cannot use strong encryption for your VPN connections.

License requirements for deploying a SASE tunnel on Umbrella

To deploy SASE tunnels on Umbrella from Firewall Management Center, you must enable your Smart License account with the export-controlled functionality. If this functionality is not enabled, you can only create a SASE topology, you cannot deploy tunnels on Umbrella.

Prerequisites for site-to-site VPN

Supported interfaces

Topology Type	Interface Type

Policy-Based	• Physical interfaces
	  • Non-management
	  • Interface Mode must be either Routed or None
	• Subinterface interfaces
	• Redundant interfaces
	• Etherchannel interfaces
	• VLAN interfaces

Route-Based	Static Virtual Tunnel Interfaces

Note The maximum number of supported security associations (SA) depends on the maximum VPN peers for your platform. For more information about maximum VPN peers, refer the data sheet of the Secure Firewall Threat Defense device.

General prerequisites

- You must have administrator privileges.
- You must be in a leaf domain to perform the site-to-site VPN configurations.

Manage site-to-site VPNs

You can view, create, modify, and deploy site-to-site VPN configurations and manage their deployment status.

The **Site-to-Site VPN** page provides a snapshot of site-to-site VPN tunnels. You can view the status of the tunnels and filter the tunnels based on the device, topology, or tunnel type. The page lists 20 topologies per page and you can navigate between pages to view more topology details. You can click individual VPN topologies to expand and view details of the endpoints.

Before you begin

For certificate authentication of your site-to-site VPNs, you must prepare the devices by allocating trustpoints as described in Certificates, on page 2481.

Procedure

Select **Devices** > **VPN** > **Site to Site** to manage your Firewall Threat Defense site-to-site VPN configurations and deployments.

The page lists the site-to-site VPNs topologies and indicates the status of tunnels using color codes:

- Active (Green)–There is an active IPsec Tunnel.
- Unknown (Amber)–No tunnel establishment event has been received from the device yet.
- Down (Red)–There are no active IPsec tunnels.
- Deployment Pending–Topology has not been deployed on the device yet.

Choose one of these actions:

- **Refresh**—View the updated status of the VPNs.
- **Add**—Create new policy based or route-based Site to Site VPNs.
- **Edit**—Modify the settings of an existing VPN topology.

Note You cannot edit the topology type after you initially save it. To change the topology type, delete the topology and create a new one.

Two users shouldn't edit the same topology simultaneously; however, the web interface doesn't prevent simultaneous editing.

- **Delete**—To delete a VPN deployment, click **Delete** ( ).
- Deploy—Choose **Deploy** > **Deploy**; see Deploy configuration changes, on page 135.

Note Some VPN settings are validated only during deployment. Be sure to verify that your deployment was successful.

Configure a policy-based site-to-site VPN

Configure a policy-based site-to-site VPN to establish secure communication channels between network endpoints using crypto maps and specified network topologies.

Procedure

Step 1 Choose **Devices > Site To Site**. Then click **+ Site To Site VPN**, or edit a listed VPN topology.

Step 2 Enter a unique **Topology Name** and click the **Policy Based (Crypto Map)** radio button, and choose the **Network Topology** for this VPN.

Step 3 Choose the IKE versions to use during IKE negotiations. Check the **IKEv1** or **IKEv2** check box.

Default is IKEv2. Select either or both options as appropriate; select IKEv1 if any device in the topology doesn't support IKEv2.

You can also configure a backup peer for point-to-point extranet VPNs. For more information, see Firewall Threat Defense VPN endpoint options, on page 1352.

Step 4 Required: Add Endpoints for this VPN deployment by clicking **Add** (+) for each node in the topology.

Configure each endpoint field as described in Firewall Threat Defense VPN endpoint options, on page 1352.

- For Point to point, configure **Node A** and **Node B**.
- For Hub and Spoke, configure a **Hub Node** and **Spoke Nodes**
- For Full Mesh, configure multiple **Nodes**

Step 5 (Optional) Specify non-default IKE options for this deployment as described in Firewall Threat Defense VPN IKE options, on page 1356

Step 6 (Optional) Specify non-default IPsec options for this deployment as described in Firewall Threat Defense VPN IPsec options, on page 1358

Step 7 (Optional) Specify non-default Advanced options for this deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 1360 and click **Save**.

The policy-based site-to-site VPN is configured with the specified endpoints, IKE settings, and topology options.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

Note Some VPN settings are validated only during deployment. Be sure to verify that your deployment was successful.

If you get an alert that your VPN tunnel is inactive even when the VPN session is up, follow the VPN troubleshooting instructions to verify and ensure that your VPN is active.

Firewall Threat Defense VPN endpoint options

Devices > Site To Site. Then click **+ Site To Site VPN**, or edit a listed VPN topology. Click the **Endpoints** tab.

Fields

Device

Choose an endpoint node for your deployment:

- A Firewall Threat Defense device managed by this Firewall Management Center
- A Firewall Threat Defense high availability container managed by this Firewall Management Center
- An **Extranet** device, any device (Cisco or third party) not managed by this Firewall Management Center .

Device Name

For extranet devices only, provide a name for this device. We recommend naming it such that it is identifiable as an unmanaged device.

Interface

If you chose a managed device as your endpoint, choose an interface on that managed device.

For 'Point to Point' deployments, you can also configure an endpoint with dynamic interface. An endpoint with a dynamic interface can pair only with an extranet device and can’t pair with an endpoint, which has a managed device.

You can configure device interfaces at **Devices** > **Device Management Add/Edit device** > **Interfaces**.

IP Address

- If you choose an extranet device, a device not managed by the Firewall Management Center, specify an IP address for the endpoint.

  For an extranet device, select **Static** and specify an IP address or select **Dynamic** to allow dynamic extranet devices.

- If you chose a managed device as an endpoint, choose a single IPv4 address or multiple IPv6 addresses from the drop-down list. These IP addresses are already assigned to this interface on the managed device.
- All endpoints in a topology must have the same IP addressing scheme. IPv4 tunnels can carry IPv6 traffic and vice versa. The **Protected Networks** define which addressing scheme the tunneled traffic uses.
- If the managed device is a high-availability container, choose from a list of interfaces.

This IP is Private

Check the check box if the endpoint resides behind a firewall with network address translation (NAT).

Note Use this option only when the peer is managed by the same Firewall Management Center and don’t use this option if the peer is an extranet device.

Public IP address

If you checked the **This IP is Private** check box, specify a public IP address for the firewall. If the endpoint is a responder, specify this value.

Connection Type

Specify the allowed negotiation as bidirectional, answer-only, or originate-only. Supported combinations for the connection type are:

Table 77: Connection Type Supported Combinations

Remote Node	Central Node
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Certificate Map

Choose a preconfigured certificate map object, or click **Add** (+) to add a certificate map object. The certificate map defines what information is necessary in the received client certificate to be valid for VPN connectivity. See Certificate map objects, on page 2457 for details.

Protected Networks

Caution Hub and Spoke topology—To avoid traffic drop for a dynamic crypto map, ensure that you don't select the protected network *any* for both the endpoints.

If the protected network is configured as *any*, on both the endpoints, the crypto ACL that works upon the tunnel is not generated.

Defines the networks that are protected by this VPN endpoint. Select the networks by selecting the list of Subnet/IP Address that define the networks that are protected by this endpoint. Click **Add** (+) to select from available Network Objects or add new Network Objects. See Create a network object, on page 2388 . Access control lists are generated from the choices made here.

- **Subnet/IP Address (Network)** —VPN endpoints can't have the same IP address and protected networks in a VPN endpoint pair cannot overlap. If protected networks for an endpoint contain IPv4 or IPv6 entries, the other endpoint's protected network must have at least one entry of the same type (IPv4 or IPv6). If it doesn't, the other endpoint's IP address must be of the same type and not overlap with the entries in the protected network. (Use /32 CIDR address blocks for IPv4 and /128 CIDR address blocks for IPv6.) If both of these checks fail, the endpoint pair is invalid.

Note By default, **Reverse Route Injection is enabled** check box is enabled in Firewall Management Center.

Subnet/IP Address (Network) remains the default selection.

When you've selected Protected Networks as *Any* and observe default route traffic being dropped, disable the Reverse Route Injection. Choose **VPN** > **Site to Site** . Edit a VPN and then click **IPsec** > **Enable Reverse Route Injection** . Deploy the configuration changes to remove set reverse-route (Reverse Route Injection) from the crypto map configuration and remove the VPN-advertised reverse route that causes the reverse tunnel traffic to be dropped.

- **Access List (Extended)** —An extended access list provides the capability to control the type of traffic that will be accepted by this endpoint, like GRE or OSPF traffic. Traffic may be restricted either by address or port. Click **Add** (+) to add access control list objects.

Note Access Control List is supported only in the point to point topology.

Enable NAT Traversal

Check this check box to allow seamless communication between the peer Firewall Threat Defense devices when there are NAT devices between these devices. For hub and spoke topologies, this option is available only for the spoke. You can uncheck this check box to disable this feature for an endpoint. This parameter is a per peer setting for an endpoint within a topology.

To view or configure the global NAT Traversal (NAT-T) setting, in the **Add/Edit VPN Topology** dialog box:

1. Click the **Advanced** tab.
2. In the left navigation pane, click **Tunnel** .
3. Under **NAT Settings**, the **Keepalive Messages Traversal** is a global setting that enables NAT-T for all endpoints within a topology.

Exempt VPN traffic from network address translation

Check this check box to exempt the VPN traffic from the Network Address Translation (NAT) rules.

If you do not exempt the VPN traffic from the NAT rules, the traffic gets dropped or is not routed through the VPN tunnel to the remote device. After you enable this option, you can view the NAT exemptions for the device in the NAT policy page (**Devices** > **NAT** , and click **NAT Exemptions**).

Inside interfaces directly connected to the internal network

Specify the security zone or interface group for the inside interface(s) where the protected networks reside. By default, the inside interface is any.

Click + to configure one or more interfaces from a security zone or an interface group that can map to one or more inside interfaces. Ensure that the interface type of the security zone or an interface group is Routed.

Advanced Settings

Enable Dynamic Reverse Route Injection —Reverse Route Injection (RRI) enables routes to be automatically inserted into the routing process, for the networks and hosts protected by a remote tunnel endpoint. Dynamic RRI routes are created only upon the successful establishment of IPsec security associations (SA's).

Note

- Dynamic RRI is supported only on IKEv2, and not supported on IKEv1 or IKEv1 + IKEv2.
- Dynamic RRI isn't supported on originate-only peer, Full Mesh topology, and Extranet peer.
- In Point-to-Point, only one peer can have dynamic RRI enabled.
- Between Hub and Spoke, only one of the endpoints can have dynamic RRI enabled.
- Dynamic RRI cannot be combined with a dynamic crypto map.

Send Local Identity to Peers —Select this option to send local identity information to the peer device. Select one of the following **Local Identity Configuration** from the list and configure the local identity:

- **IP address**—Use the IP address of the interface for the identity.
- **Auto**—Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID**—Specify the email ID to use for the identity. The email address can be up to 127 characters.
- **Hostname**—Use the fully qualified hostname.
- **Key ID**—Specify the key-id to use for the identity. The key ID must be fewer than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identity allows Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to the Cisco Umbrella Secure Internet Gateway (SIG).

For information about configuring a unique tunnel ID on Umbrella, see **Cisco Umbrella SIG User Guide**.

VPN Filter—Select an extended access list from the list or click **Add** to create a new extended access list object to filter the site-to-site VPN traffic.

The VPN filter provides more security and filters site-to-site VPN data using an extended access list. The extended access list object selected for the VPN filter lets you filter pre-encrypted traffic before entering the VPN tunnel and decrypted traffic that exits a VPN tunnel. The **sysopt permit-vpn** option, when enabled, would bypass the access control policy rules for the traffic coming from the VPN tunnel. When the **sysopt permit-vpn** option is enabled, the VPN filter helps in identifying and filtering the site-to-site VPN traffic.

Note The VPN filter is supported only on point to point, and hub and spoke topologies. It isn't supported on mesh topology.

For hub and spoke topology, you can choose to override the hub VPN filter on the spoke endpoints in case a different VPN filter needs to enabled on a specific tunnel.

Select the **Override VPN Filter on the Hub** option to override the hub VPN filter on the spokes. Select the **Remote VPN Filter** extended access list object or create an access list to override.

Note For an extranet device as a spoke, only the **Override VPN filter on the Hub** option is available.

For more information about sysopt permit-VPN, see Firewall Threat Defense advanced site-to-site VPN tunnel options , on page 1362 .

Firewall Threat Defense VPN IKE options

For the versions of IKE you have chosen for this topology, specify the **IKEv1/IKEv2 Settings**.

Note Settings in this dialog apply to the entire topology, all tunnels, and all managed devices.

Devices > Site To Site. Then click **+ Site To Site VPN**, or edit a listed VPN topology. Click the **IKE** tab.

Fields

Policy

Choose the required IKEv1 or IKEv2 policy objects from the predefined list or create new objects to use. You can choose multiple IKEv1 and IKEv2 policies. IKEv1 and IKEv2 support a maximum of 20 IKE policies, each with a different set of values. Assign a unique priority to each policy that you create. The lower the priority number, the higher the priority.
We recommend that you do NOT use values such as 10, 20 and so on because the default IKEv2 policy for remote access VPN can have these values as its priority value. Before deployment, verify that the priority values of the IKE policies (site-to-site and remote access VPN) do NOT conflict.

Note When upgrading from Version 7.4.x or earlier—where the IKEv2 policy priority field is optional—to Version 7.6.x or later—where it is mandatory—leaving the priority field blank may lead to IKEv2 policy configuration issues and affect network traffic. To avoid these problems, ensure that a priority value is set for all IKEv2 policies either before or after the upgrade.

For details, see IKE policies, on page 2470

Authentication Type

Site-to-site VPN supports two authentication methods, pre-shared key and certificate. For an explanation of the two methods, see Decide VPN authentication methods, on page 1336.

Note In a VPN topology that supports IKEv1, the **Authentication Method** specified in the chosen IKEv1 Policy object becomes the default in the IKEv1 **Authentication Type** setting. These values must match, otherwise, your configuration will error.

- **Pre-shared Automatic Key**—The Firewall Management Center automatically defines the pre-shared key for this VPN. Specify the **Pre-shared Key Length**, the number of characters in the key. The range is 1 to 27.

  The character " (double quote) isn't supported as part of pre-shared keys. If you've used " in a pre-shared key, ensure that you change the character after you upgrade to Secure Firewall Threat Defense 6.30 or higher.

- **Pre-shared Manual Key**—Manually assign the pre-shared key for this VPN. Specify the **Key** and then reenter the same to **Confirm Key**.

  When you choose this option for IKEv2, the **Enforce hex-based pre-shared key only** check box appears, check if desired. If enforced, you must enter a valid hex value for the key, an even number of 2-256 characters, using numerals 0-9, or A-F.

- **Certificate**—When you use certificates as the authentication method for VPN connections, peers obtain digital certificates from a CA server in your PKI infrastructure, and trade them to authenticate each other.

  In the **Certificate** field, select a preconfigured certificate enrollment object. This enrollment object generates a trustpoint with the same name on the managed device. The certificate enrollment object should be associated with and installed on the device, post which the enrollment process is complete, and then a trustpoint is created.

  A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

  Before you select this option, note these requirements:

  - Ensure you've enrolled a certificate enrollment object on all the endpoints in the topology—A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. Certificate Enrollment Objects are used to enroll your managed devices into your PKI infrastructure, and create trustpoints (CA objects) on devices that support VPN connections. For instructions on creating a certificate enrollment object, see Add certificate enrollment objects, on page 2402, and for instructions on enrolling the object on the endpoints see one of these as applicable:
    - Install a certificate using self-signed enrollment, on page 2486
    - Install a certificate using EST enrollment, on page 2487
    - Install a certificate using SCEP enrollment, on page 2487
    - Install a certificate using manual enrollment, on page 2488
    - Install a certificate using a PKCS12 file, on page 2489



Note For a site-to-site VPN topology, ensure that the same certificate enrollment object is enrolled in all the endpoints in the topology. For further details, see the table below.

- Refer to this table to understand the enrollment requirement for different scenarios. Some of the scenarios require you to override the certificate enrollment object for specific devices. See Manage object overrides, on page 2343 to understand how to override objects.

Certificate Enrollment Types	Device identity certificate for all endpoints is from the same CA		Device identity certificate for all endpoints is from different CAs
	Device-specific parameters are NOT specified in the certificate enrollment object	Device-specific parameters are specified in the certificate enrollment object	
Manual	No override required	Override required	Override required
EST	No override required	Override required	Override required
SCEP	No override required	Override required	Override required
PKCS	Override required	Override required	Override required
Self-signed	NOT applicable	NOT applicable	NOT applicable

- Understand the VPN certificate limitations mentioned in Secure Firewall Threat Defense VPN certificate guidelines and limitations, on page 2481.

Note If you use a Windows Certificate Authority (CA), the default application policies extension is **IP security IKE intermediate**. If you use this default setting, you must select the **Ignore IPsec Key Usage** option in the Advanced Settings section on the **Key** tab in the **PKI Certificate Enrollment** dialog box for the object you select. Otherwise, the endpoints can't complete the site-to-site VPN connection.

Firewall Threat Defense VPN IPsec options

Configure the basic parameters for a point-to-point topology in a route-based VPN as described in Configure Endpoints for a Point to Point Topology and click the **IPsec** tab.

Note Settings in this dialog apply to the entire topology, all tunnels, and all managed devices.

Crypto-Map Type

A crypto map combines all the components required to set up IPsec security associations (SA). When two peers try to establish an SA, they must each have at least one compatible crypto map entry. IPsec security negotiation uses the proposals defined in the crypto map entry to protect the data flows specified by that crypto map's IPsec rules. Choose static or dynamic for this deployment's crypto-map:

- **Static**—Use a static crypto map in a point-to-point or full mesh VPN topology.

- **Dynamic**—Dynamic crypto-maps essentially create a crypto map entry without all the parameters configured. The missing parameters are later dynamically configured (as the result of an IPsec negotiation) to match a remote peer's requirements.

  Dynamic crypto map policies are applicable to both hub-and-spoke and point-to-point VPN topologies. To apply these policies, specify a dynamic IP address for one of the peers in the topology and ensure that the dynamic crypto-map is enabled on this topology. In a full mesh VPN topology, you can apply only static crypto map policies.

IKEv2 Mode

For IPsec IKEv2 only, specify the encapsulation mode for applying ESP encryption and authentication to the tunnel. This determines what part of the original IP packet has ESP applied.

- **Tunnel mode**—(default) Encapsulation mode is set to tunnel mode. Tunnel mode applies ESP encryption and authentication to the entire original IP packet (IP header and data), hiding the ultimate source and destination addresses and becoming the payload in a new IP packet.

  The major advantage of tunnel mode is that you don't need to modify the end systems to receive the benefits of IPsec. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it onto the destination system. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

- **Transport preferred**—Encapsulation mode is set to transport mode with an option to fall back to tunnel mode if the peer doesn't support it. In transport mode only the IP payload is encrypted, and the original IP headers are left intact. Therefore, the admin must select a protected network that matches the VPN interface IP address.

  This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the layer 4 header is encrypted, which limits examination of the packet.

- **Transport required**— Encapsulation mode is set to transport mode only, falling back to tunnel mode is allowed. If the endpoints can't successfully negotiate transport mode, due to one endpoint not supporting it, the VPN connection is not made.

Proposals

Click **Edit** ( ) to specify the proposals for your chosen IKEv1 or IKEv2 method. Select from the available **IKEv1 IPsec Proposals** or **IKEv2 IPsec Proposals** objects, or create and then select a new one. See Configure an IKEv1 IPsec proposal object, on page 2469 and Configure an IKEv2 IPsec proposal object, on page 2470 for details.

Enable Security Association (SA) Strength Enforcement

Enabling this option ensures that the encryption algorithm used by the child IPsec SA isn't stronger (in terms of the number of bits in the key) than the parent IKE SA.

Enable Reverse Route Injection

Reverse Route Injection (RRI) enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint.

Enable Perfect Forward Secrecy

Whether to use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the Modulus Group list.

Modulus Group

The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For a full explanation of the options, see Decide which Diffie-Hellman modulus group to use, on page 1336.

Lifetime Duration

The number of seconds a security association exists before expiring. The default is 28,800 seconds.

Lifetime Size

The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes. Infinite data isn't allowed.

ESPv3 Settings

Validate incoming ICMP error messages

Choose whether to validate ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.

Enable 'Do Not Fragment' Policy

Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header.

Policy

- Copy DF bit—Maintains the DF bit.
- Clear DF bit—Ignores the DF bit.
- Set DF bit—Sets and uses the DF bit.

Enable Traffic Flow Confidentiality (TFC) Packets

Enable dummy TFC packets that mask the traffic profile which traverses the tunnel. Use the **Burst**, **Payload Size**, and **Timeout** parameters to generate random length packets at random intervals across the specified SA.

Note You can enable dummy Traffic Flow Confidentiality (TFC) packets at random lengths and intervals on an IPsec security association (SA). You must have an IKEv2 IPsec proposal set before enabling TFC.

Enabling TFC packets prevents the VPN tunnel from being idle. Thus the VPN idle timeout configured in the group policy doesn't work as expected when you enable the TFC packets.

Firewall Threat Defense advanced site-to-site VPN deployment options

The sections describe the advanced options you can specify in your site-to-site VPN deployment. These settings apply to the entire topology, all tunnels, and all managed devices.

Firewall Threat Defense VPN advanced IKE options

Advanced > IKE > ISAKAMP settings

IKE Keepalive

Enable or disables IKE Keepalives. You can set this option to EnableInfinite so that the device never starts the keepalive monitoring itself.

Threshold
Specifies the IKE keep alive confidence interval. This interval is the number of seconds allowing a peer to idle before beginning keepalive monitoring. The minimum and default interval is 10 seconds; the maximum interval is 3600 seconds.

Retry Interval
Specifies number of seconds to wait between IKE keep alive retries. The default is 2 seconds, the maximum is 10 seconds.

Identity Sent to Peers:
Choose the identity that the peers will use to identify themselves during IKE negotiations:

- **autoOrDN**(default)—Determines IKE negotiation by connection type: IP address for preshared key, or Cert DN for certificate authentication (not supported).
- **ipAddress**—Uses the IP addresses of the hosts exchanging ISAKMP identity information.
- **hostname**—Uses the fully qualified domain name of the hosts exchanging ISAKMP identity information. This name comprises the hostname and the domain name.

Note Enable or disable this option for all your VPN connections.

Peer Identity Validation
During IKE tunnel establishment, the peer provides its identity: either an IP address, a Fully Qualified Domain Name (FQDN), or a Distinguished Name (DN). It also presents a certificate, which contains none, some, or all of these fields.

If IKE peer identity validation is enabled, the Firewall Threat Defense compares the peer's identity to the respective field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the Firewall Threat Defense establishes the tunnel. If the information does not match, the tunnel is not established.

- **Do not check**—Firewall Threat Defense does not validate the peer identity.
- **Required**—Firewall Threat Defense validates the peer identity.
- **If supported by cert**—Firewall Threat Defense validates the peer identity only if the peer provides a certificate.

Enable Aggressive Mode
Select this negotiation method for exchanging key information if the IP address isn't known and DNS resolution might not be available on the devices. Negotiation is based on hostname and domain name.

Enable Notification on Tunnel Disconnect
Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. This notification is disabled by default.

Advanced > IKE > IKEv2 security association (SA) settings

More session controls are available for IKE v2 that limit the number of open SAs. By default, there's no limit to the number of open SAs.

Cookie Challenge
Whether to send cookie challenges to peer devices in response to SA initiate packets, which can help thwart denial of service (DoS) attacks. The default is to use cookie challenges when 50% of the available SAs are in negotiation. Select one of these options:

- Custom
- Never (default)
- Always

Threshold to Challenge Incoming Cookies
The percentage of the total allowed SAs that are in-negotiation. This triggers cookie challenges for any future SA negotiations. The range is zero to 100%.

Number of SAs Allowed in Negotiation
Limits the maximum number of SAs that can be in negotiation at any time. If used with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check.

Maximum number of SAs Allowed
Limits the number of allowed IKEv2 connections. Default is unlimited.

Enable Notification on Tunnel Disconnect
Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA doesn't match the traffic selectors for that SA. Sending this notification is disabled by default.

Firewall Threat Defense VPN advanced IPsec options

Advanced > IPsec > IPsec Settings

The advanced IPsec settings include these configuration options:

- **Enable Fragmentation Before Encryption**: This option lets traffic travel across NAT devices that don't support IP fragmentation. It doesn't impede the operation of NAT devices that do support IP fragmentation.
- **Path Maximum Transmission Unit Aging**: Check to enable Path Maximum Transmission Unit (PMTU) Aging, the interval to reset the PMTU of a Security Association (SA).
- **Value Reset Interval**: Enter the number of minutes at which the PMTU value of an SA is reset to its original value. The range is 10 to 30 minutes, default is unlimited.

Firewall Threat Defense advanced site-to-site VPN tunnel options

This topic lists the advanced site-to-site VPN tunnel options.

Navigation path

Devices > Site To Site, then click **+ Site To Site VPN**, or edit a listed VPN Topology. Click the **Advanced** tab, and select **Tunnel** in the navigation pane.

Tunnel options

Only available for Hub and Spoke, and Full Mesh topologies. This section doesn't appear for Point to Point configurations.

- **Enable Spoke to Spoke Connectivity through Hub**—Disabled by default. Choosing this field enables the devices on each end of the spokes to extend their connection through the hub node to the other device.

NAT settings

- **Keepalive Messages Traversal**—Enabled by default. This parameter is a global setting that enables NAT-T for all endpoints within a topology. Check this check box to enable keepalive messages for NAT traversal. NAT traversal keepalive is used for the transmission of keepalive messages when there's a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow.

  NAT traversal allows seamless communication between the peer Firewall Threat Defense devices when there are NAT devices between these devices. For hub and spoke topologies, this option is available only for the spoke.

  If you select this option, configure the **Interval**, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The value can be from 5 to 3600 seconds. The default is 20 seconds. You can disable this feature for an endpoint in a topology when you add it using the VPN wizard (**Enable NAT Traversal** check box in the **Add Endpoint** dialog box).

Access control for VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)—By default, the Firewall Threat Defense applies access control policy inspection on the decrypted traffic. Enable this option to bypass the ACL inspection. The Firewall Threat Defense still applies the VPN Filter ACL and authorization ACL downloaded from the AAA server to the VPN traffic.

Enable or disable the option for all your VPN connections. If you disable this option, ensure that the traffic is allowed by the access control policy or prefilter policy.



Note For route-based VPNs, **sysopt permit-vpn** does not work. You must always create access control rules to allow route-based VPN traffic.

Certificate map settings

- **Use the certificate map configured in the Endpoints to determine the tunnel**—If this option is enabled (checked), the tunnel is determined by matching the contents of the received certificate to the certificate map objects configured in the endpoint nodes.
- **Use the certificate OU field to determine the tunnel**—Indicates that if a node isn't determined based on the configured mapping (the above option) if selected, then use the value of the organizational unit (OU) in the subject distinguished name (DN) of the received certificate to determine the tunnel.

- **Use the IKE identity to determine the tunnel**—Indicates that if a node isn't determined based on a rule matching or taken from the OU (the above options) if selected, then the certificate-based IKE sessions are mapped to a tunnel based on the content of the phase1 IKE ID.
- **Use the peer IP address to determine the tunnel**—Indicates that if a tunnel isn't determined based on a rule matching or taken from the OU or IKE ID methods (the above options) if selected, then use the established peer IP address.

Configure virtual tunnel interfaces

Firewall Management Center supports a routable logical interface called the Virtual Tunnel Interface (VTI).

Virtual tunnel interfaces

A virtual tunnel interface is a routable logical interface that

- does not require static mapping of IPsec sessions to a physical interface
- associates the IPsec tunnel endpoint with a virtual interface, and
- supports static and dynamic routing policies.

Virtual tunnel interface capabilities

Firewall Management Center supports VTIs as an alternative to policy-based VPN. VTIs support route-based VPN with IPsec profiles attached to the end of each tunnel. VTIs use static or dynamic routes. The device encrypts or decrypts the traffic from or to the tunnel interface and forwards it according to the routing table. Deployments become easier, and having VTI which supports route-based VPN with dynamic routing protocol also satisfies many requirements of a virtual private cloud. Firewall Management Center enables you to easily migrate from crypto-map based VPN configuration to VTI-based VPN.

You can configure route-based VPN with static or dynamic VTI using the site-to-site VPN wizard. Traffic is encrypted using static route, BGP, OSPFv2/v3, or EIGRP.

You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic control over the VTI tunnel.

There are two types of VTI interfaces: static VTI and dynamic VTI.

You can create VTI-based VPNs between:

- Two Firewall Threat Defense devices.
- A Firewall Threat Defense and public cloud.
- One Firewall Threat Defense and another Firewall Threat Defense with service provider redundancy.
- A Firewall Threat Defense and any other device with VTI interfaces.
- A Firewall Threat Defense and another device with policy-based VPN configuration.

For more information, see Static VTI, on page 1365 and Dynamic VTI, on page 1366.

Static VTI

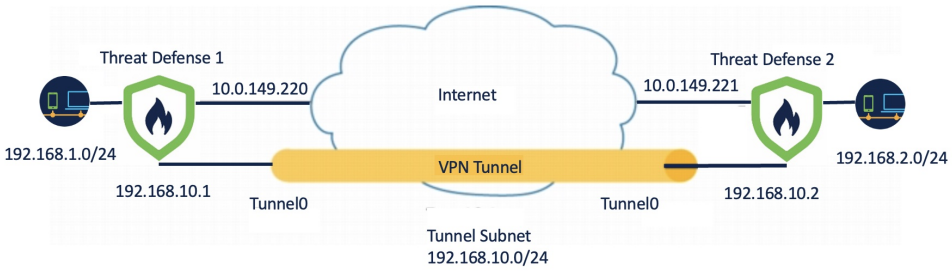
A static VTI is a virtual tunnel interface that

- uses tunnel interfaces to create a tunnel that is always-on between two sites
- requires defining a physical interface as a tunnel source, and
- supports a maximum of 1024 VTIs per device.

To create a static VTI interface in the Management Center, see Add a VTI interface, on page 1371.

The figure shows a VPN topology using static VTIs.

Figure 395: Static VTI VPN topology



On Threat Defense 1:

- Static VTI IP address is 192.168.10.1
- Tunnel source is 10.0.149.220
- Tunnel destination is 10.0.149.221

On Threat Defense 2:

- Static VTI IP address is 192.168.10.2
- Tunnel source is 10.0.149.221
- Tunnel destination is 10.0.149.220

Benefits of SVTI

Static VTI provides these benefits:

- Minimizes and simplifies configuration.

  You do not have to track all remote subnets for a crypto map access list, and configure complex access lists or crypto maps.

- Provides a routable interface.

  Supports IP routing protocols such as BGP, EIGRP, and OSPFv2/v3, and static routes.

- Supports backup VPN tunnels
- Supports load balancing using ECMP.

- Supports virtual routers.
- Provides differential access control for VPN traffic.

  You can configure a VTI with a security zone and use it in an AC policy. This configuration:

  - Allows you to classify and differentiate VPN traffic from clear-text traffic and permit VPN traffic selectively.
  - Provides differential access-control for VPN traffic across different VPN tunnels.

Dynamic VTI

A dynamic VTI is a VPN interface that

- uses a virtual template for dynamic instantiation and management of IPsec interfaces
- dynamically generates a unique virtual access interface for each VPN session
- supports multiple IPsec security associations and accepts multiple IPsec selectors proposed by the spoke.

Benefits of dynamic VTI

- Minimizes and simplifies configuration.

  You do not have to configure complex access lists or crypto maps.
- Simplifies management.
  - Easily manage peer configuration for large enterprise hub and spoke deployments.
  - Use only one dynamic VTI for multiple spokes, instead of configuring one static VTI per spoke.
- Provides a routable interface.

  Supports IP routing protocols such as BGP, EIGRP, and OSPFv2/v3.
- Simplifies scaling

  Addition of new spokes does not require any additional VPN configuration on the hub. You may need to update NAT and routing configurations depending upon the setup.
- Support for backup VPN tunnels.
- Supports dynamic spokes.

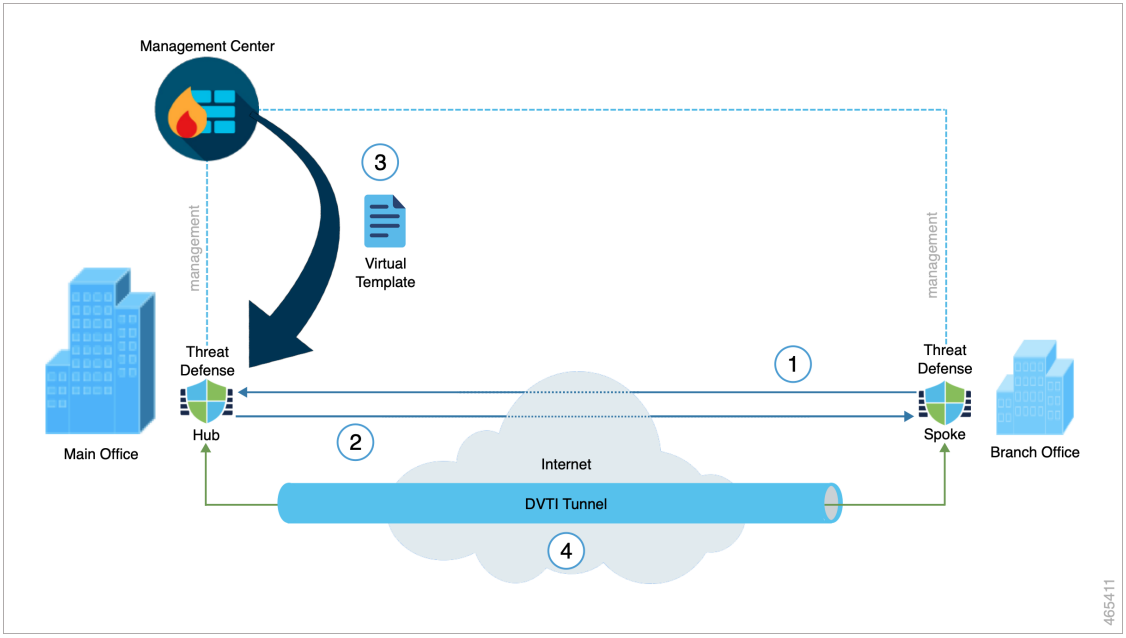
  You do not have to update the hub configuration for spoke's DHCP IP address changes.
- Conserves IP addresses.
  - Uses the IP unnumbered interface functionality to borrow the IP address from another physical or loopback interface.
  - All virtual access interfaces associated to a dynamic VTI use the same IP address.
- Supports virtual routers.
- Provides differential access control for VPN traffic.

You can configure a VTI with a security zone and use it in an AC policy. This configuration:

- Allows you to classify and differentiate VPN traffic from clear-text traffic and permit VPN traffic selectively.
- Provides differential access-control for VPN traffic across different VPN tunnels.

How Does the Firewall Management Center Create a Dynamic VTI Tunnel for a VPN Session

When a spoke initiates a tunnel request with the hub:



1. The spoke initiates an IKE exchange with the hub for a VPN connection.
2. The hub authenticates the spoke.
3. The Firewall Management Center assigns a dynamic virtual template on the hub for the spoke.

   The virtual template dynamically generates a virtual access interface on the hub. This interface is unique for the VPN session with the spoke.
4. The hub establishes a dynamic VTI tunnel with the spoke using the virtual access interface.
   a. The hub and spoke exchange traffic over the tunnel using:
      - Specific traffic proposed by the spokes over IKE exchanges.
      - BGP/OSPF/EIRGP protocols over the IPsec tunnel.
   b. After the VPN session ends, the tunnel disconnects and the hub deletes the corresponding virtual access interface.

To create a dynamic VTI interface in the Firewall Management Center, see Add a VTI interface, on page 1371.

To configure a route-based site-to-site VPN using dynamic VTI, see Configure dynamic VTI for a route-based site-to-site VPN, on page 1384.

Virtual Routers and Dynamic VTI

You can create virtual routers, associate dynamic VTIs with these virtual routers, and extend the capabilities of dynamic VTIs in your network. You can associate dynamic VTIs either with global or user-defined virtual routers. You can assign a dynamic VTI to only one virtual router.

A virtual router associated with:

- A dynamic VTI is called an Indoor VRF (IVRF).
- A tunnel source interface is known as Front Door VRF (FVRF).

A dynamic VTI and its corresponding protected network interface must be part of the same virtual router. You must map the borrow IP interface and the dynamic VTI to the same virtual router. A tunnel source interface can be part of multiple virtual routers.

To configure virtual routers using dynamic VTI for a route-based site-to-site VPN, refer to Configure a virtual router with dynamic VTI, on page 1384.

For more information about a configuration example, refer to Secure traffic from networks with multiple virtual routers over a site-to-site VPN with dynamic VTI, on page 1025

Guidelines for virtual tunnel interfaces

General configuration guidelines

- VTIs are only configurable in IPsec mode.
- Dynamic VTI supports only Firewall Threat Defense devices from Version 7.3.
- You can use static, BGP, EIGRP IPv4, OSPFv2/v3 routes for traffic using the tunnel interface.
- In an HA configuration with dynamic routing, the standby device cannot access the known subnets through the VTI tunnels as these tunnels are created with the active IP address.
- For static and dynamic VTI, ensure that you don't use the borrow IP interface as the tunnel source IP address for any VTI interface.
- When you configure a route-based site-to-site VPN using static or dynamic VTI interfaces, ensure that the value of the TTL hop is more than one if you use BGP.
- If NAT has to be applied, the IKE and ESP packets are encapsulated in the UDP header.
- Ensure that you remove unused transform sets from route-based IKE VPN configurations. If you have unused transform sets, the VPN tunnels may not come up and encapsulation and decapsulation will not happen. Use **show run crypto** and **show VPN-sessiondb detail l2l** commands to view the transform sets.

IPv6 address guidelines

- VTI supports IPv6 addresses.
- You can use an IPv6 address for the tunnel source interface and use the same address as the tunnel endpoint.

- The Firewall Management Center supports the following combinations of VTI IP (or internal networks IP version) over public IP versions: IPv6 over IPv6, IPv4 over IPv6, IPv4 over IPv4, and IPv6 over IPv4.
- VTI supports static and dynamic IPv6 addresses as the tunnel source and destination.
- The tunnel source interface can have IPv6 addresses and you can specify the tunnel endpoint address. If you don't specify the address, by default, the device uses the first IPv6 global address in the list as the tunnel endpoint.

IKE support and guidelines

- Static VTI supports IKE v1 and v2.
- Dynamic VTI supports only IKE version v2, and uses IPsec for sending and receiving data between the tunnel's source and destination.
- IKE and IPsec security associations are re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- Tunnel group name must match what the peer sends as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which aren't IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.

MTU behavior

- MTU for VTIs is automatically set based on the underlying physical interface.
- For dynamic VTI, the virtual access interface inherits MTU from the configured tunnel source interface. If you don't specify the tunnel source interface, the virtual access interface inherits the MTU from the source interface from which the device accepts the VPN session request.

VTI scaling and guidelines

- Configure a maximum of 1024 static and dynamic VTIs in a device.

  While calculating the VTI count, consider nameif subinterfaces, portchannel configurations, and platform VLAN limitations.
- If you configure more than 400 VTIs in a device in a high-availability setup, configure 45 seconds as the unit holdtime.

Routing protocol support

VTI supports multiple routing protocols for different IP versions.

- VTI supports IPv6 BGP.
- VTI supports IPv4 EIGRP.
- VTI supports IPv4 and IPv6 OSPF.

ECMP configuration guidelines

- Configure spokes' static VTIs in an ECMP zone to load balance application traffic. If you do not configure the ECMP zone, the remaining paths act as backup paths when the primary path goes down.
- You can associate VTI interfaces with ECMP zones and configure ECMP static routes to achieve these benefits:

- Load balancing (Active/Active VTIs)—Connection can flow over any of the parallel VTI tunnels.
- Seamless connection migration—When a VTI tunnel becomes unreachable, the flows are seamlessly migrated to another VTI interface that is configured in the same zone.
- Asymmetric routing—Forward traffic flow through one VTI interface and configure the reverse traffic flow through another VTI interface.

For information on configuring ECMP, see ECMP routing methods, on page 1047.

Access control rule guidelines

- By default, all traffic sent through a VTI is encrypted.
- Access control rules can be applied on a VTI interface to control traffic through VTI.
- For route-based VPNs, Bypass Access Control policy for decrypted traffic (**sysopt connection permit-VPN**) does not work. You must always create access control rules to allow route-based VPN traffic.

Crypto map guidelines

- If you use dynamic crypto maps and dynamic VTIs in your site-to-site VPNs, only the dynamic VTI tunnels will come up. This behaviour occurs because both the crypto maps and dynamic VTIs try to use the default tunnel group. We recommend that you migrate your site-to-site VPNs to dynamic VTIs or use static crypto maps with their own tunnel-groups.
- VTI and crypto map configurations can coexist on the same physical interface if the peer address configured in the crypto map and the tunnel destination for the VTI are different.

Topology guidelines

- Dynamic VTI supports only the hub and spoke topology in the management center.
- We recommend that you configure only a single hub for a route-based hub and spoke topology. To configure a topology with multiple hubs for a set of spokes, with one hub as the backup hub, configure multiple topologies with a single hub and the same set of spokes.

Dynamic VTI and virtual router guidelines

- A dynamic VTI and its corresponding protected network interface must be part of the same virtual router.
- You must map the borrow IP interface and the dynamic VTI to the same virtual router.
- User-defined virtual routers support only BGPv4/v6 and OSPFv2 routing protocols.
- A tunnel source interface can be in a different user-defined virtual router than that associated with the dynamic VTI.

Firewall mode guideline

Configure VTI only in routed mode.

Limitations for Virtual Tunnel Interfaces

This topic lists the limitations for configuring Virtual Tunnel Interfaces in Management Center.

General limitations

- VTIs do not support clustering.
- VTI tunnel interfaces are not supported for SNMP or Syslog in Platform Settings.

Static VTI limitations

- Only 20 unique IPSec profiles are supported.
- In policy-based routing, you can configure VTI only as an egress interface.
- You cannot configure a VTI interface as a network interface for a remote access VPN policy.

Dynamic VTI limitations

- Dynamic VTI does not support ECMP , VRF in multi-instance, Clustering, IKEv1, or QoS.
- If a spoke has a dynamic IP address and a hub has a dynamic VTI behind a NAT, the tunnel status will be unknown.
- For a dynamic extranet, when multiple spokes establish a connection, the site-to-site monitoring dashboard does not show the individual tunnels.
- If you configure a hub with dynamic VTI behind NAT with dynamic spokes, the VPN monitoring data will not be accurate.
- You cannot configure a VTI interface as a network interface for a remote access VPN policy.

Backup VTI limitations

- Flow resiliency across tunnel failovers isn't supported. For example, the clear text TCP connection gets lost after a tunnel failover, and you need to reinitiate any FTP transfer that took place during the failover.
- Certificate authentication isn't supported in backup VTI.

Add a VTI interface

For configuring a route-based site-to-site VPN, you must create a VTI interface on the devices at both the nodes of the VTI tunnel.

When you specify the tunnel type as dynamic and configure the related parameters, the Firewall Management Center generates a dynamic virtual template. The virtual template dynamically generates the virtual access interface that is unique for each VPN session.

Before you begin

Configure a loopback interface for redundancy of static and dynamic VTI VPN tunnels. For more information, see Configure a loopback interface, on page 662.

For a Secure Firewall 1200/3100/4200device, IPsec flow offload is also used when the device's VTI loopback interface is enabled.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click the **Edit** icon next to the device on which you want to create a VTI interface.

Step 3 Choose **Add Interfaces > Virtual Tunnel Interface**.

In the **Add Virtual Tunnel Interface** dialog box, configure these parameters:

a) Select the **Tunnel Type** as **Static** or **Dynamic**, and enter the name and description for the interface. By default, the interface is enabled.

b) (Optional) Choose a security zone from the **Security Zone** drop-down list to add the static VTI or dynamic VTI interface to that zone. In the **Priority** field, enter the priority to load balance the traffic across multiple VTIs.

If you want to perform traffic inspection based on a security zone, add the VTI interface to the security zone and configure an access control (AC) rule. To permit the VPN traffic over the tunnel, you need to add an AC rule with this security zone as the source zone.

The priority range is from 0 to 65535. The lowest number has the highest priority. This option is not applicable for dynamic VTI.

c)

d) Depending on the tunnel type, do one of the following:

- For a dynamic VTI, enter a unique ID in the range of 1 to 10413 in the **Template ID** field.
- For a static VTI, enter a unique tunnel ID in the range of 0 to 10413 in the **Tunnel ID** field.

e) (Optional for dynamic VTI) Choose the tunnel source interface from the **Tunnel Source** drop-down list.

The VPN tunnel terminates at this interface, a physical or loopback interface. Choose the IP address of the interface from the drop-down list. You can select the IP address irrespective of the IPsec tunnel mode. In case of multiple IPv6 addresses, select the address that you want to use as the tunnel endpoint.

f) Under **IPSec Tunnel Mode**, click the **IPv4** or **IPv6** radio button to specify the traffic type over the IPsec tunnel.

g) Under **IP Address**:

- **Configure IP**: Enter the IPv4 or IPv6 address for the static VTI interface. You cannot configure an IP address for a dynamic VTI interface. Use the **Borrow IP** field for the dynamic VTI interface.
- **Borrow IP (IP unnumbered)**: Choose a physical or loopback interface from the drop-down list, the VTI interface inherits this IP address.

  Ensure that you use an IP address different from the tunnel source IP address. You can use this option for a static or dynamic VTI interface.

  Click Add + to configure a loopback interface. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address assigned to the loopback interface.

Step 4 Click **OK**.

Step 5 Click **Save**.

Create a route-based site-to-site VPN

You can configure a route-based site-to-site VPN for the following two topologies:

- **Point to Point**: Configure VTIs on both nodes of the tunnel and use the wizard to configure the VPN.
- **Hub and Spoke**: Configure VTIs on the hub and the spokes. Configure the hub with a dynamic VTI and spokes with static VTIs.

You can configure an extranet device as the hub and managed devices as spokes. You can configure multiple hubs and spokes, and also configure backup hubs and spokes.

- For extranet hubs and spokes, you can configure multiple IPs as backup.
- For managed spokes, you can configure a backup static VTI interface along with the primary VTI interface.

For more information on VTI, see Virtual tunnel interfaces, on page 1364.

Note All references to VTI stands for static VTI and dynamic VTI, unless mentioned.

Procedure

Step 1 Choose **Devices** > **VPN** > **Site to Site**.

Step 2 Click **+ Site To Site VPN**.

Step 3 Enter a name for the VPN topology in the **Topology Name** field.

Step 4 Choose **Route Based (VTI)** and do one of the following:

- Select **Point to Point** as the network topology. To configure endpoints for a route-based **Point to Point** topology, refer to Configure endpoints for a point-to-point VPN topology, on page 1374.
- Select **Hub and Spoke** as the network topology. To configure endpoints for a route-based **Hub and Spoke** topology, refer to Configure endpoints for a hub and spoke topology, on page 1376.

Step 5 (Optional) Specify the **IKE**, **IPsec**, and **Advanced** options and click **Save**.

For more information, refer to these topics:

- Firewall Threat Defense VPN IKE options, on page 1356
- Firewall Threat Defense VPN IPsec options, on page 1358
- Firewall Threat Defense advanced site-to-site VPN deployment options, on page 1360

What to do next

After you configure VTI interfaces and VTI tunnel on both the devices, you must configure:

- A routing policy to route the VTI traffic between the devices over the VTI tunnel. For more information, see Configure routing and AC policies for VTI, on page 1385.
- An access control rule to allow encrypted traffic. Choose **Policies** > **Access Control**.

Configure endpoints for a point-to-point VPN topology

Configure these parameters to configure endpoints for a route-based site-to-site VPN for the **Point to Point** topology nodes:

Before you begin

Configure the basic parameters for a point-to-point topology in a route-based VPN as described in Create a route-based site-to-site VPN, on page 1373 and click the **Endpoints** tab.

Procedure

Step 1 Under **Node A**, in the **Device** drop-down menu, select the name of the registered device (Firewall Threat Defense) or extranet as the first endpoint of your VTI tunnel.

For an extranet peer, specify the following parameters:

a. Specify the name of the device.

b. Enter the primary IP address in the **Endpoint IP address** field. If you configure a backup VTI, add a comma and, specify the backup IP address.

c. Click **OK** .

After configuring the above parameters for the extranet hub, specify the pre-shared key for the extranet in the **IKE** tab.

Note The AWS VPC has **AES-GCM-NULL-SHA-LATEST** as the default policy. If the remote peer connects to AWS VPC, select **AES-GCM-NULL-SHA-LATEST** from the **Policy** drop-down list to establish the VPN connection without changing the default value in AWS.

Step 2 For a registered device, you can specify the VTI interface for Node A from the **Virtual Tunnel Interface** drop-down list.

The selected tunnel interface is the source interface for Node A and the tunnel destination for Node B.

If you want to create a new interface on Node A, click the Add + icon and configure the fields as described in Add a VTI interface, on page 1371 .

If you want to edit the configuration of an existing VTI, select the VTI in the **Virtual Tunnel Interface** drop-down field and click **Edit VTI**.

Step 3 If your Node A device is behind a NAT device, check the **Tunnel Source IP is Private** check box. In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

Step 4 **Send Local Identity to Peers** —Select this option to send local identity information to the peer device. Select one of the following **Local Identity Configuration** from the list and configure the local identity:

- **IP address** —Use the IP address of the interface for the identity.
- **Auto** —Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID** —Specify the email ID to use for the identity. The email ID can be up to 127 characters.
- **Hostname** —Use the fully qualified hostname.
- **Key ID** —Specify the key-id to use for the identity. The key ID must be fewer than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identity allows Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to a Cisco Umbrella Secure Internet Gateway (SIG).

For information about configuring a unique tunnel ID on Umbrella, see **Cisco Umbrella SIG User Guide** .

Step 5 (Optional) Click **Add Backup VTI** to specify an extra VTI as the backup interface and configure the parameters.

Note Ensure that both peers of the topology do not have the same tunnel source for the backup VTI. A device cannot have two VTIs with the same tunnel source and tunnel destination; hence, configure a unique tunnel source and tunnel destination combination.

Though the virtual tunnel interface is specified under Backup VTI, the routing configuration determines which tunnel to be used as primary or backup.

Step 6 Under **Additional Configuration** , do the following:

- To route traffic to the VTI, click **Routing Policy** . Firewall Management Center displays the **Devices** > **Routing** page.

  You can configure the Static, BGP, OSPF v2/v3, or EIGRP routing for the VPN traffic.

- To permit VPN traffic, click **AC Policy** . Firewall Management Center displays the access control policy page of the device. Proceed to add an allow/block rule specifying the security zone of the VTI. If you configure a backup VTI, ensure to include the backup tunnel to the same security zone as that of the primary VTI. No specific settings are required for the backup VTI in the AC policy page.

Step 7 Expand **Advance Settings** to configure additional configurations for the device. For more information, see Configure advanced settings for a point-to-point topology in a route-based VPN, on page 1376 .

Step 8 Repeat the above procedure for Node B and click **OK** .

What to do next

- (Optional) Specify the **IKE** options for the deployment as described in Firewall Threat Defense VPN IKE options, on page 1356.
- (Optional) Specify the **IPsec** options for the deployment as described in Firewall Threat Defense VPN IPsec options, on page 1358.

- (Optional) Specify the **Advanced** options for the deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 1360.
- Click **Save**.
- To route traffic to the VTI, choose **Devices** > **Device Management** , edit the threat defense device and click the **Routing** tab.

  You can configure the static routes, or use BGP, OSPF v2/v3, or EIGRP for routing the VPN traffic.
- To permit VPN traffic, choose **Policies** > **Access Control heading** > **Access Control**. Add a rule specifying the security zone of the VTI. For a backup VTI, ensure that you include the backup VTI in the same security zone as that of the primary VTI.

Configure advanced settings for a point-to-point topology in a route-based VPN

Configure advanced settings to enhance the functionality and security of a point-to-point topology in a route-based VPN beyond the basic configuration parameters.

Before you begin

Configure the basic parameters for a point-to-point topology in a route-based VPN as described in Configure endpoints for a point-to-point VPN topology, on page 1374 and expand **Advance Settings**.

Procedure

Step 1 Check the **Send Virtual Tunnel Interface IP to the peers** check box to send the VTI IP address to the peer device.

Step 2 Check the **Allow incoming IKEv2 routes from the peers** check box to allow incoming IKEv2 routes from the spokes and peers.

Step 3 Choose one of the following from the **Connection Type** drop-down list:

Answer Only: The device can only respond when a peer device initiates a connection, it can't initiate any connection.

Bidirectional: The device can initiate or respond to a connection. This is the default option.

Configure endpoints for a hub and spoke topology

You can create a route-based site-to-site VPN using dynamic VTI only for hub and spoke topologies. The hub can use only a dynamic VTI and the spokes can use only static VTI interfaces. You can also configure an extranet device as a hub.

Configure these parameters to configure endpoints for a route-based site-to-site VPN for the **Hub and Spoke** topology nodes:

Before you begin

Configure the basic parameters for a hub and spoke topology in a route-based VPN as described in Create a route-based site-to-site VPN, on page 1373 and click the **Endpoints** tab.

Procedure

Step 1 Under **Hub Nodes**:

a) Click Add + to configure the hub node in the **Add Endpoint** dialog box.

b) Choose a hub from the **Device** drop-down list.

For an extranet hub, configure these parameters:

1. Enter the name of the device.
2. Enter the primary IP address. If you configure a backup VTI, add a comma, and then specify the backup IP address.
3. Click **OK**.

After configuring the above parameters for the extranet hub, specify the pre-shared key for the extranet in the **IKE** tab.

Note The AWS VPC has **AES-GCM-NULL-SHA-LATEST** as the default policy. If the remote peer connects to AWS VPC, select **AES-GCM-NULL-SHA-LATEST** from the **Policy** drop-down list to establish the VPN connection without changing the default value in AWS.

c) Choose a dynamic VTI from the **Dynamic Virtual Tunnel Interface** drop-down list.

Tunnel source configuration is mandatory for a dynamic VTI as the management center needs this information to determine the tunnel destination of the spoke.

Click Add + to add a new dynamic VTI. We recommend that you configure the Borrow IP for the dynamic interface from a loopback interface.

If you want to edit an existing dynamic VTI, select the interface, and click **Edit VTI**.

d) (Optional) If your endpoint device is behind a NAT device, check the **Tunnel Source IP is Private** check box and configure the tunnel source IP address in the **Tunnel Source Public IP Address** field.

e) Click **Routing Policy** to configure the routing policy for the hub.

f) Click **AC Policy** to configure the access control policy.

g) Expand **Advance Settings** to configure additional configurations on the hub. For more information, see Configure advanced settings for hub and spokes in a route-based VPN, on page 1379 .

h) Click **OK**.

Step 2 Under **Spoke Nodes**:

a) Click Add + to configure the spoke in the **Add Endpoint** dialog box.

b) Choose a spoke from the **Device** drop-down list.

For an extranet spoke, configure these parameters:

1. Enter the name of the device.
2. In **Endpoint IP Address**, choose one of these options:
   - **Static**: Enter the IP address of the device, and the backup IP address, if required.

- **Dynamic**: Choose this option to dynamically assign the IP addresses for the extranet spokes.

3. Click **OK**.

c) Choose a static VTI from the **Static Virtual Tunnel Interface** drop-down list.

Click Add + to add a new static VTI. Tunnel IP of the static VTI is auto populated, ensure that this IP address is unique for the spoke.

If you want to edit an existing static VTI, select the interface, and click **Edit VTI**.

d) (Optional) If your endpoint device is behind a NAT device, check the **Tunnel Source IP is Private** check box. The management center needs the tunnel source interface address to configure the tunnel destination IP address on the spokes. In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

e) (Optional) **Send Local Identity to Peers** —Check this check box to send the local identity information to the peer device. Choose one of the following parameters from the **Local Identity Configuration** drop-down list and configure the local identity:

- **IP address**—Use the IP address of the interface for the identity.
- **Auto**—Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID**—Specify the email ID to use for the identity. The email ID can be up to 127 characters.
- **Hostname**—Use the fully qualified hostname.
- **Key ID**—Specify the key-id to use for the identity. The key ID must be less than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identity allows Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to the Cisco Umbrella Secure internet Gateway (SIG).

For more information about configuring a unique tunnel ID on Umbrella, see *Cisco Umbrella SIG User Guide* .

f) (Optional) Click **Add Backup VTI** to specify an extra VTI interface as the backup interface.

Note Ensure that both peers of the topology do not have backup VTI configured on the same tunnel source. For instance, if Peer A is having two VTIs (primary and a backup) configured with a single tunnel source interface, say, 10.10.10.1/30, then Peer B also can't have its 2 VTIs with a single tunnel source IP, say 20.20.20.1/30.

Though the virtual tunnel interface is specified under backup VTI, the routing configuration determines which tunnel to be used as primary or backup.

g) Click **Routing Policy** to configure the routing policy for the spoke.

h) Click **AC Policy** to configure the access control policy.

i) Expand **Advance Settings** to configure additional configurations on the spoke and click **OK** . For more information, see Configure advanced settings for hub and spokes in a route-based VPN, on page 1379.

What to do next

1. (Optional) Specify the **IKE** options for the deployment as described in Firewall Threat Defense VPN IKE options, on page 1356.
2. (Optional) Specify the **IPsec** options for the deployment as described in Firewall Threat Defense VPN IPsec options, on page 1358.
3. (Optional) Specify the **Advanced** options for the deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 1360.
4. Click **Save**.

Configure advanced settings for hub and spokes in a route-based VPN

After configuring basic parameters for a hub and spoke in a route-based VPN, you can configure additional advanced settings to optimize the VPN topology's functionality and performance.

Before you begin

Configure the basic parameters for a hub and spoke in a route-based VPN as described in Configure endpoints for a hub and spoke topology, on page 1376 and expand **Advance Settings**.

Procedure

Step 1 Check the **Send Virtual Tunnel Interface IP to the peers** check box to send the VTI IP address to the peer device.

For a hub, you must check this check box if you use BGP as the routing protocol. This configuration ensures that the loopback IP address is shared in the BGP routing table.

For a spoke, this option is enabled by default.

Step 2 Add the **Protected Networks** to define the networks protected by the VPN endpoint. Click Add + to select a protected network.

For a hub, configure the protected networks behind the hub. This information and the spoke's protected network generate the spoke access list.

You cannot create a static route for a virtual access interface on a hub with dynamic VTI. The hub creates and deletes these interfaces dynamically during tunnel establishment and termination.

For a spoke, configure the spoke's protected network.

To enable static routing for the spokes, after you configure the endpoints for your topology, click the **IPsec** tab and check the **Enable Reverse Route Injection** check box.

You do not need this option if you use BGP, OSPF, or EIGRP.

Step 3 Check the **Allow incoming IKEv2 routes from the peers** check box to allow incoming IKEv2 routes from the spokes and peers.

For a hub: During an IKE exchange, the hub advertises the dynamically created virtual access interfaces to the spokes, and the spokes advertise their VTI IP addresses to the hub.

For a spoke: By default, this option is enabled.

Step 4 In the **Connection Type** drop-down list, choose one of the following:

Answer Only: The device can only respond when a peer device initiates a connection, it can't initiate any connection.

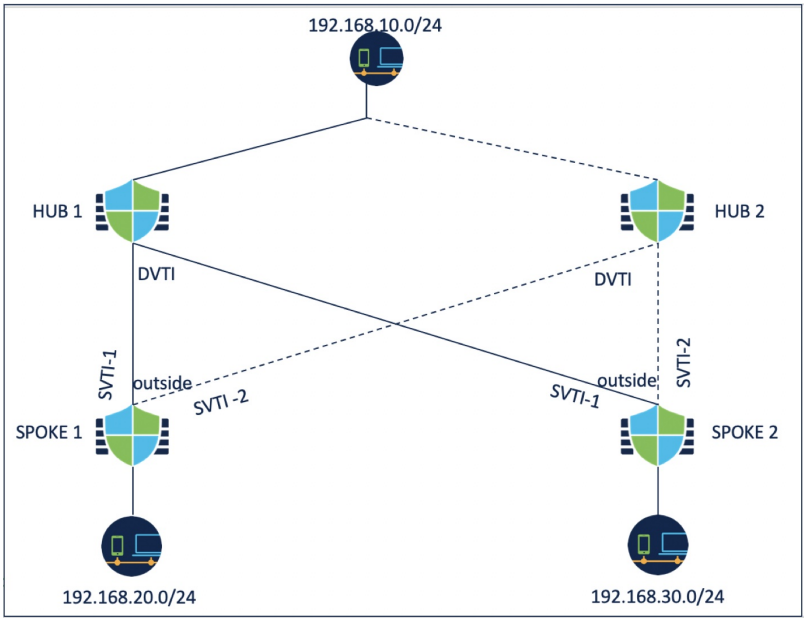
Bidirectional: The device can initiate or respond to a connection. This is the default option.

Configure multiple hubs in a route-based VPN

You can configure a topology with multiple hubs for a set of spokes. With one hub as the backup hub, you can configure multiple topologies with a single hub and the same set of spokes.

In this example, there are two hubs connected to the same set of spokes. Hub 1 is the primary hub and Hub 2 is the secondary hub. To configure this network in the Firewall Management Center, you must configure two route-based hub and spoke topologies:

- Topology 1: Hub 1 connected to spoke 1 and spoke 2.
- Topology 2: Hub 2 connected to spoke 1 and spoke 2.



To configure topology 1:

Procedure

Step 1 Choose **Devices** > **VPN** > **Site to Site** and click **+ Site To Site VPN**.

Step 2 Enter a name for the VPN topology in the **Topology Name** field.

Step 3 Choose **Route Based (VTI)** and do one of these topologies:

- Select **Point to Point** as the network topology. To configure endpoints for a route-based **Point to Point** topology, see Configure endpoints for a point-to-point VPN topology, on page 1374.

- Select **Hub and Spoke** as the network topology. To configure endpoints for a route-based **Hub and Spoke** topology, see Configure endpoints for a hub and spoke topology, on page 1376.

Step 4 Configure the IKE version and click the **Endpoints** tab.

Step 5 Under **Hub Nodes**:

a) Click Add + to add the hub.
b) Choose Hub 1 from the **Device** drop-down list.
c) Choose a dynamic VTI from the **Dynamic Virtual Tunnel Interface** drop-down list or click Add + to add a new dynamic VTI.

We recommend that you configure the Borrow IP for the dynamic interface from a loopback interface.

d) (Optional) If your endpoint device is behind a NAT device, check the **Tunnel Source IP is Private** check box and configure the tunnel source IP address in the **Tunnel Source Public IP Address** field.
e) Click **Routing Policy** to configure the routing policy for the hub. You can configure dynamic routing using BGP.
f) Expand **Advance Settings**. You can configure these advanced settings for the hub to enable IKEv2 routing, which can be used if you do not use dynamic routing.

- (Optional) Check the **Send Virtual Tunnel Interface IP to the peers** check box.
- Check the **Allow incoming IKEv2 routes from the peers** check box for the hub to accept routes from the spokes and update the routing table.
- Choose **Connection Type** as Bidirectional from the drop-down list.

g) Click **OK**.

Step 6 Under **Spoke Nodes**:

a) Click Add + to add a spoke.
b) Choose Spoke 1 from the **Device** drop-down list.
c) Choose SVTI-1 as the static VTI for the spoke from the **Static Virtual Tunnel Interface** drop-down list or click Add + to add a new static VTI.

Choose the outside interface as the tunnel source of SVTI-1. Tunnel IP of SVTI-1 is autopopulated, ensure that this IP address is unique for spoke 1 across peers in both the topologies.

d) Expand **Advance Settings**. If you do not use dynamic routing, you can configure these settings to enable IKEv2 routing for the spoke.

- Check the **Send Virtual Tunnel Interface IP to the peers** check box to send the VTI IP address to the peer device.
- Check the **Allow incoming IKEv2 routes from the peers** check box to allow incoming IKEv2 routes from the peers.
- Choose **Connection Type** as Bidirectional from the drop-down list.

e) Click **OK**.
f) Repeat steps 5a to 5e to add spoke 2. Configure SVTI-1 as the static VTI of spoke 2.

Step 7 Configure the IKE and IPSec parameters as required or use the default values.

What to do next

1. Configure topology 2 with hub 2, spoke 1, and spoke 2.

   Configure SVTI-2 as the static VTI of spoke 1 and SVTI-2 as the static VTI of spoke 2 (refer the above illustration). Tunnel source for SVTI-2 should be the same outside interface.

2. For each spoke, configure the routing policy. For more information, see Configure routing for multiple hubs in a route-based VPN, on page 1382.

3. Verify the configuration and tunnel statuses. For more information, see Verify multiple hubs configuration in a route-based VPN, on page 1383.

Configure routing for multiple hubs in a route-based VPN

Configure dynamic routing using BGP on both hub and spoke devices, and implement Policy Based Routing on spokes to enable proper traffic routing in a route-based VPN topology with multiple hubs.

Before you begin

Configure topology 1 and 2 as explained in Configure multiple hubs in a route-based VPN, on page 1380.

Procedure

Step 1 Configure dynamic routing for the hub using BGP.

a) Choose **Devices** > **Device Management**, and click **Edit** ( ) then click the **Routing** tab.
b) In the left pane, choose **General Settings** > **BGP**.
c) Check the **Enable BGP** check box and enter the **AS number**.

   You can configure the other fields AS per your requirement.

d) Click **Save**.
e) On the left pane, choose **BGP** > **IPv4**.
f) Check the **Enable IPv4** check box.
g) Click the **Neighbor** tab, click **Add** and configure these parameters.

   1. **IP Address**: Enter the tunnel interface IP address of Spoke 1.
   2. **Remote AS**: AS number of Spoke 1.
   3. Check the **Enabled Address** check box.
   4. Click **OK**.

   Repeat the above steps to add Spoke 2 as a neighbor.

h) Click **Save**.
i) Click the **Networks** tab and click **Add** to advertise the network behind the hub to the peers.

Step 2 Configure dynamic routing for the spokes using BGP.

The BGP configuration for the spokes is similar to that of the hub except for these differences:

- Configure Hub 1 and Hub 2 AS the neighbors for both the spokes and use the tunnel interface IP address of the hubs.

- When you configure networks, use the network behind each spoke.

Step 3 Configure Policy Based Routing on the spokes.

a) In the left pane, choose **Policy Based Routing** and click **Add**.
b) Choose the **Ingress Interface** from the drop-down list.
c) Click **Add** to configure a Match ACL.

For example, for spoke 1, source network is 192.168.20.0/24 and destination network is 192.168.10.0/24.

d) Choose Egress Interfaces from the **Send to** drop-down list.
e) Choose Order from the **Interface Ordering** drop-down list.
f) Select the SVTI-1 and SVTI-2 interfaces AS the egress interfaces.
g) Click **Save**.

If you want to use the hubs as a load-balancing pair, you must configure ECMP.

Step 4 Deploy the configurations on the hub and spokes.

What to do next

Verify the configurations and tunnel statuses. For more information, see Verify multiple hubs configuration in a route-based VPN, on page 1383.

Verify multiple hubs configuration in a route-based VPN

To verify the multiple hub configurations and the tunnel statuses.

- After the deployment, check the tunnel status in the dashboards.
- Use **Packet Trace**r from the **Site-to-Site VPN dashboard** to verify the selected path of the traffic (hub 1 or hub 2).
- Use these show commands for each endpoint to verify the configurations:
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

Route traffic through a backup VTI tunnel

A backup VTI tunnel ensures traffic continuity by providing an alternative path when the primary VTI tunnel fails to route traffic in route-based VPN configurations.

You can deploy the backup VTI tunnel in these scenarios:

- Both peers having service provider redundancy backup.

  In this case, there are two physical interfaces, acting as the tunnel sources for the two VTIs of the peers.
- Only one of the peers has service provider redundancy backup.

In this case, there's an interface backup on only one side of the peer and on the other end, there is only one tunnel source interface.

Before you begin

Ensure that you review the guidelines and limitations. For more information, refer to Guidelines for virtual tunnel interfaces, on page 1368.

Procedure

Step 1 Create the VTI interface.

For more information, refer to Add a VTI interface, on page 1371

Step 2 In the **Add Endpoint** dialog box of the **Create New VPN Topology** wizard, click **Add Backup VTI** to configure the respective backup interface for each peer.

For more information, refer to

- Configure endpoints for a point-to-point VPN topology, on page 1374
- Configure endpoints for a hub and spoke topology, on page 1376

Step 3 Choose **Devices > Device Management**, and edit the threat defense device and click **Routing** to configure the routing policy.

Step 4 Choose **Policies > Access Control** to configure the access control policy.

Configure dynamic VTI for a route-based site-to-site VPN

To configure dynamic VTI for a route-based site-to-site VPN in the Management Center:

Step	Do This	More Information
1	Create a dynamic VTI interface on the hub.	Add a VTI interface, on page 1371
2	Create static VTI interfaces on the spokes.	Add a VTI interface, on page 1371
3	Create a route-based site-to-site VPN.	Create a route-based site-to-site VPN, on page 1373
4	Configure the routing policy and the access control policy.	Configure endpoints for a hub and spoke topology, on page 1376

Configure a virtual router with dynamic VTI

To configure a virtual router with dynamic VTI for a route-based site-to-site VPN in the Management Center:

Step	Do This	More Information
1	Create a route-based site-to-site VPN with a dynamic VTI interface on the hub and static VTI(s) on the spoke(s).	Create a route-based site-to-site VPN, on page 1373
2	Create a virtual router.	Create a virtual router, on page 1002
3	Assign the interfaces to the virtual router.	Configure a virtual router, on page 1002
4	Configure routing policies for the hub and spoke.	Configure endpoints for a hub and spoke topology, on page 1376
5	Configure access control policies for the hub and spoke.	Configure endpoints for a hub and spoke topology, on page 1376

Configure routing and AC policies for VTI

After you configure VTI interfaces and the VTI tunnel on both the devices, you must configure these parameters:

- A routing policy to route VTI traffic between the devices over the VTI tunnel.
- An access control rule to allow encrypted traffic.

Procedure

Step 1 Configure routing for VTI interfaces.

For the VTI interfaces, you can configure static route or routing protocols such AS BGP, EIGRP, OSPF/OSPFv3.

a. Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

b. Click **Routing**.

c. Configure static route, or BGP, EIGRP, OSPF/OSPFv3.

Routing	Parameters	More Information
Static Route	• **Interface**—Select the VTI interface. For a backup tunnel, select the backup VTI interface. • **Selected Network**—Remote peer's protected network. • **Gateway**—Remote peer's tunnel interface IP address. For a backup tunnel, select the remote peer's backup tunnel interface IP address. • **Metric**—For a backup tunnel, configure a different metric to handle the failover of the traffic flow over the backup tunnel. **Note** DVTI does not support static routes.	Add a static route, on page 977

BGP	• Under **General Settings** > **BGP**, enable BGP, provide the AS number of the local device, and add Router ID (if you choose Manual).
	• Under **BGP**, enable IPv4/IPv6 and click the **Neighbor** tab to configure the neighbors.
	  • **IP Address**—Remote peer's VTI interface IP address. For a backup tunnel, add a neighbor with the remote peer's backup VTI interface IP address.
	  • **Remote AS**—Remote peer's AS number.
	• Click the **Redistribution** tab, select the **Source Protocol** AS Connected to enable connected route redistribution.
		Configure BGP, on page 1112

Routing	Parameters	More Information
EIGRP	• Enable EIGRP, provide the AS number of the local device, and select the networks or hosts that participate in the EIGRP routing process. • Click the **Neighbors** tab and define the static neighbors for the EIGRP process. • To advertise summary addresses from a VTI interface, click the **Summary Address** tab, choose the VTI interface from the **Interface** drop-down. From the **Network** drop-down, choose the network to be summarized. • Click the **Interfaces** tab to configure the interface-specific EIGRP routing properties for the VTI interface. To enable EIGRP split-horizon on the interface, check the **Split Horizon** check box. You can also configure the **Hold Time** that is advertised by the device in the EIGRP hello packets.	Configure EIGRP routing on firewall devices, on page 1098
OSPF	• Check the **Process 1** check box, and choose the OSPF role. • Click the **Interface** tab and choose a VTI interface.	OSPFv2 configuration, on page 1070
OSPFv3	• Check the **Process 1** and **Enable Process 1** check boxes, and choose the OSPFv3 role. • Click the **Interface** tab and choose a VTI interface.	OSPFv3 configuration, on page 1083

Step 2 Add an access control rule to the access control policy on the device to allow encrypted traffic between the VTI tunnels with these settings:

a. Create the rule with the Allow action.

b. Select the VTI security zone of the local device AS the source zone and the VTI security zone of the remote peer AS the destination zone.

c. Select the VTI security zone of the remote peer AS the source zone and the VTI security zone of the local device AS the destination zone.

For more information about configuring an access control rule, see Create and edit access control rules, on page 1631.

View virtual tunnel interface details

You can view details of dynamic and static VTIs of route-based VPNs on the device. For every VPN topology, you can also view details of all the dynamically generated virtual access interfaces associated with each dynamic VTI.

Before you begin

- Supported device for static VTIs: Firewall Threat Defense Version 7.0 and later
- Supported device for dynamic VTIs: Firewall Threat Defense Version 7.3 and later

Procedure

Step 1 Choose **Devices** > **Device Management** and click **Edit** (✎) for your Firewall Threat Defense device. The **Interfaces** page is selected by default.

Step 2 Click the **Virtual Tunnels** tab.

For each VTI, you can view details such as name, IP address, IPsec mode, tunnel source interface details, topology, and remote peer IP. You can also view if path monitoring is enabled for each interface.

Deploy a SASE tunnel on Umbrella

Guidelines for configuring SASE tunnels on Umbrella

SASE topology supports:

- Only PSK-based authentication
- IKEv2
- High availability

General configuration guidelines

- Firewall Management Center does not discover tunnels created directly on Umbrella or by other applications.

- You can add only devices managed by the Firewall Management Center as endpoints for the SASE topology. You cannot add extranet devices.

  For high availability pairs, the HA pair names appear in the endpoint list.

- If you check the **Deploy configuration on threat defense nodes** check box in the wizard, the Umbrella SASE topology configuration is deployed on the Firewall Threat Defense only after the tunnels are deployed on Umbrella.

  The Firewall Management Center requires the local tunnel ID to deploy the Umbrella configuration in Firewall Threat Defense. Umbrella generates the complete tunnel ID (*<prefix>@<umbrella generated ID>*-umbrella.com) only after the Firewall Management Center deploys the tunnel on Umbrella.

- After a Firewall Threat Defense HA switchover, the SASE topology will not appear in the site-to-site monitoring/VPN summary dashboard. We recommend that you bring the tunnel down using the **VPN-sessiondb logoff index** command and bring it up using packet tracer.

Version migration guideline (Pre-version 7.3)

You must create new SASE topologies in version 7.3 and delete the existing SASE topologies because Firewall Management Center does not recognize topologies using Umbrella data center as an extranet hub created before version 7.3 as SASE topologies.

Deployment status and monitoring guideline

You can track the tunnel deployment status in three places:

- Cisco Umbrella Configuration dialog box of the wizard
- Notifications page under the Deployments and Tasks tabs
- Site to Site VPN Monitoring dashboard

Tunnel deletion guidelines

- You cannot edit or delete a SASE topology while deployment to Umbrella is in progress.
- When you delete a tunnel from Firewall Management Center and if it is unable to delete the tunnel from Umbrella, you must manually delete it by logging into Umbrella.

Limitations for configuring SASE tunnels on Umbrella

SASE topology does not support these features:

- Clustering
- Certificate-based authentication
- IKEv1

Deploy a SASE tunnel on Umbrella

This section provides instructions to deploy a SASE tunnel on Umbrella from a Firewall Threat Defense device using the Firewall Management Center.

Step	Do This	More Info
1	Review the guidelines and limitations.	Guidelines for configuring SASE tunnels on Umbrella, on page 1388
2	Ensure that you meet the prerequisites.	Prerequisites for configuring Umbrella SASE tunnels, on page 1390
3	Configure Cisco Umbrella connection settings.	• Configure Cisco Umbrella Connection Settings • Map Management Center Umbrella parameters and Cisco Umbrella API keys, on page 1390
4	Configure a SASE tunnel on Umbrella.	Configure a SASE tunnel for Umbrella, on page 1392
5	View the status of the SASE tunnel.	View SASE tunnel status, on page 1394

Prerequisites for configuring Umbrella SASE tunnels

License prerequisites

- You must have a Cisco Umbrella Secure Internet Gateway (SIG) Essentials subscription.
- You must enable your Smart License account with the export-controlled features to deploy tunnels on Umbrella from the Firewall Management Center. If this license is not enabled, you can only create a SASE topology. You cannot deploy tunnels on Umbrella.

General prerequisites

- You must establish an account with Cisco Umbrella at https://umbrella.cisco.com, log into Umbrella at http://login.umbrella.com, and obtain the required information to establish connection to Cisco Umbrella.
- You must register Cisco Umbrella with the Firewall Management Center and configure the management key and the management secret in the Cisco Umbrella Connection Settings. The management center requires the management key and management secret to fetch the datacenter details from the Cisco Umbrella cloud. You must also configure the Organization ID, Network Device Key, Network Device Secret, and the Legacy Network Device Token in the Cisco Umbrella Connection Settings.

  For more information, refer to:

  - Configure Cisco Umbrella Connection Settings
  - Map Management Center Umbrella parameters and Cisco Umbrella API keys, on page 1390

- Ensure that Umbrella data center is reachable from the Firewall Threat Defense.
- You can deploy a tunnel only between Cisco Umbrella and a Firewall Threat Defense version 7.1.0 and later.

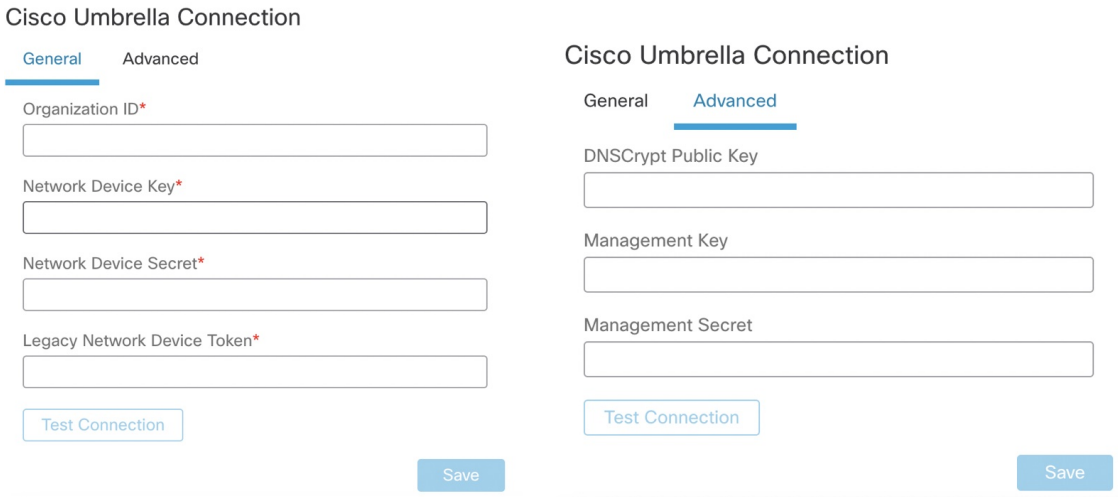
Map Management Center Umbrella parameters and Cisco Umbrella API keys

To register Cisco Umbrella with the Firewall Management Center and configure the Umbrella parameters in the Firewall Management Center, you must complete these steps:

1. Log in to Cisco Umbrella.

2. Choose **Admin** > **API Keys** > **Legacy Keys**.
3. Generate and copy the required API keys.
4. Use the API keys to configure the Cisco Umbrella connection parameters in the Firewall Management Center.

This figures show the parameters that you must configure in the Cisco Umbrella Connection in the Firewall Management Center. DNScrypt Public Key is an optional parameter.



This figure shows the Cisco Umbrella API keys that you must use to register the Cisco Umbrella with the Firewall Management Center.

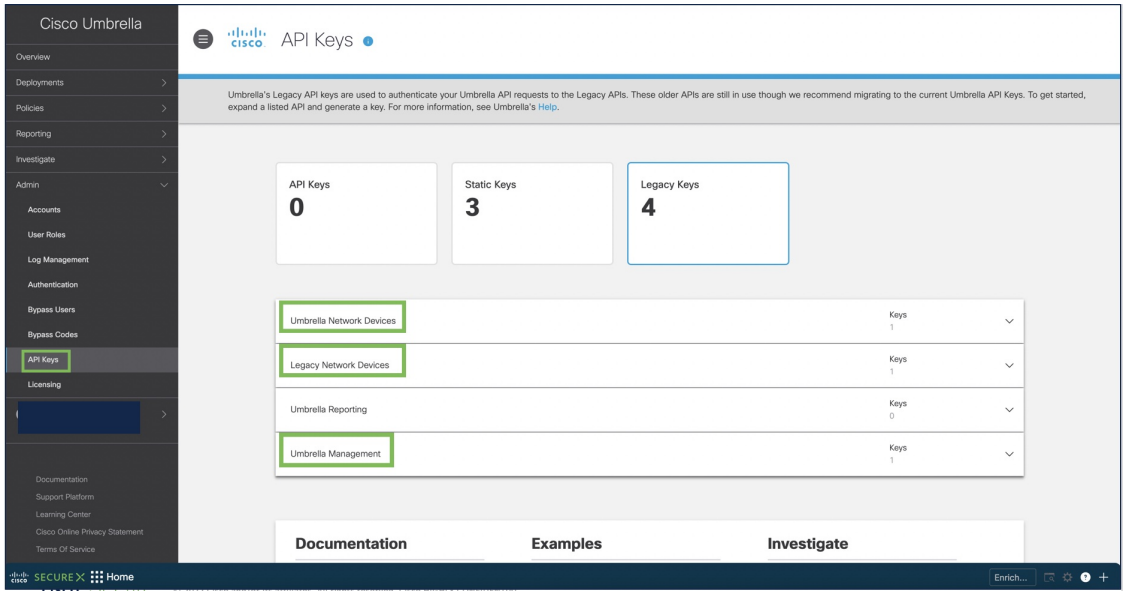


Table 78: Map Firewall Management Center Umbrella Parameters and Cisco Umbrella API Keys

Management Center Parameter	Cisco Umbrella API Keys
Network Device Key Network Device Secret	Umbrella Network Devices
Legacy Network Device Token	Legacy Network Devices
Management Key Management Secret	Umbrella Management

Configure a SASE tunnel for Umbrella

Configure a SASE tunnel to establish secure connectivity between threat defense devices and Cisco Umbrella data centers for cloud-delivered security services.

SASE (Secure Access Service Edge) tunnels provide secure connections to Umbrella data centers, enabling cloud-based security functions. These tunnels use IKEv2 with pre-shared keys for authentication and static VTI interfaces for routing traffic.

Before you begin

Ensure that you review the prerequisites and guidelines in Prerequisites for configuring Umbrella SASE tunnels, on page 1390 and Guidelines for configuring SASE tunnels on Umbrella, on page 1388.

Follow these steps to configure a SASE tunnel for Umbrella:

Procedure

Step 1 Choose **Devices** > **VPN** > **Site to Site**, click **+SASE Topology** and enter a unique **Topology Name**.

Step 2 **Pre-shared Key**: This key is auto-generated according to the Umbrella PSK requirements. For a single topology, the pre-shared key is common for all threat defense spokes and Umbrella.

The device and Umbrella share this secret key, and IKEv2 uses it for authentication. If you want to configure this key, it must be between 16 and 64 characters in length, include at least one uppercase letter, one lowercase letter, one numeral, and have no special characters. Each topology must have a unique pre-shared key. If a topology has multiple tunnels, all the tunnels have the same pre-shared key.

Step 3 Choose a data center from the **Umbrella Data center** drop-down list. (Configure routing on the Firewall Threat Defense to ensure reachability of the umbrella DC from the Firewall Threat Defense.)

Step 4 Click **Add** to add a Firewall Threat Defense node.

a) Choose a Firewall Threat Defense from the **Device** drop-down list.

Only devices managed by the Firewall Management Center appear in the list. For high availability pairs, the HA pair names appear in the endpoint list.

b) Choose a static VTI interface from the **VPN Interface** drop-down list.

To create a new static VTI interface, click Add +. The **Add Virtual Tunnel Interface** dialog box appears with the following pre-populated default configurations.

- Tunnel Type is static.

- Name is <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>. For example, outside_static_vti_2.
- Tunnel ID is auto-populated with a unique ID.
- Tunnel Source Interface is auto-populated with an interface with an 'outside' prefix.
- IPsec tunnel mode is IPv4.
- IP address is from the 169.254.x.x/30 private IP address range.

c) Enter a prefix for the local tunnel ID in the **Local Tunnel ID** field.

The prefix can have a minimum of eight characters and a maximum of 100 characters. Umbrella generates the complete tunnel ID (<*prefix*>@<*umbrella generated ID*>-umbrella.com) after the management center deploys the tunnel on Umbrella. The management center then retrieves and updates the complete tunnel ID and deploys it on the threat defense device. Each tunnel has a unique local tunnel ID.

d) Click **Save** to add the endpoint device to the topology.

You can add multiple endpoints in a SASE topology.

Step 5 Click **Next** to view the summary of the Umbrella SASE tunnel configuration.

- **Endpoints** pane: Displays the summary of the configured endpoints.
- **Encryption Settings** pane: Displays the default IKEv2 policies and IKEv2 IPsec transform sets for the topology.

Step 6 Check the **Deploy configuration on threat defense nodes** check box to trigger deployment of the network tunnels to the threat defense. This deployment occurs after the tunnels are deployed on Umbrella. Local tunnel ID is required for the threat defense deployment.

Step 7 Click **Save**.

This action:

a. Saves the topology in the management center.

b. Triggers deployment of the network tunnels to the Umbrella.

c. Triggers deployment of the network tunnels to the threat defense devices, if the option is enabled. This action commits and deploys all the updated configurations and policies, including non-VPN policies, since the last deployment on the device.

d. Opens the **Cisco Umbrella Configuration** window and displays the status of the tunnel deployment on Umbrella. For more details, see View SASE tunnel status, on page 1394.

What to do next

For the interesting traffic intended to flow through the SASE tunnel, configure a PBR policy with a specific match criteria to send the traffic through the VTI interface.

Ensure that you configure a PBR policy for each endpoint of the SASE topology.

View SASE tunnel status

After configuring Umbrella SASE topology, you need to monitor the tunnel deployment status and verify that the configuration has been successfully pushed to Umbrella.

Procedure

Step 1 Choose **Devices** > **VPN** > **Site to Site**.

Step 2 Click **+SASE Topology**.

Step 3 Enter a unique **Topology Name**, **Pre-shared Key**, choose a data center, add a device, and click **Next**.

Step 4 View the summary of the Umbrella SASE Tunnel configuration and click **Save**.

The **Cisco Umbrella Configuration** window appears.

You can view the topology details such as name, data center, data center IP address, start, and end time of the tunnel deployment.

You can view the deployment status of the tunnels on Umbrella. The different tunnel deployment statuses are:

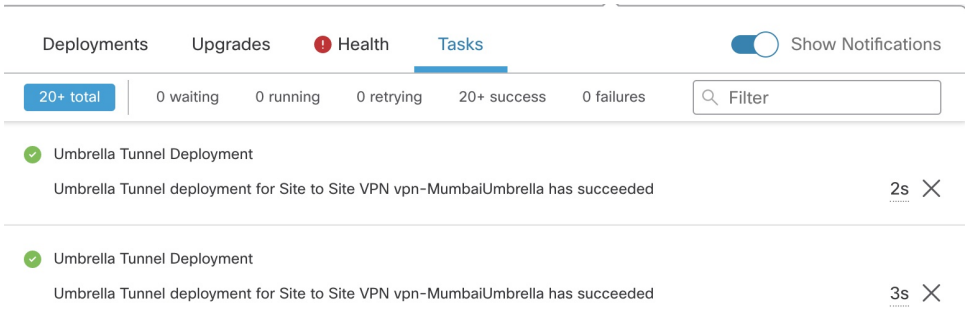
- Pending: The management center hasn't pushed the configuration to Umbrella.
- Success: The management center successfully configured a tunnel on Umbrella.
- In Progress: The management center is deploying the tunnel on Umbrella.
- Failure: The management center couldn't configure a tunnel on Umbrella.

If the status appears as pending, or failure, use the transcript to troubleshoot the tunnel creation. Click the **Transcript** button to view the transcript details such as the APIs, request payload, and the response received from Umbrella.

Step 5 Click **Umbrella Dashboard** to view the network tunnels in Cisco Umbrella.

Step 6 View the Umbrella tunnel deployment status in:

- The **Notifications** page under the **Deployments** and **Tasks** tabs.



- The **Site to Site** VPN dashboard (**Overview** > **Dashboards** > **Site to Site VPN**).

The dashboard provides a summary of the site to site VPN topologies including the Umbrella SASE topologies. You can view the tunnels between the peer devices and the status of each tunnel. You can also troubleshoot any problems with the tunnel deployment using CLI commands and packet tracer.

Monitor site-to-site topologies

This section provides information about the different ways to monitor your site-to-site topologies.

Monitor site-to-site VPNs using Site-to-Site VPN summary page

You can view a summary of your site-to-site VPN topologies in the **Site-to-Site VPN Summary** page. For each topology, you can view details such as VPN type, network topology, VPN interfaces, VPN devices, and tunnel statuses.

You can edit or delete the topology using the edit and delete buttons. For SASE topology VPNs, you have options to deploy, edit and delete any topology.

Monitor site-to-site VPNs using Site-to-Site VPN dashboard

Choose **Overview** > **Dashboards** > **Site to Site VPN** to open the site to site dashboard.

The **Site-to-Site VPN** dashboard provides a snapshot and status of the site-to-site VPN tunnels. You can view the list of tunnels between peer devices and the status of each tunnel: Active, Inactive, or No Active Data. You can filter the data in the table according to the topology, device, and status. The dashboard shows live data and you can also configure the refresh interval.

Benefits of the dashboard

The dashboard provides these benefits:

- Identify problematic VPN tunnels and troubleshoot them.
- Verify connectivity between the site-to-site VPN peers devices.
- Monitor the health of the VPN tunnels to provide uninterrupted VPN connectivity between sites.
- Use Packet tracer to troubleshoot VPN tunnels.

Widgets of the dashboard

- **Tunnel Status**—A table listing the tunnel status of the site-to-site VPNs , including the SASE tunnels for Umbrella, configured using the Firewall Management Center. For more information, refer to Tunnel status widget, on page 1396.
- **Tunnel Summary**—Aggregated status of the tunnels in a donut graph.
- **Topology**—Status of tunnels summarized by topology.

Status of VPN tunnels

The different VPN tunnel statuses that you can view in the Site-to-Site dashboard are:

- **Inactive**—A policy-based (crypto map-based) VPN tunnel is inactive if all the IPSec tunnels are down. A VTI or and SASE topology VPN tunnel is down if the tunnel encounters any configuration or connectivity issues.
- **Active**—In the Firewall Management Center, policy-based site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. A policy-based VPN tunnel is in the Active state if the Firewall Management Center identifies interesting traffic through the tunnel after the deployment. An IKE tunnel is up only if a minimum of one IPsec tunnel is up.

  Route-based VPN (VTI) and SASE topology VPN tunnels do not require interesting traffic to be in the Active state. They are in the Active state if they are configured and deployed without errors.
- **No Active Data**—Policy-based and SASE topology VPN tunnels remain in the No Active Data state until there is a traffic flow event through the tunnel for the first time. The No Active Data state also lists the policy-based and route-based VPNs that have been deployed with errors.

Important notes about tunnel statuses in Firewall Management Center

- The VPN statuses in the Firewall Management Center are event-based. The Firewall Management Center does not initiate status updates. Hence, there might be mismatches between the tunnel statuses in the dashboard and the Firewall Threat Defense . You can view the correct status in the **CLI Details** tab of the **Tunnel Status** widget.
- When a Firewall Threat Defense switches over to a secondary Firewall Threat Defense , there is a mismatch between the status of the VPN tunnels in the Firewall Management Center and the Firewall Threat Defense . When the device switches back to the primary device, the correct tunnel status appears.
- The Firewall Management Center does not update the tunnel status of Firewall Threat Defense devices earlier than 7.3 after the devices reboot. We recommend that you bring the tunnel down using the command **vpn-sessiondb logoff index** and bring it up using the packet tracer.

Limitations of the dashboard

- The table shows the list of site-to-site , including SASE topology, VPNs that are deployed. It does not show the tunnels that are created and not deployed.
- The table does not show the information about the backup tunnels of policy-based VPNs and backup VTIs.
- For cluster deployments, the table does not show director change in real-time data. It shows only the director information that existed when the VPN was deployed. The director change reflects in the table only after the tunnel AM redeployed after the change.

Tunnel status widget

This widget lists the site-to-site VPNs, including SASE topology VPN, configured using the Firewall Management Center and their tunnel statuses.

Features of the widget

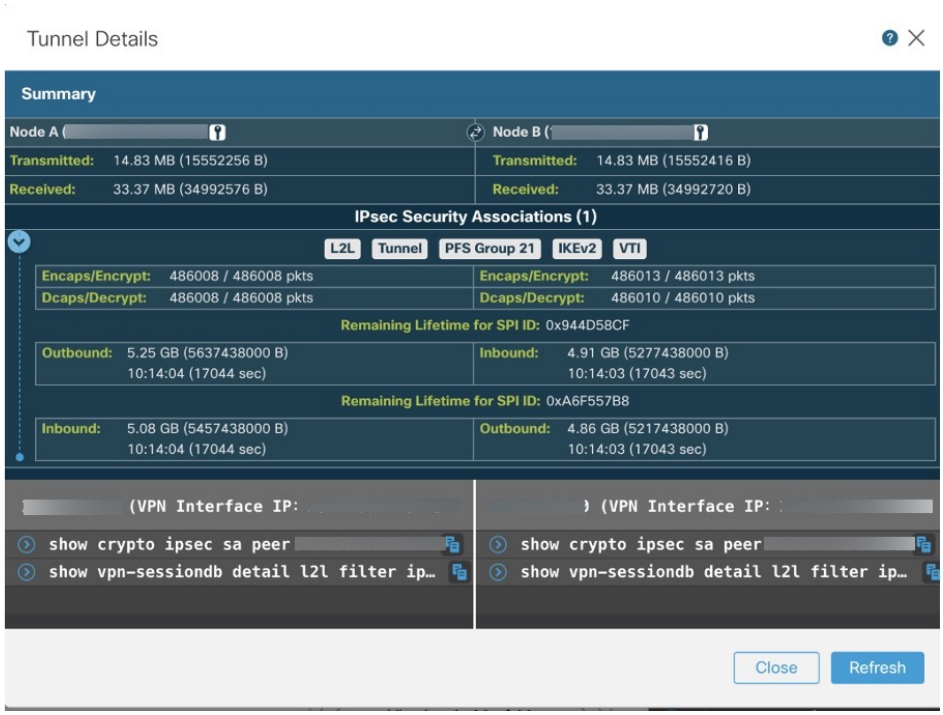
Hover over a topology and click **View** ( ) to view these details about the topology:

- **General**—Displays more information about the nodes such as IP address and interface name.
- **CLI Details**—Displays the CLI outputs for the following commands:
  - **show crypto ipsec sa peer**: Displays the IPsec SAs built between Node A and B.
  - **show vpn-sessiondb l2l filter ipaddress** : Displays information about VPN sessions.

  For an extranet device, no command output appears.

  Important details about the IKE and IPsec sessions, derived from the above command outputs, appear in a summarized, and user-friendly format. You can view the details of both nodes at a time. The icon next to the node name specifies the authentication type: preshared key or client certificate. The details include IKE statistics per tunnel and IPsec SA statistics as shown below:

Figure 396: Tunnel Status > View > CLI Details



- **Packet Tracer**—Use packet tracer to troubleshoot the VPN tunnels.

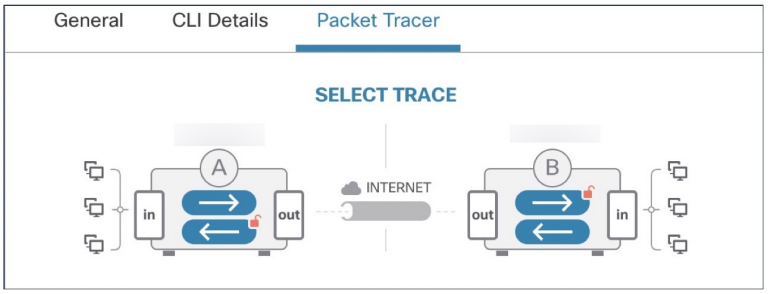
Packet Tracer

Packet tracer allows you to troubleshoot VPN tunnels between two threat defense devices. You can check if the VPN connection between device A and device B is up. This tool performs these actions:

- Injects a packet into the device and tracks the packet flow from the ingress to the egress ports.
- Simulates traffic after you configure the ingress interfaces of the devices along with the protected networks.

- Evaluates the packet against modules such as flow and route lookups, ACLs, protocol inspection, NAT, and QoS.

Figure 397: Packet Tracer



For each device, the tool runs an encrypted trace and a decrypted trace (packet is treated as decrypted VPN traffic). You can run four different traces between the ingress and egress ports of the devices. Click the individual encrypt and decrypt options to enable or disable the trace.

When you run the trace, the tool executes the trace sequentially in the following order:

1. Encrypted trace of A.
2. Decrypted trace of B.
3. Encrypted trace of B.
4. Decrypted trace of A.

After the trace completes, you can view the output of the trace with the results of each module.

Note You cannot run a decrypt trace for route-based (VTI-based) VPNs.

To run the Packet Tracer:

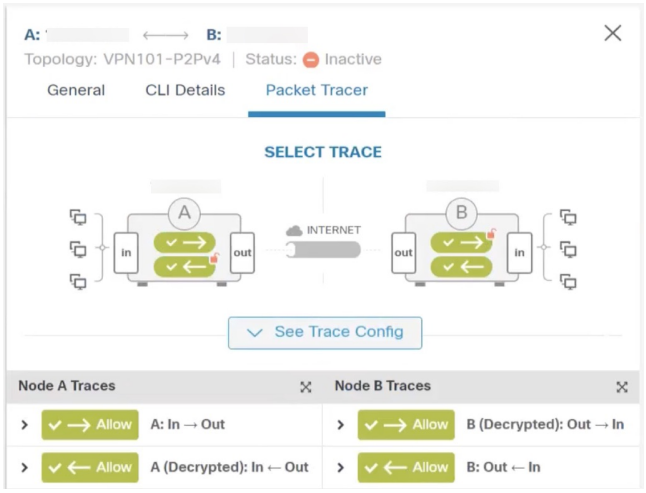
1. Click **See Detailed Config** to view the VPN interface name, VPN interface IP address, VTI interface name, and the VTI Interface IP address.
2. (Optional) Choose a protocol from the **Protocol** drop-down list. You can choose ICMP/8/0, TCP, or UDP.

   ICMP/8/0 is the default option. If you choose ICMP/8/0, 8 indicates the ICMP type as Echo Request and 0 indicates the ICMP code. If you choose TCP or UDP, choose the destination port from the **Destination Port** drop-down list. The range is from 0 to 65535.
3. Choose the ingress interface for both the devices on which to trace the packet from the **Ingress Interface** drop-down lists.
4. Enter an IP address from the same subnet as the ingress interface in the **Protected Network IP Address** fields.
5. Click **Trace Now**.

   After you initiate the trace, you can view if the trace is successful or not for each module. If the tunnel is down, the path appears in red. If the tunnel is up, the path appears in green. If a tunnel is down, click

Re-trace to run the tool again. For a crypto-map based VPN, when the tunnel is inactive with no interesting traffic, the initial trace can be red. Click **Re-trace** to run the trace again.

Figure 398: Packet Tracer after a Successful Trace



Extranet Nodes: You can initiate a packet trace for VPN tunnels with one node as an extranet. For an extranet node, you cannot choose the ingress interface. The remaining steps for the packet trace are the same. You can't run trace on the extranet side.

For example, if Node A is a managed threat defense and Node B is an extranet:

- Configure the ingress interface for node A.
- Configure the protected network for Node A and B.
- Click **Trace Now**. The traces appear for Node A and not for Node B.

Site-to-site VPN connection event monitoring

The site-to-site VPN connection event allows you to know if the VPN encrypts or do not encrypts the connection and helps you to troubleshoot connectivity issues, especially in multi-hop VPN deployments. The event dashboard of the Firewall Management Center displays the IP address of the VPN peer (peer's IKE address) which encrypts or decrypts the traffic and displays the VPN action.

The VPN actions displayed are:

- If the connection is decrypted by the VPN, the column **Decrypt Peer** displays the IP address of the peer's address from where the flow was received and displays **Decrypt** as the VPN action.
- If the connection is encrypted by the VPN, the column **Encrypt Peer** displays the IP address of the VPN peer to which the flow is sent and displays **Encrypt** as the VPN action.
- If the VPN server cascades the connection, it gets decrypted on one tunnel and gets re-encrypted on another tunnel. In this case, both **Encrypt Peer** and **Decrypt Peer** IP addresses get appears in the event. The column **VPN Action** displays **VPN Routing** as the action to indicate that the connection transit through the VPN server.

If you enable the **Bypass Access Control Policy for decrypted traffic (sysopt permit-VPN)** option, the system bypasses the access control policy and do not log events for decrypted traffic. This option is disabled by default and all decrypted traffic in the VPN tunnel undergoes ACL inspection.

View site-to-site VPN connection events

Access the connection event viewer of the Firewall Management Center to know if the VPN encrypts or do not encrypts the connection traffic and to retrieve the VPN peer details.

Before you begin

Ensure that you enable logging of connection events at the beginning of connection and at the end of connection in the access control rule.

Procedure

Step 1 Choose **Analysis** > **Connections** > **Events**.

Step 2 Click **Table View of Connection Events** tab.

Step 3 In the table view of events, multiple fields are hidden by default. To change the fields that appear, click the **x** icon in any column name to display a field chooser.

Step 4 Choose these columns:

- Decrypt Peer
- Encrypt Peer
- VPN Action

Step 5 Click **Apply**.

See *Connection and Security-Related Connection Events* in the Secure Firewall Management Center Administration Guide for more information on the connection events.

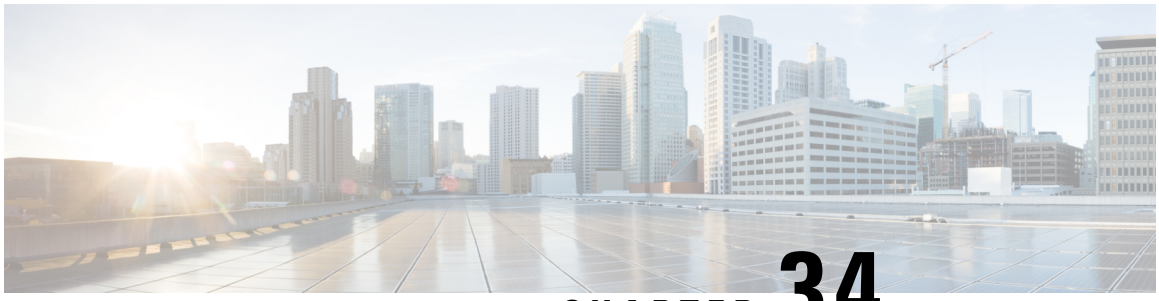
History for site-to-site VPN

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
View Virtual Tunnel Information	7.4.1	Any	You can view details of dynamic and static VTIs of route-based VPNs on the device. For every VPN topology, you can also view details of all the virtual access interfaces of the dynamic VTIs. New/Modified screens: **Device** > **Device Management** > **Edit a device** > **Interfaces** and click the **Virtual Tunnels** tab.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
IPsec flow offload	7.4	Any	IPsec flow offload is automatically enabled on the VTI loopback interface on Secure Firewall 3100 and Secure Firewall 4200 devices.
Umbrella SASE Topology	7.3	Any	You can configure an Umbrella SASE topology and deploy IPsec IKEv2 tunnels between a threat defense device and Umbrella. This tunnel forwards all internet-bound traffic to the Umbrella Secure Internet Gateway (SIG) for inspection and filtering.
Support for Dynamic Virtual Tunnel Interface	7.3	Any	You can create a dynamic VTI and use it to configure a route-based site-to-site VPN in a hub and spoke topology.
EIGRP IPv4 support for VTI	7.3	Any	Static and dynamic VTI interfaces support EIGRP IPv4 routing protocol.
OSPFv2/v3 IPv4/v6 support for VTI	7.3	Any	Static and dynamic VTI interfaces support OSPFv2/v3 IPv4/v6 routing protocol.
Packet Tracer in Site to Site VPN Monitoring Dashboard	7.3	Any	Use the packet tracer tool in the site-to-site VPN monitoring dashboard to troubleshoot the threat defense VPN tunnels. New/Modified screens: **Overview** > **Dashboards** > **Site to Site VPN**
Remote Access VPN Dashboard	7.3	Any	Use the Remote Access VPN dashboard to monitor real-time data from active remote access VPN sessions on the devices. New/Modified screens: **Overview** > **Dashboards> Remote Access VPN**
IPsec flow offload	7.2	Any	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.
Site-to-Site VPN Filter	7.1	Any	You can control site-to-site VPN traffic by using an access control policy.
Local tunnel ID support	7.1	Any	For each endpoint on a site-to-site VPN, you can configure a unique tunnel ID to be shared with the peers.
Multiple IKE Policy Support	7.1	Any	You can add multiple IKEv1 and IKEv2 policy objects for each endpoint.
Site-to-Site VPN Monitoring Dashboard	7.1	Any	Use the Site-to-Site VPN Monitoring dashboard to view and monitor the status of site-to-site VPN tunnels.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	7.0	Any	When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel. Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider. You can add a backup VTI in the site-to-site VPN wizard by selecting route-based as the VPN type for a point-to-point connection.
Enhance the number of VTI from 100 per interface to 1024 per device	7.0	Any	Support for maximum number of VTIs is enhanced from 100 per physical interface to 1024 VTIs per device.
IPv6 Support	7.0	Any	You can configure IPv6 addressed VTIs. While only static IPv6 address is supported as the tunnel source and destination, IPv6 BGP isn't supported over VTI.
Removal and deprecation of weak ciphers	6.7	Any	Support has been removed for less secure ciphers. We recommend that you update your VPN configuration before you upgrade to Firewall Threat Defense 6.70 to supported DH and encryption algorithms to ensure the VPN works correctly. Update your IKE proposals and IPSec policies to match the ones supported in Firewall Threat Defense 6.70 and then deploy the configuration changes. These less secure ciphers have been removed or deprecated in Firewall Threat Defense 6.70 onwards: • **Diffie-Hellman Group 5** is deprecated for IKEv1 and removed for IKEv2 • Diffie-Hellman groups 2 and 24 have been removed. • **Encryption algorithms**: 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256 have been removed. **Note** **DES** is supported in evaluation mode or for users who do not satisfy export controls for strong encryption. **NULL** is removed in IKEv2 policy, but supported in both IKEv1 and IKEv2 IPsec transform-sets.
Dynamic RRI support	6.7	Any	Dynamic Reverse Route Injection is supported with IKEv2 based static crypto maps.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Backup peer for site-to-site VPN	6.6	Any	You can use the Firewall Management Center to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. New/modified pages: **Devices** > **VPN** > **Site to Site**. When adding or editing a point to point or hub and spoke FTD VPN topology to add an endpoint, the **IP Address** field supports comma-separated backup peers.



CHAPTER 34

SD-WAN

This chapter describes the SD-WAN capabilities supported in Management Center.

- SD-WAN capabilities, on page 1405
- SD-WAN features, on page 1406
- Use cases for SD-WAN capabilities, on page 1407
- Monitor SD-WAN topologies, on page 1408

SD-WAN capabilities

SD-WAN capabilities are software-defined networking features that

- replace traditional WAN routers and are agnostic to WAN transport technologies
- provide dynamic, policy-based, application path selection across multiple WAN connections, and
- support service chaining for additional services such as WAN optimization and firewalls.

SD-WAN capabilities in Secure Firewall

As organizations expand their operations across multiple branch locations, ensuring secure and streamlined connectivity becomes paramount. Deploying a secure branch network infrastructure involves complex configurations, which can be time-consuming and prone to configuration errors if not handled properly. However, organizations can overcome these challenges by leveraging Management Center and Threat Defense devices for a simplified and secure branch deployment.

By integrating Secure Firewall as a foundational component of the branch network architecture, organizations can establish a strong security baseline while simplifying the deployment process. This approach enables organizations to enforce unified security policies, optimize traffic routing, and ensure resilient connectivity.

Some of the SD-WAN capabilities supported on the Cisco Secure Firewall include:

- **Simplified management:**
  - SASE: Umbrella auto tunnel deployment
  - Dynamic VTI (DVTI) hub spoke topology simplification
- **Application awareness:**
  - Direct Internet Access (DIA) for public cloud and guest user

- Policy based routing (PBR) using applications as a match criteria
- Local tunnel ID support for Umbrella

- **Increased usable bandwidth:**
  - ECMP support for load balancing across multiple ISPs and VTIs
  - Application-based load balancing using PBR

- **High availability with near zero network downtime:**
  - Dual ISP configuration
  - Optimal path selection based on application-based interface monitoring.

- **Secure elastic connectivity:**
  - Route-based (VTI) VPN tunnels between headquarters (hub) and branches (spokes)
  - IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP over VTI
  - DVTI hubs that support spokes with static or dynamic IP

SD-WAN features

This table lists the SD-WAN features of Management Center, including their introduction releases and links to detailed information.

Feature	Introduced in	More Information
Application monitoring using SD-WAN Summary dashboard	Release 7.4.1	SD-WAN summary dashboard, on page 1408
SD-WAN Summary Dashboard	Release 7.4	SD-WAN summary dashboard, on page 1408
Policy-based routing with user identity and SGTs	Release 7.4	Policy-Based Routing, on page 1159
Policy-based routing using HTTP path monitoring	Release 7.4	Policy-Based Routing, on page 1159
Loopback interface support for VTIs	Release 7.3	Loopback interfaces, on page 661
Support for dynamic VTI (DVTI) with site-to-site VPN	Release 7.3	Dynamic VTI, on page 1366
Umbrella auto tunnel	Release 7.3	Deploy a SASE Tunnel on Umbrella

Feature	Introduced in	More Information
Support for IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP for VTIs	Release 7.3	BGP, on page 1107 OSPF, on page 1063 EIGRP, on page 1095
Route-based site-to-site VPN with hub and spoke topology	Release 7.2	Create a route-based site-to-site VPN, on page 1373
Policy-based routing with path monitoring	Release 7.2	Policy-Based Routing, on page 1159
Site to Site VPN Monitoring Dashboard	Release 7.1	Monitor Site-to-Site VPNs Using Site-to-Site VPN Dashboard
Direct Internet Access/Policy Based Routing	Release 7.1	Policy-Based Routing, on page 1159
Equal-Cost-Multi-Path (ECMP) zone with WAN interfaces	Release 7.1	ECMP, on page 1047
ECMP zone with VTI interfaces	Release 7.1	ECMP, on page 1047
Backup VTI for route-based site-to-site VPN	Release 7.0	Route traffic through a backup VTI tunnel, on page 1383
Support for static VTI (SVTI) with site-to-site VPN	Release 6.7	Static VTI, on page 1365

Use cases for SD-WAN capabilities

Use the Cisco Secure Firewall Threat Defense SD-WAN Design and Deployment Guide to design and deploy SD-WAN architectures using Firewall Threat Defense and Firewall Management Center. This guide explains design principles, configuration workflows, and best practices.

Use these guides for detailed instructions for the primary use cases leveraging the SD-WAN capabilities supported by Cisco Secure Firewall.

- Simplify Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)
- Route Application Traffic from the Branch to the Internet Using Direct Internet Access (DIA)
- Secure Internet Traffic Using Umbrella Auto Tunnel
- Empower Remote Workers with Secure Connectivity: DIA, Umbrella Auto Tunnel, and DVTI in Action
- Set Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates
- Set Up SD-WAN Branch Office with Dual ISPs Using Serial Numbers and Device Template

Monitor SD-WAN topologies

This section provides information about the different ways to monitor your SD-WAN topologies.

SD-WAN summary dashboard

The SD-WAN Summary dashboard (**Overview** > **Dashboards** > **SD-WAN Summary**) provides a snapshot of your WAN devices and their interfaces. This dashboard helps you to:

- Identify issues with the underlay and overlay (VPN) topologies.
- Troubleshoot VPN issues using the existing **Health Monitoring**, **Device Management**, and **Site-to-Site Monitoring** pages.
- Monitor application performance metrics of WAN interfaces. The threat defense steers application traffic based on these metrics.

For clusters, this dashboard displays application performance metrics of only the control node and not the data nodes.

WAN device criteria

A WAN device must meet one of these criteria:

- The device must be a VPN peer.
- The device must have WAN interface.

WAN interface criteria

A WAN interface must meet one of these criteria:

- The interface has IP address-based path monitoring enabled on it.
- The interface has a Policy Based Routing (PBR) policy with at least one application configured to monitor it.

For more information about PBR policy and path monitoring, see Policy-Based Routing, on page 1159.

Uplink decisions

Click **Uplink Decisions** to view the **VPN Troubleshooting** page. You can view syslogs with ID: 880001. These syslogs show the threat defense interfaces through which it steers traffic based on the configured PBR policy.

To view the above syslogs and to view the data on this dashboard, ensure that you review Prerequisites for using SD-WAN summary dashboard, on page 1408.

Prerequisites for using SD-WAN summary dashboard

Ensure that you review these prerequisites before using the SD-WAN summary dashboard.

General prerequisites

- You must be an Admin, Security Analyst, or Maintenance user to view this dashboard.
- Threat Defense devices must be Version 7.2 or later.
- Enable IP-based path monitoring and HTTP-based application monitoring on the WAN interfaces.

  To do this:

  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click the edit icon adjacent to the interface that you want to edit.
  4. Click the **Path Monitoring** tab.
  5. Check the **Enable IP based Monitoring** check box.
  6. Check the **Enable HTTP based Application Monitoring** check box.
  7. Click **OK**.

- Configure a PBR policy with at least one application configured to monitor it:

  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **Policy Based Routing**.
  5. Click **Add**.
  6. From the **Ingress Interface** drop-down list, choose an interface.
  7. Click **Add** to configure a forwarding action.
  8. Configure the parameters.
  9. Click **Save**.

- To view syslogs when you click **Uplink Decisions**, you must:
  - Choose **Devices** > **Platform Settings** and create or edit a threat defense policy.
  - In the left pane, click **Syslog**.
  - Click the **Logging Setup** tab.
  - Check the **Enable Logging** check box to turn on the data plane system logging for the threat defense device.
  - Click the **All Logs** radio button to enable logging of all the troubleshooting syslog messages.

    or

    Click the **VPN Logs** radio button to enable logging of only the VPN troubleshooting messages.
  - Click **Save**.

Prerequisites to view application performance metrics in the dashboard

- Threat Defense devices must be Version 7.4.1.
- Enable data collection from the SD-WAN module in the health policy.
  1. Choose **System** (⚙) > **Health** > **Policy**.
  2. Click the **Edit health policy** icon.
  3. In the **Health Modules** tab, under **SD-WAN**, click the **SD-WAN Monitoring** toggle button.
- Configure applications for the PBR policies.
  1. Choose **Objects** > **Object Management** > **Access List** > **Extended**.
  2. Click the edit icon adjacent to the access list and add the applications for the PBR policy.
- Configure the forwarding action for the policy with one of the four application metrics.
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **Policy Based Routing**.
  5. Click the edit icon adjacent to the policy that you want to edit.
  6. In the **Edit Policy Based Route** dialog box, click the edit icon adjacent to the corresponding ACL.
  7. In the **Edit Forwarding Actions** dialog box, from the **Interface Ordering** drop-down list, choose one of these options:
     - **Minimal Jitter**
     - **Maximum Mean Opinion Score**
     - **Minimal Round-Trip Time**
     - **Minimal Packet Loss**

     If you choose **Interface Priority** or **Order**, application monitoring is not enabled on the interface.
- Configure ECMP on the WAN interfaces:
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **ECMP**.
  5. Click **Add** and specify a name for the ECMP zone.
  6. Click **Add** to move interfaces from **Available Interfaces** to **Selected Interfaces**.
  7. Click **OK**.

- Ensure that traffic passes through the interface.
- Enable DNS inspection on each WAN device so that the Threat Defense device can do DNS snooping, and configure the trusted DNS servers:
  1. Choose **Devices** > **Platform Settings**.
  2. Click the edit icon adjacent to the threat defense policy that you want to edit.
  3. In the left pane, click **DNS**.
  4. Click the **DNS Settings** tab.
  5. Check the **Enable DNS name resolution by device** check box.
  6. Click the **Trusted DNS Servers** tab.
  7. Do one of these options:
     - Click the **Trust Any DNS server** toggle button.
     - Under **Specify DNS Servers**, click **Edit** to add trusted DNS servers.

Monitor WAN devices and interfaces using the SD-WAN summary dashboard

The SD-WAN Summary dashboard has these widgets under the **Overview** tab:

- Top applications, on page 1411
- WAN connectivity, on page 1411
- VPN topology, on page 1412
- interface throughput, on page 1412
- Device inventory, on page 1412
- WAN device health, on page 1412

Top applications

This widget displays the top 10 applications ranked according to throughput.

You can choose a time range for the widget data from the **Show Last** drop-down list. The range is 15 minutes to two weeks.

WAN connectivity

This widget provides a summary of the WAN interfaces statuses. It shows the number of WAN interfaces that are in the **Online**, **Offline** or **No Data** states. Note that you cannot monitor subinterfaces using this widget.

Click **View All Interfaces** to view more details about the interfaces in the health monitor page.

If a WAN interface is in the **Offline** or **No Data** state, you can troubleshoot it from the health monitor page:

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.

3. Click the **Interface** tab to view the interface status and aggregate traffic statistics for a specific time.

   Alternatively, you can click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

VPN topology

This widget provides a summary of the site-to-site VPN tunnel statuses. It shows the number of **Active**, **Inactive**, and **No Active Data** VPN tunnels.

Click **View All Connections** to view the VPN tunnel details in the **Site-to-site VPN Monitoring** dashboard.

If the tunnels are in the **Inactive** or **No Active Data** state, you can troubleshoot using the **Site-to-site VPN Monitoring** dashboard. In the **Tunnel Status** widget, hover your cursor over a topology, click **View** ( ) and do one of these actions:

- Click the **CLI Details** tab to view the details of the VPN tunnels.
- Click the **Packet Tracer** tab to use the packet tracer tool for the topology.

interface throughput

This widget monitors the average throughput of the WAN interfaces during the chosen time period.

The interface throughput is classified into four bands. These details aid in cost planning and resourcing. You can choose a time range for the widget data from the **Show Last** drop-down list. The range is from 15 minutes to two weeks.

Click **View Health Monitoring** to view more details about the interface in the health monitor page.

Device inventory

This widget lists all the managed WAN devices and groups them according to the model.

Click **View Device Management** to view more details about the device in the **Device Management** page.

WAN device health

This widget displays the device count according to the health of the WAN devices. You can view the number of devices with errors, warnings, or those that are in **Disabled** state.

Click **View Health Monitoring** to view the alarms, and quickly identify, isolate, and resolve issues.

If the health of a device is affected, you can troubleshoot it from the health monitor page.

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

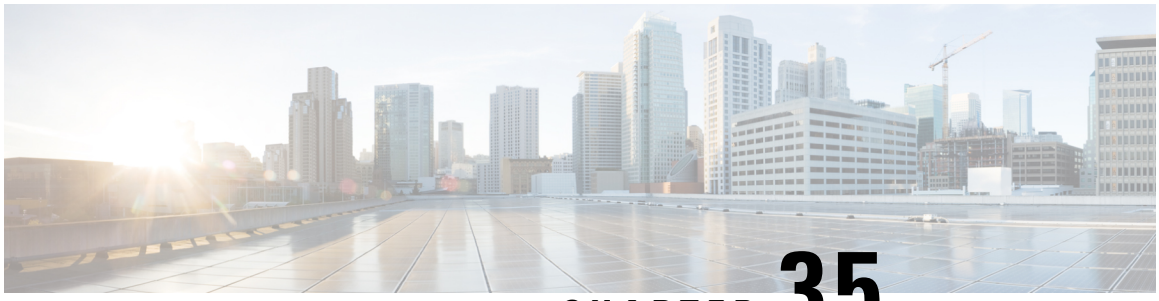
A device can be in **Disabled** state for multiple reasons, including these:

- Management interface is disabled.
- Device is powered off.
- Device is being upgraded.

Monitor application performance metrics of WAN interfaces using SD-WAN summary dashboard

You can monitor application performance metrics of WAN interfaces using the **Application Monitoring** tab of the SD-WAN Summary dashboard. These metrics include Jitter, Round Trip Time (RTT), Mean Opinion Score (MOS), and Packet Loss.

By default, the metrics data is refreshed every 5 minutes. You can change the refresh time; the range is from 5 to 30 minutes. You can view the metrics in tabular and graphical formats. For each WAN interface, the latest metric value appears in the table. For graphical data, you can choose a time interval of up to 24 hours to view the metrics data for the corresponding WAN interfaces.



CHAPTER 35

Remote Access VPN

Remote Access virtual private network (VPN) allows individual users to connect to your network from a remote location using a computer or other supported devices connected to the Internet. This allows mobile workers to connect from their home networks or a public Wi-Fi network, for example.

The following topics explain how to configure remote access VPN for your network.

- Remote Access VPN Overview, on page 1415
- License Requirements for Remote Access VPN, on page 1421
- Requirements and Prerequisites for Remote Access VPN, on page 1421
- Guidelines and Limitations for Remote Access VPNs, on page 1422
- Configuring a New Remote Access VPN Connection, on page 1425
- Create a Copy of an Existing Remote Access VPN Policy, on page 1435
- Set Target Devices for a Remote Access VPN Policy, on page 1435
- Associate Local Realm with Remote Access VPN Policy, on page 1436
- Additional Remote Access VPN Configurations, on page 1436
- Customizing Remote Access VPN AAA Settings, on page 1490
- Advanced Secure Client Configurations, on page 1511
- Remote Access VPN Examples, on page 1519
- Monitor Remote Access VPNs, on page 1524
- History for Remote Access VPNs, on page 1526

Remote Access VPN Overview

Secure Firewall Threat Defense provides secure gateway capabilities that support remote access SSL and IPsec-IKEv2 VPNs. The full tunnel client, Secure Client, provides secure SSL and IPsec-IKEv2 connections to the security gateway for remote users. When the client negotiates an SSL VPN connection with Firewall Threat Defense, it connects using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS)

Secure Client is the only client supported on endpoint devices for remote VPN connectivity to Firewall Threat Defense devices. The client gives remote users the benefits of an SSL or IPsec-IKEv2 VPN client without the need for network administrators to install and configure clients on remote computers. The Secure Client for Windows, Mac, and Linux is deployed from the secure gateway upon connectivity. The Secure Client apps for Apple iOS and Android devices are installed from the platform app store.

Use the Remote Access VPN policy wizard to set up SSL and IPsec-IKEv2 remote access VPNs with basic capabilities. Then, enhance the policy configuration as you want and deploy it to your Firewall Threat Defense secure gateway devices.

Remote Access VPN Features

The following table describes the features of Secure Firewall Threat Defense remote access VPN:

Table 79: Remote access VPN features

	Description
Secure Firewall Threat Defense remote access VPN features	• SSL and IPsec-IKEv2 remote access using the Secure Client. • Secure Firewall Management Center supports all combinations such as IPv6 over an IPv4 tunnel. • Configuration support on both Firewall Management Center and Firewall Device Manager. Device-specific overrides. • Support for both Secure Firewall Management Center and Firewall Threat Defense HA environments. • Support for multiple interfaces and multiple AAA servers. • Rapid Threat Containment support using RADIUS CoA or RADIUS dynamic authorization. • Support for DTLS v1.2 protocol with Cisco Secure Client version 4.7 or higher. • Secure Client modules support for additional security services for remote access VPN connections. • VPN load balancing.

	Description
AAA features	• Server authentication using self-signed or CA-signed identity certificates. • AAA username and password-based remote authentication using RADIUS server or LDAP or AD. • RADIUS group and user authorization attributes, and RADIUS accounting. • Double authentication support using an additional AAA server for secondary authentication. • NGFW Access Control integration using VPN Identity. • LDAP or AD authorization attributes using Secure Firewall Management Center web interface. • Support for single sign-on using SAML 2.0. • Support for multiple identity provider trustpoints with Microsoft Azure that can have multiple applications for the same Entity ID, but a unique identity certificate.
VPN tunneling features	• Address assignment. • Split tunneling. • Split DNS. • Client Firewall ACLs. • Session Timeouts for maximum connect and idle time.
Remote access VPN monitoring features	• New VPN Dashboard Widget showing VPN users by various characteristics such as duration and client application. • Remote access VPN events including authentication information such as username and OS platform. • Tunnel statistics available using the Firewall Threat Defense Unified CLI.

Secure Client Components

Secure Client Deployment

Your remote access VPN policy can include the Secure Client Image and the Secure Client Profile for distribution to connecting endpoints. Or, the client software can be distributed using other methods. See the *Deploy Cisco Secure Client* chapter in the Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.

Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL or IPsec-IKEv2 VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, remote users must enter the URL in the form https://*address*. After the user enters the URL, the browser connects to that interface and displays the login screen.

After a user logs in, if the secure gateway identifies the user as requiring the VPN client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure connection, and either remains or uninstalls itself (depending on the security appliance configuration) when the connection stops. In the case of a previously installed client, after login, the Firewall Threat Defense security gateway examines the client version and upgrades it as necessary.

Secure Client Operation

When the client negotiates a connection with the security appliance, the client connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

When an IPsec-IKEv2 VPN client initiates a connection to the secure gateway, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). The group profile is pushed to the VPN client and an IPsec security association (SA) is created to complete the VPN.

Secure Client Profile and Editor

The Secure Client Profile is a group of configuration parameters, stored in an XML file that the VPN client uses to configure its operation and appearance. These parameters (XML tags) include the names and addresses of host computers and settings to enable more client features.

You can configure a profile using the Secure Client Profile Editor. This editor is a convenient GUI-based configuration tool that is available as part of the Secure Client software package. It is an independent program that you run outside of the Firewall Management Center.

Remote Access VPN Authentication

Remote Access VPN Server Authentication

Secure Firewall Threat Defense secure gateways always use certificates to identify and authenticate themselves to the VPN client endpoint.

While you use the Remote Access VPN Policy Wizard, you can enroll the selected certificate on the targeted Firewall Threat Defense device. In the wizard, under **Access & Certificate** phase, select “Enroll the selected certificate object on the target devices” option. The certificate enrollment gets automatically initiated on the specified devices. As you complete the remote access VPN policy configuration, you can view the status of

the enrolled certificate under the device certificate homepage. The status provides a clear standing as to whether the certificate enrollment was successful or not. Your remote access VPN policy configuration is now fully completed and ready for deployment.

Obtaining a certificate for the secure gateway, also known as PKI enrollment, is explained in Certificates, on page 2481. This chapter contains a full description of configuring, enrolling, and maintaining gateway certificates.

Remote Access VPN Client AAA

For both SSL and IPsec-IKEv2, remote user authentication is done using usernames and passwords only, certificates only, or both.



Note If you are using client certificates in your deployment, they must be added to your client's platform independent of the Secure Firewall Threat Defense or Secure Firewall Management Center. Facilities such as SCEP or CA Services are not provided to populate your clients with certificates.

AAA servers enable managed devices acting as secure gateways to determine who a user is (authentication), what the user is permitted to do (authorization), and what the user did (accounting). Some examples of the AAA servers are RADIUS, LDAP/AD, TACACS+, and Kerberos. For Remote Access VPN on Firewall Threat Defense devices, AD, LDAP, and RADIUS AAA servers are supported for authentication.

Refer to the section Understanding Policy Enforcement of Permissions and Attributes to understand more about remote access VPN authorization.

Before you add or edit the remote access VPN policy, you must configure the Realm and RADIUS server groups you want to specify. For more information, see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860 and Add a RADIUS server group, on page 2346.

Without DNS configured, the device cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames, it can only resolve IP addresses.

The login information provided by a remote user is validated by an LDAP or AD realm or a RADIUS server group. These entities are integrated with the Secure Firewall Threat Defense secure gateway.



Note If users authenticate with remote access VPN using Active Directory as the authentication source, users must log in using their username; the format `domain\username` or `username@domain` fails. (Active Directory refers to this username as the *logon name* or sometimes as `sAMAccountName`.) For more information, see User Naming Attributes on MSDN.

If you use RADIUS to authenticate, users can log in with any of the preceding formats.

Once authenticated via a VPN connection, the remote user takes on a *VPN Identity*. This VPN Identity is used by *identity policies* on the Secure Firewall Threat Defense secure gateway to recognize and filter network traffic belonging to that remote user.

Identity policies are associated with access control policies, which determine who has access to network resources. It is in this way that the remote user blocked or allowed to access your network resources.

For more information, see the Identity policies, on page 1941 and Access Control Policies, on page 1569 sections.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 1439

Understanding Policy Enforcement of Permissions and Attributes

The Secure Firewall Threat Defense device supports applying user authorization attributes (also called user entitlements or permissions) to VPN connections from an external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the Firewall Threat Defense device. If the Firewall Threat Defense device receives attributes from the external AAA server that conflicts with those configured on the group policy, then attributes from the AAA server always take the precedence.

The Firewall Threat Defense device applies attributes in the following order:

1. **User attributes on the external AAA server**—The server returns these attributes after successful user authentication and/or authorization.
2. **Group policy configured on the Firepower Threat Defense device**—If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the Firewall Threat Defense device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.
3. **Group policy assigned by the Connection Profile (also known as Tunnel Group)**—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication.



Note The Firewall Threat Defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. The attributes on the group policy assigned to the connection profile are used for the user session, if they are not overridden by user attributes or the group policy from the AAA server as indicated above.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 1439

Understanding AAA Server Connectivity

LDAP, AD, and RADIUS AAA servers must be reachable from the Firewall Threat Defense device for your intended purposes: user-identity handling only, VPN authentication only, or both activities. AAA servers are used in remote access VPN for the following activities:

- **User-identity handling**— the servers must be reachable over the Management interface.

  On the Firewall Threat Defense, the Management interface has a separate routing process and configuration from data interfaces.

- **VPN authentication**—the servers must be reachable over a data interface or the Management interface.

  To use the Management interface, you must explicitly select Management as the source interface. Other management-only interfaces cannot be used.

To use the same AAA servers for both activities, we recommend specifying the Management interface as the source interface.

For more information about various interfaces, see Regular Firewall Interfaces, on page 649.

After deployment, use the following CLI commands to monitor and troubleshoot AAA server connectivity from the Firewall Threat Defense device:

- **show aaa-server** to display AAA server statistics.
- **show network** and **show network-static-routes** to view the Management interface default route and static routes.
- **show route** to view data traffic routing table entries.
- **ping system** and **traceroute system** to verify the path to the AAA server through the Management interface.
- **ping interface** *ifname* and **traceroute** *destination* to verify the path to the AAA server through the data interfaces.
- **test aaa-server authentication** and **test aaa-server authorization** to test authentication and authorization on the AAA server.
- **clear aaa-server statistics** *groupname* or **clear aaa-server statistics protocol** *protocol* to clear AAA server statistics by group or protocol.
- **aaa-server** *groupname* **active host** *hostname* to activate a failed AAA server, or **aaa-server** *groupname* **fail host** *hostname* to fail a AAA server.
- **debug ldap level**, **debug aaa authentication**, **debug aaa authorization**, and **debug aaa accounting**.

License Requirements for Remote Access VPN

Threat Defense License

Firewall Threat Defense remote access VPN requires Strong Encryption and one of the following licenses for Secure Client:

- Secure Client Advantage
- Secure Client Premier
- Secure Client VPN Only

Requirements and Prerequisites for Remote Access VPN

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

Guidelines and Limitations for Remote Access VPNs

Remote Access VPN Policy Configuration

- You can add a new remote access VPN policy only by using the wizard. You must proceed through the entire wizard to create a new policy; the policy will not be saved if you cancel before completing the wizard.
- Two users must **not** edit a remote access VPN policy at the same time; however, the web interface does not prevent simultaneous editing. If this occurs, the last saved configuration persists.
- Moving a Secure Firewall Threat Defense device from one domain to another domain is not possible if remote access VPN policy is assigned to that device.
- Remote access VPN does not support SSL while using ECMP. We recommend that you use IPsec-IKEv2.
- Remote access VPN does not support clustering.
- Remote access VPN connectivity could fail if there is a misconfigured Firewall Threat Defense NAT rule.
- If you are using DHCP to provide IP addresses to the client, and the client cannot obtain an address, check the NAT rules. Any NAT rule that applies to the RA VPN network should include the route lookup option. Route lookup can help ensure the DHCP requests are sent to the DHCP server through an appropriate interface.
- Whenever IKE ports 500/4500 or SSL port 443 is in use or when there are some PAT translations that are active, the Secure Client IPSec-IKEv2 or SSL remote access VPN cannot be configured on the same port as it fails to start the service on those ports. These ports must not be used on the Firewall Threat Defense device before configuring remote access VPN policy.
- While configuring remote access VPNs using the wizard, you can create in-line certificate enrollment objects, but you cannot use them to install the identity certificate. Certificate enrollment objects are used for generating the identity certificate on the Firewall Threat Defense device being configured as the remote access VPN gateway. Install the identity certificate on the device before deploying the remote access VPN policy to the device.

  For more information about how to install the identity certificate based on the certificate enrollment object, see Use the object manager, on page 2334.
- The ECMP zone interfaces can be used in remote access VPN with IPsec enabled.
- The ECMP zone interfaces cannot be used in remote access VPN with SSL enabled. Deployment of remote access VPN (SSL enabled) configuration fails if all the remote access VPN interfaces that belong to security zones or interface groups also belong to one or more ECMP zones. However, if only some of the remote access VPN interfaces belonging to the security zones or interface groups also belongs to one or more ECMP zones, deployment of the remote access VPN configuration succeeds excluding those interfaces.
- After you change the remote access VPN policy configurations, re-deploy the changes to the Firewall Threat Defense devices. The time it takes to deploy configuration changes depends on multiple factors such as complexity of the policies and rules, type and volume of configurations you send to the device, and memory and device model. Before deploying remote access VPN policy changes, review the Best practices for deploying configuration changes, on page 133.

- Issuing commands such as **curl** against the RA VPN headend is not directly supported, and might not have desirable results. For example, the headend does not respond to HTTP HEAD requests.
- Firewall Threat Defense does not accept remote access VPN sessions if the third-party client sends a null user agent.
- You can configure browser proxy using FlexConfig.
- When **Bypass Access Control policy for decrypted traffic** is disabled on a Firewall Threat Defense and ISE issues a DACL, traffic is first matched against the ACP: if permitted, it proceeds to DACL checking; if denied, it bypasses DACL matching.

Concurrent VPN Sessions Capacity Planning (Firewall Threat Defense Virtual Models)

The maximum concurrent VPN sessions are governed by the installed Firewall Threat Defense Virtual smart-licensed entitlement tier, and enforced via a rate limiter. There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the licensed device model. This limit is designed so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firewall Threat Defense Virtual5	50
Firewall Threat Defense Virtual10	250
Firewall Threat Defense Virtual20	250
Firewall Threat Defense Virtual30	250
Firewall Threat Defense Virtual50	750
Firewall Threat Defense Virtual100	10,000

Concurrent VPN Sessions Capacity Planning (Hardware Models)

The maximum concurrent VPN sessions are governed by platform-specific limits and have no dependency on the license. There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the device model. This limit is designed so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100, all models	10,000
Firepower 9300 appliance, all models	20,000
ISA 3000	25

For capacity of other hardware models, contact your sales representative.



Note The Firewall Threat Defense device denies the VPN connections once the maximum session limit per platform is reached. The connection is denied with a syslog message. Refer the syslog messages %ASA-4-113029 and %ASA-4-113038 in the syslog messaging guide. For more information, see Cisco Secure Firewall ASA Series Syslog Messages.

Controlling Cipher Usage for VPN

To prevent use of ciphers greater than DES, pre-deployment checks are available at the following locations in the Firewall Management Center:

Devices > **Platform Settings**, click **Edit** and then **SSL**.

Devices > **VPN** > **Remote Access**, click **Edit**, and then from **Advanced** drop-down list, choose **IPsec**.

For more information about SSL settings and IPsec, see Configure SSL settings, on page 884 and Configure Remote Access VPN IPsec/IKEv2 Parameters, on page 1471.

Authentication, Authorization, and Accounting

Configure DNS on each device in the topology in to use remote access VPN. Without DNS, the device cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames; it can only resolve IP addresses.

You can configure DNS using the **Platform Settings**. For more information, see Configure DNS server settings, on page 852 and DNS server groups, on page 2366.

Client Certificates

If you are using client certificates in your deployment, they must be added to your client's platform independent of the Secure Firewall Threat Defense or Secure Firewall Management Center. Facilities such as SCEP or CA Services are not provided to populate your clients with certificates.

Unsupported Features of Secure Client

The only supported VPN client is the Cisco Secure Client. No other clients or native VPNs are supported. Clientless VPN is not supported for VPN connectivity; it is only used to deploy the Secure Client using a web browser.

Note Using multiple Secure Client packages on Firewall Threat Defense devices can increase memory usage and affect the device's performance. We recommend that you do not use multiple Secure Client packages on low-end threat defense devices to avoid continuous reboots because of memory exhaustion.

The following Secure Client features are not supported when connecting to a Firewall Threat Defense secure gateway:

- TACACS, Kerberos (KCD Authentication and RSA SDI), and SDI.

Configuring a New Remote Access VPN Connection

This section provides instructions to configure a new remote access VPN policy with Secure Firewall Threat Defense devices as VPN gateways and Cisco Secure Client as the VPN client.

Step	Do This	More Info
1	Review the guidelines and prerequisites.	Guidelines and Limitations for Remote Access VPNs, on page 1422 Prerequisites for Configuring Remote Access VPN, on page 1426
2	Create a new remote access VPN policy using the wizard.	Create a New Remote Access VPN Policy, on page 1426
3	Update the access control policy deployed on the device.	Update the Access Control Policy on the Secure Firewall Threat Defense Device, on page 1429
4	(Optional) Configure a NAT exemption rule if NAT is configured on the device.	(Optional) Configure NAT Exemption, on page 1430
5	Configure DNS.	Configure DNS, on page 1431
6	Add Secure Client Profile.	Add Secure Client Profile XML File, on page 1431
7	Deploy the remote access VPN policy.	Deploy configuration changes, on page 135
8	(Optional) Verify the remote access VPN policy configuration.	Verify the Configuration, on page 1434

Prerequisites for Configuring Remote Access VPN

- Deploy Secure Firewall Threat Defense devices and configure Secure Firewall Management Center to manage the device with required licenses with export-controlled features enabled. For more information, see VPN licensing, on page 1334.
- Configure the certificate enrollment object that is used to obtain the identity certificate for each Firewall Threat Defense device that act as a remote access VPN gateway.
- Configure any AD or LDAP realms being used by remote access VPN policies.
- Ensure that the AAA server is reachable from the Firewall Threat Defense device. Configure routing (**Devices** > **Device Management**, click the **Edit** icon. From the left pane, choose **Routing**) to ensure connectivity to the AAA servers.

  For remote access VPN double authentication, ensure that both the primary and secondary authentication servers are reachable from the Firewall Threat Defense device.
- Purchase and enable one of the following Cisco Secure Client licenses: Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only to enable the Firewall Threat Defense remote access VPN.
- Download the latest Secure Client image files from Cisco Software Download Center.

  On your Secure Firewall Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **Secure Client File** and add the new Secure Client image files.
- Create a security zone or interface group that contains the network interfaces that users will access for VPN connections. See Interfaces, on page 2383.
- Download the Secure Client Profile Editor from Cisco Software Download Center to create the Secure Client profile. You can use the standalone profile editor to create a new or modify an existing Secure Client profile.

Create a New Remote Access VPN Policy

The Remote Access VPN Policy Wizard guides you to quickly and easily set up remote access VPNs with basic capabilities. You can further enhance the policy configuration by specifying additional attributes as you want and deploy it to your Secure Firewall Threat Defense secure gateway devices.

Before you begin

- Ensure that you complete all the prerequisites listed in Prerequisites for Configuring Remote Access VPN, on page 1426.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Add** to create a new remote access VPN policy with basic policy configuration, using the Remote Access VPN Policy wizard.

You must proceed through the entire wizard to create a new policy; the policy is not saved if you cancel before you complete the wizard.

Step 3 Select the target devices and protocols.

The Firewall Threat Defense devices that you select here functions as your remote access VPN gateways for the VPN client users.

You can select Firewall Threat Defense devices when you create a remote access VPN policy or change them later. See Set Target Devices for a Remote Access VPN Policy, on page 1435.

You can select **SSL** or **IPSec-IKEv2**, or both the VPN protocols. Firewall Threat Defense supports both the protocols to establish secure connections over a public network through VPN tunnels.

Note Firewall Threat Defense does not support IPSec tunnels with NULL encryption. If you have selected IPSec-IKEv2, make sure that you do not choose NULL encryption for IPSec IKEv2 proposal. See Configure an IKEv2 IPsec proposal object, on page 2470.

For SSL settings, see Configure SSL settings, on page 884.

Step 4 Click **Next**.

Step 5 Configure the **Connection Profile** and **Group Policy** settings.

A connection profile specifies a set of parameters that define how the remote users connect to the VPN device. The parameters include settings and attributes for authentication, address assignments to VPN clients, and group policies. Firewall Threat Defense device provides a default connection profile named *DefaultWEBVPNGroup* when you configure a remote access VPN policy.

For more information, see Configure Connection Profile Settings, on page 1436.

Step 6 Configure the **Authentication, Authorization & Accounting** settings.

For information about configuring,

- AAA settings, see Configure AAA Settings for Remote Access VPN, on page 1439
- LDAP attribute maps, see Configuring LDAP Attribute Mapping, on page 1462
- SAML 2.0 single sign-on authentication, see Configuring a SAML Single Sign-On Authentication, on page 1508

Step 7 Configure the **Client Address Assignment** settings.

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is done in the order of AAA server, DHCP server, and IP address pool. Assignment of client IP addresses from the AAA server is supported only for realm and RADIUS authorization. Ensure that realm or RADIUS server is configured to provide client IP address.

Step 8 Configure the **Group Policy** settings.

A group policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience for VPN users. You configure attributes such as user authorization profile, IP addresses, Secure Client settings, VLAN mapping, and user session settings and so on using the group policy. The RADIUS authorization server assigns the group policy, or it is obtained from the current connection profile. For more information, see Configuring Group Policies, on page 1461.

Step 9 Click **Next**.

Step 10 Select the **Secure Client Image** that the VPN users will use to connect to the remote access VPN.

The Secure Client provides secure SSL or IPSec (IKEv2) connections to the Secure Firewall Threat Defense device for remote users with full VPN profiling to corporate resources. After the remote access VPN policy is deployed on the Firewall Threat Defense device, VPN users can enter the IP address of the configured device interface in their browser to download and install the Secure Client.

For information about configuring the client profile and client modules, see Group policy options for Secure Client, on page 2464.

Step 11 Click **Next**.

Step 12 Configure **Network Interface for Incoming VPN Access**.

Interface objects segment your network to help you manage and classify traffic flow. A security zone object simply groups interfaces. These groups may span multiple devices; you can also configure multiple zones interface objects on a single device. There are two types of interface objects:

- Security zones—An interface can belong to only one security zone.
- Interface groups—An interface can belong to multiple interface groups (and to one security zone).

(Optional) Check the **Enable DTLS on member interfaces** check box, if required. DTLS is applicable only for SSL protocol.

Step 13 Configure **Device Certificates**.

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway. From the **Certificate Enrollment** drop-down list, choose a certificate or click + to add a certificate to authenticate the VPN gateway.

Step 14 Configure **Access Control for VPN Traffic** .

By default, all decrypted traffic in the VPN tunnel is subjected to the Access Control Policy. Check the **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** check box to bypass decrypted traffic from the Access Control Policy. This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.



Note If you select this option, you need not update the access control policy for remote access VPN as specified in Update the Access Control Policy on the Secure Firewall Threat Defense Device, on page 1429.

Step 15 Click **Next**.

Step 16 View the **Summary** of the remote access VPN policy configuration.

The Summary page displays all the remote access VPN settings you have configured so far and provides links to the additional configurations that need to be performed before deploying the remote access VPN policy on the selected devices.

Click **Back** to make changes to the configuration, if required.

Step 17 Click **Finish** to complete the basic configuration for the remote access VPN policy.

When you complete the Remote Access VPN Policy Wizard, the policy listing page appears. Later, set up DNS configuration, configure access control for VPN users, and enable NAT exemption (if necessary) to complete a basic remote access VPN Policy configuration.

What to do next

Use the Remote Access VPN dashboard (**Overview** > **Dashboards** > **Remote Access VPN**) to monitor real-time data from active remote access VPN sessions on the devices. You can quickly determine problems related to user sessions and mitigate the problems for your network and users. For more information, see Remote Access VPN Dashboard, on page 1524.

Update the Access Control Policy on the Secure Firewall Threat Defense Device

Before deploying the remote access VPN policy, you must update the access control policy on the targeted Secure Firewall Threat Defense device with a rule that allows VPN traffic. The rule must allow all traffic coming in from the outside interface, with source as the defined VPN pool networks and destination as the corporate network.

Note If you have selected the **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** option on the Access Interface tab, you need not update the access control policy for remote access VPN.

Enable or disable the option for all your VPN connections. If you disable this option, make sure that the traffic is allowed by the access control policy or pre-filter policy.

For more information, see Configure Access Interfaces for Remote Access VPN, on page 1455.

Before you begin

Complete the remote access VPN policy configuration using the Remote Access VPN Policy wizard.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** on the access control policy that you want to update.

Step 3 Click **Add Rule** to add a new rule.

Step 4 Specify the **Name** for the rule and select **Enabled**.

Step 5 Select the **Action**, **Allow** or **Trust**.

Step 6 Select the following on the **Zones** tab:

a) Select the outside zone from Available Zones and click **Add to Source**.

b) Select the inside zone from Available Zones and click **Add to Destination**.

Step 7 Select the following on the **Networks** tab:

a) Select the inside network (inside interface and/or a corporate network) from Available networks and click **Add to Destination**.

b) Select the VPN address pool network from **Available Networks** and click **Add to Source Networks**.

Step 8 Configure other required access control rule settings and click **Add**.

Step 9 Save the rule and access control policy.

(Optional) Configure NAT Exemption

NAT exemption exempts addresses from translation and allows both translated and remote hosts to initiate connections with your protected hosts. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption enables you to specify the real and destination addresses when determining the real addresses to translate (similar to policy NAT). Use static identity NAT to consider ports in the access list.

When you configure static identity NAT for remote access or site-to-site VPN, you must configure NAT with the route lookup option. Without route lookup, the Firewall Threat Defense sends traffic out of the interface specified in the NAT command, regardless of what the routing table says. For example, you do not want the Firewall Threat Defense to send the DHCP scope traffic through an incorrect interface; it will never return to the interface IP address. The route lookup option lets the Firewall Threat Defense send, or intercept, the traffic directly on the interface IP address instead of through the interface. For traffic from the VPN client to a host on the inside network, the route lookup option will still result in the correct egress interface (inside), so normal traffic flow is not affected.

Before you begin

Check if NAT is configured on the targeted devices where remote access VPN policy is deployed. If NAT is enabled on the targeted devices, you must define a NAT policy to exempt VPN traffic.

Procedure

Step 1 On your Secure Firewall Management Center web interface, click **Devices** > **NAT**.

Step 2 Select a NAT policy to update or click **New Policy** > **Threat Defense NAT** to create a NAT policy with a NAT rule to allow connections through all interfaces.

Step 3 Click **Add Rule** to add a NAT rule.

Step 4 On the Add NAT Rule window, select the following:

a) Select the NAT Rule as **Manual NAT Rule**.

b) Select the Type as **Static**.

c) Click **Interface Objects** and select the Source and destination interface objects.

Note This interface object must be the same as the interface selected in the remote access VPN policy.

For more information, see Configure Access Interfaces for Remote Access VPN, on page 1455.

a) Click **Translation** and select the source and destination networks:

- **Original Source** and **Translated Source**
- **Original Destination** and **Translated Destination**

Step 5 On the Advanced tab, select **Do not proxy ARP on Destination Interface**.

Do not proxy ARP on Destination Interface—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router.

Step 6 Click **OK**.

Configure DNS

Configure DNS on each Firewall Threat Defense device in order to use remote access VPN. Without DNS, the devices cannot resolve AAA server names, named URLs, and CA Servers with FQDN or Hostnames. It can only resolve IP addresses.

Procedure

Step 1 Configure DNS server details and domain-lookup interfaces using the Platform Settings. For more information, see Configure DNS server settings, on page 852 and DNS server groups, on page 2366.

Step 2 Configure split-tunnel in group policy to allow DNS traffic through remote access VPN tunnel if the DNS server is reachable through VNP network. For more information, see Configure a group policy object, on page 2461.

Add Secure Client Profile XML File

The Secure Client Profile is a group of configuration parameters stored in an XML file that the client uses to configure its operation and appearance. These parameters (XML tags) include the names and addresses of host computers and settings to enable more client features.

You can create the Secure Client Profile using the Secure Client Profile Editor, a GUI-based configuration tool that is available as part of the Secure Client software package. It is an independent program that you run outside of the Firewall Management Center. For more information about Secure Client Profile Editor, see Cisco Secure Client (including AnyConnect) Administrator Guide.

Before you begin

A Secure Firewall Threat Defense remote access VPN policy requires assignment of the Secure Client Profile to the VPN clients. You can attach the client profile to a group policy.

Download the Secure Client Profile Editor from Cisco Software Download Center.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy which you want to update.

Step 3 Click **Edit** on the connection profile to which you want to add the Secure Client profile.

Step 4 Click **Edit Group Policy**. If you choose to add a new group policy, click **Add**.

Step 5 Choose **Secure Client** > **Profile**.

Step 6 Choose a profile from the **Client Profile** drop-down list. If you choose to add a new client profile, click **Add** and do the following:

a) Specify the profile **Name**.

b) Click **Browse** and select the Secure Client Profile XML file.

Note For two-factor authentication, make sure that the timeout is set to 60 seconds or more in the Secure Client profile.

c) Click **Save**.

Step 7 Save your changes.

(Optional) Configure Split Tunneling

Split tunnel allows VPN connectivity to a remote network across a secure tunnel and also to a network outside VPN tunnel. Configure split tunneling if you want to allow your VPN users to access an outside network while they remain connected to the remote access VPN. To configure a split-tunnel list, you must create a Standard Access List or Extended Access List.

For more information, see Configuring Group Policies, on page 1461.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy for which you want to configure split tunneling.

Step 3 Click **Edit** on the required connection profile.

Step 4 Click **Add** to add a group policy or click **Edit Group Policy**.

Step 5 Choose **General** > **Split Tunneling**.

Step 6 From the **IPv4 Split Tunneling** or **IPv6 Split Tunneling** list, select **Exclude networks specified below** and then select the networks that you want to exclude from VPN traffic.

The default setting allows all traffic over the VPN tunnel.

Step 7 Click **Standard Access List** or **Extended Access List**, and select an access list from the drop-down or add a new one.

Step 8 If you choose to add a new standard or extended access list, do the following:

a) Specify the **Name** for the new access list and click **Add**.

b) Choose **Allow** from the **Action** drop-down.

c) Select the network traffic that you want to allow over the VPN tunnel and click **Add**.

Step 9 Save your changes.

Related Topics

Access lists, on page 2351

(Optional) Configure Dynamic Split Tunneling

Dynamic split tunneling allows you to fine-tune split tunneling based on DNS domain names. You can configure domains that must be included or excluded in the remote access VPN tunnel. Excluded domains are not blocked. Instead, traffic to those domains is kept outside the VPN tunnel. For example, you could send traffic to Cisco WebEx on the public Internet, thus freeing bandwidth in your VPN tunnel for traffic that is targeted to servers within your protected network. For more information about configuring this feature, see Configure AnyConnect Dynamic Split Tunnel on FTD Managed by FMC.

Before you begin

You can configure this feature using the Firewall Management Center and Firewall Threat Defense from versions 7.0 or later. If you have an older version of the Firewall Management Center, you can configure it using FlexConfig as instructed in the Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC.

Procedure

Step 1 Configure the group policy to use Dynamic Split Tunnel.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click **Edit** on the remote access VPN policy for which you want to configure dynamic split tunneling.
c) Click **Edit** on the required connection profile.
d) Click **Edit Group Policy**.

Step 2 Configure the Secure Client custom attribute in the **Add/Edit Group Policy** dialog box.

a) Click the Secure Client tab.
b) Click **Custom Attributes** and click **+**.
c) Choose **Dynamic Split Tunneling** from the **Secure Client Attribute** drop-down list.
d) Click **+** to create a new custom attribute object.
e) Enter the name for the custom attribute object.
f) **Include domains**—Specify domain names that will be included in the remote access VPN tunnel.

You can include domains in the tunnel that will be excluded based on IP addresses.

g) **Exclude domains**—Specify domain names that will be excluded from the remote access VPN.

Excluded domains are not blocked, traffic to these domains is kept outside the VPN tunnel.

h) Click **Save**.
i) Click **Add**.

Step 3 Verify the configured custom attribute and click **Save** to save the group policy.

Step 4 Click **Save** to save the connection profile.

Step 5 Click **Save** to save the remote access VPN policy.

What to do next

1. Deploy the configuration to Firewall Threat Defense.
2. Verify the configured dynamic split tunnel configuration on the Firewall Threat Defense and the Secure Client. For more information, see Verify Dynamic Split Tunneling Configuration, on page 1434.

Verify Dynamic Split Tunneling Configuration

On the Firewall Threat Defense

Use the following commands to verify the dynamic split tunneling configuration:

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *<group-policy-name>*

On the Secure Client

Click the Statistics () icon and choose **VPN > Statistics**. You can confirm the domains under the Dynamic Split Exclusion/Inclusion category.

Verify the Configuration

Procedure

Step 1 Open a web browser on a machine on the outside network.

Step 2 Enter the URL of the Firewall Threat Defense remote access VPN gateway device.

Step 3 Enter the username and password when prompted, and click **Logon**.



Note Connection to the VPN establishes automatically if you install Secure Client on the system.

The VPN prompts you to download Secure Client if Secure Client is not installed.

Step 4 Download Secure Client if it is not installed and connect to the VPN.
The Secure Client installs itself. On successful authentication, you establish connection to the Secure Firewall Threat Defense remote access VPN gateway. The remote access VPN enforces the applicable identity or QoS policy according to your VPN policy configuration.

Create a Copy of an Existing Remote Access VPN Policy

You can copy an existing remote access VPN policy to create a new one with all the settings, including the connection profiles and access interfaces. You can then assign devices to the new policy and deploy the VPN on the assigned devices as required.

Note Users with read-only permission for remote access VPN cannot create copy of the VPN. Users with read-only privileges in the domain can copy the remote access VPNs.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Copy** on the policy that you want to copy.

Step 3 Specify a **Name** for the new remote access VPN.

Step 4 Click **OK**.

What to do next

To assign devices to the new policy, see Set Target Devices for a Remote Access VPN Policy, on page 1435.

Set Target Devices for a Remote Access VPN Policy

After you create remote access VPN policy, you can assign the policy to threat defense devices.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** ( ) next to the remote access VPN policy that you want to edit.

Step 3 Click **Policy Assignments**.

Step 4 Do any of the following:

- To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add**. You can also drag and drop the available devices to select.
- To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** list.

Step 5 Click **OK**.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Associate Local Realm with Remote Access VPN Policy

You can associate local realm to remote access VPN policy to enable local user authentication.

For information about creating and managing realms, see Manage a realm, on page 1876.

For information about configuring local user authentication for remote access VPNs, see Configure AAA Settings for Remote Access VPN, on page 1439.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** ( ) next to the remote access VPN policy that you want to edit.

Step 3 Click the link next to **Local Realm**.

Step 4 Select the **Local Realm Server** from the list, or click **Add** to add a new local realm.

Step 5 Click **OK**.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Additional Remote Access VPN Configurations

Configure Connection Profile Settings

Remote Access VPN policy contains the connection profiles targeted for specific devices. These policies pertain to creating the tunnel itself, such as, how AAA is accomplished, and how addresses are assigned (DHCP or Address Pools) to VPN clients. They also include user attributes, which are identified in group policies configured on the Firewall Threat Defense device or obtained from a AAA server. A device also provides a default connection profile named *DefaultWEBVPNGroup*. The connection profile that is configured using the wizard appears in the list.

If you decide to grant different rights to different groups of VPN users, then you can add specific connection profiles for each of the user groups and maintain multiple connection profiles in your remote access VPN policy.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Select a **Connection Profile** and click **Edit**.

Step 4 (Optional) If you choose to add new connection profile, click **Add**.

Step 5 Configure IP Addresses for VPN Clients.
Configure IP Addresses for VPN Clients, on page 1437

Step 6 (Optional) Update AAA Settings for remote access VPNs.
Configure AAA Settings for Remote Access VPN, on page 1439

Step 7 (Optional) Create or update Aliases.
Create or Update Aliases for a Connection Profile, on page 1454

Step 8 Save your changes.

Configure IP Addresses for VPN Clients

Client address assignment allows you to assign IP addresses for the remote access VPN users.

You can assign IP Address for remote VPN clients from the local IP address pools, DHCP Servers, and AAA servers. The AAA servers are assigned first, followed by others. Configure the **Client Address Assignment** policy in the **Advanced** tab to define the assignment criteria. The IP pools defined in this connection profile will only be used if no IP pools are defined in group policy associated with the connection profile, or the system default group policy **DfltGrpPolicy**.

IPv4 Address Pools—SSL VPN clients receive new IP addresses when they connect to the Firewall Threat Defense device. Address pools define a range of addresses that remote clients can receive. You can add a maximum of six pools for IPv4 and IPv6 addresses each.



Note You can use the IP address from the existing IP pools in the Firewall Management Center or create a new pool using the **Add** option. Also, you can create an IP pool in Firewall Management Center using the **Objects** > **Object Management** > **Address Pools** path. For more information, see Configure address pools, on page 2356.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.
Existing remote access policies are listed.

Step 2 Select a remote access VPN policy and click the edit icon.

Step 3 Select the connection profile that you want to update and click the edit icon.

Step 4 Under the **Client Address Assignment** tab, do the following:

Step 5 Click + next to **Address Pools**:

a) Click + next to **Address Pools** to add IP addresses, and select **IPv4** or **IPv6** to add the corresponding address pool. Select the IP address pool from **Available Pools** and click **Add**.

Note If you share your remote access VPN policy among multiple Secure Firewall Threat Defense devices, bear in mind that all devices share the same address pool unless you use device-level object overrides to replace the global definition with a unique address pool for each device. Unique address pools are required to avoid overlapping addresses in cases where the devices are not using NAT.

b) Click + next to **Available Pools** in the **Address Pools** window to add a new IPv4 or IPv6 address pool. When you choose the IPv4 pool, provide a starting and ending IP address. When you choose to include a new IPv6 address pool, enter **`Number of Addresses`** in the range 1-16384. Select the **Allow Overrides** option to avoid conflicts with IP address when objects are shared across many devices. For more information, see Configure address pools, on page 2356.

c) Click **OK**.

If you plan to edit the IP address pools, we recommend that you perform the following steps during a maintenance window:

1. Unassign the device from the remote access VPN.
2. Select the device and click **Deploy**.

   This deployment removes all the remote access VPN configurations from the device, terminates the remote access VPN sessions, the sessions are not reestablished.
3. Click the edit icon next to the IP address pools to edit it, edit any other remote access VPN configurations, if required, on the Firewall Management Center.
4. Assign the device to the updated remote access VPN policy.
5. Deploy the configurations on the device.

   The remote access VPN clients can connect to the device after the maintenance window.

Step 6 Click + next to **DHCP Servers** to add DHCP servers:

Note The DHCP server address can be configured only with IPv4 address.

a) Specify the name and DHCP (Dynamic Host Configuration Protocol) server address as network objects. Click **Add** to choose the server from the object list. Click **Delete** to delete a DHCP server.

b) Click **Add** in the **New Objects** page to add a new network object. Enter the new object name, description, network, and select the **Allow Overrides** option as applicable. For more information, see Create a network object, on page 2388 and Allow object overrides, on page 2344.

c) Click **OK**.

Step 7 Click **Save**.

Related Topics

Configure Connection Profile Settings, on page 1436

Configure AAA Settings for Remote Access VPN

Before you begin

- Ensure that the required machine and user certificates are deployed on the endpoints. For information about Firewall Threat Defense certificates, see Manage Firewall Threat Defense certificates, on page 2483.
- Configure Secure Client profiles with required certificates. For more information, see *Cisco Secure Client (including AnyConnect) Administrator Guide*.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Select a connection profile to update AAA settings, click **Edit** and then choose**AAA**.

Step 4 Select the following for **Authentication**:

- **Authentication Method**—Determines how a user is identified before being allowed access to the network and network services. It controls access by requiring valid user credentials, which are typically a username and password. It may also include the certificate from the client. Supported authentication methods are **AAA only**, **Client Certificate only**, and **AAA + Client Certificate**.

  When you select the **Authentication Method** as:

  - **AAA Only**—If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must select the **Authorization Server** and **Accounting Server** manually.
  - **SAML**—Each user is authenticated using the SAML single sign-on server. For more information, see Single Sign-On Authentication with SAML 2.0, on page 1506.

    Override Identity Provider Certificate—Select to override the primary identity provider certificate of the SAML provider with an IdP certificate specific to a connection profile or SAML application. Select the IdP certificate from the drop-down.

    Microsoft Azure can support multiple applications for the same entity ID. Each application (mapped to a different connection profile) requires a unique certificate. If you want to retain an existing entity ID for the single-sign-on object in current connection profile and use a different IdP certificate, you can select this option.

    This enables support for multiple SAML applications per Microsoft Azure SAML identity provider.

    The primary identity certificate is configured in the single sign-on server object.

    For information about configuring a single sign-on server object, see Add a single sign-on server, on page 2349.

    Choose your **SAML Login Experience** to configure a browser for SAML web authentication:

    - **VPN client embedded browser**—Choose this option to use the browser embedded with the VPN client for web authentication. The authentication applies to the VPN connection only.

- **Default OS Browser**—Choose this option to configure the operating system that default or native browser that supports WebAuthN (FIDO2 standard for web authentication). This option enables single sign-on(SSO) support for web authentication methods such as biometric authentication.

  The default browser requires an external browser package for web authentication. The package Default-External-Browser-Package is configured by default. You can change the default external browser package by editing a remote access VPN policy and selecting the file under **Advanced** and choose **AnyConnect Client ImagesSecure Client Image**s, then click **Package File**.

  You can also add a new package file by selecting. **Objects** > **Object Management** > **VPN** > **Secure Client File** and then click **Add Secure Client File**.

- **Client Certificate Only**—Each user is authenticated with a client certificate. The client certificate must be configured on VPN client endpoints. By default, the user name is derived from the client certificate fields CN and OU. If the user name is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.

  Select **Enable multiple certificate authentication** to authenticate the VPN client using the machine and user certificates.

  If have enabled multiple certificate authentication, you can select one of the following certificates to map the username and authenticate the VPN user:

  - **First Certificate**—Select this option to map the username from the machine certificate sent from the VPN client.
  - **Second Certificate**—Select this option to map the username from the user certificate sent from the client.



Note If you do not enable multiple certificate authentication, the user certificate (second certificate) is used for authentication by default.

  If you select the **Map specific field** option, which includes the username from the client certificate, the **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

  The primary and Secondary fields pertaining to the **Map specific field** option contain these common values:

  - C (Country)
  - CN (Common Name)
  - DNQ (DN Qualifier)
  - EA (Email Address)
  - GENQ (Generational Qualifier)
  - GN (Given Name)

- I (Initial)
- L (Locality)
- N (Name)
- O (Organisation)
- OU (Organisational Unit)
- SER (Serial Number)
- SN (Surname)
- SP (State Province)
- T (Title)
- UID (User ID)
- UPN (User Principal Name)

- **Client Certificate & AAA**— Each user is authenticated with both a client certificate and AAA server. Select the required certificate and AAA configurations for authentication.

  Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

- **Client Certificate & SAML**— Each user is authenticated with both a client certificate and SAML server. Select the required certificate and SAML configurations for authentication.
  - **Allow connection only if username from certificate and SAML are the same**—Select to allow VPN connection only if the username from the certificate matches the SAML single sign-on username.
  - **Use username from client certificate for Authorization**—When you choose the option to pick username from client certificate for authorization, you must configure the fields to pick from the client certificate.

    You can choose to map a specific filed as the username or use the entire distinguished name (DN) for authorization:
    - **Map specific field**— Select to include the username from the client certificate; the **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively.
    - **Use entire DN as username**— The system automatically retrieves the user identity for authorization.

  You can also create a Dynamic Access Policy (DAP) to match user-specific SAML assertion attributes or username to DAP certificate attributes. See Configure AAA criteria settings for a DAP record, on page 1535.

- **Authentication Server**—Authentication is the way a user is identified before being allowed access to the network and network services. Authentication requires valid user credentials, a certificate, or both. You can use authentication alone, or with authorization and accounting.

Select an authentication server from the list if you have added a server already or else create an authentication server:

- **LOCAL**—Use a local database from the Firewall Threat Defense for user authentication. To configure local authentication, Firewall Threat Defense must be Version 7.0 and later.
  - **Local Realm**—Select a local realm or click **Add** to configure a realm. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- **Realm**—Configure an LDAP or AD realm. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- **RADIUS Server Group**—Add a RADIUS server group object with RADIUS servers. See Add a RADIUS server group, on page 2346.
- **Single Sign-On Server**—Create a single sign-on server object for SAML authentication. See Add a single sign-on server, on page 2349.

Fallback to LOCAL Authentication— The user is authenticated using the local database and the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured.

- **Use secondary authentication** — Secondary authentication is configured in addition to primary authentication to provide additional security for VPN sessions. Secondary authentication is applicable only to **AAA only** and **Client Certificate & AAA** authentication methods.

  Secondary authentication is an optional feature that requires a VPN user to enter two sets of username and password on the Secure Client login screen. You can also configure to pre-fill the secondary username from the authentication server or client certificate. Remote access VPN authentication is granted only if both primary and secondary authentications are successful. VPN authentication is denied if any one of the authentication servers is not reachable or one authentication fails.

  You must configure a secondary authentication server group (AAA server) for the second username and password before configuring secondary authentication. For example, you can set the primary authentication server to an LDAP or Active Directory realm and the secondary authentication to a RADIUS server.



Note By default, secondary authentication is not required.

Authentication Server— Secondary authentication server to provide secondary username and password for VPN users.

- **Fallback to LOCAL Authentication**— This user is authenticated using the local database and the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured.

Select the following under **Username for secondary authentication**:

- **Prompt**: Prompts the users to enter the username and password while logging on to VPN gateway.
- **Use primary authentication username**: The username is taken from the primary authentication server for both primary and secondary authentication; you must enter two passwords.
- **Map username from client certificate**: Prefills the secondary username from the client certificate.

  If you have enabled multiple certificate authentication, you can select one of the following certificates:

- **First Certificate**— Select this option to map the username from the machine certificate sent from the VPN client.
- **Second Certificate**— Select this option to map the username from the user certificate sent from the client.
- If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN (Distinguished Name) as username** option, the system automatically retrieves the user identity.

  See **Authentication Method** descriptions for more information about primary and secondary field mapping.
- **Prefill username from certificate on user login window**: Prefills the secondary username from the client certificate when the user connects via Secure Client.
  - **Hide username in login window**: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.

- **Use secondary username for VPN session**: The secondary username is used for reporting user activity during a VPN session.

Step 5 Select the following for **Authorization**:

- **Authorization Server**—After authentication is complete, authorization controls the services and commands available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform, their actual capabilities, and restrictions. When you do not use authorization, authentication alone provides the same access to all authenticated users. Authorization requires authentication.

  To know more about how remote access VPN authorization works, see Understanding Policy Enforcement of Permissions and Attributes, on page 1420.

  When a RADIUS Server is configured for user authorization in the connection profile, the remote access VPN system administrator can configure multiple authorization attributes for users or user-groups. The authorization attributes that are configured on the RADIUS server can be specific for a user or a user-group. Once users are authenticated, these specific authorization attributes are pushed to the Firewall Threat Defense device.



Note The AAA server attributes obtained from the authorization server override the attribute values that may have been previously configured on the group policy or the connection profile.

- Check **Allow connection only if user exists in authorization database** if desired.

  When enabled, the system checks the username of the client must exist in the authorization database to allow a successful connection. If the username does not exist in the authorization database, then the connection is denied.

- When you select a realm as the Authorization Server, you must configure an LDAP attribute map. You can choose a single server for authentication and authorization or a different servers. Click **Configure LDAP Attribute Map** to add LDAP attribute maps for authorization.

Note Firewall Threat Defense does not support SAML Identity Provider as the Authorization server. If the Active Directory behind the SAML Identity Provider is reachable via Firewall Management Center and Firewall Threat Defense, you can configure authorization following these steps:

- Add realm for the AD Server. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- Select the realm object as the Authorization Server in remote access VPN connection profile.
- Configure LDAP attribute map for the selected realm.

For information about configuring LDAP attribute maps, see Configuring LDAP Attribute Mapping, on page 1462.

Step 6 Select the following for **Accounting**:

- **Accounting Server**—Accounting is used to track the services that users are accessing and the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS server. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the services used, and the duration of each session. This data can then be analyzed for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

  Specify the RADIUS Server Group object that will be used to account for the remote access VPN session.

Step 7 Select the following **Advanced Settings**:

- **Strip Realm from username**—Select to remove the realm from the username before passing the username on to the AAA server. For example, if you select this option and provide *domain\username*, the domain is stripped off from the username and sent to AAA server for authentication. By default this option is unchecked.
- **Strip Group from username**—Select to remove the group name from the username before passing the username on to the AAA server. By default this option is unchecked.

Note A realm is an administrative domain. Enabling these options allows the authentication to be based on the username alone. You can enable any combination of these options. However, you must select both check boxes if your server cannot parse delimiters.

- **Password Management**—Enable managing the password for the remote access VPN users. Select to notify ahead of the password expiry or on the day the password expires.

Step 8 Click **Save**.

Related Topics

Understanding Policy Enforcement of Permissions and Attributes, on page 1420
Manage a realm, on page 1876

RADIUS Server Attributes for Secure Firewall Threat Defense

The Firewall Threat Defense device supports applying user authorization attributes (also called user entitlements or permissions) to VPN connections from the external RADIUS server that are configured for authentication and/or authorization in the remote access VPN policy.

Note Secure Firewall Threat Defense devices support attributes with vendor ID 3076.

The following user authorization attributes are sent to the Firewall Threat Defense device from the RADIUS server.

- RADIUS attributes 146 and 150 are sent from Firewall Threat Defense devices to the RADIUS server for authentication and authorization requests.
- All three (146, 150, and 151) attributes are sent from Firewall Threat Defense devices to the RADIUS server for accounting start, interim-update, and stop requests.

Table 80: RADIUS Attributes Sent from Secure Firewall Threat Defense to RADIUS Server

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Connection Profile Name or Tunnel Group Name	146	String	Single	1-253 characters
Client Type	150	Integer	Single	2 = Secure Client SSL VPN, 6 = Secure Client IPsec VPN (IKEv2)
Session Type	151	Integer	Single	1 = Secure Client SSL VPN, 2 = Secure Client IPsec VPN (IKEv2)

Table 81: Supported RADIUS Authorization Attributes

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Access-Hours	Y	1	String	Single	Name of the time range, for example, Busine

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Access-List-Inbound	Y	86	String	Single	Both of the Access-List attributes take the name ACL that is configured on the Firewall Threat D device. Create these ACLs using the Smart CLI E Access List object type (select **Device** > **Advan Configuration** > **Smart CLI** > **Objects**). These ACLs control traffic flow in the inbound entering the Firewall Threat Defense device) or o (traffic leaving the Firewall Threat Defense devi direction.
Access-List-Outbound	Y	87	String	Single	
Address-Pools	Y	217	String	Single	The name of a network object defined on the Fi Threat Defense device that identifies a subnet, wh be used as the address pool for clients connectin remote access VPN. Define the network object **Objects** page and then associate the network obj a group policy or a connection profile.
Allow-Network-Extension-Mode	Y	64	Boolean	Single	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	Y	50	Integer	Single	1-35791394 minutes
Authorization-DN-Field	Y	67	String	Single	Possible values: UID, OU, O, CN, L, SP, C, EA, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	Integer	Single	0 = No 1 = Yes
Authorization-Type	Y	65	Integer	Single	0 = None 1 = RADIUS 2 = LDAP
Banner1	Y	15	String	Single	Banner string to display for Cisco VPN remote a sessions: IPsec IKEv1, Secure Client SSL-TLS/DTLS/IKEv2, and Clientless SSL
Banner2	Y	36	String	Single	Banner string to display for Cisco VPN remote a sessions: IPsec IKEv1, Secure Client SSL-TLS/DTLS/IKEv2, and Clientless SSL. The string is concatenated to the Banner1 string , if con
Cisco-IP-Phone-Bypass	Y	51	Integer	Single	0 = Disabled 1 = Enabled
Cisco-LEAP-Bypass	Y	75	Integer	Single	0 = Disabled 1 = Enabled
Client Type	Y	150	Integer	Single	1 = Cisco VPN Client (IKEv1) 2 = Secure Clien VPN 3 = Clientless SSL VPN 4 = Cut-Through- = L2TP/IPsec SSL VPN 6 = Secure Client IPsec (IKEv2)
Client-Type-Version-Limiting	Y	77	String	Single	IPsec VPN version number string
DHCP-Network-Scope	Y	61	String	Single	IP Address

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Extended-Authentication-On-Rekey	Y	122	Integer	Single	0 = Disabled 1 = Enabled
Framed-Interface-Id	Y	96	String	Single	Assigned IPv6 interface ID. Combines with Framed-IPv6-Prefix to create a complete ass address. For example: Framed-Interface-ID= combined with Framed-IPv6-Prefix=2001:0db the assigned IP address 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	Y	97	String	Single	Assigned IPv6 prefix and length. Combines Framed-Interface-Id to create a complete ass address. For example: prefix 2001:0db8::/64 with Framed-Interface-Id=1:1:1:1 gives the 2001:0db8::1:1:1:1. You can use this attribut an IP address without using Framed-Interfac assigning the full IPv6 address with prefix le for example, Framed-IPv6-Prefix=2001:0db
Group-Policy	Y	25	String	Single	Sets the group policy for the remote access V You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
IE-Proxy-Bypass-Local		83	Integer	Single	0 = None 1 = Local
IE-Proxy-Exception-List		82	String	Single	New line (\n) separated list of DNS domains
IE-Proxy-PAC-URL	Y	133	String	Single	PAC address string
IE-Proxy-Server		80	String	Single	IP address
IE-Proxy-Server-Policy		81	Integer	Single	1 = No Modify 2 = No Proxy 3 = Auto detec Concentrator Setting
IKE-KeepAlive-Confidence-Interval	Y	68	Integer	Single	10-300 seconds
IKE-Keepalive-Retry-Interval	Y	84	Integer	Single	2-10 seconds
IKE-Keep-Alives	Y	41	Boolean	Single	0 = Disabled 1 = Enabled
Intercept-DHCP-Configure-Msg	Y	62	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Allow-Passwd-Store	Y	16	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Authentication		13	Integer	Single	0 = None 1 = RADIUS 2 = LDAP (authoriza = NT Domain 4 = SDI 5 = Internal 6 = RAD Expiry 7 = Kerberos/Active Directory

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
IPsec-Auth-On-Rekey	Y	42	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Backup-Server-List	Y	60	String	Single	Server Addresses (space delimited)
IPsec-Backup-Servers	Y	59	String	Single	1 = Use Client-Configured list 2 = Disable and cle list 3 = Use Backup Server list
IPsec-Client-Firewall-Filter-Name		57	String	Single	Specifies the name of the filter to be pushed to t as firewall policy
IPsec-Client-Firewall-Filter-Optional	Y	58	Integer	Single	0 = Required 1 = Optional
IPsec-Default-Domain	Y	28	String	Single	Specifies the single default domain name to sen client (1-255 characters).
IPsec-IKE-Peer-ID-Check	Y	40	Integer	Single	1 = Required 2 = If supported by peer certificate not check
IPsec-IP-Compression	Y	39	Integer	Single	0 = Disabled 1 = Enabled
IPsec-Mode-Config	Y	31	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP	Y	34	Boolean	Single	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	Y	35	Integer	Single	4001- 49151. The default is 10000.
IPsec-Required-Client-Firewall-Capability	Y	56	Integer	Single	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = from server
IPsec-Sec-Association		12	String	Single	Name of the security association
IPsec-Split-DNS-Names	Y	29	String	Single	Specifies the list of secondary domain names to the client (1-255 characters).
IPsec-Split-Tunneling-Policy	Y	55	Integer	Single	0 = No split tunneling 1 = Split tunneling 2 = Loc permitted
IPsec-Split-Tunnel-List	Y	27	String	Single	Specifies the name of the network or ACL that d the split tunnel inclusion list.
IPsec-Tunnel-Type	Y	30	Integer	Single	1 = LAN-to-LAN 2 = Remote access
IPsec-User-Group-Lock		33	Boolean	Single	0 = Disabled 1 = Enabled
IPv6-Address-Pools	Y	218	String	Single	Name of IP local pool-IPv6
IPv6-VPN-Filter	Y	219	String	Single	ACL value
L2TP-Encryption		21	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 8 = Stateless-Req 15= 40/128-Encr/Stateless-Re

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
L2TP-MPPC-Compression		38	Integer	Single	0 = Disabled 1 = Enabled
Member-Of	Y	145	String	Single	Comma-delimited string, for example: `Engineering, Sales` An administrative attribute that can be used access policies. It does not set a group policy
MS-Client-Subnet-Mask	Y	63	Boolean	Single	An IP address
NAC-Default-ACL		92	String		ACL
NAC-Enable		89	Integer	Single	0 = No 1 = Yes
NAC-Revalidation-Timer		91	Integer	Single	300-86400 seconds
NAC-Settings	Y	141	String	Single	Name of the NAC policy
NAC-Status-Query-Timer		90	Integer	Single	30-1800 seconds
Perfect-Forward-Secrecy-Enable	Y	88	Boolean	Single	0 = No 1 = Yes
PPTP-Encryption		20	Integer	Single	Bitmap: 1 = Encryption required 2 = 40 bits 8 = Stateless-Required 15= 40/128-Encr/Stat
PPTP-MPPC-Compression		37	Integer	Single	0 = Disabled 1 = Enabled
Primary-DNS	Y	5	String	Single	An IP address
Primary-WINS	Y	7	String	Single	An IP address
Privilege-Level	Y	220	Integer	Single	An integer between 0 and 15.
Required-Client- Firewall-Vendor-Code	Y	45	Integer	Single	1 = Cisco Systems (with Cisco Integrated Cl Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cis (with Cisco Intrusion Prevention Security Ag
Required-Client-Firewall-Description	Y	47	String	Single	String
Required-Client-Firewall-Product-Code	Y	46	Integer	Single	Cisco Systems Products: 1 = Cisco Intrusion Prevention Security Age Integrated Client (CIC) Zone Labs Products: 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE Product: 1 = BlackIce Defende Sygate Products: 1 = Personal Firewall 2 = P Firewall Pro 3 = Security Agent

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Required-Individual-User-Auth	Y	49	Integer	Single	0 = Disabled 1 = Enabled
Require-HW-Client-Auth	Y	48	Boolean	Single	0 = Disabled 1 = Enabled
Secondary-DNS	Y	6	String	Single	An IP address
Secondary-WINS	Y	8	String	Single	An IP address
SEP-Card-Assignment		9	Integer	Single	Not used
Session Subtype	Y	152	Integer	Single	0 = None 1 = Clientless 2 = Client 3 = Client Or Session Subtype applies only when the Session T (151) attribute has the following values: 1, 2, 3,
Session Type	Y	151	Integer	Single	0 = None 1 = Secure Client SSL VPN 2 = Secur IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client (I = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VI Balancing
Simultaneous-Logins	Y	2	Integer	Single	0-2147483647
Smart-Tunnel	Y	136	String	Single	Name of a Smart Tunnel
Smart-Tunnel-Auto	Y	138	Integer	Single	0 = Disabled 1 = Enabled 2 = AutoStart
Smart-Tunnel-Auto-Signon-Enable	Y	139	String	Single	Name of a Smart Tunnel Auto Signon list appen the domain name
Strip-Realm	Y	135	Boolean	Single	0 = Disabled 1 = Enabled
SVC-Ask	Y	131	String	Single	0 = Disabled 1 = Enabled 3 = Enable default ser Enable default clientless (2 and 4 not used)
SVC-Ask-Timeout	Y	132	Integer	Single	5-120 seconds
SVC-DPD-Interval-Client	Y	108	Integer	Single	0 = Off 5-3600 seconds
SVC-DPD-Interval-Gateway	Y	109	Integer	Single	0 = Off) 5-3600 seconds
SVC-DTLS	Y	123	Integer	Single	0 = False 1 = True
SVC-Keepalive	Y	107	Integer	Single	0 = Off 15-600 seconds
SVC-Modules	Y	127	String	Single	String (name of a module)
SVC-MTU	Y	125	Integer	Single	MTU value 256-1406 in bytes
SVC-Profiles	Y	128	String	Single	String (name of a profile)
SVC-Rekey-Time	Y	110	Integer	Single	0 = Disabled 1-10080 minutes

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
Tunnel Group Name	Y	146	String	Single	1-253 characters
Tunnel-Group-Lock	Y	85	String	Single	Name of the tunnel group or “none”
Tunneling-Protocols	Y	11	Integer	Single	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) mutually exclusive. 0 - 11, 16 - 27, 32 - 43, 4 legal values.
Use-Client-Address		17	Boolean	Single	0 = Disabled 1 = Enabled
VLAN	Y	140	Integer	Single	0-4094
WebVPN-Access-List	Y	73	String	Single	Access-List name
WebVPN ACL	Y	73	String	Single	Name of a WebVPN ACL on the device
WebVPN-ActiveX-Relay	Y	137	Integer	Single	0 = Disabled Otherwise = Enabled
WebVPN-Apply-ACL	Y	102	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Auto-HTTP-Signon	Y	124	String	Single	Reserved
WebVPN-Citrix-Metaframe-Enable	Y	101	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Content-Filter-Parameters	Y	69	Integer	Single	1 = Java ActiveX 2 = Java Script 4 = Image 8 in images
WebVPN-Customization	Y	113	String	Single	Name of the customization
WebVPN-Default-Homepage	Y	76	String	Single	A URL such as http://example-example.com
WebVPN-Deny-Message	Y	116	String	Single	Valid string (up to 500 characters)
WebVPN-Download_Max-Size	Y	157	Integer	Single	0x7fffffff
WebVPN-File-Access-Enable	Y	94	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	Y	96	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-File-Server-Entry-Enable	Y	95	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	String	Single	Comma-separated DNS/IP with an optional v (for example *.cisco.com, 192.168.1.*, wwwin
WebVPN-Hidden-Shares	Y	126	Integer	Single	0 = None 1 = Visible
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	Boolean	Single	Enabled if clientless home page is to be rende Smart Tunnel.
WebVPN-HTML-Filter	Y	69	Bitmap	Single	1 = Java ActiveX 2 = Scripts 4 = Image 8 =

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
WebVPN-HTTP-Compression	Y	120	Integer	Single	0 = Off 1 = Deflate Compression
WebVPN-HTTP-Proxy-IP-Address	Y	74	String	Single	Comma-separated DNS/IP:port, with http= or ht prefix (for example http=10.10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	Y	148	Integer	Single	0-30. 0 = Disabled.
WebVPN-Keepalive-Ignore	Y	121	Integer	Single	0-900
WebVPN-Macro-Substitution	Y	223	String	Single	Unbounded.
WebVPN-Macro-Substitution	Y	224	String	Single	Unbounded.
WebVPN-Port-Forwarding-Enable	Y	97	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-List	Y	72	String	Single	Port forwarding list name
WebVPN-Port-Forwarding-Name	Y	79	String	Single	String name (example, “Corporate-Apps”). This text replaces the default string, “Application A on the clientless portal home page.
WebVPN-Post-Max-Size	Y	159	Integer	Single	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	Integer	Single	0-30. 0 = Disabled.
WebVPN Smart-Card-Removal-Disconnect	Y	225	Boolean	Single	0 = Disabled 1 = Enabled
WebVPN-Smart-Tunnel	Y	136	String	Single	Name of a Smart Tunnel
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	String	Single	Name of a Smart Tunnel auto sign-on list appen the domain name
WebVPN-Smart-Tunnel-Auto-Start	Y	138	Integer	Single	0 = Disabled 1 = Enabled 2 = Auto Start
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	String	Single	One of “e networkname,” “i networkname,” or “a networkname is the name of a Smart Tunnel netw e indicates the tunnel excluded, i indicates the tu specified, and a indicates all tunnels.
WebVPN-SSL-VPN-Client-Enable	Y	103	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	Y	104	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SSO-Server-Name	Y	114	String	Single	Valid string

Attribute Name	Firewall Threat Defense	Attr. No.	Syntax/Type	Single or Multi- Valued	Description or Value
WebVPN-Storage-Key	Y	162	String	Single	
WebVPN-Storage-Objects	Y	161	String	Single	
WebVPN-SVC-Keepalive-Frequency	Y	107	Integer	Single	15-600 seconds, 0=Off
WebVPN-SVC-Client-DPD-Frequency	Y	108	Integer	Single	5-3600 seconds, 0=Off
WebVPN-SVC-DTLS-Enable	Y	123	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-SVC-DTLS-MTU	Y	125	Integer	Single	MTU value is from 256-1406 bytes.
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	Integer	Single	5-3600 seconds, 0=Off
WebVPN-SVC-Rekey-Time	Y	110	Integer	Single	4-10080 minutes, 0=Off
WebVPN-SVC-Rekey-Method	Y	111	Integer	Single	0 (Off), 1 (SSL), 2 (New Tunnel)
WebVPN-SVC-Compression	Y	112	Integer	Single	0 (Off), 1 (Deflate Compression)
WebVPN-UNIX-Group-ID (GID)	Y	222	Integer	Single	Valid UNIX group IDs
WebVPN-UNIX-User-ID (UIDs)	Y	221	Integer	Single	Valid UNIX user IDs
WebVPN-Upload-Max-Size	Y	158	Integer	Single	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	Integer	Single	0 = Disabled 1 = Enabled
WebVPN-URL-List	Y	71	String	Single	URL list name
WebVPN-User-Storage	Y	160	String	Single	
WebVPN-VDI	Y	163	String	Single	List of settings

Table 82: RADIUS Attributes Sent to Secure Firewall Threat Defense

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Address-Pools	217	String	Single	The name of a network object defined on the Firewall Threat Defense device that identifies a subnet, which will be used as the address pool for clients connecting to the remote access VPN. Define the network object on the **Objects** page.
Banner1	15	String	Single	The banner to display when the user logs in.
Banner2	36	String	Single	The second part of the banner to display when the user logs in. Banner2 is appended to Banner1.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Downloadable ACLs	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Supported via Cisco-AV-Pair configuration.
Filter ACLs	86, 87	String	Single	Filter ACLs are referred to by ACL name in the RADIUS server. It requires the ACL configuration to be already present on the Firewall Threat Defense device, so that it can be used during RADIUS authorization. 86=Access-List-Inbound 87=Access-List-Outbound
Group-Policy	25	String	Single	The group policy to use in the connection. You must create the group policy on the remote access VPN **Group Policy** page. You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	Integer	Single	The number of separate simultaneous connections the user is allowed to establish, 0 - 2147483647.
VLAN	140	Integer	Single	The VLAN on which to confine the user's connection, 0 - 4094. You must also configure this VLAN on a subinterface on the Firewall Threat Defense device.

You must set the values of the IE-Proxy-Server-Method attribute returned from ISE to one of the following:

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

Firewall Threat Defense will deliver a proxy setting only if one of the above values is used for the IE-Proxy-Server-Method attribute.

Create or Update Aliases for a Connection Profile

Aliases contain alternate names or URLs for a specific connection profile. Remote access VPN administrators can enable or disable the Alias names and Alias URLs. VPN users can choose an Alias name when they connect to the Secure Firewall Threat Defense device. Aliases names for all connections configured on this device can be turned on or off for display. You can also configure the list of Alias URLs, which your endpoints

can select while initiating the remote access VPN connection. If users connect using the Alias URL, system will automatically log them using the connection profile that matches the Alias URL.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the policy that you want to modify.

Step 3 Click **Edit** on the connection profile for which you want to create or update aliases.

Step 4 Click **Aliases**.

Step 5 To add an Alias name, do the following:

a) Click **Add** under **Alias Names**.
b) Specify the **Alias Name**.
c) Select the **Enabled** check box in each window to enable the aliases.
d) Click **OK**.

Step 6 To add an Alias URL, do the following:

a) Click **Add** under **URL Alias**.
b) Select the **Alias URL** from the list or create a new URL object. For more information see Create a URL object, on page 2438.
c) Select the **Enabled** check box in each window to enable the aliases.
d) Click **OK**.

Step 7 Save your changes.

Related Topics

Configure Connection Profile Settings, on page 1436

Configure Access Interfaces for Remote Access VPN

The **Access Interface** table lists the interface groups and security zones that contain the device interfaces. These are configured for remote access SSL or IPsec IKEv2 VPN connections. The table displays the name of each interface group or security-zone, the interface trustpoints used by the interface, and whether Datagram Transport Layer Security (DTLS) is enabled.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Click the **Access Interface** tab.

Step 4 To add an access interface, click + and specify values for the following in the **Add Access Interface** dialog box:

a) **Access Interface**—Select the interface group or security zone to which the interface belongs.

The interface group or security zone must be a Routed type. Other interface types are not supported for remote access VPN connectivity.

b) Associate the **Protocol** object with the access interface by selecting the following options:

- **Enable IPSet-IKEv2**—Select this option to enable **IKEv2** settings.
- **Enable SSL**—Select this option to enable **SSL** settings.
  - Select **Enable Datagram Transport Layer Security**.

    When selected, it enables Datagram Transport Layer Security (DTLS) on the interface and allows the AnyConnect VPN module of Cisco Secure Client to establish an SSL VPN connection using two simultaneous tunnels—an SSL tunnel and a DTLS tunnel.

    Enabling DTLS avoids the latency and bandwidth problems associated with certain SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

    To configure SSL settings, and TLS and DTLS versions, see Configure SSL settings, on page 885.

    To configure SSL settings for the AnyConnect VPN module of Cisco Secure Client, see Group policy options for Secure Client, on page 2464.
  - Select the **Configure Interface Specific Identity Certificate** check box and select **Interface Identity Certificate** from the drop-down list.

    If you do not select the Interface Identity Certificate, the **Trustpoint** will be used by default.

    If you do not select the Interface Identity Certificate or Trustpoint, the **SSL Global Identity Certificate** will be used by default.

c) Click **OK** to save the changes.

Step 5 Select the following under **Access Settings**:

- **Allow Users to select connection profile while logging in**—If you have multiple connection profiles, check this check box to allow user to select the correct connection profile during login. You must select this option for **IPsec-IKEv2** VPNs.

Step 6 Use the following options to configure **SSL Settings**:

- **Web Access Port Number**—The port to use for VPN sessions. The default port is 443.
- **DTLS Port Number**—The UDP port to use for DTLS connections. The default port is 443.
- **SSL Global Identity Certificate**— The selected **SSL Global Identity Certificate** will be used for all the associated interfaces if the **Interface Specific Identity Certificate** is not provided.

Step 7 For **IPsec-IKEv2 Settings**, select the **IKEv2 Identity Certificate** from the list or add an identity certificate.

Step 8 Under the **Access Control for VPN Traffic** section, select the following option if you want to bypass access control policy:

- **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** — Decrypted traffic is subjected to Access Control Policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the ACL inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Note If you select this option, you need not update the access control policy for remote access VPN as specified in Update the Access Control Policy on the Secure Firewall Threat Defense Device, on page 1429.

Step 9 Click **Save** to save the access interface changes.

Related Topics

Interfaces, on page 2383

Configure Advanced Options for Remote Access VPN

Cisco Secure Client Image

Secure Client Image

The Secure Client provides secure SSL or IPsec (IKEv2) connections to the Firewall Threat Defense device for remote users with full VPN profiling to corporate resources. Without a previously-installed client, remote users can enter the IP address of an interface configured to accept clientless VPN connections in their browser to download and install the Secure Client. The Firewall Threat Defense device downloads the client that matches the operating system of the remote computer. After downloading, the client installs and establishes a secure connection. In case of a previously installed client, when the user authenticates, the Firewall Threat Defense device, examines the version of the client, and upgrades the client if necessary.

The Remote Access VPN administrator associates any new or additional Secure Client images to the VPN policy. The administrator can unassociate the unsupported or end of life client packages that are no longer required.

The Secure Firewall Management Center determines the type of operating system by using the file package name. If the user renamed the file without indicating the operating system information, the valid operating system type must be selected from the list box.

Download the Secure Client image file by visiting Cisco Software Download Center.

Related Topics

Adding a Secure Client Image to the Secure Firewall Management Center, on page 1457

Adding a Secure Client Image to the Secure Firewall Management Center

You can upload the Secure Client image to the Secure Firewall Management Center by using the **Secure Client File** object. For more information, see File objects, on page 2474. For more information about the client image, see Cisco Secure Client Image, on page 1457.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**, choose and edit a listed remote access policy, then choose the **Advanced** tab.

Step 2 Click **Add** to add a Secure Client image.

Step 3 Click **Add** in the **Available Secure Client Images** portion of the **Secure Client Images** dialog.

Step 4 Enter the **Name** and **Description**(optional) for the available Secure Client Image.

Step 5 Click **Browse**, locate and select the client image that you want to upload.

Step 6 Click **Save** to upload the image to the Firewall Management Center.

When you upload the client image to the Secure Firewall Management Center, the operating system information for the image appears automatically.

Step 7 To change the order of client images, Click **Show Re-order buttons** and move the client image up or down.

Related Topics

Cisco Secure Client Image, on page 1457

Update Secure Client Image for Remote Access VPN Clients

When new Secure Client updates are available in Cisco Software Download Center, you can download the packages manually and add them to the remote access VPN policy so that the new client packages are upgraded on the VPN client systems according to their operating systems.

Before you begin

Instructions in this section help you update new Secure Client images to remote access VPN clients connecting to Secure Firewall Threat Defense VPN gateway. Ensure that the following configurations are complete before updating your Secure Client images:

- Download the latest Secure Client image files from Cisco Software Download Center.
- On your Secure Firewall Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **Secure Client File** and add the new Secure Client image files.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy that you want to update.

Step 3 From **Advanced** drop-down menu, choose **AnyConnect Client ImagesSecure Client Image** and then click **Add**.

Step 4 Select a client image file from **Available Secure Client Images** and click **Add**.

If the required client image is not listed, click **Add** to browse and upload an image.

Step 5 Click **OK**.

Step 6 Save the remote access VPN policy.
After the remote access VPN policy changes are deployed, the new Secure Client images are updated on the Secure Firewall Threat Defense device that is configured as the remote access VPN gateway. When a new VPN user connects to the VPN gateway, the user gets the new Secure Client image to download depending on the operating system of the client system. For existing VPN users, the Secure Client image gets updated in their next VPN session.

Add a Cisco Secure Client External Browser Package to the Secure Firewall Management Center

If you have the Secure Client external browser package image on your local disk, use this procedure to upload the same to the Secure Firewall Management Center. After you upload the external browser package, you can update the external browser package for your remote access VPN connections.

You can upload the external browser package file to the Secure Firewall Management Center by using the **Secure Client File** object. For more information, see File objects, on page 2474.

Points to Remember

- Only one external browser package can be added to the Firewall Threat Defense device.
- After the external browser package is added to the Firewall Management Center, the browser is pushed to the Firewall Threat Defense only after the external browser is enabled in the remote access VPN configuration.

Procedure

Step 1 On the Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**, choose and edit a listed remote access policy, then choose the **Advanced** tab.

Step 2 Click **Add** in the **Secure Client External Browser Package** portion of the **Secure Client Images** page.

Step 3 Enter the **Name** and **Description** for the Secure Client package.

Step 4 Click **Browse** and locate the external browser package file to upload.

Step 5 Click **Save** to upload the image to the Secure Firewall Management Center.

Note If you want to update the remote access VPN connection with an existing external browser package, select the file from the **Package File** drop-down.

Step 6 Save the remote access VPN policy.

Related Topics

Cisco Secure Client Image, on page 1457

Remote Access VPN Address Assignment Policy

The Firewall Threat Defense device can use an IPv4 or IPv6 policy for assigning IP addresses to Remote Access VPN clients. If you configure more than one address assignment method, the Firewall Threat Defense device tries each of the options until it finds an IP address.

IPv4 or IPv6 Policy

You can use the IPv4 or IPv6 policy to address an IP address to remote access VPN clients. You must try with the IPv4 policy to begin and later followed by IPv6 policy.

- **Use Authorization Server**—Retrieves the address from an external authorization server on a per-user basis. If you are using an authorization server that has IP address configured, we recommend using this method. Address assignment is supported by RADIUS-based authorization server only. It is not supported for AD/LDAP. This method is available for both IPv4 and IPv6 assignment policies.

- **Use DHCP**—Obtains IP addresses from a DHCP server configured in a connection profile. You can also define the range of IP addresses that the DHCP server can use by configuring DHCP network scope in the group policy. If you use DHCP, configure the server in the **Objects** > **Object Management** > **Network** pane. This method is available for IPv4 assignment policies.

  For more information about DHCP network scope configuration, see Group policy general options, on page 2462.

- **Use an internal address pool**—Internally configured address pools are the easiest method of address pool assignment to configure. If you use this method, create the IP address pools in the **Objects** > **Object Management** > **Address Pools** pane and select the same in the connection profile. This method is available for both IPv4 and IPv6 assignment policies.

- **Allow reuse an IP address so many minutes after it is released**—Delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewalls can experience when an IP address is reassigned quickly. By default, the delay is set to zero. If you want to extend the delay, enter the number of minutes in the range of 0–480 to delay the IP address reassignment. This configurable element is available for IPv4 assignment policies.

Related Topics

Configure Connection Profile Settings, on page 1436
Remote Access VPN Authentication, on page 1418

Configure Certificate Maps

Certificate maps let you define rules matching a user certificate to a connection profile based on the contents of the certificate fields. Certificate maps provide certificate authentication on secure gateways.

The rules or the certificate maps are defined in Certificate map objects, on page 2457.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Choose **Advanced** > **Certificate Maps**.

Step 4 Select the following options from the **General Settings for Connection Profile Mapping** pane:

Selections are priority-based, matching continues down the list of options when the first selection does not match. Matching is complete when the rules are satisfied. If the rules are not satisfied, the default connection profile listed at the bottom of this page is used for the connection. Select any, or all of the following options to establish authentication and to determine which connection profile (tunnel group) must be mapped to the client.

- **Use Group URL if Group URL and Certificate Map match different Connection profiles**
- **Use the configured rules to match a certificate to a Connection Profile**—Enable this to use the rules defined in the Connection Profile Maps.

Note Configuring a certificate mapping implies certificate-based authentication. The remote user will be prompted for a client certificate regardless of the configured authentication method.

Step 5 Under the **Certificate to Connection Profile Mapping** section, click **Add Mapping** to create certificate to connection profile mapping for this policy.

a) Choose or create a **Certificate Map Name** object.
b) Select the **Connection Profile** that want to use if the rules in the certificate map object are satisfied.
c) Click **OK** to create the mapping.

Step 6 Click **Save**.

Configuring Group Policies

A group policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. For example, in the group policy object, you configure general attributes such as addresses, protocols, and connection settings.

The group policy applied to a user is determined when the VPN tunnel is established. The RADIUS authorization server assigns the group policy, or it is obtained from the current connection profile.

Note There is no group policy attribute inheritance on the Firewall Threat Defense. A group policy object is used, in its entirety, for a user. The group policy object identified by the AAA server upon login is used, or, if that is not specified, the default group policy configured for the VPN connection is used. The provided default group policy can be set to your default values, but will only be used if it is assigned to a connection profile and no other group policy has been identified for the user.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Choose **Advanced** > **Group Policies** > **Add**.

Step 4 Select group policies from the **Available Group Policy** list and click **Add**. You can select one or more group policies to associate with this remote access VPN policy.

Step 5 Click **OK** to complete the group policy selection.

Step 6 Save your changes.

Related Topics

Configure a group policy object, on page 2461

Configuring LDAP Attribute Mapping

An LDAP attribute name maps LDAP user or group attribute name to a Cisco-understandable name. The attribute map equates attributes that exist in the Active Directory (AD) or LDAP server with Cisco attribute names. You can map any standard LDAP attribute to a well-known vendor specific attribute (VSA). You can map one or more LDAP attributes to one or more Cisco LDAP attributes. When the AD or LDAP server returns authentication to the Firewall Threat Defense device during remote access VPN connection establishment, the Firewall Threat Defense device can use the information to adjust how the Secure Client completes the connection.

When you want to provide VPN users with different access permissions or VPN content, you can configure different VPN policies on the VPN server and assign these policy-sets to each user based on their credentials. You can achieve this in Firewall Threat Defense by configuring LDAP authorization, with LDAP attribute maps. In order to use LDAP to assign a group policy to a user, you must configure a map that maps an LDAP attribute.

An LDAP attribute map consists of three components:

- **Realm**—Specifies the name for the LDAP attribute map; the name is generated based on the selected realm.
- **Attribute Name Map**—Maps the LDAP user or group attribute name to Cisco-understandable name.
- **Attribute Value Map**—Maps value in the LDAP user or group attribute to the value of a Cisco attribute for the selected name mapping.

The group policies that are used in an LDAP attribute map get added to the list of group policies in the remote access VPN configuration. Removing a group policy from the remote access VPN configuration also removes the associated LDAP attribute mapping.

In versions 6.4 to 6.6, you can configure LDAP attribute maps only using FlexConfig. For more information, see Configure AnyConnect Modules and Profiles Using FlexConfig.

In versions 7.0 and later, you can use the following procedure:

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select an existing remote access VPN policy in the list and click the corresponding **Edit** icon.

Step 3 Click **Advanced** > **LDAP Attribute Mapping**.

Step 4 Click **Add**.

Step 5 On the Configure LDAP Attribute Map page, select a **Realm** to configure the attribute map.

Step 6 Click **Add**.

You can configure multiple attribute maps. Each attribute map requires that you configure a name map and value maps.

Note Ensure that you follow these guidelines while creating an LDAP attribute map:

- Configure at least one mapping for an LDAP attribute; multiple mappings with the same LDAP attribute name is not allowed.
- Configure a minimum of one name map to create an LDAP attribute map.
- You can remove any LDAP attribute map if the attribute map is not associated with any connection profile in the remote access VPN configuration.
- Use the correct spelling and capitalization in the LDAP attribute map for ***both*** the Cisco and LDAP attribute names and values.

a) Specify the **LDAP Attribute Name** and then select the required **Cisco Attribute Name** from the list.
b) Click **Add Value Map** and Specify the **LDAP Attribute Value** and **Cisco Attribute Value**.

Repeat this step to add more value maps.

Step 7 Click **OK** to complete LDAP attribute map configuration.

Step 8 Click **Save** to save the changes to the LDAP attribute mapping.

Example

For a detailed example, see Configure RA VPN with LDAP Authentication and Authorization for FTD.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 1439
Understanding Policy Enforcement of Permissions and Attributes, on page 1420

Configuring VPN Load Balancing

About VPN Load Balancing

VPN load balancing in Firewall Threat Defense allows you group two or more devices logically and distribute remote access VPN sessions among the devices equally. VPN load balancing shares Secure Client VPN sessions among the devices in a load balancing group.

VPN load balancing is based on simple distribution of traffic without taking into account throughput or other factors. A VPN load-balancing group consists of two or more Firewall Threat Defense devices. One device acts as the director, and the other devices are member devices. Devices in a group do not need to be of the exact same type, or have identical software versions or configurations. Any Firewall Threat Defense device that supports remote access VPN can participate in a load balancing group. Firewall Threat Defense supports VPN load balancing with Secure Client SAML authentication.

All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

Components of VPN Load Balancing

Following are the components of VPN load balancing:

- **Load-balancing group**—A virtual group of two or more Firewall Threat Defense devices to share the VPN sessions.

  A VPN load-balancing group can consist of Firewall Threat Defense devices of the same release or of mixed releases; but the device must support remote access VPN configuration.

  See Configure Group Settings for VPN Load Balancing, on page 1465 and Configure Additional Settings for Load Balancing, on page 1465.

- **Director**—One device from the group acts a director. It distributes the load among other members in the group and participate is serving the VPN sessions.

  The director monitors all devices in the group, keeps track of how loaded each device is, and distributes the session load accordingly. The role of director is not tied to a physical device; it can shift among devices. For example, if the current director fails, one of the member devices in the group takes over that role and immediately becomes the new director.

- **Members**—Devices other than the director in a group are called members. They participate in load balancing and share the remote access VPN connections.

  Configure Settings for Participating Devices, on page 1466.

Prerequisites for VPN Load Balancing

- **Certificates**—Firewall Threat Defense's certificate must contain the IP addresses or FQDN of the director and members to which the connection is redirected. Or else, the certificate will be deemed untrusted. The certificate must use Subject Alternate Name (SAN) or wildcard certificate
- **Group URL**—Add the group URL for VPN load-balancing group IP address to the connection profiles. Specify a group URL to eliminate the need for the user to select a group at login.
- **IP Address Pool**—Choose unique IP address pool for member devices, and override the IP pool in Firewall Management Center for each of the member devices.
- Devices that are behind Network Address Translation (NAT) can also be part of a load balancing group.

Guidelines and Limitations for VPN Load Balancing

- VPN load balancing is disabled by default. You must explicitly enable VPN load balancing.
- Only the Firewall Threat Defense devices that are co-located can be added to a load-balancing group.
- A load-balancing group must have a minimum of two Firewall Threat Defense devices.
- Devices in Firewall Threat Defense high availability can participate in a load-balancing group.
- Devices that are behind Network Address Translation (NAT) can also be part of a load balancing group.
- When a member or a director device goes down, remote access VPN connections that are served by that device will be dropped. You must initiate the VPN connection again.
- Identity certificate on each device must have Subject Alternate Name (SAN) or wildcard.

Configure Group Settings for VPN Load Balancing

You can enable VPN load balancing and configure group settings that are applicable to all the members of the load-balancing group. When you create the group, you can configure participation settings for load balancing.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy that you want to update.

Step 3 Click **Advanced** > **Load Balancing**.

Step 4 Click the **Enable Load balancing between member devices** toggle button to enable load balancing. The **Edit Group Configuration** page opens. Group parameters apply to all devices under the load-balancing group.

Step 5 Specify the **Group IPv4 Address** and **Group IPv6 Address** as applicable.

The IP address that you specify here is for the entire load-balancing group and the director opens this IP address for incoming VPN connections.

Step 6 Select the **Communication Interface** for the load-balancing group. Click **Add** to add an interface group or security zone.

Communication interface is a private interface through which the director and members share information about their load.

Step 7 Enter the **UDP Port** for communication between the director and members in a group. The default port is 9023.

Step 8 Enable the **IPsec Encryption** toggle button to activate IPsec encryption for the communication between the director and members.

Enabling the encryption establishes an IPsec tunnel between the director and members using a pre-shared key.

When you upgrade or downgrade Firewall Threat Defense devices with the **IPsec Encryption** option enabled, ensure there is no configuration mismatch between the Firewall Management Center and the Firewall Threat Defense to prevent deployment failures.

Step 9 Enter **Encryption Key** for IPsec encryption and confirm the encryption key.

Step 10 Click **OK**.

Configure Additional Settings for Load Balancing

The additional settings for VPN load balancing include FQDN and IKEv2 redirection.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy that you want to update.

Step 3 Click **Advanced** > **Load Balancing**.

Step 4 Turn on the **Enable Load balancing between member devices** toggle button to enable load balancing if not done already.

Step 5 Click **Settings**.

Step 6 Turn on the **Send FQDN to peer devices instead of IP** toggle button to enable redirection using a fully qualified domain name.

By default, Firewall Threat Defense sends only IP addresses in VPN load balancing redirection to a client.

Step 7 Select one of the **IKEv2 Redirect** phases:

- **Redirect during SA authentication**
- **Redirect during SA initialization**

Step 8 Click **OK**.

Step 9 Save your changes.

Configure Settings for Participating Devices

The device participation settings determine how the devices share load in VPN load balancing. Configure a participating device by enabling VPN load balancing on the device and defining device-specific properties. These values vary from device to device. You can provide a priority number for the devices participating in load balancing. A higher priority number gives the device a better chance to become the director over other devices. But you cannot select a device to be the director of the group.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** next to the remote access VPN policy that you want to modify.

Step 3 Click **Advanced** > **Load Balancing**.

Step 4 Turn on the **Enable Load balancing between member devices** toggle button to enable load balancing if you have not enabled already.

Step 5 Configure **Device Participation** settings:

The **Device Participation** section lists all the target devices of the selected remote access VPN configuration. You can configure these devices to share the load of the incoming VPN sessions.

a) Turn on the **Load Balancing** toggle button to enable load balancing for a device and then click **Edit**.
b) Enter the device **Priority**.

By default, the device priority is set to 5. You can choose a number from 1 trough 10.

c) Specify the **IPv4 NAT** or **IPv6 NAT** address for VPN interface IP address if the device is behind NAT.
d) Click **OK**.

Step 6 Click **Save** to save the remote access VPN policy settings.

Configuring IPsec Settings for Remote Access VPNs

The IPsec settings are applicable only if you selected IPsec as the VPN protocol while configuring your remote access VPN policy. If not, you can enable IKEv2 using the Edit Access Interface dialog box. See Configure Access Interfaces for Remote Access VPN, on page 1455 for more information.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced**.

The list of IPsec settings appears in a navigation pane on the left of the screen.

Step 4 Use the navigation pane to edit the following IPsec options:

a) **Crypto Maps**—The Crypto Maps page lists the interface groups on which IKEv2 protocol is enabled. Crypto Maps are auto generated for the interfaces on which IKEv2 protocol is enabled. To edit a Crypto Map, see Configure Remote Access VPN Crypto Maps, on page 1467. You can add or remove interface groups to the selected VPN policy in **Access Interface**. See Configure Access Interfaces for Remote Access VPN, on page 1455 for more information.

b) **IKE Policy**—The IKE Policy page lists all the IKE policy objects applicable for the selected VPN policy when Secure Client endpoints connect using the IPsec protocol. See IKE Policies in Remote Access VPNs, on page 1469 for more information. To add a new IKE policy, see Configure an IKEv2 policy object, on page 2472. Firewall Threat Defense supports only Secure Client IKEv2 clients. Third-party standard IKEv2 clients are not supported.

c) **IPsec/IKEv2 Parameters**—The IPsec/IKEv2 Parameters page enables you to modify the IKEv2 session settings, IKEv2 Security Association settings, IPsec settings, and NAT Transparency settings. See Configure Remote Access VPN IPsec/IKEv2 Parameters, on page 1471 for more information.

Step 5 Click **Save**.

Configure Remote Access VPN Crypto Maps

Crypto maps are automatically generated for the interfaces on which IPsec-IKEv2 protocol has been enabled. You can add or remove interface groups to the selected VPN policy in **Access Interface**. See Configure Access Interfaces for Remote Access VPN, on page 1455 for more information.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click the **Advanced** > **Crypto Maps**, and select a row in the table and click **Edit** to edit the Crypto map options.

Step 4 Select **IKEv2 IPsec Proposals** and select the transform sets to specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel.

Step 5 Select **Enable Reverse Route Injection** to enable static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint.

Step 6 Select **Enable Client Services** and specify the port number.

The Client Services Server provides HTTPS (SSL) access to allow the Secure Client Downloader to receive software upgrades, profiles, localization and customization files, CSD, SCEP, and other file downloads required by the client. If you select this option, specify the client services port number. If you do not enable the Client Services Server, users will not be able to download any of these files that the Secure Client might need.



Note You can use the same port that you use for SSL VPN running on the same device. Even if you have an SSL VPN configured, you must select this option to enable file downloads over SSL for IPsec-IKEv2 clients.

Step 7 Select **Enable Perfect Forward Secrecy** and select the **Modulus group**.

Use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the **Modulus Group** list.

Modulus group is the Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select the modulus group that you want to allow in the remote access VPN configuration:

- 1—Diffie-Hellman Group 1 (768-bit modulus).
- 2—Diffie-Hellman Group 2 (1024-bit modulus).
- 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher).
- 14—Diffie-Hellman Group 14 (2048-bit modulus, considered good protection for 128-bit keys).
- 19—Diffie-Hellman Group 19 (256-bit elliptical curve field size).
- 20—Diffie-Hellman Group 20 (384-bit elliptical curve field size).
- 21—Diffie-Hellman Group 21 (521-bit elliptical curve field size).
- 24—Diffie-Hellman Group 24 (2048-bit modulus and 256-bit prime order subgroup).

Step 8 Specify the **Lifetime Duration (seconds)**.

The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.

You can specify a value from 120 to 2147483647 seconds. The default is 28800 seconds.

Step 9 Specify the **Lifetime Size (kbytes)**.

The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires.

You can specify a value from 10 to 2147483647 kbytes. The default is 4,608,000 kilobytes. No specification allows infinite data.

Step 10 Select the following **ESPv3 Settings**:

- **Validate incoming ICMP error messages**—Choose whether to validate ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.
- **Enable 'Do Not Fragment' Policy**—Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header, and select one of the following from the **Policy** list:
  - Copy—Maintains the DF bit.
  - Clear—Ignores the DF bit.
  - Set—Sets and uses the DF bit.
- Select **Enable Traffic Flow Confidentiality (TFC) Packets**— Enable dummy TFC packets that mask the traffic profile which traverses the tunnel. Use the **Burst**, **Payload Size**, and **Timeout** parameters to generate random length packets at random intervals across the specified SA.

Note Enabling traffic flow confidentiality (TFC) packets prevents the VPN tunnel from being idle. Thus the VPN idle timeout configured in the group policy does not work as expected when you enable the TFC packets. See Advanced group policy option fields and values, on page 2467.

  - Burst—Specify a value from 1 to 16 bytes.
  - Payload Size—Specify a value from 64 to 1024 bytes.
  - Timeout—Specify a value from 10 to 60 seconds.

Step 11 Click **OK**.

Related Topics

Interfaces, on page 2383

IKE Policies in Remote Access VPNs

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

Note Firewall Threat Defense supports only IKEv2 for remote access VPNs.

Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy. Since peers choose during the Phase 1 negotiation, this makes it possible to create a single IKE proposal, but consider creating multiple, different proposals to give higher priority to your most desired options. For IKEv2, the policy object does not specify authentication, other policies must define the authentication requirements.

An IKE policy is required when you configure a remote access IPsec VPN.

Configuring Remote Access VPN IKE Policies

The IKE Policy table specifies all the IKE policy objects applicable for the selected VPN configuration when Secure Client endpoints connect using the IPsec protocol. For more information, see IKE Policies in Remote Access VPNs, on page 1469.



Note Firewall Threat Defense supports only IKEv2 for remote access VPNs.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced** > **IKE Policy**.

Step 4 Click **Add** to select from the available IKEv2 policies, or add a new IKEv2 policy and specify the following:

- **Name**—Name of the IKEv2 policy.
- **Description**—Optional description of the IKEv2 policy
- **Priority**—The priority value determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA).
- **Lifetime**— Lifetime of the security association (SA), in seconds
- **Integrity**—The Integrity Algorithms portion of the Hash Algorithm used in the IKEv2 policy.
- **Encryption**—The Encryption Algorithm used to establish the Phase 1 SA for protecting Phase 2 negotiations.
- **PRF Hash**—The pseudorandom function (PRF) portion of the Hash Algorithm used in the IKE policy. In IKEv2, you can specify different algorithms for these elements.
- **DH Group**—The Diffie-Hellman group used for encryption.

Step 5 Click **Save**.

Configure Remote Access VPN IPsec/IKEv2 Parameters

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 From the list of available VPN policies, select the policy for which you want to modify the settings.

Step 3 Click **Advanced** > **IPsec**> **IPsec/IKEv2 Parameters**.

Step 4 Select the following for **IKEv2 Session Settings**:

- **Identity Sent to Peers**—Choose the identity that the peers will use to identify themselves during IKE negotiations:
  - **Auto**—Determines the IKE negotiation by connection type: IP address for preshared key, or Cert DN for certificate authentication (not supported).
  - **IP address**—Uses the IP addresses of the hosts exchanging ISAKMP identity information.
  - **Hostname**—Uses the fully qualified domain name (FQDN) of the hosts exchanging ISAKMP identity information. This name comprises the hostname and the domain name.
- **Enable Notification on Tunnel Disconnect**—Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. Sending this notification is disabled by default.
- **Do not allow device reboot until all sessions are terminated**—Check to enable waiting for all active sessions to voluntarily terminate before the system reboots. This is disabled by default.

Step 5 Select the following for **IKEv2 Security Association (SA) Settings**:

- **Cookie Challenge**—Whether to send cookie challenges to peer devices in response to SA initiated packets, which can help thwart denial of service (DoS) attacks. The default is to use cookie challenges when 50% of the available SAs are in negotiation. Select one of these options:
  - **Custom**—Specify **Threshold to Challenge Incoming Cookies**, the percentage of the total allowed SAs that are in-negotiation. This triggers cookie challenges for any future SA negotiations. The range is zero to 100%. The default is 50%.
  - Always— Select to send cookie challenges to peer devices always.
  - Never— Select to never send cookie challenges to peer devices.
- **Number of SAs Allowed in Negotiation**—Limits the maximum number of SAs that can be in negotiation at any time. If used with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check. The default is 100 %.
- **Maximum number of SAs Allowed**—Limits the number of allowed IKEv2 connections.

Step 6 Select the following for **IPsec Settings**:

- **Enable Fragmentation Before Encryption**—This option lets traffic travel across NAT devices that do not support IP fragmentation. It does not impede the operation of NAT devices that do support IP fragmentation.

- **Path Maximum Transmission Unit Aging**—Check to enable PMTU (Path Maximum Transmission Unit) Aging, the interval to Reset PMTU of an SA (Security Association).
- **Value Reset Interval**—Enter the number of minutes at which the PMTU value of an SA (Security Association) is reset to its original value. Valid range is 10 to 30 minutes, default is unlimited.

Step 7 Select the following for **NAT Settings**:

- **Keepalive Messages Traversal**—Select whether to enable NAT keepalive message traversal. NAT traversal keepalive is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow. If you select this option, configure the interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The value can be from 10 to 3600 seconds. The default is 20 seconds.
- **Interval**—Sets the NAT keepalive interval, from 10 to 3600 seconds. The default is 20 seconds.

Step 8 Click **Save**.

Customize Cisco Secure Client

You can configure the Secure Client customizations using the management center and deploy them to the VPN headend. The threat defense device distributes these customizations to the endpoint when a user connects from the Secure Client. Administrators can customize the following elements at the endpoint:

Table 83: Secure Client Customizations Available in Management Center

Customization	Description	More Info
GUI text and messages	Customize or localize Secure Client GUI text and informational/error messages.	Customize and Localize Secure Client GUI Text and Messages, on page 1476
Icons and images	Customize the logo, images, or icons of the Secure Client GUI.	Customize Secure Client Icons and Images, on page 1477
Scripts	Deploy scripts on the endpoint devices when a client establishes or disconnects a VPN session.	Deploy Scripts on Endpoint Devices Using Secure Client, on page 1478
Binaries	Deploy custom applications using Secure Client APIs.	Deploy Custom Applications Using Cisco Secure Client APIs, on page 1480
Custom Installer Transforms	Customize the Secure Client installer.	Customize the Secure Client Installer, on page 1481
Localized Installer Transforms	Localize the Secure Client installer.	Localize the Client Installer, on page 1481

Overview of the customization file

The customization file is an XML-based configuration object in the Threat Defense device that controls the visual appearance and layout of Secure Client to remote VPN users. It defines:

- Branding—logos and color schemes
- Page structure—logon page and portal layout
- Content elements—titles, banners, and button labels
- Messaging—error messages and other user-facing text

By default, a Threat Defense device has two customization objects:

- Template: A blank XML template file that you can update to add the required customizations. You cannot delete this file.
- DfltCustomization: An XML file with a set of URLs and basic customization to bring up the Secure Client. This is the default customization file.

  To view these customization files, run the **show import webvpn customization** command on the Threat Defense device:

```
FTD(config)# show import webvpn customization
Template
DfltCustomization
```

Customize the customization file

To update the **Template** XML file:

1. Export the file to disk0. You can rename the file, if required.

```
FTD(config)# export webvpn customization Template disk0:ABCTemplate
```

2. Copy the XML file to a remote PC.
3. Edit the XML file with the required customizations and copy it back to disk0.
4. Import the file to the Threat Defense device.

```
FTD(config)# import webvpn customization ABCTemplate disk0:ABCTemplate
```

5. Verify the customization files in the device.

```
FTD(config)# show import webvpn customization
Template
DfltCustomization
ABCTemplate
```



Note You can also update the **DfltCustomization** file using the same procedure as above. You can also rename this file.

Upload the customization file to Management Center

1. Choose **Objects** > **Object Management** > **VPN** > **Secure Client File** and click **Add Secure Client File**.

2. In the **Add Secure Client File** dialog box, configure these parameters:
   a. In the **Name** file, enter the name of the customization file.
   b. From the **File Type** drop-down list, choose **Secure Client VPN Profile**.
   c. Click **Browse**, locate and select the customization file that you want to upload.
   d. Click **Save**.
3. Choose **Devices** > **VPN** > **Remote Access**.
4. Click the edit icon next to the remote access VPN policy.
5. Click the **Advanced** tab.
6. In the left pane, click **Group policies**.
7. Click **+** to add a group policy.
8. In the **Add Group Policy** dialog box, configure these parameters:
   a. Enter a **Name** and optionally a **Description** for this policy.
   b. Click the **Secure Client** tab, and from the **Client Profile** drop-down list, choose the customization file.
   c. Click **Save**.
9. Choose this group policy as the selected policy in the **Group Policy** dialog box, click **OK**, and click **Deploy**.

Guidelines and Limitations for Secure Client Customizations

Guidelines

- Ensure that you import the xml file to the object defined as `DfltCustomization`. When you import the customization object, the Firewall Management Center checks the XML code for validity.

  For example:

  ```
  hostname# import webvpn customization DfltCustomization
  disk0:/csm/defaultcustomizationwebvpn.xml
  ```

- Add the Windows Cisco Secure Client headend deployment package to the remote access VPN policy before deploying customization commands. This package must be included when supporting Windows, MacOS, or Linux clients.

General Limitations

- If there are any customizations earlier than 7.4 configured directly on the threat defense using the CLI, the management center removes these customizations during deployment.
- No clustering support.

Table 84: Limitations for Secure Client Customizations

Customization	Limitations

GUI Text and Message Customizations	• You must restart Secure Client before you use this customization.
	• No support for right-to-left languages.
	• Some strings are truncated in the GUI due to hardcoded field lengths.
	• Some messages are hardcoded in the client. For example:
	  • Status messages (during an update)
	  • Untrusted server messages
	  • Deferred update messages
	• Localization is version-specific.
	If an Administrator created a translation table based on a template of an old Secure Client version, the new messages do not appear to the remote users. The Administrator must merge the latest template with the translation table so that the table has the new messages. You can use third-party tools like Get text to perform the merge.

Icons and Images Customizations	• You must restart Secure Client before you use this customization. • The customization object names must match the Secure Client GUI filenames. File names are different for each operating system and are case-sensitive. For more information about the filenames, extensions, and sizes for each OS, see the Cisco Secure Client Administrator Guide. • Images do not appear properly if the image size is not correct. The management center or the threat defense device does not verify the image size. • MacOS does not support customization of Secure Client images and icons.
Deploy Customized Scripts	• Secure Client runs only one OnConnect and one OnDisconnect script; however, these scripts may launch other scripts. • Scripts can only execute functions that the user has the right to invoke. • You cannot launch the OnConnect script from the Start Before Logon (SBL) GUI.
Deploy Custom Applications Using Cisco Secure Client APIs (Binaries)	• After you use this customization, if you deploy an updated version of the Secure Client on the management center, the client will download the update and replace your custom UI.

Customization	Limitations
Customize the Client Installer	• This customization is available only for Windows.

Customize and Localize Secure Client GUI Text and Messages

You can customize the Secure Client GUI text and the informational/error messages. You also can customize the GUI text and all messages to appear in a preferred language.

Customize GUI Text and Messages

To customize the GUI text or messages, you can edit the messages in the message file. You can update the messages to include more details in the error messages. For example:

- Modify any label in the login dialog box such as **Password** to **Domain Password**.
- Add your support contact details in the error messages.

Localize GUI Text and Messages

Threat defense devices use translation tables to translate the labels and user messages displayed in the Secure Client. When a user connects to the remote access VPN, the Secure Client identifies the locale set on the endpoint and downloads the translation file. Threat defense devices support 128 locales. By default, Secure Client is installed in English.

- For Cisco Secure Client 5.0, the default localization files for various languages are part of the application.
- For AnyConnect Clients 4.x, you can download the localization files for a few languages from Cisco.com and upload them to the management center.

How to Customize Secure Client GUI Text and Messages

Before you begin

Configure one or more remote access VPN policies.

Procedure

Step 1 Get the base template or translation file either from the Secure Client package or from Cisco.com. For example, AnyConnect.po.

Step 2 Use a text editor to add the translations or customize the labels or messages.

Step 3 Update the **msgstr** string corresponding to each **msgid**.

Step 4 Save the file.

Step 5 Create a new Secure Client Customization object.

a) Choose **Objects** > **Object Management** > **VPN** > **Secure Client Customization**.
b) Click **Add Secure Client Customization**.
c) Enter the name and description for the customization.
d) From the **Customization Type** drop-down list, choose **GUI Text and Messages**.
e) From the **Language** drop-down list, choose a language for which you are adding the translation.

f) Click **Browse** and select the translation file. The supported file extensions are .po, .mo, and .txt.

Step 6 Add the customization to the remote access VPN policy.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click the edit icon of the remote access VPN policy.
c) Click **Advanced > Secure Client Customizations > Localization**.
d) Click **+** to select the translation file.
e) Click **Add**.
f) Click **OK**.

Step 7 Click **Save**.

Step 8 Choose **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Verify the Secure Client customizations. For more information, see Verify Secure Client Customizations, on page 1482.

Customize Secure Client Icons and Images

You can customize the logo, images, and icons of the Secure Client GUI using the management center.

To customize the logo, images, and icons of the Secure Client GUI, you must create a Secure Client customization object in the management center. The name of this customization object must match the Secure Client GUI filename. File names are different for each operating system and are case-sensitive. For more information about the filenames, extensions, and sizes for each OS, see the Cisco Secure Client Administrator Guide.

For example, if you want to replace the corporate logo for Windows clients, you must create a customization object with the name as `company_logo` and add this customization object to the remote access VPN policy. If you use a different name for the customization object, the Secure Client installer does not change the component. However, if you deploy your own executable to customize the GUI, the customization object can have any name.

Location of all images files:

- Windows: **%PROGRAMFILES%\Cisco\Cisco Secure Client\res**
- Linux: **/opt/cisco/secureclient/resources** or **/opt/cisco/anyconnect/resources**
- macOS: Not supported



Note When the remote access VPN connection is established, the logo or images are downloaded to the client directory. Ensure that you restart the client for the updated logo or images to appear in your client.

How to Customize Secure Client Images and Icons

Before you begin

Configure one or more remote access VPN policies.

Procedure

Step 1 Create the icons or images using the correct extensions, and sizes.

Images do not appear properly if the image size is not correct. The management center or the threat defense device does not verify the image size.

For more information about the filenames, extensions, and sizes, see the Cisco Secure Client Administrator Guide.

Step 2 Create a new Secure Client Customization object.

a) Choose **Objects** > **Object Management** > **VPN** > **Secure Client Customization**.
b) Click **Add Secure Client Customization**.
c) Enter the name and description for the customization object.

Ensure that the customization object name matches the Secure Client GUI filenames. For more information about the filenames, see the Cisco Secure Client Administrator Guide.

d) From the **Customization Type** drop-down list, choose **Icon and Images**.
e) From the **Platform** drop-down list, choose a platform.
f) Click **Browse** and select the file. The supported file extensions are .png, .ico, and .jpeg.
g) Repeat the steps from 2a - f to add multiple icons and images.

Step 3 Add the customization object to the remote access VPN policy.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click the edit icon of the remote access VPN policy.
c) Click **Advanced > Secure Client Customizations > Icons and Images**.
d) Click **+** to select the file.
e) Click **Add**.
f) Click **OK**.

Step 4 Click **Save**.

Step 5 Choose **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Verify the Secure Client customizations. For more information, see Verify Secure Client Customizations, on page 1482.

Deploy Scripts on Endpoint Devices Using Secure Client

Secure Client lets you download and run scripts when the following events occur:

- Establishment of a new client VPN session with the threat defense. The script triggered by this event is an OnConnect script because it requires this filename prefix. Reconnection of the VPN session does not trigger this script.
- Disconnection of a client VPN session with the threat defense. The script triggered by this event is an OnDisconnect script because it requires this filename prefix.

These scripts run asynchronously and do not delay the connection establishment or disconnection. They can be of any extension and must be executable on the endpoint. Secure Client identifies the OnConnect and OnDisconnect scripts by the filename. It looks for a file whose name begins with OnConnect or OnDisconnect regardless of the file extension.

Some examples of this feature are:

- Refresh the group policy upon VPN connection.
- Mount a network drive upon a VPN connection.
- Unmount a network drive upon a VPN disconnection.

To enable scripts, check the **Enable Scripting** option in the VPN profile. By default, the client does not launch scripts. The client does not require the script to be written in a specific language. It requires an application that can run the script to be installed on the client computer. For the client to launch the script, the script must run from the command line.

Secure Client can only launch scripts after the user logs in and establishes a VPN session. You cannot launch the OnConnect script from the Start Before Logon (SBL) GUI. You must check the **Enable Post SBL On Connect Script** option in the VPN profile to trigger the scripts once the user logs in. Secure Client is a 32-bit application. When the scripts run on a 64-bit Windows version, they use the 32-bit version of cmd.exe.

How to Add Customized Scripts for Secure Client

Before you begin

1. Configure a remote access VPN.
2. Enable scripting in the VPN profile.
3. Add the VPN profile to the remote access VPN group policy.

Procedure

Step 1 Create OnConnect and OnDisconnect scripts for a platform.

Step 2 Create a new Secure Client Customization object.

a) Choose **Objects** > **Object Management** > **VPN** > **Secure Client Customization**.
b) Click **Add Secure Client Customization**.
c) Enter the name and description for the customization.
d) From the **Customization Type** drop-down list, choose **Scripts**.
e) From the **Platform** drop-down list, choose a platform.
f) Select one of the following:

- **On Connect**: To select an OnConnect script.

- **On Disconnect**: To select an OnDisconnect script.

g) Click **Browse** and select the script you want to execute on the endpoint.

Step 3 Add the customization to the remote access VPN policy.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click the edit icon of the remote access VPN policy.
c) Click **Advanced > Secure Client Customizations > Localization**.
d) Click **+** to select the translation file.
e) Click **Add**.
f) Click **OK**.

Step 4 Click **Save**.

Step 5 Choose **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Verify the Secure Client customizations. For more information, see Verify Secure Client Customizations, on page 1482.

Deploy Custom Applications Using Cisco Secure Client APIs

For Windows, Linux, or MacOs machines, you can create and deploy a custom client that uses the Secure Client APIs. You can use this client binary file to replace the Secure Client GUI or CLI binary files.

Your executable can call any resource files such as logo images that you import to the management center. When you deploy your own executable, you can use any filenames for your resource files.

The following table lists the filenames of the client executable files for the different operating systems:

Table 85: Filenames of the Secure Client Executable Files

Client OS	Client GUI File	Client CLI File
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
MacOS	Not supported by the management center deployment. However, you can deploy an executable for the macOS that replaces the client GUI using other means, such as Altiris Agent.	vpn

How to Deploy Custom Applications Using Cisco Secure Client API

Before you begin

Configure one or more remote access VPN policies.

Procedure

Step 1 Create the custom application using the Cisco Secure Client APIs.

Step 2 Create a new Secure Client Customization object.

a) Choose **Objects** > **Object Management** > **VPN** > **Secure Client Customization**.
b) Click **Add Secure Client Customization**.
c) Enter the name and description for the customization.
d) From the **Customization Type** drop-down list, choose **Binary**.
e) From the **Platform** drop-down list, choose a platform.
f) Click **Browse** and select the custom application.

Step 3 Add the customization to the remote access VPN policy.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click the edit icon of the remote access VPN policy.
c) Click **Advanced > Secure Client Customizations > Binaries**.
d) Click **+** to select the translation file.
e) Click **Add**.
f) Click **OK**.

Step 4 Click **Save**.

Step 5 Choose **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Customize the Secure Client Installer

You can customize the Secure Client GUI by creating a custom transform that deploys with the client installer program. You can import the transform to the management center and deploy it to the threat defense device. The threat defense deploys this transform to the endpoint using the client installer program.

Note This customization is available only for Windows.

Localize the Client Installer

You can translate the messages displayed by the Cisco Secure Client installer. The management center uses a transform to translate the messages displayed by the installer. The transform alters the installation but leaves the original security-signed MSI intact. These transforms only translate the installer screens and do not translate the client GUI screens.

Every release of Cisco Secure Client includes a localized transform that administrators can upload to the management center whenever they upload Cisco Secure Client packages with new software. If you use our localization transform, ensure that you update them with the latest release from Cisco.com whenever you upload a new Cisco Secure Client package.

How to Customize or Localize the Client Installer

Before you begin

Configure one or more remote access VPN policies.

Procedure

Step 1 Create a customized or localized transform.

Step 2 Create a new Secure Client Customization object.

a) Choose **Objects** > **Object Management** > **VPN** > **Secure Client Customization**.
b) Click **Add Secure Client Customization**.
c) Enter the name and description for the customization.
d) From the **Customization Type** drop-down list, choose **Customized Installer Transform** or **Localized Installer Transform**.
e) From the **Platform** drop-down list, choose a platform.
f) Click **Browse** and select the transform.

Step 3 Add the customization to the remote access VPN policy.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click the edit icon of the remote access VPN policy.
c) Click **Advanced > Secure Client Customizations > Custom Installer Transforms** or **Localized Installer Transforms**.
d) Click **+** to select the transform.
e) Click **Add**.
f) Click **OK**.

Step 4 Click **Save**.

Step 5 Choose **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Verify Secure Client Customizations

Validate the Deployment

After the deployment is complete, validate the deployment in the management center. Click the **Transcript Details** ( )) icon to verify the commands generated for the customizations.

Examples

1. The example below shows the transcript details of a GUI text and messages customization: Secure Client en_us localization with customized prompts.

```
import webvpn translation-table AnyConnect language en-us disk0:/AnyConnect_en-us.po
```

2. The example below shows the transcript details of customized icons and images: customization of the Secure Client logo to ABC logo.

```
import webvpn AnyConnect-customization type resource platform win name company_logo.png
 disk0:/company_logo.png
```

3. The example below shows the transcript details of the customized OnConnect and OnDisconnect scripts. The On connect script mounts the network drive and the On disconnect script unmounts the network drive.

```
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnConnect_mount.bat disk0:/mount.bat
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnDisconnect_unmount.bat disk0:/unmount.bat
```

Verify Customizations Using Threat Defense Commands

Use the following commands on the threat defense to verify the customizations:

- **show import webvpn translation-table detailed**: Shows the available translation tables.

```
HQ-FTD# show import webvpn translation-table detailed
 Translation Tables' Templates:
   AnyConnect           ia4DaAXNSvl5pZboQRGJcs9KMXY=
   customization
 Translation Tables:
   fr                   customization        BWWodsOt1PbvDvYOp8hLb3W7a64=
   ja                   customization        lNvUk1+qTLNZyNrBcApMQPHnm1M=
   ru                   customization        UqyKyUAcjR+xTGUtdiIFnoIiW5U=
```

- **show import webvpn AnyConnect-customization detailed**: Shows the details of the Secure Client customizations.

```
HQ-FTD# show import webvpn AnyConnect-customization detailed
OEM resources for AnyConnect client:
  linux-64/binary/scripts_OnConnect_conn.sh           w6+n7z80D/8AR+ul2f7DvTmcDTw=
  linux-64/binary/scripts_OnDisconnect_discon.sh      jx5LJC2XBEmEkGeww59CAkszvnI=
  linux-64/resource/company-logo.png                  GsfBDroqGSQEEwuBDS/3DJNVv88=
  win/binary/scripts_OnConnect_mount.bat              dzjfsLYYft/XMlPlzskKl+Wv1bw=
  win/binary/scripts_OnDisconnect_unmount.bat         k6xlKhF1l2IRyJu08+sdYXgKNgM=
  win/resource/company_logo.png                       cmEvxwqvtaS+Pz/6sb9n3NZudS4=
```

Verify Customizations in Secure Client

- In Secure Client, click the **Message History** tab to verify that the customizations are downloaded.

  Use the DART tool to view the client-side diagnostics.

Table 86: Verifying the Customizations in Secure Client

Customization	Verification
GUI text and message customizations	• Verify if Secure Client has the language localization or customized files in the following locations: • Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<language-code>\LC_MESSAGES (AnyConnect versions 4.9 and earlier) • Windows: %ProgramData%\Cisco\Cisco Secure Client\l10n\<language-code>\LC_MESSAGES (Secure Client versions 5.0 and later) • For Mac OS and Linux: /opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES /opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES • Verify the contents of the localized or customized file and confirm if they have the customized or localized strings. For example: AnyConnect.mo
Image and icon customizations	• Verify if Secure Client has the customized files in the following locations: • Windows: %PROGRAMFILES%\ Cisco\Cisco AnyConnect Secure Mobility Client\res\ (AnyConnect versions 4.10 and earlier) • Windows: %PROGRAMFILES%\ Cisco\Cisco Secure Client\UI\res (Cisco Secure Client 5.0 and above) • Linux: /opt/cisco/anyconnect/resources or /opt/cisco/secureclient/resources • Verify the content of the customized icon or image file.
Customized OnConnect and OnDisconnect scripts	• Verify if the customized scripts are in the following locations: • Windows: %ProgramData%\Cisco\Cisco Secure Client\Script (Cisco Secure Client 5.0 and above) • Windows: %ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Script (AnyConnect versions 4.9 and earlier) • Mac OS and Linux: /opt/cisco/anyconnect/script or /opt/cisco/secureclient/vpn/script • Verify the script.

Configure Secure Client Management VPN Tunnel

A management VPN tunnel provides connectivity to the corporate network whenever a client system is powered up, without the VPN users having to connect to the VPN. This helps organizations keep their endpoints up-to-date with software patches and updates. Management tunnel disconnects when the user-initiated VPN tunnel is established.

This section provides information about configuring Secure Client management VPN tunnel on Firewall Threat Defense. Configuring the Secure Client management tunnel on Firewall Threat Defense using the Firewall Management Center web interface requires the following settings:

- A **Connection profile** with certificate-based authentication and a group URL.
- **Secure Client management VPN profile file**, configured a server with group URL and backup servers if required.
- A **Group policy** with the management VPN profile, split tunneling with explicitly included networks, client bypass protocol, and no banner.

For detailed instructions on configuring the Secure Client Management VPN tunnel, see Configuring Secure Client Management VPN Tunnel on Firewall Threat Defense, on page 1486.

Requirements and Prerequisites for Secure Client Management VPN Tunnel

Software and Configuration Requirements

Ensure that you have the following before you configure the Secure Client Management tunnel on using the Firewall Threat Defense using the Firewall Management Center web interface:

- Ensure that you are using Firewall Threat Defense and Firewall Management Center versions 6.7.0 or above.
- Download the Secure ClientSecure Client VPN Webdeploy package 4.7 or above and upload it to Firewall Threat Defense remote access VPN.
- Ensure that the certificate authentication is configured in the connection profile.
- Ensure that no banner is configured in the group policy.
- Check the split tunneling configuration in the management tunnel-group policy.

Certificate Requirements

- Firewall Threat Defense must have a valid identity certificate for remote access VPN and the root certificate from the local certifying authority (CA) must be present on the Firewall Threat Defense.
- Endpoints connecting to the management VPN tunnel must have a valid identity certificate.
- CA certificate for Firewall Threat Defense's identity certificate must be installed on the endpoints and the CA certificate for the endpoints must be installed on the Firewall Threat Defense.
- The identity certificate issued by the same local CA must be present in the Machine store.

  Certificate Store (For Windows) and/or in System Keychain (For macOS).

Limitations of Secure Client Management VPN Tunnel

- Secure Client Management VPN Tunnel supports only certificate authentication, it does not support AAA-based authentication.
- Public or private proxy settings are not supported.
- Secure Client upgrade and AnyConnect module download are not supported when the management VPN tunnel is connected.

Configuring Secure Client Management VPN Tunnel on Firewall Threat Defense

Procedure

Step 1 **Create a remote access VPN policy configuration using the wizard**:

For information about configuring a remote access VPN, see Configuring a New Remote Access VPN Connection, on page 1425.

Step 2 **Configure connection profile settings for management VPN tunnel**:

Note It is advisable to create a new connection profile to be used only for Secure Client management VPN tunnel.

a) Edit the remote access VPN policy you have created.
b) Select and edit the connection profile that will be used for management VPN tunnel.
c) From **AAA** drop-down menu, choose **Authentication Method** and click **Client Certificate Only**. Configure the authorization and accounting settings as required.
d) Click the **Aliases** tab of the connection profile.
e) Click **Add (+)** under URL Aliases and **URL Alias** for the connection profile.
f) Click **Enabled** to enable the URL.
g) Click **OK** and then click **Save** to save the connection profile settings.

For more information about connection profile settings, see Configure Connection Profile Settings, on page 1436.

Step 3 **Create a management tunnel profile using the Secure Client profile editor**:

a) Download the Secure Client **VPN Management Tunnel Standalone Profile Editor** from Cisco Software Download Center if you have not done already.
b) Create a management tunnel profile with the required settings for your VPN users and save the file.
c) Configure a server in the Server List with the group URL you have configured in the connection profile.

For information about creating a management profile using the Profile Editor, see the *Cisco Secure Client (including AnyConnect) Administrator Guide*.

Step 4 **Create a management tunnel object**:

a) On your Secure Firewall Management Center web interface, navigate to **Objects** > **Object Management** > **VPN** > **Secure Client File**
b) Click **Add Secure Client File**.

c) Specify the **Name** for the Secure Client file.
d) Click **Browse** and select the management tunnel profile file you have saved.
e) Click the **File Type** drop-down and select **Secure Client Management VPN Profile**.
f) Click **Save**.

Note You an also create the management tunnel object when you create or update Secure Client settings for a group policy. See Group policy options for Secure Client, on page 2464.

Step 5 **Associate a management profile with a group policy and configure group policy settings**:

You must add the management VPN profile to the group policy associated with the connection profile used for the management tunnel VPN connection. When the user connects, the management VPN profile is downloaded along with the user VPN profile already mapped to the group policy, enabling the management VPN tunnel feature.

Caution **No Banner**: Check and ensure that no banner is configured in the group policy settings. You can check the banner settings under **Group Policy** > **General Settings** > **Banner**.

a) Edit the connect profile you have created for management VPN tunnel.
b) Click **Edit Group Policy** > **Secure Client** > **Management Profile Edit Group Policy** and choose **AnyConnect Secure Client**, then click **Management Profile**.
c) Click the **Management VPN Profile** drop-down and select the management profile file object you have created.

Note You can also click + and add a new Secure Client Management VPN Profile object.

d) Click **Save**.

Step 6 **Configure split tunneling in group policy**:

a) Click **Edit Group Policy** and then choose **General**, then click **Split Tunneling**.
b) From the IPv4 or IPv6 split tunneling drop-down, select **Tunnel networks specified below**.
c) Select the Split Tunnel Network List Type: **Standard Access List** or **Extended Access List**, and then select the required access list to allow the traffic over the management VPN tunnel.
d) Click **Save** to save the split tunnel settings.

Secure Client Custom Attribute

Secure Client Management VPN tunnel requires split include tunneling configuration by default. If you are configuring Secure Client custom attribute in the group policy to deploy the management VPN tunnel with split tunneling to tunnel all, you can do so using FlexConfig because Firewall Management Center 6.7 web interface does not support Secure Client custom attribute .

The following is an example command for Secure Client custom attribute:

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
```

```
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

Step 7 **Deploy, verify, and monitor the remote access VPN policy**:

a) Deploy the management VPN tunnel configuration to Firewall Threat Defense.

Note Client systems must connect to the Firewall Threat Defense remote access VPN once to download the management tunnel VPN profile to the client machines.

b) You can verify the Secure Client management VPN tunnel at **AnyConnect Secure Mobility ClientSecure Mobility Client** and choose **VPN**, then click **Statistics**.

You can also check the management VPN session details on the Firewall Threat Defense command prompt using the **show vpn-sessiondb anyconnect** command.

c) On your Firewall Management Center web interface, click **Analysis** to view the management tunnel session information.

Related Topics

Configure Connection Profile Settings, on page 1436
Firewall Threat Defense group policy objects, on page 2460

Multiple Certificate Authentication

Multiple certificate based authentication gives the ability to have the Firewall Threat Defense validate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow VPN access using the Secure Client during SSL or IKEv2 EAP phase.

The multiple certificates option allows certificate authentication of both the machine and user via certificates. Without this option, you could only do certificate authentication of either machine or the user, but not both.

Guidelines and Limitations of Multiple Certificate Authentication

Note When you configure multiple certificate authentication, ensure that you set the value of **AutomaticCertSelection** to true in the Cisco Secure Client Profile settings.

- Multiple certificate authentication currently limits the number of certificates to two.
- Secure Client must indicate support for multiple certificate authentication. If that is not the case then the gateway uses one of the legacy authentication methods or fails the connection. Secure Client version 4.4.04030 or later supports Multi-Certificate based authentication.
- Secure Client supports only RSA-based certificates.
- Only SHA256, SHA384, and SHA512 based certificate are supported during the Secure Client aggregate authentication.

- Certificate authentication cannot be combined with SAML authentication.

Configuring Multiple Certificate Authentication

Before you begin

Before you configure multiple certificate authentication, ensure that you have configured the certificate enrollment object that is used to obtain the identity certificate for each Firewall Threat Defense device. For more information, see Certificate map objects, on page 2457.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select the remote access VPN policy and click **Edit**.

Note If you have not configured a remote access VPN, click **Add** to create a new remote access VPN policy.

Step 3 Select and **Edit** a connection profile to configure multiple certificate authentication.

Step 4 Click **AAA** settings and select **Authentication Method** > **Client Certificate Only** or **Client Certificate & AAA**.

Note Select the **Authentication Server** if you have selected the Client Certificate & AAA authentication method

Step 5 Select the **Enable multiple certificate authentication** checkbox.

Step 6 Choose one of the certificates to **Map username from client certificate**:

- **First Certificate**— Select this option to map the username from the machine certificate sent from the VPN client.
- **Second Certificate**— Select this option to map the username from the user certificate sent from the client.

The username sent from the client is used as the VPN session username when certificate only authentication is enabled. When AAA and certificate authentication is enabled, VPN session username will be based on prefill option.

Note If you select the **Map specific field** option, which includes the username from the client certificate, the **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively.

If you select the **Use entire DN (Distinguished Name) as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields that can be used as the identifier when matching users to a connection profile DN rules are used for enhanced certificate authentication.

If you have selected the Client Certificate & AAA authentication, select the **Prefill username from certificate on user login window** option to prefill the secondary username from the client certificate when the user connects via AnyConnect VPN module of Cisco Secure Client.

- **Hide username in login window**: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.

Step 7 Configure the required AAA settings and connection profile settings for the remote access VPN.

Step 8 Save the connection profile and remote access VPN configuration and deploy it on your Firewall Threat Defense device.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 1439

Customizing Remote Access VPN AAA Settings

This section provides information about customizing your AAA preferences for remote access VPNs. For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.

Authenticate VPN Users via Client Certificates

You can configure remote access VPN authentication using client certificate when you create a new remote access VPN policy using the wizard or by editing the policy later.

Before you begin

Configure the certificate enrollment object that is used to obtain the identity certificate for each Firewall Threat Defense device that acts as a VPN gateway.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**; or click **Add** to create a new remote access VPN policy.

Step 3 For a new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Click **AAA** > **Authentication Method** > **Client Certificate Only**.

With this authentication method, the user is authenticated using a client certificate. You must configure the client certificate on VPN client endpoints. By default, the user name is derived from client certificate fields CN and OU respectively. If the user name is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.

If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display the following default values, respectively: **CN (Common Name)** and **OU (Organisational Unit)**. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

- Primary and Secondary fields pertaining to the **Map specific field** option contain these common values:
  - C (Country)
  - CN (Common Name)
  - DNQ (DN Qualifier
  - EA (Email Address)
  - GENQ (Generational Qualifier)
  - GN (Given Name)
  - I (Initial)
  - L (Locality)
  - N (Name)
  - O (Organisation)
  - OU (Organisational Unit)
  - SER (Serial Number)
  - SN (Surname)
  - SP (State Province)
  - T (Title)
  - UID (User ID)
  - UPN (User Principal Name)
- Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.

Step 5 Save your changes.

Related Topics

Configure Connection Profile Settings, on page 1436

Add certificate enrollment objects, on page 2402

Configure VPN User Authentication via Client Certificate and AAA Server

When you configure remote access VPN authentication to use both client certificate and authentication server, VPN client authentication is done using both the client certificate validation and AAA server.

Before you begin

- Configure the certificate enrollment object that you use to obtain the identity certificate for each Firewall Threat Defense device that acts as a VPN gateway.
- Configure the RADIUS server group object and any AD or LDAP realms to use in the remote access VPN policy configuration.
- Ensure that the AAA Server is reachable from the Secure Firewall Threat Defense device for the remote access VPN configuration to work.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy for which you want to update the authentication or click **Add** to create new one.

Step 3 If you choose to create new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Go to **AAA** and from the **Authentication Method** drop-down, choose **Client Certificate & AAA**.

- When you select the **Authentication Method** as:

  Client Certificate & AAA—Both types of authentication are done.

  - **AAA**—If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must manually select the **Authorization Server** and **Accounting Server** respectively.
  - **Client Certificate**—Authenticates the user with client certificate. You must configure client certificate on the VPN client endpoints. By default, the username is derived from client certificate fields CN & OU respectively. If you use any other field in the client profile to specify the username, use **Primary Field** and **Secondary Field** to map appropriate fields.

    If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN as username** option, the system automatically retrieves the user identity. A distinguished name (DN) is a unique identification, made up of individual fields that can be used as the identifier when matching users to a connection profile. DN rules are used for enhanced certificate authentication.

    Primary and Secondary fields pertaining to the **Map specific field** option contains these common values:

- C (Country)
- CN (Common Name)
- DNQ (DN Qualifier
- EA (Email Address)
- GENQ (Generational Qualifier)
- GN (Given Name)
- I (Initial)
- L (Locality)
- N (Name)
- O (Organisation)
- OU (Organisational Unit)
- SER (Serial Number)
- SN (Surname)
- SP (State Province)
- T (Title)
- UID (User ID)
- UPN (User Principal Name)

- Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.

Step 5 Save your changes.

Related Topics

Configure Connection Profile Settings, on page 1436
Add certificate enrollment objects, on page 2402

Manage Password Changes over VPN Sessions

Password management allows remote access VPN policy administrator to configure the notification settings for the remote access VPN users on their password expiry. Password management is available in AAA settings with authentication methods AAA Only and Client Certificate & AAA. For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access VPN policy that you want to update.

Step 3 Click **Edit** on the connection profile that includes AAA settings.

Step 4 Choose **AAA** > **Advanced Settings** > **Password Management**.

Step 5 Check the **Enable Password Management** check-box and select one of the following:

- Notify User - days ahead of password expiry and specify the number of days in the box.
- Notify user on the day of password expiration.

Step 6 Save your changes.

Related Topics

Configure Connection Profile Settings, on page 1436

Send Accounting Records to the RADIUS Server

Accounting records in remote access VPN help the VPN administrator track the services that users access and the amount of network resources that they consume. Accounting information includes when user session start and stop, username, the number of bytes that pass through the device for each session, the service used, and the duration of each session.

You can use accounting alone or together with authentication and authorization. When you activate AAA accounting, the network access server reports the user activity to the configured accounting server. You can configure a RADIUS server as the accounting server so that the Firewall Management Center sends all the user activity information to the RADIUS server.

Note You can use the same RADIUS server or separate RADIUS servers for authentication, authorization, and accounting in remote access VPN AAA settings.

Before you begin

- Configure a RADIUS group object with RADIUS servers to receive authentication requests or accounting records. For more information, see RADIUS server group configuration options, on page 2346.
- Ensure that the RADIUS server is reachable from the Firewall Threat Defense device. Configure routing on your Secure Firewall Management Center at **Devices** > **Device Management**, and click **Edit** (✎). Then, click the **Routing** tab to ensure connectivity to the RADIUS server.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** on the remote access policy for which you want to configure RADIUS server, or create new remote access VPN policy.

Step 3 Click **Edit** on the connection profile that includes AAA settings and choose **AAA**.

Step 4 Select the RADIUS server from the **Accounting Server** drop-down.

Step 5 Save your changes.

Related Topics

Configure Connection Profile Settings, on page 1436
Configure AAA Settings for Remote Access VPN, on page 1439

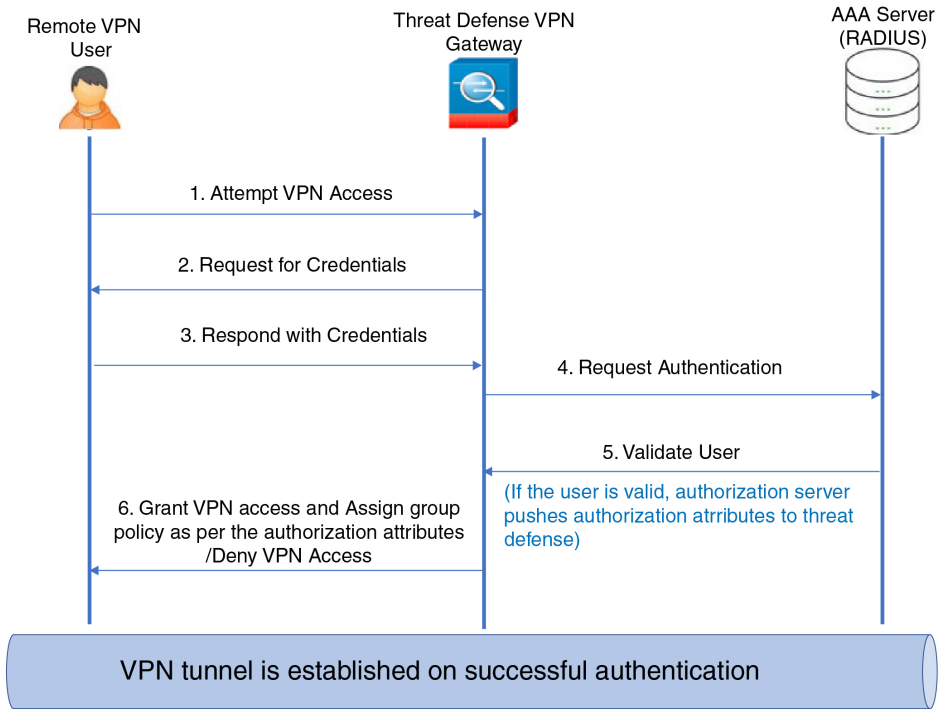
Delegating Group Policy Selection to Authorization Server

The group policy applied to a user is determined when the VPN tunnel is being established. You can select a group policy for a connection profile while creating a remote access VPN policy using the wizard or update the connection policy for connection profiles later. However, you can configure the AAA (RADIUS) server to assign the group policy or it is obtained from the current connection profile. If the Firewall Threat Defense device receives attributes from the external AAA server that conflicts with those configured on the connection profile, then attributes from the AAA server always take the precedence.

You can configure ISE or the RADIUS Server to set the Authorization Profile for a user or user-group by sending IETF RADIUS Attribute 25 and map to the corresponding group policy name. You can configure specific group policy to a user or user group to push a Downloadable ACL, set a banner, Restrict VLAN, and configure the advanced option of applying an SGT to the session. These attributes are applied to all users that are part of that group when the VPN connection is established.

For more information, see the Configure Standard Authorization Policies section of Cisco Identity Services Engine Administrator Guide and RADIUS Server Attributes for Secure Firewall Threat Defense, on page 1445.

Figure 399: Remote Access VPN Group Policy Selection by AAA Server



Related Topics

Configure a group policy object, on page 2461
Configure Connection Profile Settings, on page 1436

Override the Selection of Group Policy or Other Attributes by the Authorization Server

When a remote access VPN user connects to the VPN, the group policy and other attributes configured in the connection profile are assigned to the user. However, the remote access VPN system administrator can delegate the selection of group policy and other attributes to the authorization server by configuring ISE or the RADIUS Server to set the Authorization Profile for a user or user-group. Once users are authenticated, these specific authorization attributes are pushed to the Firewall Threat Defense device.

Before you begin

Ensure that you configure a remote access VPN policy with RADIUS as the authentication server.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select RADIUS or ISE as the authorization server if not configured already.

Step 4 Select **Advanced** > **Group Policies** and add the required group policy. For detailed information about a group policy object, see Configure a group policy object, on page 2461.

You can map only one group policy to a connection profile; but you can create multiple group policies in a remote access VPN policy. These group policies can be referenced in ISE or the RADIUS server and configured to override the group policy configured in the connection profile by assigning the authorization attributes in the authorization server.

Step 5 Deploy the configuration on the target Firewall Threat Defense device.

Step 6 On the authorization server, create an Authorization Profile with RADIUS attributes for IP address and downloadable ACLs.

When the group policy is configured in the authorization server selected for remote access VPN, the group policy overrides the group policy configured in the connection profile for the remote access VPN user after the user is authenticated.

Related Topics

Configure a group policy object, on page 2461

Deny VPN Access to a User Group

When you do not want an authenticated user or user group to be able to use VPN, you can configure a group policy to deny VPN access. You can configure a group policy in a remote access VPN policy and reference it in the ISE or RADIUS server configuration for authorization.

Before you begin

Ensure that you have configured remote access VPN using the Remote Access Policy wizard and configured authentication settings for the remote access VPN policy.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select **AdvancedGroup Policies**.

Step 4 Select a group policy and click **Edit** or add a new group policy.

Step 5 Select **AdvancedSession Settings** and set **Simultaneous Login Per User** to 0 (zero).
This stops the user or user group from connecting to the VPN even once.

Step 6 Click **Save** to save the group policy and then save the remote access VPN configuration.

Step 7 Configure ISE or the RADIUS server to set the Authorization Profile for that user/user-group to send IETF RADIUS Attribute 25 and map to the corresponding group policy name.

Step 8 Configure the ISE or RADIUS server as the authorization server in the remote access VPN policy.

Step 9 Save and deploy the remote access VPN policy.

Related Topics

Configure Connection Profile Settings, on page 1436

Restrict Connection Profile Selection for a User Group

When you want to enforce a single connection profile on a user or user group, you can choose to disable the connection profile so that the group alias or URLs are not available for the users to select when they connect using the AnyConnect VPN module of Cisco Secure Client.

For example, if your organization wants to use specific configurations for different VPN user groups such as mobile users, corporate-issued laptop users, or personal laptop users, you can configure connection a profile specific to each of these user groups and apply the appropriate connection profile when the user connects to the VPN.

The AnyConnect VPN module of Cisco Secure Client, by default, shows a list of the connection profiles (by connection profile name, alias, or alias URL) configured in Firewall Management Center and deployed on Firewall Threat Defense. If custom connection profiles are not configured, AnyConnect VPN module of Cisco Secure Client shows the *DefaultWEBVPNGroup* connection profile. Use the following procedure to enforce a single connection profile for a user group.

Before you begin

- On your Secure Firewall Management Center web interface, configure remote access VPN using the remote access VPN policy wizard with Authentication Method as 'Client Certificate Only' or 'Client Certificate + AAA'. Choose the username fields from the certificate.
- Configure ISE or RADIUS server for authorization and associate the group policy with the authorization server.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access policy and click **Edit**.

Step 3 Select **Access Interfaces** and disable **Allow users to select connection profile while logging in**.

Step 4 Click **Advanced Certificate Maps**.

Step 5 Select **Use the configured rules to match a certificate to a Connection Profile**.

Step 6 Select the **Certificate Map Name** or click the **Add** icon to add a certificate rule.

Step 7 Select the **Connection Profile**, and click **Ok**.
With this configuration, when a user connects from the AnyConnect VPN module of Cisco Secure Client, the user will have the mapped connection profile and will be authenticated to use the VPN.

Related Topics

Configure a group policy object, on page 2461
Configure Connection Profile Settings, on page 1436

Update the Secure Client Profile for Remote Access VPN Clients

Secure Client Profile is an XML file that contains an administrator-defined end user requirements and authentication policies to be deployed on a VPN client system as part of Secure Client. It makes the preconfigured network profiles available to end users.

You can use the GUI-based Secure Client Profile Editor, an independent configuration tool, to create them. The standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from Cisco Software Download Center.

See the Secure Client Profile Editor chapter in the appropriate release of the Cisco Secure Client (including AnyConnect) Administrator Guide for details.

Before you begin

- Ensure that you have configured remote access VPN using the Remote Access Policy wizard and deployed the configuration on Firewall Threat Defense device. See Create a New Remote Access VPN Policy, on page 1426.
- On your Secure Firewall Management Center web interface, go to **Objects** > **Object Management** > **VPN** > **Secure Client File** and add the new Secure Client image.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access VPN policy and click **Edit**.

Step 3 Select the connection profile that includes the client profile to be edited, and click **Edit**.

Step 4 Click **Edit Group Policy** > **Secure Client** > **Profiles**.

Step 5 Select the client profile XML file from the list or click **Add** to add a new client profile.

Step 6 Save the group policy, connection profile, and then the remote access VPN policy.

Step 7 Deploy the changes.
Changes to the client profile will be updated on the VPN clients when they connect to the remote access VPN gateway.

Related Topics

Configure a group policy object, on page 2461

RADIUS Dynamic Authorization

Secure Firewall Threat Defense has the capability to use RADIUS servers for user authorization of VPN remote access and firewall cut-through-proxy sessions using dynamic access control lists (ACLs) or ACL names per user. To implement dynamic ACLs for dynamic authorization or RADIUS Change of Authorization (RADIUS CoA), you must configure the RADIUS server to support them. When the user tries to authenticate, the RADIUS server sends a downloadable ACL or ACL name to the Firewall Threat Defense. Access to a given service is either permitted or denied by the ACL. Secure Firewall Threat Defense deletes the ACL when the authentication session expires.

Related Topics

Add a RADIUS server group, on page 2346
Interfaces, on page 2383
Configuring RADIUS Dynamic Authorization, on page 1500
RADIUS Server Attributes for Secure Firewall Threat Defense, on page 1445

Configuring RADIUS Dynamic Authorization

Before you begin:

- Only one interface can be configured in the security zone or interface group if it is referred in a RADIUS Server.
- A dynamic authorization enabled RADIUS server requires Secure Firewall Threat Defense 6.3 or later for the dynamic authorization to work.
- Interface selection in RADIUS server is not supported on Secure Firewall Threat Defense 6.2.3 or earlier versions. The interface option will be ignored during deployment.
- Firewall Threat Defense posture VPN does not support group policy change through dynamic authorization or RADIUS change of authorization (CoA).

Table 87: Procedure

	Do This	More Info
Step 1	Log in to your Secure Firewall Management Center web interface.	
Step 2	Configure a RADIUS server object with dynamic authorization.	RADIUS server group configuration options, on page 2346
Step 3	Configure a route to ISE server through an interface enabled for change of authorization (CoA) to establish connectivity from Firewall Threat Defense to RADIUS server through routing or a specific interface.	RADIUS server group configuration options, on page 2346
Step 4	Configure a remote access VPN policy and select the RADIUS server group object that you have created with dynamic authorization.	Create a New Remote Access VPN Policy, on page 1426
Step 5	Configure the DNS server details and domain-lookup interfaces using the Platform Settings.	Configure DNS, on page 1431 DNS server groups, on page 2366
Step 6	Configure split tunnelling in the remote access VPN group policy to allow DNS traffic through the VPN tunnel.	Configure a group policy object, on page 2461
Step 7	Deploy the configuration changes.	Deploy configuration changes, on page 135

Two-Factor Authentication

You can configure two-factor authentication for the remote access VPN. With two-factor authentication, the user must supply a username and static password, plus an additional item such as an RSA token or a passcode. Two-factor authentication differs from using a second authentication source in that two-factor is configured on a single authentication source, with the relationship to the RSA server tied to the primary authentication source.

Secure Firewall Threat Defense supports RSA tokens and Duo Push authentication requests to Duo Mobile for the second factor in conjunction with any RADIUS or AD server as the first factor in the two-factor authentication process.

Configuring RSA Two-Factor Authentication

About this task:

You can configure the RADIUS or AD server as the authentication agent in the RSA server, and use the server in Secure Firewall Management Center as the primary authentication source in the remote access VPN.

When using this approach, the user must authenticate using a username that is configured in the RADIUS or AD server, and concatenate the password with the one-time temporary RSA token, separating the password and token with a comma: *password*,*token*.

In this configuration, it is typical to use a separate RADIUS server (such as one supplied in Cisco ISE) to provide authorization services. You would configure the second RADIUS server as the authorization and, optionally, accounting server.

Before you begin:

Ensure that the following configurations are complete before configuring RADIUS two-factor authentication on Secure Firewall Threat Defense:

On the RSA Server

- Configure RADIUS or Active Directory server as an authentication agent.
- Generate and download the configuration (*sdconf.rec*) file.
- Create a token profile, assign the token to the user, and distribute the token to the user. Download and install the token on the remote access VPN client system.

For more information, see RSA SecureID Suite documentation.

On the ISE Server

- Import the configuration (*sdconf.rec*) file generated on the RSA server.
- Add the RSA server as the external identity source and specify the shared secret.

Table 88: Procedure

	Do This	More Info
Step 1	Log on to your Secure Firewall Management Center web interface.	

	Do This	More Info
Step 2	Create a RADIUS server group.	RADIUS server group configuration options, on page 2346
Step 3	Create a RADIUS Server object within the new RADIUS server group, with RADIUS or AD server as the host and with a timeout of 60 seconds or more.	RADIUS server group configuration options, on page 2346 **Note** The RADIUS or AD server must be the same server that is configured as the authentication agent in RSA server. For two-factor authentication, make sure that the timeout is updated to 60 seconds or more in the Secure Client Profile XML file as well.
Step 4	Configure a new remote access VPN policy using the wizard or edit an existing remote access VPN policy.	Create a New Remote Access VPN Policy, on page 1426
Step 5	Select RADIUS as the authentication server and then select the newly-created RADIUS server group as the authentication server.	Configure AAA Settings for Remote Access VPN, on page 1439
Step 7	Deploy the configuration changes.	Deploy configuration changes, on page 135

Configuring Duo Two-Factor Authentication

About this task:

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy. (You cannot use a direct connection with the Duo Cloud Service over LDAPS.)

For the detailed steps to configure Duo, see https://duo.com/docs/cisco-firepower.

You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or an AD server, as the first authentication factor, and the Duo Cloud Service as the second factor.

When using this approach, the user must authenticate using a username that is configured on both the Duo Cloud or web server, and the associated RADIUS server. The user must enter the password configured in the RADIUS server, followed by one of the following Duo codes:

- **Duo-passcode**. For example, *my-password*,123456.
- **push**. For example, *my-password*,**push**. Use push to tell Duo to send a push authentication to the Duo Mobile app, which the user must have already installed and registered.
- **sms**. For example, *my-password*,**sms**. Use **sms** to tell Duo to send an SMS message with a new batch of passcodes to the user's mobile device. The user's authentication attempt will fail when using **sms**. The user must then re-authenticate and enter the new passcode as the secondary factor.
- **phone**. For example, *my-password*,**phone**. Use **phone** to authenticate using phone callback.

For more information on login options with examples, see https://guide.duo.com/anyconnect.

Before you begin:

Before configuring two-factor authentication with Duo Authentication Proxy on Firewall Threat Defense, ensure that you complete the following configurations:

- Configure a working primary authentication (RADIUS or AD) for your remote access VPN users before you begin to deploy Duo.
- Install Duo proxy service on a Windows or Linux machine within your network to integrate Duo with Secure Firewall Threat Defense remote access VPN. This Duo proxy server also acts as a RADIUS server.

  Download and install the most recent Duo authentication proxy from the following location:

  - **Windows**: https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**: https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - Verify the checksum at https://duo.com/docs/checksums#duo-authentication-proxy.

- Configure Duo authentication file `authproxy.cfg`. Follow instructions on the https://duo.com/docs/cisco-firepower#configure-the-proxy page to configure the authentication configuration settings.

  The `authproxy.cfg` configuration file must contain the details for RADIUS or ISE server, Firewall Threat Defense device, Duo proxy server details, Integration Key, Secret key, and API host details.
- Ensure that you have the right API host information in the `authproxy.cfg` file.
- Configure other required settings such as secondary authentication factor in the newly installed Duo proxy server at **Duo Security Server** > **Duo Admin Panel** > **Applications** > **CISCO RADIUS VPN**.

Table 89: Procedure

	Do This	More Info
Step 1	Log on to your Secure Firewall Management Center web interface.	
Step 2	Create a RADIUS server group.	RADIUS server group configuration options, on page 2346
Step 3	Create a RADIUS Server object within the new RADIUS server group with Duo proxy server as the host with a timeout of 60 seconds or more.	Configure RADIUS server options, on page 2347 **Note** For two-factor authentication, make sure that the timeout is updated to 60 seconds or more in the Secure Client Profile XML file as well.
Step 4	Configure a new remote access VPN policy using the wizard or edit an existing remote access VPN policy.	Create a New Remote Access VPN Policy, on page 1426
Step 5	Select RADIUS as the authentication server and then select the RADIUS server group created with the Duo proxy server as the authentication server.	Configure AAA Settings for Remote Access VPN, on page 1439

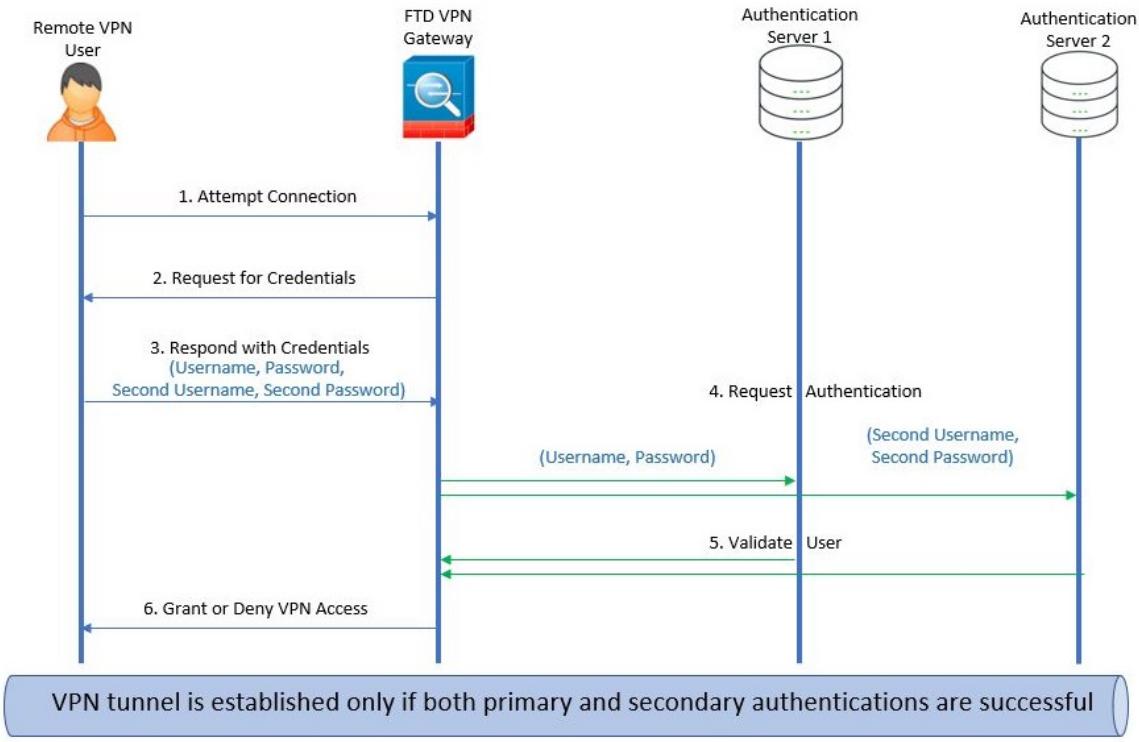
	Do This	More Info
Step 7	Deploy the configuration changes.	Deploy configuration changes, on page 135

Secondary Authentication

Secondary authentication or double authentication in Secure Firewall Threat Defense adds an additional layer of security to remote access VPN connections by using two different authentication servers. With secondary authentication enabled, the Secure Client VPN users must provide two sets of credentials to login to the VPN gateway.

Secure Firewall Threat Defense remote access VPN supports secondary authentication in AAA Only and Client Certificate & AAA authentication methods.

Figure 400: Remote Access VPN Secondary or Double Authentication



Related Topics

Configure Remote Access VPN Secondary Authentication, on page 1504

Configure Remote Access VPN Secondary Authentication

When remote access VPN authentication is configured to use both client certificate and authentication sever, VPN client authentication is done using both the client certificate validation and AAA server.

Before you begin

- Configure two authentication (AAA) servers— the primary and secondary authentication servers, and required identity certificates. The authentication servers can be RADIUS server, and AD or LDAP realms.
- Ensure that the AAA servers are reachable from the Secure Firewall Threat Defense device for the remote access VPN configuration to work. Configure routing (at **Devices** > **Device Management**, click **Edit** (). Then, click **Device > Routing**) to ensure connectivity to the AAA servers.

Procedure

Step 1 On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access** .

Step 2 Select a remote access policy and click **Edit**; or click **Add** to create a new remote access VPN policy.

Step 3 For a new remote access VPN policy, configure the authentication while selecting connection profile settings. For an existing configuration, select the connection profile that includes the client profile, and click **Edit**.

Step 4 Click **AAA** > **Authentication Method**, **AAA** or **Client Certificate & AAA**.

- When you select the **Authentication Method** as:

  Client Certificate & AAA—Authentication is done using both client certificate and AAA server.

  - **AAA**—If you select the **Authentication Server** as **RADIUS**, by default, the Authorization Server has the same value. Select the **Accounting Server** from the drop-down list. Whenever you select **AD** and **LDAP** from the Authentication Server drop-down list, you must manually select the **Authorization Server** and **Accounting Server** respectively.
  - Whichever authentication method you choose, select or deselect **Allow connection only if user exists in authorization database**.

- **Use secondary authentication** — Secondary authentication is configured in addition to primary authentication to provide additional security for VPN sessions. Secondary authentication is applicable only to **AAA only** and **Client Certificate & AAA** authentication methods.

  Secondary authentication is an optional feature that requires a VPN user to enter two sets of username and password on the Secure Client login screen. You can also configure to pre-fill the secondary username from the authentication server or client certificate. Remote access VPN authentication is granted only if both primary and secondary authentications are successful. VPN authentication is denied if any one of the authentication servers is not reachable or one authentication fails.

  You must configure a secondary authentication server group (AAA server) for the second username and password before configuring secondary authentication. For example, you can set the primary authentication server to an LDAP or Active Directory realm and the secondary authentication to a RADIUS server.

Note By default, secondary authentication is not required.

Authentication Server— Secondary authentication server to provide secondary username and password for VPN users.

Select the following under **Username for secondary authentication**:

- **Prompt**: Prompts the users to enter the username and password while logging on to VPN gateway.
- **Use primary authentication username**: The username is taken from the primary authentication server for both primary and secondary authentication; you must enter two passwords.
- **Map username from client certificate**: Prefills the secondary username from the client certificate.
  - If you select **Map specific field** option, which includes the username from the client certificate. The **Primary** and **Secondary** fields display default values: **CN (Common Name)** and **OU (Organisational Unit)** respectively. If you select the **Use entire DN (Distinguished Name) as username** option, the system automatically retrieves the user identity.

    See **Authentication Method** descriptions for more information about primary and secondary field mapping.
  - **Prefill username from certificate on user login window**: Prefills the secondary username from the client certificate when the user connects via Secure Client.
    - **Hide username in login window**: The secondary username is pre-filled from the client certificate, but hidden to the user so that the user does not modify the pre-filled username.
- **Use secondary username for VPN session**: The secondary username is used for reporting user activity during a VPN session.

For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.

Related Topics

Configure Connection Profile Settings, on page 1436

Single Sign-On Authentication with SAML 2.0

About SAML Single Sign-On Authentication

Security Assertion Markup Language (SAML) is an open standard for logging users into applications using their sessions in another context. Organizations already know the identity of users when users log in to their Active Directory (AD) domain or the intranet. They use this identity information to log in users to other applications, such as web-based applications using SAML. Individual applications do not need to store credentials and users do not have to remember and manage different sets of credentials for individual applications. SAML single sign-on (SSO) works by transferring the user's identity from one place (the identity provider) to another (the service provider).

SAML Single Sign-On with Secure Firewall Threat Defense

The Secure Firewall Threat Defense device supports SAML 2.0 single sign-on (SSO) authentication for remote access VPN connections using the Secure Client. You need the following to configure SAML 2.0 SSO on Secure Firewall Threat Defense:

- **Identity Provider (IdP)**—The Duo Access Gateway acts as the identity provider to perform user authentication and issues assertions.
- **Service Provider (SP)**—The Firewall Threat Defense device acts as the service provider and obtains the authentication assertion from the identity provider.

- **VPN Client**—The Secure Client performs SAML 2.0 authentication via the embedded browser.

Guidelines and Limitations for SAML 2.0

- Firewall Threat Defense supports the following signatures for SAML authentication:
  - SHA1 with RSA and HMAC
  - SHA2 with RSA and HMAC
- Firewall Threat Defense supports SAML 2.0 Redirect-POST binding , which is supported by all SAML IdPs.
- The Firewall Threat Defense functions as a SAML SP only. It cannot act as an Identity Provider in gateway mode or peer mode.
- You can enforce an access policy on a SAML-authenticated user if you have an associated identity policy with an AD realm matching the SAML domain. However, it does not work for Azure AD SAML because it requires additional mapping from the tenant ID of the Azure AD to an associated realm ID on the threat defense device.
- Having SAML authentication attributes available in DAP evaluation (similar to RADIUS attributes sent in RADIUS auth response from AAA server) is not supported. Firewall Threat Defense supports SAML enabled group policy on DAP policy; however, you cannot check the username attribute while using SAML authentication, because the username attribute is masked by the SAML Identity provider.
- Firewall Threat Defense administrators need to ensure clock synchronization between the Firewall Threat Defense and the SAML IdP for proper handling of authentication assertions and proper timeout behavior.
- Firewall Threat Defense administrators have the responsibility to maintain a valid signing certificate on both Firewall Threat Defense and IdP considering the following:
  - The IdP signing certificate is mandatory when configuring an IdP on the Firewall Threat Defense.
  - The Firewall Threat Defense does not do a revocation check on the signing certificate received from the IdP.
- In SAML assertions, there are NotBefore and NotOnOrAfter conditions. The Firewall Threat Defense SAML configured timeout interacts with these conditions as follows:
  - Timeout overrides NotOnOrAfter if the sum of NotBefore and timeout is earlier than NotOnOrAfter.
  - If NotBefore + timeout is later than NotOnOrAfter, then NotOnOrAfter takes effect.
  - If the NotBefore attribute is absent, the Firewall Threat Defense denies the login request. If the NotOnOrAfter attribute is absent and SAML timeout is not set, Firewall Threat Defense denies the login request.
- Firewall Threat Defense does not work with Duo in a deployment using an internal SAML, which forces the Firewall Threat Defense to proxy for the client to authenticate, due to the FQDN change that occurs during challenge/response for Two-factor authentication (push, code, password).
- When using SAML with Secure Client, follow these guidelines:
  - Untrusted server certificates are not allowed in the embedded browser.
  - The embedded browser SAML integration is not supported in CLI or SBL modes.

- SAML authentication established in a web browser is not shared with Secure Client and vice versa.
- Depending on the configuration, various methods are used when connecting to the headend with the embedded browser. For example, while Secure Client might prefer an IPv4 connection over an IPv6 connection, the embedded browser might prefer IPv6, or vice versa. Similarly, Secure Client may fall back to no proxy after trying proxy and getting a failure, while the embedded browser may stop navigation after trying proxy and getting a failure.
- You must synchronize your Firewall Threat Defense's Network Time Protocol (NTP) server with the IdP NTP server in order to use the SAML feature.
- You cannot access internal servers with SSO after logging in using an internal IdP.
- The SAML IdP NameID attribute determines the user's username and is used for authorization, accounting, and VPN session database.

- SAML does not support Start Before Logon (SBL).
- Multiple attributes received with a SAML assertion are not supported.
- A firewall uses the Identity Provider Entity ID as the SAML object name from the single sign-on server object created in the Firewall Management Center (**Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**). Hence, you cannot use multiple SAML objects with the same Identity Provider Entity ID on a single firewall.

Configuring a SAML Single Sign-On Authentication

Before you begin

Ensure that you have done the following before you configure SAML single sign-on with Firewall Threat Defense remote access VPN:

- Create an account with Duo.
- Download and install the Duo Access Gateway.
- Obtain the following from your SAML identity provider (Duo).
  - Identity Provider Entity ID URL
  - Sign-in URL
  - Sign-out URL
  - Identity provider certificate
- Create a SAML single sign-on server object. For more information, see Add a single sign-on server, on page 2349.



Note You can create a single sign-on server object in the **Connection Profile** settings when you create a new policy using the Remote Access VPN policy Wizard.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Edit** next to the remote access VPN policy for which you want to configure SAML authentication. If you want to create a new policy, click **Add**.

Step 3 Click **Edit** on the connection profile that you want to modify.

Step 4 Choose **AAA** settings and select **SAML** from the **Authentication Method** drop-down.

Step 5 Choose the required SAML single sign-on server as the **Authentication Server**.

Step 6 Configure the required settings for the remote access VPN.

Step 7 Save and deploy the remote access VPN policy on your Firewall Threat Defense device.

Related Topics

Configure AAA Settings for Remote Access VPN, on page 1439

Configuring SAML Authorization

About SAML Authorization

SAML authorization supports user attributes delivered in SAML assertions within the AAA and Dynamic Access Policy (DAP) frameworks. You can configure the SAML assertion attributes on the Identity Provider as name-value pairs which then parses as strings. The attributes received are made available to DAP so that they can be used when defining selection criteria within a DAP record. The SAML assertion *cisco_group_policy* is used to determine the Group Policy to be applied to the VPN session.

Dynamic Access Policy Attribute Representation

In the DAP table, the DAP attributes are represented in the following format:

```
aaa.saml.name = "value”
```

Example, *aaa.saml.department = ”finance"*

This attribute can be used in DAP selection as follows:

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

Multi-Valued Attributes

Multi-valued attributes are also supported in DAP and the DAP table is indexed :

```
aaa.saml.name.1 = "value”
aaa.saml.name.2 = "value"
```

Active Directory memberOf Attributes

The Active Directory (AD) memberOf attribute receives a special processing that is consistent with the way it is handled through an LDAP query.

Group names are represented by the CN attribute of the DN.

Example Attributes received from the authorization server:

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us”
```

Dynamic Access Policy attributes:

```
aaa.saml.memberOf.1 = "FTD-VPN-Group”
aaa.saml.memberOf.2 = "Domain Admins"
```

Interpretation of the cisco_group_policy Attribute

A group-policy can be specified by a SAML assertion attribute. When an attribute "cisco_group_policy" is received by the Firewall Threat Defense, the corresponding value is used to select the connection group-policy

Configure SAML Authorization

Before you begin

Ensure that you have configured a single sign-on server like DUO and completed the required Identity Provider (IdP) and Service Provider (SP) settings.

For more information, see Single Sign-On Authentication with SAML 2.0, on page 1506.

Procedure

Step 1 Configure a single sign-on server object if not configured already.

a) Choose **Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**.
b) Click **Add Single Sign-on Server**.
c) Enter the single sign-on server details and click **Save**.

For more information, see Add a single sign-on server, on page 2349.

Step 2 Configure SAML authentication in the remote access VPN connection profile.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Click **Edit** on the remote access VPN policy for which you want to configure SAML authorization or create a new policy.
c) Edit the required connection profile and select **AAA**.
d) Select the single sign-on server object from the **Authentication Server** drop-down.
e) Save the remote access VPN configuration.

Step 3 Match a SAML criteria in DAP policy.

a) Select **Devices** > **VPN** > **Dynamic Access Policy**.
b) Create a new DAP or edit an existing one.
c) Create a DAP record or edit and existing record.
d) Click **AAA Criteria** > **SAML Criteria** > **Add SAML Criteria**.
e) Create a SAML criteria based on the SAML assertions returned by the SSO server.

Step 4 Deploy the remote access VPN configuration.

Related Topics

Configure Connection Profile Settings, on page 1436
Firewall Threat Defense group policy objects, on page 2460

Advanced Secure Client Configurations

Configure Secure Client Modules on a Firewall Threat Defense

Secure Client can integrate with various Cisco endpoint security solutions and offer enhanced security using different Secure Client modules.

You can use the managed headend Firewall Threat Defense to distribute and manage Secure Client modules to the endpoints. When a user connects to the Firewall Threat Defense, it downloads and installs Secure Client and the required modules on the endpoint.

In version 6.7 and later, you can use the headend Firewall Threat Defense, managed by a Firewall Management Center, to distribute and manage Secure Client modules to the endpoints. These modules then integrate with the corresponding Cisco endpoint security solution.

In versions 6.4 to 6.6, you can enable these modules and profiles on a Firewall Threat Defense using FlexConfig. For more information, see Configure AnyConnect Modules and Profiles Using FlexConfig.

Benefits

If you use a Firewall Threat Defense to distribute and manage Secure Client modules to the endpoints, you can easily perform the following tasks:

- Distribute and manage Secure Client modules and profiles on each endpoint.
- Upgrade Secure Client on each endpoint.

Types of Secure Client Modules

AMP Enabler

Use this module to deploy Secure Endpoint, on endpoints. The module pushes Secure Endpoint to endpoints from a server hosted locally within the enterprise. This module provides an additional security agent that detects potential malware threats in the network, removes these threats, and protects the enterprise.

In Cisco Secure Client 5.0, AMP Enabler is only for macOS. Cisco Secure Client for Windows offers full integration with Cisco Secure Endpoint.

ISE Posture

Use this module to perform endpoint posture checks such as antivirus, antispyware, operating system and so on using Cisco Identity Services Engine (ISE) and assess the endpoint's compliance. ISE provides next generation identity and access control policy. ISE Posture performs a client-side evaluation. The client receives the posture requirement policy from the headend, performs the posture data collection, compares the results against the policy, and sends the assessment results back to the headend.

Network Visibility

Use this module to monitor the endpoint application usage using the Network visibility module. You can uncover potential behavior anomalies and make informed network design decisions. It enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics. You can share the usage data with NetFlow analysis tools such as Cisco Stealthwatch.

Umbrella Roaming Security

Use this module for a DNS-layer security using the Cisco Umbrella Roaming Security service. Cisco Umbrella provides content filtering, multiple policies, robust reporting, active directory integration, and much more.

Web Security

Use this module to enable Cisco Secure Web Appliance (SWA), powered by Cisco Talos. This module protects the endpoint by blocking risky sites and testing unknown sites before allowing users to access them. It can deploy web security either through the on-prem WSA or the cloud-based Cisco Cloud Web Security. This module is not part of the AnyConnect package from release 4.5 and in Secure Client 5.0.

Network Access Manager

This module provides a secure layer 2 network and performs device authentication to access wired and wireless networks. Network Access Manager manages user and device identity and the network access protocols required for secure access.

Network Access Manager is not supported on macOS or Linux.

Start Before Login

Start Before Login (SBL) allows users to establish their VPN connection to the enterprise infrastructure before logging onto Windows. After the SBL module installation, you must enable SBL in the Secure Client VPN profile and add it to the remote access VPN group policy.

DART

Diagnostics and Reporting Tool (DART) collates system logs and other diagnostic information to troubleshoot AnyConnect installation and connection problems. You can send this data to Cisco TAC for troubleshooting.

By default, DART is not enabled in new RA VPN group policies for 6.7 and later versions. In 6.6 and earlier versions, DART is enabled by default.

Feedback

The customer experience feedback (CEF) module provides information about which features and modules you use and have enabled. This information gives an insight into the user experience so that Cisco can continue to improve the quality, reliability, performance, and user experience of the Cisco Secure Client. Secure Client does not download the Feedback module to the endpoint. The feedback data is sent to the Cisco Feedback Server.

Prerequisites for Configuring Secure Client Modules

- Configure the associated products depending on the module that you are going to use.
- Download the following Secure Client-related packages from Cisco Software Download Center to your local host.

- Cisco Secure Client Headend Deployment Package for the required platforms.

  This package is for the headend and contains all the Secure Client modules. For Windows, the filename is cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg.

- Profile Editor: Create profiles for the modules that require profiles.

  Secure Client needs a Secure Client profile for some of the modules. A profile contains configurations to enable the modules and connect to the corresponding security services. The profile editor supports only Windows.

  The following table lists if the modules require a client profile:

Secure Client Module	Requires a Client Profile
AMP Enabler	Yes
ISE Posture	Yes
Network Access Manager	Yes
Network Visibility Module	Yes
Umbrella Roaming Secure Module	Yes
Feedback	Yes
Web Security	Yes
DART	No
Start Before Login	No

- Licensing
  - You need one of the following Secure Client licenses: Secure Client Premier, Secure Client Advantage, or Secure Client VPN Only
  - Your Firewall Management Center Essentials license must allow export-controlled functionality.

    Choose **System** (⚙) > **Licenses** > **Smart Licenses** to verify this functionality in the management center.

Guidelines for Configuring Secure Client Modules

- All Secure Client modules are supported from AnyConnect 4.8 and later, and Secure Client 5.0.
- Different modules support profiles with different file extensions. The following table lists the modules and the supported file extensions of their profiles:

Table 90: Supported File Extensions of Profiles

Module	File Extension
AMP Enabler	*.xml, *.asp

Module	File Extension
Feedback	*.xml
ISE Posture	*.xml, *.isp
Network Access Manager	*.xml, *.nsp
Network Visibility	*.xml, *.nvmsp
Umbrella Roaming Security	*.xml, *.json
Web Security	*.xml, *.wsp, *.wso

- You can add only one entry per client module. You can edit or delete an entry for a module.
- If you plan to use ISE posture and Network Access Manager modules on a Windows OS, you must install Network Access Manager before you use the ISE Posture module.
- If you enable the Umbrella Roaming Security module, ensure that you disable the **Always send DNS requests over tunnel** option under split tunnelling in the VPN group policy.
- If you want to use SBL, then you must enable SBL in the Secure Client VPN profile.

Install Secure Client Modules using a Firewall Threat Defense

Before you begin

Ensure that you review the Prerequisites for Configuring Secure Client Modules, on page 1512 and Guidelines for Configuring Secure Client Modules, on page 1513 topics.

Procedure

Step 1 The administrator creates profiles, if needed, for the required Secure Client modules.

Step 2 The administrator uses the Firewall Management Center to:

a) Configure the modules and add the profiles in the remote access VPN group policy.

b) Deploy the configuration on the Firewall Threat Defense.

Step 3 The user uses Secure Client to initiate a VPN connection to the Firewall Threat Defense.

Step 4 The Firewall Threat Defense authenticates the user.

Step 5 The Secure Client checks for updates.

Step 6 The Firewall Threat Defense distributes the Secure Client modules and the profiles on the endpoint.

What to do next

Configure a Remote Access VPN Group Policy with Secure Client Modules, on page 1515.

Configure a Remote Access VPN Group Policy with Secure Client Modules

To install and update the Secure Client modules on the endpoint using a Firewall Threat Defense managed by a Firewall Management Center, you must update the remote access VPN group policy with the Secure Client module configurations.

Before you begin

Ensure that you have configured a remote access VPN policy in the Firewall Management Center.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Select a remote access VPN policy and click **Edit**.

Step 3 Select a connection profile and click **Edit**.

Step 4 Click **Edit Group Policy**.

Step 5 Click the **Secure Client** tab.

Step 6 Click **Client Modules**.

Step 7 Click **+**.

Step 8 Choose a module from the **Client Module** drop-down list.

Step 9 Choose a profile for the module from the **Profile to download** drop-down list or click **+** to add a profile.

Step 10 Check the **Enable module download** check box to download the module on the endpoint.

Step 11 Click **Add**.

Step 12 Repeat steps 7 to 11 if you want to add more modules.

Step 13 Click **Save**.

What to do next

1. Deploy the configuration on the threat defense.
2. Launch the Secure Client, select the VPN profile, and connect to the VPN. Secure Client installs the configured modules on it.
3. Verify the configuration. For more information, see Verify Secure Client Modules Configuration, on page 1515.

Verify Secure Client Modules Configuration

On the Firewall Threat Defense

Use the following commands on the Firewall Threat Defense to view the profiles and the Secure Client modules configuration:

- **show disk0:**- View the profiles and their configuration.
- **show run webvpn** - View details of the Secure Client configurations.

- **show run group-policy <ravpn_group_policy_name>** - View details of the RA VPN group policy for Secure Client.
- **show vpn-sessiondb anyconnect** - View details of the active Secure Client VPN sessions.

On the Endpoint

1. Use the Secure Client to establish a VPN connection to the Firewall Threat Defense.
2. Verify if the configured modules are downloaded and installed as part of the Secure Client.
3. Verify if the configured profiles, if any, are available in the locations documented in Profile Locations for all Operating Systems.

On the Firewall Management Center

You can monitor remote access VPN active sessions on the Firewall Management Center using the Remote Access VPN dashboard (**Overview** > **Dashboards** > **Remote Access VPN**). You can quickly determine problems related to user sessions and mitigate the problems for your network and users.

Configure Application-Based (Per App VPN) Remote Access VPN on Mobile Devices

When you use Secure Client to establish a VPN connection from a mobile device, all the traffic including the traffic from personal applications is routed through the VPN.

For mobile devices that run on Android or iOS, you can restrict the applications that use the VPN tunnel. This application-based remote access VPN is called Per App VPN. To use Per App VPN, you must install and configure a third-party Mobile Device Manager (MDM) application. You must define the list of approved applications that can be used over the VPN tunnel in the MDM. You can enable Per App VPN on the Firewall Threat Defense headend so that your MDM can apply your policies on mobile devices.

Benefits

Benefits of restricting the remote access VPN to approved applications include:

- Performance—Limits VPN traffic over the corporate network and frees up resources of the VPN headend.
- Protection—Protects the corporate VPN tunnel from unapproved malicious applications on the mobile device.

Prerequisites and Licensing for Configuring Per App VPN Tunnels

Prerequisites

- Install and configure a third-party Mobile Device Manager (MDM).

  You must configure the applications that will be allowed in the VPN in the MDM itself, not on the Firewall Threat Defense headend device.

- Download the Cisco AnyConnect Enterprise Application Selector from Cisco Software Download Center.

  You need this tool to define the Per App VPN policy.

Licensing

- Secure Client Premier, or Secure Client Advantage.
- Essentials license must allow export-controlled functionality.

  To verify this functionality in the Firewall Management Center, choose **System** (⚙) > **Licenses** > **Specific Licenses**.

Determine the Application IDs for Mobile Applications

Before configuring the Firewall Threat Defense headend to allow application-based VPN from mobile devices, you must determine which applications should be allowed in the tunnel.

We strongly recommend that you configure the per-app policy in the MDM on the user's mobile device. This simplifies the headend configuration. If you decide to configure the list of allowed applications on the headend, you must determine the application IDs for each application on each type of endpoint.

The application ID, called the bundle ID in iOS, is a reverse DNS name. You can use an asterisk as a wildcard. For example, *.* indicates all applications, com.cisco.* indicates all Cisco applications.

To determine the application IDs:

- **Android**—Go to Google Play in a web browser and select the Apps category. Click (or hover over) an application that you want to allow, then look at the URL. The app id is in the URL, on the **id=** parameter. For example, the following URL is for Facebook Messenger, so the app id is com.facebook.orca.

  https://play.google.com/store/apps/details?id=com.facebook.orca

  For applications that are not available through Google Play, such as your own applications, download a package name viewer application to extract the app ID. There are many of these applications available, one of them should provide what you need, but Cisco does not endorse any of them.

- **iOS**—There is no straight-forward way to get the bundle ID. Following is one way to find it:

  1. Use a desktop web browser such as Chrome to search for the application name.
  2. In the search results, look for the link to download the app from the Apple App Store. For example, Facebook Messager would be similar to:

     https://apps.apple.com/us/app/messenger/id454638411
  3. Copy the number after the **id** string. In this example, **454638411**.
  4. Open a new browser window, and add the number to the end of the following URL:

     https://itunes.apple.com/lookup?id=

     For this example: https://itunes.apple.com/lookup?id=454638411
  5. You will be prompted to download a text file, usually named 1.txt. Download the file.
  6. Open the file in a text editor such as WordPad, and search for bundleId. For example:

     "bundleId":"com.facebook.Messenger",

     In this example, the bundle ID is com.facebook.Messenger. Use this as the app ID.

Once you have your list of application IDs, you can configure the policy as explained in .

Configure Application-Based VPN Tunnels

After you install and configure your MDM software, you can enable Per App VPN on the Firewall Threat Defense headend device. Once enabled on the headend, your MDM software will control which applications are tunneled over the VPN to the corporate network.

Before you begin

- Ensure that you have a remote access VPN policy in the Firewall Management Center.
- Configure Per App VPN using MDM and enroll each device to the MDM server.
- Download the Cisco AnyConnect Enterprise Application Selector.

Procedure

Step 1 Use the Cisco AnyConnect Enterprise Application Selector to define the Per App VPN policy.

We recommend that you create a simple **Allow All** policy, and define the allowed applications in the MDM. However, you can specify a list of applications to allow and control the list from the headend. If you want to include specific applications, create a separate rule for each application, using a unique name and the application's app ID. For more information on getting the app IDs, see Determine the Application IDs for Mobile Apps.

To create an **Allow All** policy that supports both Android and iOS platforms using the AnyConnect Enterprise Application Selector:

a) Choose **Android** from the drop-down list as the platform type and configure the following options:
   - **Friendly Name**—Enter a name for the policy. For example, Allow_All.
   - **App ID**—Enter *.* to match all possible applications.
   - Leave the other options.

b) Choose **iOS** from the drop-down list as the platform type and configure the following options:
   - **Friendly Name**—Enter a name for the policy. For example, Allow_All.
   - **App ID**—Enter *.* to match all possible applications.
   - Leave the other options.

c) Choose **Policy > View Policy** to get the base64 encoded string for the policy.

   This string contains an encrypted XML file that allows the Firewall Threat Defense to see the policies. Copy this value. You need this string when you configure Per App VPN on the Firewall Threat Defense.

Step 2 Use the Firewall Management Center to enable the Per App on the Firewall Threat Defense headend device.

a) Choose **Devices** > **VPN** > **Remote Access**.
b) Select a remote access VPN policy and click **Edit**.
c) Select a connection profile and click **Edit**.
d) Click **Edit Group Policy**.
e) Click the **Secure Client** tab.

f) Click **Custom Attributes** and click +.
g) Choose **Per App VPN** from the **Secure Client Attribute** drop-down list.
h) Choose an object from the **Custom Attribute Object** drop-down list or click + to add an object.

When you add a new custom attribute object for Per App VPN, enter the name, description, and the base64 encoded policy string from the Cisco AnyConnect Enterprise Application Selector.

i) Click **Save**.
j) Click **Add** and click **Save**.

Step 3 Deploy your changes on the Firewall Management Center.

What to do next

1. Launch the Secure Client, select the VPN profile, and connect to the VPN.
2. Verify the configuration. For more information, see Verify Per App Configuration, on page 1519.

Verify Per App Configuration

On the Firewall Threat Defense

Use the following commands on the Firewall Threat Defense to view the Per App configuration:

- **show run webvpn**
- **show run group-policy <ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

On the Endpoint

After the endpoint establishes a VPN connection with the Firewall Threat Defense:

1. Click the **Statistics** icon of the Secure Client.
2. **Tunnel Mode** will be “Application Tunnel” instead of “Tunnel All Traffic.”
3. **Tunneled Apps** will list the applications you enabled for tunneling in the MDM.

Remote Access VPN Examples

How to Limit Secure Client Bandwidth Per User

This section provides instructions to limit the maximum bandwidth that the VPN users consume when they connect using the Secure Client to Secure Firewall Threat Defense remote access VPN gateway. You can limit the maximum bandwidth by using a Quality of service (QoS) policy in Firewall Threat Defense, to ensure that a single user or group or users do not take over the entire resource. This configuration lets you give priority to critical traffic, prevent bandwidth hogging, and manage the network. If a When traffic exceeds the maximum rate, the Firewall Threat Defense drops the excess traffic.

Step	Do This	More Info
1	Create and set up a realm.	Create an LDAP realm or an Active Directory realm and realm directory, on page 1860
2	Create a QoS policy and QoS rule for the user or group available in the newly created realm.	• See Create a QoS policy, on page 1316 to create a QoS policy. • See Configuring QoS rules, on page 1318 to create a QoS rule.
3	Configure remote access VPN policy and select the newly created realm for user authentication.	Create a New Remote Access VPN Policy, on page 1426
4	Deploy the remote access VPN policy.	Deploy configuration changes, on page 135

How to Use VPN Identity for User-Id Based Access Control Rules

Step	Do This	More Info
1	Create and set up a realm.	Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
2	Create an identity policy and add an identity rule.	• See Create an identity policy, on page 1943 to create an identity policy. • See Create an identity rule, on page 1952 to create an identity rule.
3	Associate the identity policy with an access control policy.	Associate prefilter, decryption, and identity policies with an access control, on page 1585
4	Configure remote access VPN policy and select the newly created realm for user authentication.	Create a New Remote Access VPN Policy, on page 1426
5	Deploy the remote access VPN policy.	Deploy configuration changes, on page 135

Configure Firewall Threat Defense Multiple Certificate Authentication

Multiple Certificate-based Authentication

Multiple certificate-based authentication allows the Firewall Threat Defense to validate the machine or device certificate. Multiple certificates can be enabled for certificate-based authentication in the remote access VPN connection profile. It can be combined with AAA authentication. The multiple certificates option in the remote access VPN connection profile allows certificate authentication of both the machine and user via certificates. This ensures that the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow RA VPN access. The administrator can choose if the username for the session should be taken from the machine certificate or user certificate.

When multiple certificate-based authentication is configured, two certificates are obtained from the VPN client:

- **First Certificate** —Machine certificate to authenticate the endpoint.
- **Second Certificate**—User certificate to authenticate the VPN user.

For detailed information about Firewall Threat Defense certificates, see Manage Firewall Threat Defense certificates, on page 2483.

Limitations

- Multiple certificate authentication currently limits the number of certificates to two.
- Secure Client supports only RSA-based certificates.
- Only SHA256, SHA384, and SHA512 based certificates are supported during the Secure Client aggregate authentication.
- Certificate authentication cannot be combined with SAML authentication.

Pre-fill Username from Certificate

The Pre-fill username option allows a field from the certificates to be parsed and used for subsequent AAA authentication (primary and secondary). When two certificates are used for authentication, the Administrator can choose the certificate from which the username should be derived for the prefill functionality. By default, username for prefill is retrieved from the User certificate (second certificate received from Secure Client). The prefilled username is used as the VPN session username when the Certificate Only authentication method is enabled. When AAA and certificate authentication is enabled, VPN session username will be based on the pre-fill option.

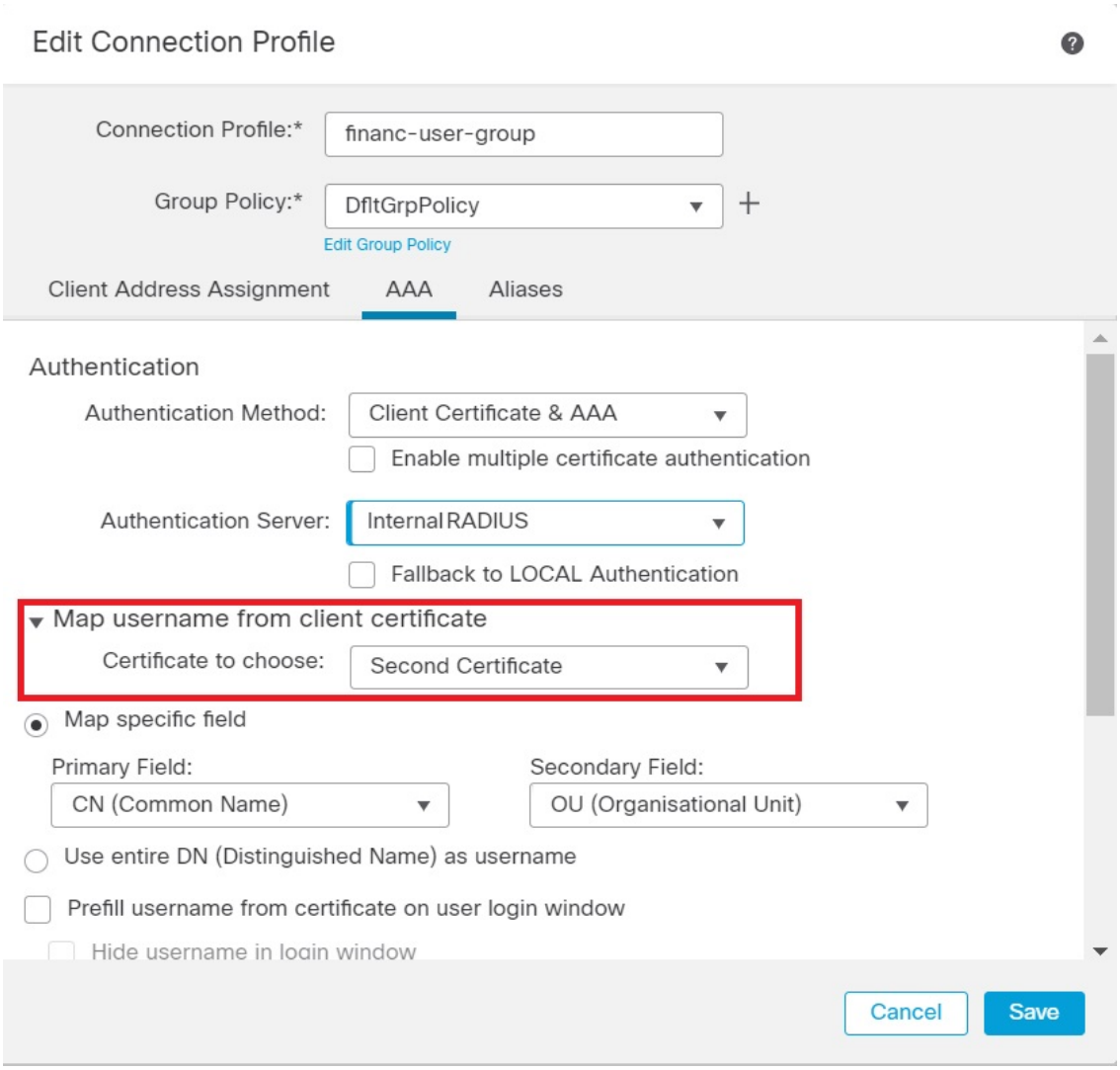
Configure Multiple Certificate Authentication for Remote Access VPN

1. On your Secure Firewall Management Center web interface, choose **Devices** > **VPN** > **Remote Access**.
2. Edit an existing remote access policy, or create a new one and then edit.

   See Create a New Remote Access VPN Policy, on page 1426.
3. Select the connection profile to configure multiple certificate authentication, and click **Edit**.

   See Configure Connection Profile Settings, on page 1436.
4. Choose **AAA**, and then select an **Authentication Method**:

Figure 401:



- **Client Certificate Only**—User is authenticated using client certificate. Client certificate must be configured on VPN client endpoints. By default, the username is derived from client certificate fields CN & OU respectively. In case, the username is specified in other fields in the client certificate, use 'Primary' and 'Secondary' field to map appropriate fields.
- **Client Certificate & AAA**—User is authenticated using both the types of authentication, AAA and client certificate.

5. Select **Enable multiple certificate authentication**.
6. Select **Map username from client certificate** and select a certificate from the **Certificate to choose** drop-down to choose the username for the VPN session from the machine certificate or user certificate.
   - **First Certificate** —Map the username from the Machine Certificate.
   - **Second Certificate**—Map the username from the User certificate to authenticate the VPN user.

7. Configure the required connection profile settings and remote access VPN settings.
8. Save the connection profile and remote access VPN policy. Deploy the remote access VPN on Firewall Threat Defense.

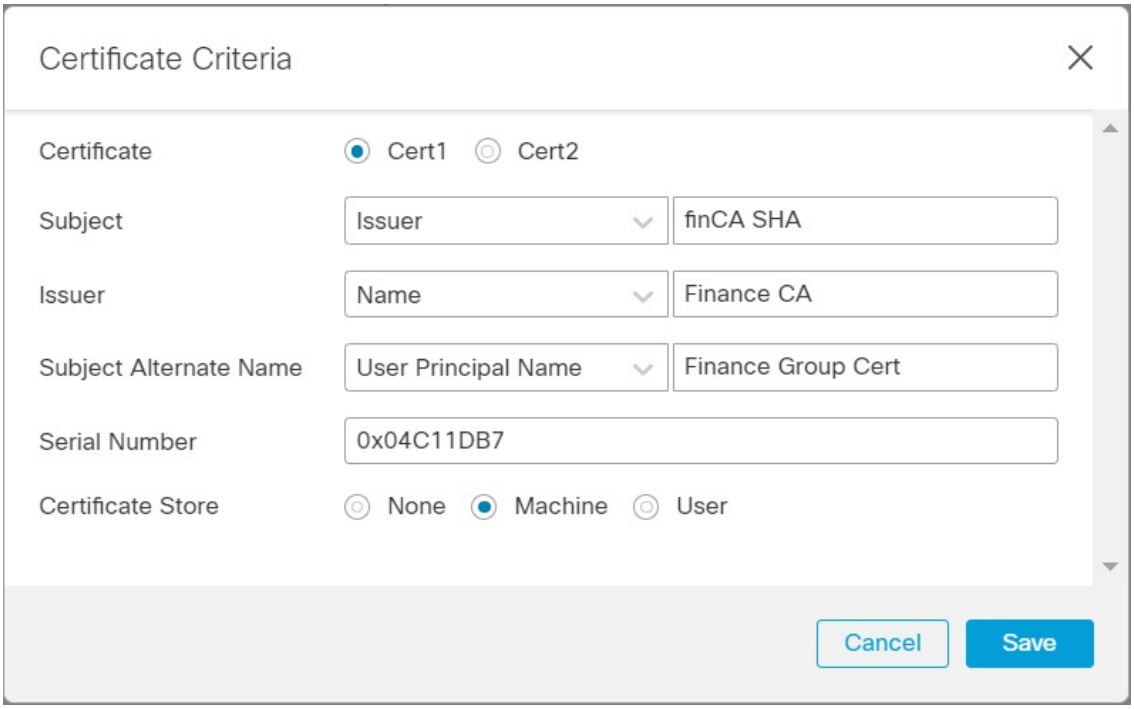
For information about remote access VPN AAA settings, see Configure AAA Settings for Remote Access VPN, on page 1439.

Certificate Configuration in DAP

You can also configure certificate criteria attributes in a DAP record. The user and machine certificate received from the VPN client during multiple-certificate authentication is loaded into dynamic access policy (DAP) to allow policies to be configured based on the field of the certificate. You can make policy decisions based on the fields of a certificate used to authenticate that connection attempt.

1. Choose **Devices** > **VPN** > **Dynamic Access Policy**.
2. Edit an existing DAP policy or create a new one and then edit the policy.
3. Choose an existing DAP record, or create a new one and then edit the record.
4. Select **Endpoint Criteria** > **Certificate**.
5. Select the Match Criteria **All** or **Any**.
6. Click **Add** to add certificate attributes.

Figure 402:



7. Select the certificate, **Cert1** or **Cert2**.
8. Select the **Subject** and specify the certificate subject value.

9. Select the **Issuer** and specify the certificate issuer name.
10. Select the **Subject Alternate Name** and specify the alternate name for the subject.
11. Specify the **Serial Number**.
12. Select the **Certificate Store**: None, Machine, or User.

    This option adds a condition to check for the store from which the certificate is picked on the endpoint.
13. Click **Save** to complete the certificate criteria settings.

    Configure the required DAP record settings and then associate the DAP with the remote access VPN.

For more information about DAP, see Dynamic Access Policies , on page 1531.

Monitor Remote Access VPNs

Remote Access VPN Dashboard

Remote Access Virtual Private Network (RA VPN) allows remote users to securely connect to your network. The RA VPN dashboard allows you to monitor real-time data from active RA VPN sessions on the devices. You can quickly determine problems related to user sessions and mitigate the problems for your network and users.

RA VPN dashboard (**Overview** > **Dashboards** > **Remote Access VPN**) provides a snapshot of the active RA VPN sessions on the threat defense devices managed by the Firewall Management Center.

The dashboard provides:

- Visualization of active user sessions based on their location.
- Detailed information about the active user sessions.
- Mitigation of user session problems by terminating sessions, if required.
- Distribution of active user sessions per device, encryption type, Secure Client version, operating system, and connection profile.
- Device identity certificate expiration details of the devices.

The dashboard has the following widgets:

- Active Sessions (Tabular View)
- Active Sessions (Map view)
- Sessions
- Device Identity Certificates

Active Sessions (Tabular View)

This widget provides a tabular view of the active RA VPN users connected. You can view details of the active RA VPN sessions such as username, assigned IP, public IP, login time, VPN gateway (threat defense device), client application, client operating system, connection profile, and group policy. You can use the filter to

narrow down your search based on the different criteria. You can also perform the following actions on the individual sessions:

- Terminate a session of a specific user.
- Terminate all sessions of a specific user connected to a specific VPN gateway.
- Terminate all sessions that are connected to a specific VPN gateway.

If a client device supports dual address stack and the RA VPN configuration on the Firewall Threat Defense device allows IPv4 and IPv6 address pools, when a client establishes an RA VPN session with the headend device, it assigns an IPv4 and an IPv6 address to the client's tunnel interface. The RA VPN session has two IP addresses, an IPv4 and an IPv6 address on the threat defense device. The Firewall Management Center shows two sessions for the same user, one with an IPv4 address and another with an IPv6 address, and the session count is two.

Hence, even when there is only a single RA VPN session from a user as per **show vpn-sessiondb l2l filter ipaddress** command on the device, the Firewall Management Center shows two different sessions.

Active Sessions (Map View)

This widget shows an interactive heat map to visualize the location of the users connected through RA VPN sessions on the devices.

- Countries that have user sessions appear in shades of blue.
- Legend of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue for the country.
- Hover the mouse pointer over the map to view the country name and the total number of active user sessions.
- Zoom in, zoom out, and reset options are available.

Sessions

This widget allows you to monitor real-time data from active RA VPN sessions on the devices. You can filter and view the distribution of active RA VPN sessions according to:

- Device: Displays the number of sessions per device.
- Encryption Type: Displays the number of Secure Client SSL or IPsec sessions.
- Secure Client Version: Displays the sessions per Secure Client version.
- Operating System: Displays the sessions per operating systems. For example, Windows, Linux, Mac, Mobile OS, and so on.
- Connection Profile: Displays the sessions per connection profile.

Device Identity Certificates

This widget provides information about the identity certificate expiry of the RA VPN gateways. You can view expired certificates and certificates that are due for expiry within a month. Click **View Details** to view the certificates in the **Devices** > **Certificates** page.

VPN Session and User Information

The system generates events that communicate the details of user activity on your network, including VPN-related activity. The system monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users. Optionally, you can log out remote access VPN users as needed.

Viewing Remote Access VPN Active Sessions

Analysis > **Users heading** > **Active Sessions**

Lets you view the currently logged-in VPN users at any given point in time with supporting information such as the user name, login duration, authentication type, assigned/public IP address, device details, client version, endpoint information, throughput, bandwidth consumed group policy, tunnel group and so on. The system allows you to filter current user information, log users out, and delete users from the summary list.



Note If you configure your VPN in a high-availability deployment, the device name displayed against active VPN sessions can be the primary or secondary device that identified the user session.

Viewing Remote Access VPN User Activity

Analysis > **Users heading** > **User Activity**

Lets you view the details of user activity on your network. The system logs historical events and includes VPN-related information such as connection profile information, IP address, geolocation information, connection duration, throughput, and device information.

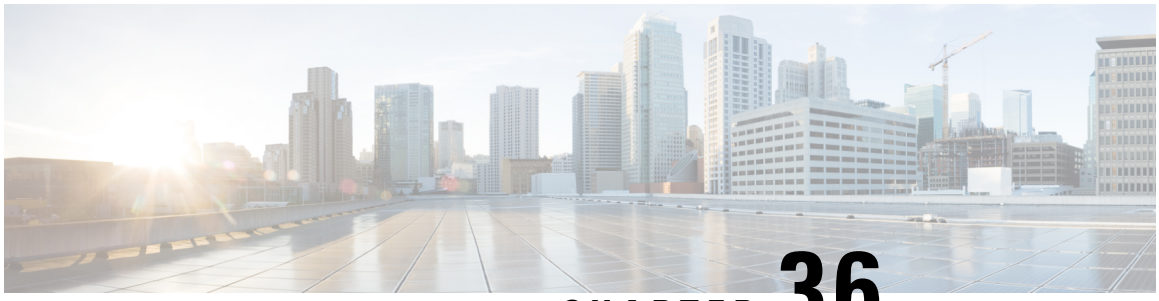
History for Remote Access VPNs

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
IPsec flow offload on the VTI loopback interface	7.4	Any	On the Secure Firewall 3100 and Secure Firewall 4200 devices, IPsec flow offload is enabled automatically on the VTI loopback interface.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Secure Client Customizations	7.4	Any	You can configure Secure Client customizations and deploy them to the VPN headend. The threat defense distributes these customizations to the endpoint when a user connects from the Secure Client: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms New/Modified Screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > **Advanced** > **Secure Client Customization**
WAN Summary Dashboard	7.4	Any	The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. New/Modified Screen: **Overview** > **Dashboard** > **WAN Summary**
Remote Access VPN dashboard	7.3	Any	The Remote Access VPN (RA VPN) dashboard that allows you to monitor real-time data from active remote access VPN sessions on the devices. So that you can quickly determine problems related to user sessions and mitigate the problems for your network and users. New/Modified Screen: **Overview** > **Dashboards** > **Remote Access VPN**
SAML with Certificate Support	7.2	Any	We have updated the remote access VPN configuration wizard to support user authentication with Certificate and SAML. You can configure a remote access VPN to authenticate machine or user certificate before a SAML authentication is initiated.
IPsec flow offload.	7.2	Any	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multiple IDP trustpoint support	7.1	Any	Secure Firewall Management Center supports multiple identity provider trustpoints with Microsoft Azure that can have multiple applications for the same Entity ID, but a unique identity certificate.
AnyConnect VPN SAML External Browser	7.1	Any	You can now configure AnyConnect VPN SAML External Browser to enable additional authentication choices, such as password less authentication, WebAuthN, FIDO, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser. We updated the remote access VPN connection profile wizard to allow you to configure the **SAML Login Experience**.
Multi-Certificate Authentication	7.0	Any	Secure Firewall Management Center now supports multiple certificate-based authentication for Firewall Threat Defense to validate the machine or device certificate, to ensure that the device is a corporate-issued device in addition to authenticating the user's identity certificate to allow VPN access using AnyConnect client.
VPN Load balancing	7.0	Any	VPN load balancing logically group two or more devices and distributes remote access VPN sessions among the grouped devices equally without considering throughput and other traffic parameters.
AnyConnect Custom Attributes	7.0	Any	Secure Firewall Management Center now supported AnyConnect custom attributes and provides an infrastructure to configure the AnyConnect client feature without adding hard-coded support for these features on Firewall Threat Defense.
Local User Authentication	7.0	Any	You can now configure and manage users locally on Firewall Threat Defense using the Secure Firewall Management Center web interface, and configure the local users for primary and secondary remote access VPN authentication.
Selective Policy Deployment	7.0	Any	You can now choose to include or exclude changes to remote access VPN and site-to-site VPN configurations during the deployment.
Support for AnyConnect Modules Configuration	6.7	Any	Secure Firewall Management Center now supports configuring AnyConnect modules and profiles for additional security.
Support for LDAP Authorization	6.7	Any	You can configure LDAP authorization for remote access VPN using the Secure Firewall Management Center.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
SAML single sign-on support for remote access VPN	6.7	Any	You can configure a SAML 2.0 server as the single sign-on authentication server for remote access VPNs.
AnyConnect Management VPN tunnel support	6.7	Any	Firewall Threat Defense remote access VPN supports configuring AnyConnect Management VPN tunnel that allows VPN connectivity to endpoints when the corporate endpoints are powered on, without the VPN users connecting to the VPN.
Support for Datagram Transport Layer Security (DTLS) 1.2	6.6	Any	DTLS 1.2 is now part of the default SSL cipher group and it can be configured along with TLS 1.2.



CHAPTER 36

Dynamic Access Policies

Dynamic access policies (DAP) enable you to configure authorization that addresses the dynamics of VPN environments. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security.

- Firewall Threat Defense dynamic access policies, on page 1531
- Prerequisites for dynamic access policy, on page 1533
- Guidelines and limitations for dynamic access policies, on page 1533
- Configure a Dynamic Access Policy (DAP), on page 1534
- Associate dynamic access policy with remote access VPN, on page 1544
- History for dynamic access policy, on page 1544

Firewall Threat Defense dynamic access policies

A Secure Firewall Threat Defense dynamic access policy is a collection of access control attributes that

- addresses issues of multiple group memberships and endpoint security in VPN environments
- grants access to particular users for particular sessions according to defined policies, and
- adapts to dynamic environments with multiple variables affecting each VPN connection.

Dynamic access policy operation

VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection. For example, intranet configurations that frequently change, the various roles each user inhabits within an organization, and log in attempts from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

You can create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. The Firewall Threat Defense device generates a DAP during user authentication by selecting or aggregating attributes from one or more DAP records. The device then selects these DAP records based on the endpoint security information of the remote device and AAA authorization information for the authenticated user. Then the device applies the DAP record to the user tunnel or session.

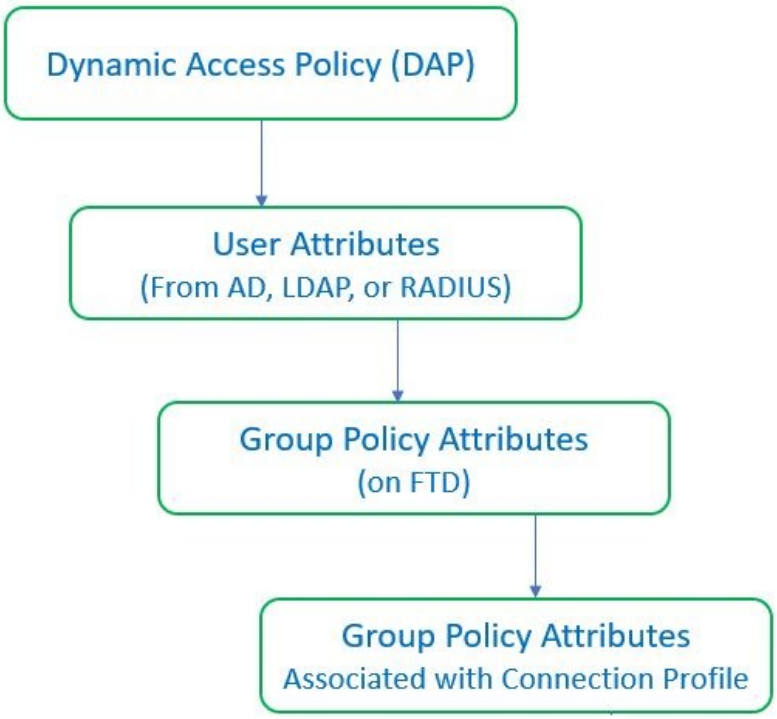
Hierarchy of policy enforcement of permissions and attributes in a Firewall Threat Defense device

The Firewall Threat Defense device supports applying user authorization attributes, also called user entitlements or permissions, to VPN connections. The attributes are applied from a DAP on the Firewall Threat Defense, external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the Firewall Threat Defense device.

If the Firewall Threat Defense device receives attributes from all sources, the device evaluates, merges, and applies the attributes to the user policy. If there are conflicts between attributes coming from the DAP, the AAA server, or the group policy, the attributes from the DAP always take precedence.

The Firewall Threat Defense device applies attributes in this order:

Figure 403: Policy enforcement flow



1. **DAP attributes on the FTD**—The DAP attributes take precedence over all others.
2. **User attributes on the external AAA server**—The server returns these attributes after successful user authentication and/or authorization.
3. **Group policy configured on the FTD**—If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the Firewall Threat Defense device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

4. **Group policy assigned by the Connection Profile (also known as Tunnel Group)**—The Connection Profile has the preliminary settings for the connection, and includes a default group policy that is applied to the user before authentication.

Note The Firewall Threat Defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. For the user session, the device uses the attributes on the group policy that you assign to the connection profile, unless the user attributes or the group policy from the AAA server overrides them.

Prerequisites for dynamic access policy

This reference provides the licensing prerequisites that must be met before configuring Dynamic Access Policy features.

Licensing prerequisites

- Firewall Threat Defense must have at least one of these Secure Client licenses:
  - Secure Client Premier
  - Secure Client Advantage
  - Secure Client VPN Only
- The Firewall Threat Defense Essentials license must allow export-controlled functionality.

General prerequisite

Ensure that you have the Secure Firewall Posture package before you configure the dynamic access policy. You can add the Secure Firewall Posture file at **Objects** > **Object Management** > **VPN** > **Secure Client File**.

Guidelines and limitations for dynamic access policies

Consider these guidelines and limitations when implementing Dynamic Access Policies:

- Matching of AAA attributes in a DAP will work only if a AAA server is configured to return the correct attributes when authenticating or authorizing a remote access VPN session.
- Minimum Secure Client and Secure Firewall Posture package version supported for DAP is 4.6. But it is highly recommended to use the latest version of Secure Client.
- DAP does not support clustering or multi-instance mode.
- DAP condition with an assigned IPv4 or IPv6 address does not work for local authentication.

Configure a Dynamic Access Policy (DAP)

Create a dynamic access policy

Create a dynamic access policy to enable conditional access control for VPN users based on their endpoint security posture and compliance status.

Dynamic access policies evaluate endpoint attributes and security posture to determine appropriate access permissions for VPN users. These policies work in conjunction with posture assessment packages to enforce security compliance.

Before you begin

Ensure that you have the Secure Firewall Posture package before you configure the dynamic access policy. You can add the Secure Firewall Posture file at **Objects** > **Object Management** > **VPN** > **Secure Client File**.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**, and click **Create Dynamic Access Policy**.

Step 2 Specify the **Name** for the DAP policy and an optional **Description**.

Step 3 Choose the **HostScan Package** from the drop-down list.

Step 4 Click **Save**.

What to do next

To configure DAP record, see Create Dynamic Access Policy Record

Create a dynamic access policy record

A dynamic access policy (DAP) can contain multiple DAP records, where you configure user and endpoint attributes. You can prioritize the DAP records within a DAP so that the Firewall Threat Defense device can select and sequence the required criteria when a user attempts VPN connection.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Edit an existing dynamic access policy or click **Create Dynamic Access Policy** to create a new one and then edit the policy.

Step 3 Click **Create DAP Record**.

Step 4 Click the **General** tab.

Step 5 Specify the **Name** for the DAP record.

Step 6 Enter the **Priority** for the DAP record.

The lower the number, the higher the priority.

Step 7 Select one of these actions to take when a DAP record matches:

- **Continue**—Applies access policy attributes to the session. If any, the next DAP record (next policy line with less priority) is then evaluated.
- **Terminate**—Terminates the session.
- **Quarantine**—Quarantines the connection.

Step 8 Check the **Display User Message on Criterion Match** check-box and add the user message.

The Firewall Threat Defense displays this message to the user when the DAP record matches.

Step 9 Check the **Apply a Network ACL on Traffic** check box and select the access control list from the drop-down.

Step 10 Check the **Apply one or more Secure Client Custom Attributes** check box and select the custom attributes object from the drop-down.

Step 11 Click **Save**.

Configure AAA criteria settings for a DAP record

Configure AAA criteria settings to specify the conditions under which DAP records are selected and applied to user sessions based on AAA authorization and posture assessment information.

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. The Firewall Threat Defense device selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The Firewall Threat Defense device can choose multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Edit an existing DAP policy or create a new one and then edit the policy.

Step 3 Select a DAP record or create a new one, and edit the DAP record.

Step 4 Click **AAA Criteria**.

Step 5 Select one of the **Match criteria between sections**.

- Any—Matches any of the criteria.
- All—Matches all the criteria.
- None—Matches none of the set criteria.

Step 6 Click **Add** to add the required **Cisco VPN Criteria**.

Cisco VPN criteria include attributes for group policy, assigned IPv4 address, assigned IPv6 address, connection profile, username, username 2, and SCEP required.

a) Select an attribute and specify the **Value**.
b) Click **Add another criteria** to add more criteria.
c) Click **Save**.

Step 7 Select **LDAP Criteria**, **RADIUS Criteria**, or **SAML Criteria** and specify the **Attribute ID** and **Value**.

Step 8 Click **Save**.

Configure endpoint attribute selection criteria in DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. A Firewall Threat Defense device dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database that is associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the Firewall Threat Defense device to choose it for a session. The Firewall Threat Defense device selects only DAP records that satisfy every condition configured.

Note When using remote Access VPN with DAP or Secure Firewall Posture (formerly HostScan) and change of authorization (CoA), endpoint attribute checks differ between initial authentication and CoA-triggered authorization.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**, and click **Create Dynamic Access Policy**.

Step 2 Create or edit a DAP record.

Step 3 Click **Endpoint Criteria** and configure attributes such as anti-malware, device, Secure Client, NAC, application, personal firewall, operating system, process, registry, file, and certificate authentication.

Note You can create multiple instances of each type of endpoint attribute. There is no limit for the number of endpoint attributes for each DAP record.

Step 4 Click **Save**.

Add an anti-malware endpoint attribute to a DAP record

Add anti-malware endpoint attributes to a DAP to control access based on the presence and configuration of anti-malware software on client devices.

Anti-malware endpoint attributes allow you to create access policies that verify client devices have appropriate anti-malware protection before granting network access.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Anti-Malware**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add the anti-malware attributes.

In the **Anti-Malware** dialog box, configure these parameters:

a) Check the **Installed** check box to indicate whether the selected endpoint attribute and its accompanying qualifiers are installed or not installed.
b) In **Real Time Scanning**, choose **Enabled** or **Disabled** to activate or deactivate real-time malware scanning.
c) Choose the anti-malware vendor from the **Vendor** drop-down list.
d) Choose the anti-malware description from the **Product Description** drop-down list.
e) Choose the **Version** of the anti-malware product.
f) Specify the number of days since the **Last Update**.

You can indicate that an anti-malware update must occur in less than (<) or more than (>) the number of days you specify.

g) Click **Save**.

Add a device endpoint attribute to a DAP record

Add device endpoint attributes to a DAP to control access based on specific device characteristics such as hostname, MAC address, BIOS serial number, or port configuration.

Device endpoint attributes allow you to create policies that evaluate device-specific criteria to determine access permissions. These attributes help enforce security policies based on device identity and configuration.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Device**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add application attributes.

In the **Device** dialog box, configure these parameters:

Select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter for these attributes:

- **Host Name**—Hostname of the device. Use the computer's host name only, not the fully qualified domain name (FQDN).
- **MAC Address**—MAC address of the network interface card you are testing for. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
- **BIOS Serial Number**—BIOS serial number value of the device you are testing for. The number format is manufacturer-specific.
- **Port Number**—Listening port number of the device.
- **Secure Desktop Version**—Version of the Secure Firewall Posture image running on the endpoint.
- **OPSWAT Version**—The OPSWAT client version.
- **Privacy Protection**—None, Cache cleaner, Secure Desktop.
- **TCP/UDP Port Number**—TCP or UDP port in the listening state.

Step 6 Click **Save**.

Add Secure Client endpoint attributes to a DAP record

Add specific endpoint attributes to a Dynamic Access Policy (DAP) record to control client access based on Secure Client characteristics such as client version, platform, and device identifiers.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Secure Client**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add the attributes.

In the **Secure Client** dialog box, configure these parameters:

Select the **=** or **≠** operator to check the attribute to be equal to or not equal to the value you enter.

a) Specify the **Client Version**.
b) Choose the platform from the **Platform** drop-down list.
c) Choose the platform version from the **Platform Version** drop-down list.
d) Specify the **Device Type** and **Device Unique ID**.
e) Add the **MAC Addresses**.

Note The MAC Address must be in the format XX-XX-XX-XX-XX-XX, where each X is a hexadecimal character. You can click **Add another MAC Address** to add more addresses.

f) Click **Save**.

Add NAC endpoint attributes to a DAP record

You can configure Network Access Control (NAC) endpoint attributes within a DAP (Dynamic Access Policy) record to evaluate endpoint posture status based on a defined criteria.

NAC endpoint attributes in DAP records help determine access permissions based on endpoint posture compliance. You can specify whether endpoints must match all criteria or any criteria, and define specific posture token strings for evaluation.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **NAC**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add NAC attributes.

Step 6 In the **NAC** dialog box, set the operator to be equal to **=** or not equal to **≠** the posture status.

Step 7 Choose one of these options from the **Posture Status** drop-down list:

- Compliant
- Non-Compliant
- Unknown

Step 8 Click **Save**.

Add an application attribute to a DAP record

This task allows you to define application-specific criteria within a DAP record to control access based on the type of remote access client.

Application attributes in DAP records help determine access policies by evaluating the client application type used for remote connections. You can configure these attributes to match all or any specified criteria.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Application**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add application attributes.

Step 6 In the **Application** dialog box, choose equals (=) or does not equal (≠) and specify the **Client Type** to indicate the type of remote access connection. Choose from one of these options:

- Clientless
- Cut-Through-Proxy
- Secure Client
- IPsec
- L2TP
- IPsec-IKEv2-Generic-RA

Step 7 Click **Save**.

Add a personal firewall endpoint attribute to a DAP record

Adding personal firewall endpoint attributes to a DAP allows you to control network access based on whether client devices have specific firewall software installed, enabled, and meeting version requirements.

Personal firewall endpoint attributes help enforce security policies by ensuring that connecting devices meet firewall protection standards before granting network access.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Personal Firewall**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add personal firewall attributes.

In the **Personal Firewall** dialog box, configure these parameters:

a) Click **Installed** to indicate whether the personal firewall endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.
b) Select **Enabled** or **Disabled** to activate or deactivate firewall protection.
c) Choose the name of the firewall vendor from the **Vendor** drop-down list.
d) Choose the firewall description from the **Product Description** drop-down list.
e) Select the equals (=) or does not equal (≠) operator and choose the **Version** of the personal firewall product.
f) Click **Save**.

Add an operating system endpoint attribute to a DAP record

Operating system endpoint attributes help create granular access policies by identifying and filtering client devices based on their operating system characteristics. This is useful for implementing different access levels or restrictions based on device types.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Operating System**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add endpoint attributes.

In the **Operating System** dialog box, configure these parameters:

a) Select the equals (=) or does not equal (≠) operator and then choose the operating system from the **Operating System** drop-down list.
b) Select the equals (=) or does not equal (≠) operator and then specify the operating system version in the **Version** field.
c) Click **Save**.

Add a process endpoint attribute to a DAP

Configure process endpoint attributes to define specific criteria for device access policy enforcement based on running processes.

Process endpoint attributes allow you to create device access policies based on specific processes running on endpoints. This helps ensure that only devices with approved processes can access network resources.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Process**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click + to add process attributes.

In the **Process** dialog box, configure these parameters:

a) Select **Exists** or **Does not exist**.
b) Specify the **Process Name**.
c) Click **Save**.

Add a registry endpoint attribute to a DAP record

Registry endpoint attributes allow you to define specific registry keys that the system scans during posture assessment to determine endpoint compliance status.

Scanning for registry endpoint attributes applies to Windows operating systems only.

Before you begin

Before configuring a registry endpoint attribute, define the registry key for which you want to scan in the Secure Firewall Posture window for Cisco Secure Desktop.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **Registry**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add registry attributes.

In the **Registry** dialog box, configure these parameters:

a) Select the **Entry Path** for the registry and specify the path.
b) Choose the existence of the registry, **Exists** or **Does not exist**.
c) Select the registry **Type** from the list.
d) Select the equals (**=**) or does not equal (**≠**) operator and enter the **Value** of the registry key.
e) Select **Case insensitive** to disregard the case of the registry entry while scanning.
f) Click **Save**.

Add a file endpoint attribute to a DAP record

You can configure file endpoint criteria within a DAP (Device Access Policy) record to specify file attributes used for posture assessment and device authorization.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.

Step 2 Create or edit a DAP policy and a DAP record.

Step 3 Click the **Endpoint Criteria** tab and click **File**.

Step 4 Select the **Match criteria** as **All** or **Any**.

Step 5 Click **+** to add file attributes.

In the **File** dialog box, configure these parameters:

a) Specify the **File Path**.
b) Select **Exists** or **Does not exist** to indicate the presence of the file.
c) Select less than (**<**) or greater than (**>**) and specify the **Last Modified** days for the file.

d) Select the equal to (=) or not equal to ≠ operator and enter the **Checksum**.
e) Click **Save**.

Add certificate authentication attributes to a DAP record

Adding certificate authentication attributes to a DAP allows you to control access based on specific certificate fields such as subject, issuer, and serial number.

You can index each certificate to allow referencing to any of the received certificates, by the configured rules. Based on these certificate fields, you can configure DAP rules to allow or disallow connection attempts.



Note This configuration is applicable only for certificates used with multiple certificate authentication. It does not apply for single client certificate authentication.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.
Step 2 Create or edit a DAP record.
Step 3 Click the **Endpoint Criteria** tab and click **Multiple Certificate Authentication**.
Step 4 Select the **Match criteria** as **All** or **Any**.
Step 5 Click + to add certification authentication criteria.

In the **Multiple Certificate Authentication Criteria** dialog box, configure these parameters:

a) Select **Cert1** or **Cert2** certificate.
b) Select the **Subject** and specify the subject value.
c) Select the **Issuer** and specify the issuer value.
d) Select the **Subject Alternate Name** and specify the subject value.
e) Specify the **Serial Number**.
f) Choose the **Certificate Store** as **None**, **Machine**, or **User**.

The VPN client sends the certificate store information.

g) Click **Save**.

Configure advanced settings for DAP

This task allows you to configure selection criteria for DAP records using Lua scripts when the standard AAA AND endpoint attribute areas are insufficient for your requirements.

You can use the **Advanced** tab for adding selection criteria other than what is possible in the AAA AND endpoint attribute areas. For example, while you can configure the Firewall Threat Defense to use AAA attributes that satisfy any, all, OR none of the specified criteria, the endpoint attributes are cumulative, AND

must satisfy all. To let the security appliance employ one endpoint attribute OR another, you must create appropriate logical expressions in Lua AND enter them here.

Procedure

Step 1 Choose **Devices** > **VPN** > **Dynamic Access Policy**.
Step 2 Create or edit a DAP record.
Step 3 Click the **Advanced** tab.
Step 4 Select **AND** OR **OR** as the match criteria to use in the DAP configuration.
Step 5 Add the Lua script in the **Lua script for advanced attribute matching** field.
Step 6 Click **Save**.

Associate dynamic access policy with remote access VPN

You can associate Dynamic Access Policy (DAP) with remote access VPN policy for the dynamic access policy attributes to match during VPN session authentication and authorization. You can then deploy the remote access VPN on the Firewall Threat Defense.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.
Step 2 Click **Edit** next to the remote access VPN policy to which you want to associate dynamic access policy.
Step 3 Click the link in remote access VPN to select the dynamic access policy.
Step 4 Select the policy from the **Dynamic Access Policy** drop-down or click **Create a new Dynamic Access Policy** to configure a new dynamic access policy.
Step 5 Click **OK**.
Step 6 Click **Save** to save the remote access VPN policy.

When the remote access VPN user tries to connect, the VPN checks the configured dynamic access policy records and attributes. VPN creates a dynamic access policy based on the matching dynamic access policy records and takes appropriate action on the VPN session.

History for dynamic access policy

This reference provides the version history for dynamic access policy features, including when they were introduced and what changes were made in each release.

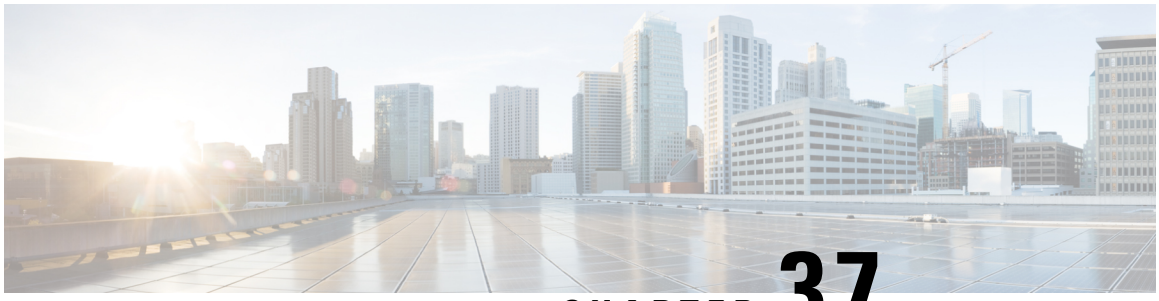
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dynamic Access Policy	7.0	Any	The feature was introduced.



PART VII

Zero Trust Network Access

- Zero Trust Network Access Overview, on page 1549



CHAPTER 37

Zero Trust Network Access Overview

Zero Trust Network Access (ZTNA) secures internal resources by verifying user identity and device posture to grant least-privilege access. Organizations implement either browser-based Clientless ZTNA for web applications or agent-based Universal ZTNA for comprehensive, protocol-wide support using existing threat defense infrastructure.

- Zero Trust Access, on page 1549
- History for zero trust network access, on page 1564

Zero Trust Access

Zero Trust Access is based on Zero Trust Access principles. Zero Trust Access is a zero trust security model that eliminates implicit trust. The model grants the least privilege access after verifying the user, the context of the request, and after analyzing the risk if access is granted.

Zero Trust Access enables you to authenticate and authorize access to protected web-based resources and applications from inside (on-premises) or outside (remote) the network using an external Security Assertion Markup Language (SAML) identity provider (IdP) policy.

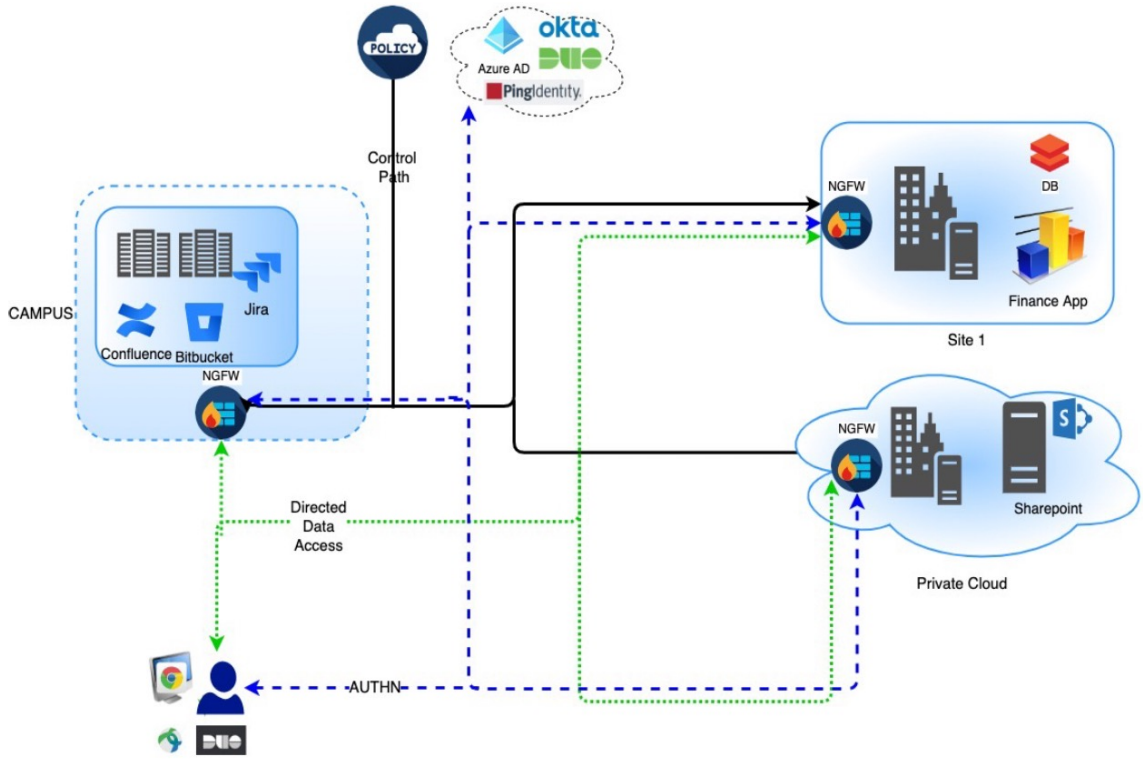
The features are:

- Supports multiple SAML-based identity providers such as Duo, Azure Active Directory (Azure AD), Okta, and other identity providers.
- Client applications such as Cisco Secure Client are not required on the endpoint (client devices) for secure access.
- Access and authentication is through the browser.
- Supports only TLS web applications.
- Client device posture is supported through agents such as Duo Health, using which the posture of the device can be evaluated against a policy in Duo, and access can be provided based on the same. The same functionality can be performed in conjunction with third-party identity providers that support posture evaluation with their agents such as Okta or PingID.
- Supports HTTP-Redirect SAML binding.
- Supports application groups that make it easier to enable zero trust access protection on a set of applications.
- Leverages threat defense intrusion and malware protection on zero trust application traffic.

You can use the Secure Firewall Management Center web interface to create a Zero Trust Application Policy that allows you to define private applications and assign threat policies to them. The policy is application specific where the administrator decides the inspection levels based on the threat perception for that application.

How Threat Defense Works with Zero Trust Access

Figure 404: Threat Defense Deployment



1. Using a browser, a remote or on-prem user sends a HTTPS request to connect to an application from an endpoint.
2. The HTTPS request is intercepted by the firewall that protects the application.
3. The firewall redirects the user to application's configured IdP for authentication.

Note In the figure, each firewall protects a set of web applications. The user can directly access the applications behind the firewall after authentication and authorization.

4. After the authentication and authorization process is complete, the firewall allows the user to access the application.

Zero trust network access

Zero Trust Network Access (ZTNA) provides secure, segmented application access by requiring explicit authorization for every connection. This approach reduces the attack surface and simplifies secure migrations without adding devices.

Key characteristics

ZTNA uses your existing Threat Defense deployment as an enforcement point for application access, enabling segmented and per-application authorization. ZTNA establishes individual tunnels for both remote and on-premises users.

ZTNA hides the network from users and ensures that they can only access applications for which they have been explicitly authorized. Authorization for one application does not provide implicit access to other applications, which significantly reduces the attack surface. In other words, every access to an application or a resource must be explicitly authorized.

You can adopt a more secure access model by adding zero trust access functionality to Threat Defense. This eliminates the need to install or manage additional devices in the network.

Components of a Clientless Zero Trust Network Access Configuration

A new configuration consists of a Zero Trust Application Policy, Application Group, and Applications.

- **Zero Trust Application Policy**— Consists of application groups, and grouped or ungrouped applications. Security Zones and Security Controls settings are associated at a global level for all the ungrouped applications and group of applications.

  A global port pool is assigned to the policy, by default. A unique port is automatically assigned from this pool to each private application that is configured.

  Zero Trust Application policy consists of application groups, and grouped or ungrouped applications.

- **Application Groups**—Consists of a logical group of applications that share SAML authentication settings and can optionally share Security Zones and Security Controls settings.

  Application Groups inherit the Security Zones and Security Controls settings from the global policy and can override the values.

  When an Application Group is created, the same SAML IdP configuration can be used for authenticating multiple applications. Applications that are part of an Application Group inherit the Application Group's SAML configuration. This eliminates the need to configure the SAML settings for each application. After the Application Group is created, new applications can be added to it without configuring the IdP for it.

  When an end user tries to access an Application that is part of group, the user is authenticated to the Application Group for the first time. When the user tries to access other applications that are part of the same Application Group, the user is provided access without being redirected again to the IdP for authentication. This prevents overloading the IdP with requests for application access and optimizes the usage of the IdP if a limit is enabled.

- **Applications**—There are two types:

  - **Ungrouped Applications**— Are standalone applications. SAML settings must be configured for every application. The applications inherit the Security Zones and Security Controls settings from the global policy and can be overridden by the application.

- **Grouped Applications**— Are multiple applications that are grouped under an Application Group. The SAML settings are inherited from the Application Group and cannot be overridden. However, the Security Zones and Security Controls settings can be overridden for each application.

The following certificates are required for the configuration:

- **Identity Certificate**—This certificate is used by Firewall Threat Defense to masquerade as the applications. Firewall Threat Defense behaves as a SAML Service Provider (SP). This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications. It is a common certificate for all applications protected by Firewall Threat Defense. Upload the public key from the same certificate to the identity provider (IDP), designating it as the SP certificate. The identity provider uses this certificate to verify the authentication request it receives. By default, Firewall Threat Defense signs the SAML authentication request before sending it to IDP. You cannot disable authentication request signing, and it is not configurable.
- **IdP Certificate**—The IdP provides a certificate for each defined Application or Application Group. This certificate must be configured so that Firewall Threat Defense can verify the IDP's signature on incoming SAML assertions.

Note IdP certificates are commonly included within the metadata file; otherwise, users are required to have the IdP certificate readily available during the configuration of applications.

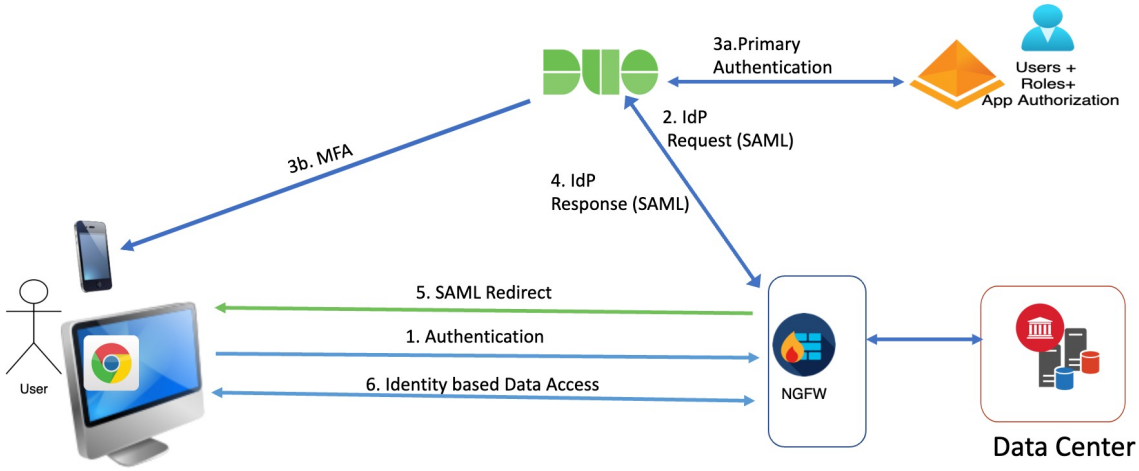
- **Application Certificate**—The encrypted traffic from user to the application is decrypted by Firewall Threat Defense using this certificate for the purpose of inspection.

Note This certificate is required to verify the cookies in the header to authorize connections, even if we are not conducting an IPS/Malware inspection.

Clientless Zero Trust Network Access Workflow

This figure depicts the Zero Trust Access workflow.

Figure 405: Clientless Zero Trust Network Access Workflow



The workflow is as follows:

1. User types the application URL in the browser.
   - If the HTTPS request is valid, the user is redirected to the mapped port (Step 6).
   - If the HTTPS request is invalid, the user is sent for authentication per application (Step 2).
2. The user is redirected to the configured identity provider (IdP).
3. **a.** The user is redirected to the configured primary authentication source.
   b. The user is challenged with the configured secondary multi-factor authentication, if any.
4. The IdP sends a SAML response to threat defense. The user ID and other necessary parameters are retrieved from the SAML response through the browser.
5. The user is redirected to the application.
6. The user is allowed access to the application after validation is successful.

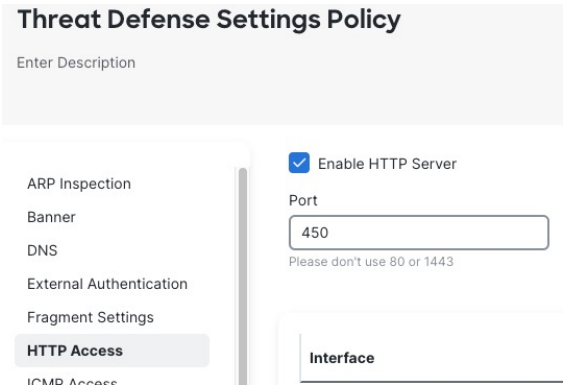
Limitations for Clientless Zero Trust Network Access

- Supports only TLS-enabled web applications. All traffic must be decrypted.
- Supports only SAML identity providers.
- IPv6 is not supported.

  NAT66, NAT64, and NAT46 scenarios are not supported.
- Clientless zero trust network access is available on Firewall Threat Defense only if Snort 3 is enabled.
- By default, the Firewall Threat Defense device uses port 443 for secure communications. Because this is the same port used by TLS-enabled applications likely to be configured for zero trust network access, you must change the device's HTTP server port.

Go to **Devices** > **Platform Settings**, then edit the Threat Defense Settings policy for the device, click **HTTP Access**, select the **Enable HTTP Server** check box, and enter a port other than 443 in the field. When you're finished, click **Save** in the upper right corner of the page.

The following figure shows an example.



- All hyperlinks in protected web applications must have a relative path and are not supported on individual mode clusters.
- Protected web applications running on a virtual host or behind internal load balancers must use the same external and internal URL.
- Not supported on applications with strict HTTP Host Header validation enabled.
- If the application server hosts multiple applications and serves content based on the Server Name Indication (SNI) header in the TLS Client Hello, the external URL of the zero trust application configuration must match the SNI of that specific application.

Prerequisites for Zero Trust Application Policy

Prerequisite Type	Description
Licensing	• Smart license account with export-controlled features • (Optional) IPS and Threat licenses—It is required if security controls are used.
Configurations	Create a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of private applications. For more information, see Add certificate enrollment objects, on page 2402.
	Create a security zone through which access to private applications are regulated. For more information, see Create security zone and interface group objects, on page 610.

Manage Zero Trust Application Policies

You can create, edit, and delete zero trust application policies.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Manage the zero trust access policies:

- Create—Click **New Policy**. See Create a Zero Trust Application Policy, on page 1555
- Edit—Click **Edit** ( ). See Edit a Zero Trust Application Policy, on page 1560
- Report—Click **Report** ( ).
- Delete—Click **Delete** ( ).

Step 3 Click **Save**.

What to do next

Ensure that there are no warnings before you deploy the configuration to threat defense. To deploy configuration changes, see Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create a Zero Trust Application Policy

This tasks configures a Zero Trust Application Policy.

Before you begin

Ensure that you complete all the prerequisites listed in Prerequisites for Zero Trust Application Policy, on page 1554.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**.

Step 2 Click **Add Policy**.

Step 3 In the **General** section, enter the policy name in the **Name** field. The description field is optional.

Step 4 Enter a domain name in the **Domain Name** field.

Ensure that the domain name is added to the DNS. The domain name resolves to the Firewall Threat Defense gateway interface from where the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.

Step 5 Choose an existing certificate from the **Identity Certificate** drop-down list.

Click the **Add** (+) icon to configure a certificate enrollment object. For more information, see Add certificate enrollment objects, on page 2402.

Step 6 Choose a security zone from the **Security Zones** drop-down list.

Click the **Add** (+) icon to add a new security zone.

To add security zones, see Create security zone and interface group objects, on page 610.

Step 7 In the **Global Port Pool** section, a default port range is displayed. Modify, if required. Port values range from 1024 to 65535. A unique port from this pool is assigned to each private application.

Note This port range should avoid any conflicts with the existing NAT range.

Step 8 (Optional) In the **Security Controls** section, you can add an Intrusion or Malware and File policy:

- **Intrusion Policy**—Choose a default policy from the drop-down list or click the **Add** (+) icon to create a new custom intrusion policy. For more information, see Creating a Custom Snort 3 Intrusion Policy topic in the latest version of the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
- **Variable Set**—Choose a default variable set from the drop-down list or click the **Add** (+) icon to create a new variable set. For more information, see Create a variable set, on page 2452.

Note To use variable sets, you must have the Secure Firewall Threat Defense IPS license for your managed devices.

- **Malware and File Policy**—Choose an existing policy from the drop-down list. Click the **Add** (+) icon to create a new malware and file policy. For more information, see Manage file policies, on page 2039.

Step 9 Click **Save** to save the policy.

What to do next

1. Create an Application Group. See Create an Application Group, on page 1557.
2. Create an Application. See Create an Application, on page 1558.
3. Associate a Zero Trust Application Policy with a device. See Set Targeted Devices for Zero Trust Access Policy, on page 1560
4. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create an Application Group

Before you begin

Create a Zero Trust Application Policy, on page 1555

Procedure

Step 1 Click **Add Application Group**.

Step 2 In the **Application Group** section, type the name in the **Name** field and click **Next**.

Step 3 In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the values of the **Entity ID** and **Assertion Consumer Service (ACS) URL** fields or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.

Step 4 In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:

- **XML File Upload**—Choose a file or drag and drop the XML file.

  The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.

- **Manual Configuration**—Perform these steps:
  - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
  - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.
  - **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

    Click the **Add** (+) icon to configure a new certificate enrollment object. For more information, see Add a certificate enrollment, on page 2403.

- **Configure Later**—In the event you do not have the IdP metadata, you can configure it later.

Click **Next**.

Step 5 In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**.

The re-authentication interval allows you to provide a value that determines when a user must authenticate again.

Step 6 In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy. You can override these settings. Click **Next**.

Step 7 Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.

Step 8 Click **Save**.

The Application Group is created and is displayed on the Zero Trust Application page.

What to do next

1. Create an Application, on page 1558.

2. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create an Application

Use this task to create a Grouped or Ungrouped Application.

Before you begin

1. Create a Zero Trust Application Policy, on page 1555.
2. Create an Application Group, on page 1557 (required only for Grouped Applications).

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Choose the policy.

Step 3 Click **Add Application**.

Step 4 In the **Application Settings** section, complete the following fields.

- **Application Name**—Enter the application name.
- **External URL**—Enter the URL that is used by the user to access the application.
- **Application URL**—By default, the external URL is used as the Application URL. Uncheck the **Use External URL as Application URL** check box to specify a different URL.

  If Threat Defense uses an internal DNS, the Application URL must match an entry within that DNS to ensure it resolves to the application.

- **Application Certificate**—Choose the certificate for the private application. Click the **Add** (+) icon to configure an internal certificate object. For more information, see Add internal certificate objects, on page 2400.
- **IPv4 Source Translation**—Choose the source network for NAT from the list. Click **Add** (+) to create a network object. For more information, see Networks, on page 2386.

  This Network Object or Object Group is used to translate a public network source IPv4 address of an incoming request to a routable IPv4 address inside the corporate network.

Note Only object or object groups of type Host or Range are supported.

- **Application Group**—Choose the Application Group from the drop-down list. See Create an Application Group, on page 1557.

Note This field is not applicable for an ungrouped application.

Step 5 Click **Next**.

Step 6 Depending on the type of application:

- For a Grouped Application, the **SAML Service Provider (SP) Metadata**, **SAML Identity Provider (IdP) Metadata** , and **Re-authentication Interval** are inherited from the Application Group and do not need to be configured by the user.
- For an Ungrouped Application, perform these steps:

  a. In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the **Entity ID**, **Assertion Consumer Service (ACS) URL** of the IdP, or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.

  b. In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:

  - **XML File Upload**—Choose a file or drag and drop the XML file.

    The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.

  - **Manual Configuration**—Perform these steps:
    - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
    - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.
    - **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

      Click the **Add** (+) icon to configure a new certificate enrollment object. For more information, see Add a certificate enrollment, on page 2403.

  - **Configure Later**—If you do not have the IdP metadata, you can configure it later.

  Click **Next**.

  c. In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**. The reauthentication interval allows you to provide a value that determines when a user must authenticate again.

Step 7 In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy or application group. You can override these settings. Click **Next**.

Step 8 Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.

Step 9 Click **Save**.

The application is listed on the Zero Trust Application page and enabled by default.

What to do next

1. Set Targeted Devices for Zero Trust Access Policy, on page 1560.
2. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Set Targeted Devices for Zero Trust Access Policy

Each Zero Trust Application policy can target multiple devices; each device can have one deployed policy at a time.

Before you begin

1. Create a Zero Trust Application Policy, on page 1555.
2. Create an Application Group, on page 1557.
3. Create an Application, on page 1558.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Choose the policy.

Step 3 Click **Targeted Devices**.

Step 4 Choose the devices where you want to deploy the policy using any one of the methods:

- Choose a device in the **Available Devices** list and click >> or the **Add** (⊕) icon.
- To remove a device from the **Selected Devices** list, choose a device and click << or the **Delete** ( ) icon.

Step 5 Click **Apply** to save policy assignments.

Step 6 Click **Save** to save the policy.

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Edit a Zero Trust Application Policy

You can edit the settings of a Zero Trust Application Policy, Application Group, or Application.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Click **Edit** (✎) next to the Zero Trust Application Policy you want to edit.

Step 3 Edit your Zero Trust Application Policy.

You can change the following settings or perform these actions:

- Name and Description—Click **Edit** (✎) next to the policy name, make your changes, and click **Apply**.
- To modify the policy settings:
  - Click **Settings**
  - Modify the settings as required.

Important Editing the domain name for the SAML ACS URL interrupts application access.

  - Click **Save**.

- To modify the Application Group settings:
  - Click **Applications**.
  - Click **Edit** (✎) next to the Application Group you want to edit.
  - In each section, click **Edit** to modify the settings, as required

Important Editing the Application Group name interrupts application access.

  - Click **Apply** after you modify the settings in a section.
  - Click **Finish**.
  - Click **Save**.

- To modify the Application settings:
  - Click **Applications**.
  - Click **Edit** (✎) next to the Application you want to edit.
  - In each section, click **Edit** to modify the settings, as required.

Important Editing the Application name interrupts application access.

  - Click **Apply** after you modify the settings in a section.

- Click **Finish**.
- Click **Save**.

- To enable, disable, or delete multiple Applications, choose the Applications, click the required bulk action, and click **Save**.

Note These actions are also available in the right-click menu.

- To enable all Applications, click **Bulk Actions** > **Enable**.
- To disable all Applications, click **Bulk Actions** > **Disable**.
- To delete all Applications, click **Bulk Actions** > **Delete**.

- Click **Return to Zero Trust Application** to return to the policy page.

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Monitor Zero Trust Sessions

Connection Events

After a Zero Trust Application Policy is deployed, new fields are available. To add the fields to the table view:

1. Choose **Analysis** > **Unified Events**.
2. Click the column picker ( ) icon and add these columns:
   - **Authentication Source**
   - **Zero Trust Application**
   - **Zero Trust Application Group**
   - **Zero Trust Application Policy**
3. Click **Apply**.

See the Connection and Security-Related Connection Events in the Secure Firewall Management Center Administration Guide for more information on the connection events.

Zero Trust Dashboard

The Zero Trust dashboard allows you to monitor real-time data from active zero trust sessions on the devices.

The Zero Trust dashboard provides a summary of the top zero trust applications and zero trust users that are managed by the management center. Choose **Overview** > **Dashboards heading** > **Dashboard**, and click the **Zero Trust** tab to access the dashboard.

The dashboard has the following widgets:

- Top Zero Trust Applications
- Top Zero Trust Users

CLI Commands

Log in to the device CLI and use the following commands:

CLI Command	Description
show running-config zero-trust	To view the running configuration for a zero trust configuration.
show zero-trust	To display the run-time zero trust statistics and session information.
show cluster zero-trust	To display the summary of zero trust statistics across nodes in a cluster.
clear zero-trust	To clear zero trust sessions and statistics.
show counters protocol zero_trust	To view the counters that are hit for zero trust flow.

Diagnostics Tool

The diagnostics tool facilitates the troubleshooting process by detecting possible issues with zero trust configurations. The diagnostics can be classified into two types:

- **Application-specific diagnostics** are used to detect issues such as:
  - DNS-related issues
  - Misconfigurations such as socket not open, and issues with classification and NAT rules.
  - Issues with deployment of zero trust policy or SSL rules
  - Issues with source NAT issues and exhaustion of PAT pool
- **General diagnostics** are used to detect issues such as:
  - Strong cipher license not enabled
  - Invalid application certificate
  - SAML-related issues
  - Home agent and cluster bulk sync issues

To run the diagnostic tool:

1. Click Diagnostics ( ) next to the zero trust application that you want to troubleshoot. The **Diagnostics** dialog box appears.
2. Choose the device from the **Select Device** drop-down list and click **Run**. A report is generated in the **Reports** tab after the diagnostic process is complete.
3. To view, copy, or download the logs, click the **Logs** tab.

History for zero trust network access

This reference provides the minimum Firewall Management Center and Threat Defense versions needed to support zero trust application policies and monitoring.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Zero trust access enhancements.	7.4.1	7.4.1 with Snort 3	Firewall Management Center now includes the following zero trust access enhancements: • You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. • You can troubleshoot the zero trust configuration issues using the diagnostics tool. New/modified screens: **Policies** > **Access Control** > **Zero Trust Application** New/modified CLI commands: **show running-config zero-trust**, **show zero-trust statistics**

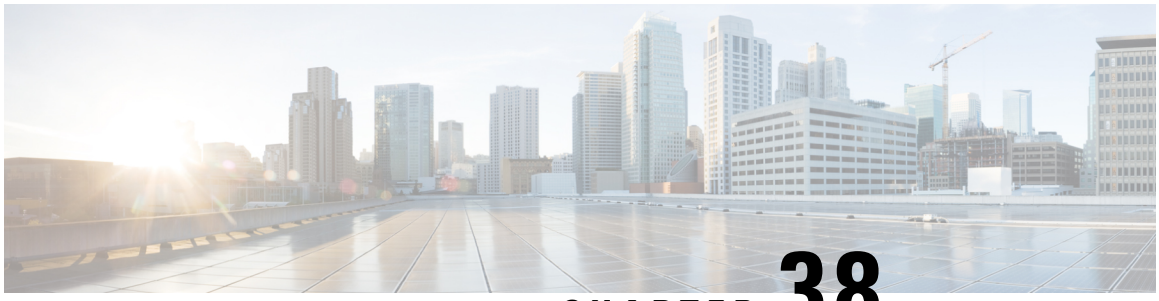
Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Clientless zero-trust access.	7.4.0	7.4.0 with Snort 3	Zero Trust Access allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics**



PART VIII

Access Control Policy Basics

- Access Control Policies, on page 1569
- Security Intelligence, on page 1595
- Access Control Rules, on page 1609
- URL Filtering Rules, on page 1651
- Content Restriction, on page 1681
- Intrusion Prevention Overview, on page 1687



CHAPTER 38

Access Control Policies

These topics describe how to work with access control policies:

- Access control policies, on page 1569
- Requirements and prerequisites for access control policies, on page 1574
- Manage access control policies, on page 1575
- History for access control policies, on page 1591

Access control policies

An access control policy is a hierarchical policy that allows you to specify, inspect, and log network traffic. You can use the characteristics of each connection to allow, trust, block, or monitor the connection.

Each managed device can be assigned to one access control policy. The data that the policy's assigned (also known as targeted) devices collect about your network traffic can be used to filter and control that traffic based on:

- simple, easily determined transport and network layer characteristics: source and destination, port, protocol, and so on
- the latest contextual information on the traffic, including characteristics such as reputation, risk, business relevance, application used, or URL visited
- realm, user, user group, or ISE attribute
- custom Security Group Tag (SGT)
- characteristics of encrypted traffic; you can also decrypt this traffic for further analysis
- whether unencrypted or decrypted traffic contains a prohibited file, detected malware, or intrusion attempt
- time and day (on supported devices)

Each type of traffic inspection and control occurs where it makes the most sense for maximum flexibility and performance. For example, reputation-based blocking uses simple source and destination data, so it can block prohibited traffic early in the process. In contrast, detecting and blocking intrusions and exploits is a last-line of defense.

Access control policy components

This list describes the main components of an access control policy.

- Name and description: Each access control policy must have a unique name. A description is optional.
- Inheritance settings: Policy inheritance allows you to create a hierarchy of access control policies. A parent (or base) policy defines and enforces default settings for its descendants. A policy's inheritance settings allow you to select its base policy. You can also lock settings in the current policy to force any descendants to inherit them. Descendant policies can override unlocked settings.
- Policy assignment: Every access control policy identifies which devices use it. Each device can use only one access control policy.
- Rules: Access control rules provide a granular method of handling network traffic. Rules are numbered, starting at 1, including rules inherited from ancestor policies. The system matches traffic to rules from the top down, ascending by rule number.

  Traffic is handled by the first rule for which all conditions match. Conditions can be simple or complex, and often depend on licensing.
- Default action: The default action determines how the system handles and logs traffic that is not handled by any other access control configuration. It can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data. Although an access control policy can inherit its default action from an ancestor policy, you cannot enforce this inheritance.
- Security Intelligence: This feature acts as the first line of defense against malicious internet content. It enables blocking of connections based on IP address, URL, and domain name reputation intelligence. To ensure continual access to vital resources, you can override block list entries with custom do not block list entries.
- HTTP responses: When a user's website request is blocked, you can display either a generic response page or a custom page. Alternatively, you can warn users but allow them to proceed to the requested site.
- Logging: Logging settings enable configuration of default syslog destinations for the policy. These settings apply to the policy and all included decryption, prefilter, and intrusion policies unless overridden in individual rules or policies.
- Advanced access control options: Advanced policy settings typically require little modification, and defaults are often suitable. Modifiable options include traffic preprocessing, decryption, identity, and various performance configurations.

Access control policy default actions

The default action is the access control policy configuration that determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data.

In a simple access control policy, the default action specifies how a device handles all traffic. In a more complex policy, the default action handles traffic that:

- is not fast pathed by the prefilter policy
- is not on a Security Intelligence block list

- is not blocked by the decryption policy (encrypted traffic only)
- matches none of the rules in the policy (except monitor rules, which match and log—but do not handle or inspect—traffic)

Note You cannot perform file or malware inspection on traffic handled by the default action. Logging of connections handled by the default action is initially disabled but can be enabled.

If you are using policy inheritance, the default action for the lowest-level descendant determines how traffic is handled. An access control policy can inherit its default action from the base policy, but this inheritance is not enforced.

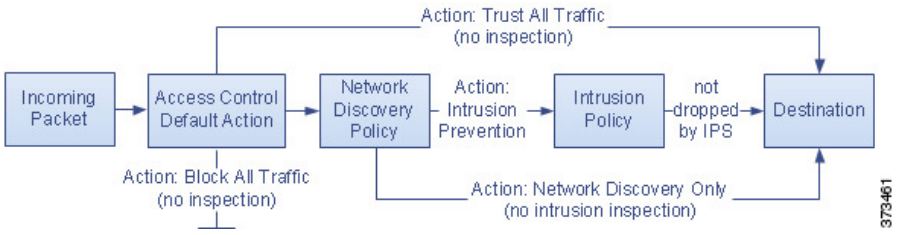
This table describes the types of inspection you can perform on traffic handled by each default action.

Table 91: Types of default actions and inspection options

Default action	Effect on traffic	Inspection type and policy
Access Control: Block All Traffic	Block without further inspection.	None.
Access Control: Trust All Traffic	Trust (allow to its final destination without further inspection).	None.
Intrusion Prevention	Allow, as long as it is passed by the intrusion policy you specify.	Intrusion, using the specified intrusion policy and associated variable set. Discovery, using the network discovery policy.
Network Discovery Only	Allow.	Discovery only, using the network discovery policy.
Inherit from base policy	Defined in base policy.	Defined in base policy.

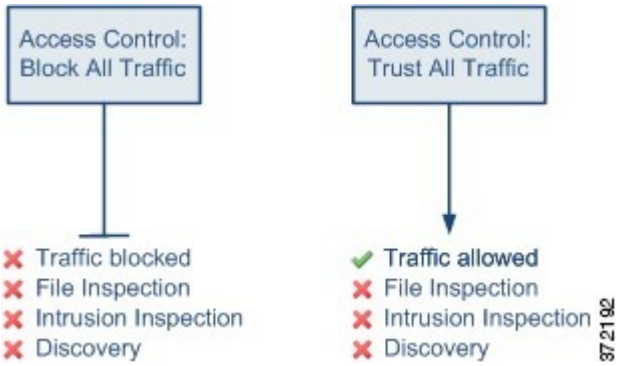
This diagram illustrates the table.

Figure 406: Default action configuration options



This diagram illustrates the **Block All Traffic** and **Trust All Traffic** default actions.

Figure 407: Block all traffic and trust all traffic default actions



This diagram illustrates the **Intrusion Prevention** and **Network Discovery Only** default actions.

Figure 408: Intrusion prevention and network discovery only default actions



Note The purpose of **Network Discovery Only** is to improve performance in a discovery-only deployment. Different configurations can disable discovery if you are only interested in intrusion detection and prevention.

Access control policy inheritance

Access control policy inheritance is a hierarchical policy-based implementation that allows child policies to inherit rules and settings from ancestor or base policies. This structure ensures that mandatory rules defined in parent policies are consistently enforced, while providing the flexibility for child policies to selectively override default configurations.

Access control policy hierarchy structure

You can nest access control policies, where each policy inherits the rules and settings from an ancestor policy. You can enforce this inheritance, or allow lower-level policies to override their ancestors.

Just as you create a domain hierarchy, you can create a corresponding hierarchy of access control policies. A descendant, or child, access control policy inherits rules and settings from its direct parent, or base, policy. That base policy may have its own parent policy from which it inherits rules and settings, and so on.

An access control policy's rules are nested between its parent policy's Mandatory and Default rule sections. This implementation enforces Mandatory rules from ancestor policies, but allows the current policy to write rules that preempt Default rules from ancestor policies.

You can lock these settings to enforce them in all descendant policies:

- Security Intelligence—Connections that are allowed or blocked based on the latest reputation intelligence for IP addresses, URLs, and domain names.
- HTTP response pages—Displaying a custom or system-provided response page when you block a user's website request.
- Advanced settings—Specifying associated subpolicies, network analysis settings, performance settings, and other general options.

When using policy inheritance, the default action for the lowest-level descendant determines final traffic handling. Although an access control policy can inherit its default action from an ancestor policy, you cannot enforce this inheritance.

Policy inheritance and multitenancy

Access control's hierarchical policy-based implementation complements multitenancy.

In a typical multidomain deployment, access control policy hierarchy corresponds to domain structure, and you apply the lowest-level access control policy to managed devices. This implementation allows selective access control enforcement at a higher domain level, while lower-level domain administrators can tailor deployment-specific settings. (You must use roles, not policy inheritance and enforcement alone, to restrict administrators in descendant domains.)

For example, as a Global domain administrator for your organization, you can create an access control policy at the Global level. You can then require that all your devices, which are divided into subdomain by function, use that Global-level policy as a base policy.

When subdomain administrators log into the Secure Firewall Management Center to configure access control, they can deploy the Global-level policy as-is. Or, they can create and deploy a descendant access control policy within the boundaries of the Global-level policy.

Note Although the most useful implementation of access control inheritance and enforcement complements multitenancy, you can create a hierarchy of access control policies within a single domain. You can also assign and deploy access control policies at any level.

Rule and other policy warnings

Policy and rule editors use icons to mark configurations that could adversely affect traffic analysis and flow. Depending on the issue, the system may warn you when you deploy or prevent you from deploying entirely.

Note Move your pointer over an icon to read the warning, error, or informational text.

Table 92: Policy error icons

Icon	Description	Example
Errors ( )	If a rule or configuration has an error, you cannot deploy until you correct the issue, even if you disable any affected rules.	A rule that performs category and reputation-based URL filtering is valid until you assign a device that does not have a URL Filtering license. At that point, an error icon appears next to the rule, and you cannot deploy until you edit or delete the rule, unassign the device, or enable the license.
Warning ( )	You can deploy a policy that displays rule or other warnings. However, misconfigurations marked with warnings have no effect. If you disable a rule with a warning, the warning icon disappears. It reappears if you enable the rule without correcting the underlying issue.	Preempted rules or rules that cannot match traffic due to misconfiguration have no effect. This includes conditions using empty object groups, application filters that match no applications, excluded LDAP users, invalid ports, and so on. However, if a warning icon marks a licensing error or model mismatch, you cannot deploy until you correct the issue.
Information ( )	Information icons convey helpful information about configurations that may affect the flow of traffic. These issues do not prevent you from deploying.	The system might skip matching the first few packets of a connection against some rules, until the system identifies the application or web traffic in that connection. This allows connections to be established so that applications and HTTP requests can be identified.
Rule Conflict ( )	When you enable rule conflict analysis, this icon appears in the rule table for rules that have conflicts.	Conflicts include redundant rules, redundant objects, and shadowed rules. Redundant and shadowed rules do not match traffic because previous rules would already match the criteria. Redundant objects make your rules unnecessarily complex.

Requirements and prerequisites for access control policies

Ensure that your environment meets these requirements before configuring access control policies.

- You must have **Administrator**, **Network Admin**, or **Access Admin** privileges to configure access control policies.
- Custom roles: You can define custom user roles to differentiate between the intrusion configuration in access control policy and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. The existing pre-defined user roles that included the Modify Access Control Policy permission support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions.
  - **Policies** > **Access Control heading** > **Access Control** and choose the **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** allows the selection of intrusion

policy, variable set, and file policy in a rule, the configuration of the advanced options for network analysis and intrusion policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. If a user has this option only, the user can modify no other part of the policy or rule.

- **Modify Remaining Access Control Policy Configuration** controls the ability to edit all other aspects of the policy.

Manage access control policies

Configure and manage access control policies by editing system-provided policies and creating custom access control policies.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

At the top of the page, there are convenient links to some related features: Object management, Intrusion policies, Network Analysis policies, DNS policies, and policy Import/Export.

Step 2 These actions help you to manage your policy:

- Create—Click **New Policy**; see Creating a basic access control policy, on page 1575.
- Edit—Click **Edit** ( ); see Editing an access control policy, on page 1576
- Delete—Click **Delete** ( ). You must remove any device assignments before deleting a policy.
- Copy—Click **Copy** ( ). Device assignments are not retained in the copy.
- Lock or unlock a policy—See Lock an access control policy, on page 1578.

Step 3 These options help you to analyze, monitor, and customize your policies:

- Inheritance—Click **Plus** next to a policy with descendants to expand your view of the policy's hierarchy.
- Report—Click **Report** ( ).. The report is generated as a background process. Go to the message/notifications center and look in the tasks list. When the report is finished, you can download it from the notification.

Creating a basic access control policy

When you create a new access control policy, it contains default actions and settings. After creating the policy, you are immediately placed in an edit session so that you can adjust the policy to suit your requirements.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **New Policy**.

Step 3 Enter a unique **Name** and, optionally, a **Description**.

Step 4 Optionally, choose a base policy.

If an access control policy is enforced on your domain, this step is not optional. You must choose the enforced policy or one of its descendants as the base policy.

If you select a base policy, the base policy defines the default action and you cannot select a new one in this dialog box. Logging for connections handled by the default action depends on the base policy.

Step 5 When you do not select a base policy, specify the initial **Default Action**:

- **Block all traffic** creates a policy with the **Access Control: Block All Traffic** default action.
- **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action, associated with the default intrusion variable set.
- **Network Discovery** creates a policy with the **Network Discovery Only** default action.

When you select a default action, logging of connections handled by the default action is initially disabled. You can enable it later when you edit the policy.

Note If you want to trust all traffic by default, or if you chose a base policy and do not want to inherit the default action, you can change the default action later.

Step 6 Optionally, choose the devices to assign to the policy. To narrow the devices that appear, enter a search string.

If you want to deploy this policy immediately, you must perform this step.

Step 7 Click **Save**.

The new policy opens for edit. You can add rules to it and make other changes as needed. See Editing an access control policy, on page 1576.

Editing an access control policy

When you edit an access control policy, you should lock it to ensure that your changes do not get overridden by another person who might edit it simultaneously.

You can only edit access control policies that were created in the current domain. Also, you cannot edit settings that are locked by an ancestor access control policy.

To protect the privacy of your session, a warning appears after 30 minutes of inactivity on the policy editor. After 60 minutes, the system discards your changes.

Note If you do not lock the policy, consider the following: Only one person should edit a policy at a time, using a single browser window. Although more than one user can edit an access control policy at a time, when one user saves changes, all changes made by the other users are immediately deleted and these users are moved out of edit mode and back to the access control policy listing page. These other users must start again.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control** .

Step 2 Click **Edit** ( ) next to the access control policy you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Edit your access control policy.

Note You can operate on multiple rules at one time by selecting their checkboxes in the left column, then selecting the action you want to perform from the **Select Bulk Rule Actions** drop-down list next to the search box. Bulk editing is available for enabling and disabling, copying, moving, deleting, and editing rules, or viewing hit counts or related events.

You can change the following settings or perform these actions:

- Name and description—Click **Edit** ( ) next to the name, make your changes, and click **Save** .
- Default action and settings—Choose a value from the **Default Action** drop-down list, then click **Cog** ( ) , make your changes to the settings, and click **OK** . For detailed information, see Configure the access control default action, on page 1579 .
- Associated policies—To edit or change policies in the packet flow, click the policy type in the packet flow representation below the policy name. You can select the **Prefilter Rules** , **Decryption** , **Security Intelligence** , and **Identity** policies. When necessary, click **Access Control** to return to the access control rules.
- Policy assignment—To identify the managed devices targeted by this policy, or enforce this policy in a subdomain, click the **Targeted: x devices** link.
- Rules—To manage access control rules, and to inspect and block malicious traffic using intrusion and file policies, click **Add Rule** , or right-click an existing rule and select **Edit** or another appropriate action. The actions are also available from the **More** ( ) button for each rule. See Create and edit access control rules, on page 1631 .
- Layout—Use the **Grid/Table View** icon above the list of rules to change the layout. Grid view provides color-coded objects in an easy-to-see layout. Table view provides a summary list so that you can see more rules at once. You can freely switch views without impacting the rules.

- Columns (table view only)—Click the **Show/Hide Columns** icon above the list of rules to select which information to show in the table. Click **Show/Hide Empty Columns** to quickly add, or remove, all columns that have no information, that is, you are not using those conditions in any rule. Click **Revert to Default** to undo all of your customizations.
- Analyze rule logic—You can select the following options from the **Analyze** menu to examine the logic of your rules:
  - **Manage Rule Hit Counts** —To view statistics on how many connections matched each rule. See View rule hit counts, on page 1586 .
  - **Enable/Disable Rule Conflicts** —Select whether you want to see information on whether rules interfere with each other. You can then view the results using the following commands. See Analyzing rule conflicts and warnings, on page 1588
    - **Show Warnings and Errors** —See whether there are rules with configuration issues that you need to address.
    - **Show Policy Warnings** —See whether there are configuration issues with the policy.
    - **Show Rule Conflicts** —See whether you have redundant or shadowed rules. These conflicts could prevent certain rules from ever being matched by connections, meaning either that you need to fix the match criteria, move the rule, or simply delete the rule.

Step 4 To change additional settings for the policy, select one of these options from the **More** drop-down arrow at the end of the packet flow line.

- **Advanced Settings** —To set preprocessing, decryption, identity, performance, and other advanced options. See Configure advanced settings for the access control policy, on page 2170 .
- **HTTP Responses** —To specify what the user sees in a browser when the system blocks a website request. See Choose HTTP response pages, on page 1671 .
- **Inheritance Settings** —To change the base access control policy for this policy, and to enforce this policy's settings in its descendant policies. See Choose a base access control policy, on page 1581 and Lock settings in descendant access control policies, on page 1581 .
- **Logging** —To set the default logging options for the policy.

Step 5 Click **Save** .

Lock an access control policy

Lock an access control policy to prevent other administrators from editing it, ensuring that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes.

Without locking, if multiple administrators edit the policy simultaneously, the first person who saves changes wins, and all other users have their changes erased.

The lock is for the access control policy itself. The lock does not apply to objects used in the policy. For example, another user can edit a network object that is used in a locked access control policy. Your lock remains in place until you explicitly unlock the policy, so you can log out and come back to your edits later.

When locked, other administrators have read-only access to the policy. However, other administrators can assign a locked policy to a managed device.

Before you begin

Any user role that has permission to modify the access control policy has permission to lock it, and to unlock a policy that was locked by another user.

However, the ability to unlock a policy that was locked by another administrator is controlled by the following permission: **Policies** > **Access Control heading** > **Access Control** and choose the **Access Control Policy** > **Modify Access Control Policy** > **Override Access Control Policy Lock**.

If you are using custom roles, your organization might have limited your unlocking abilities by not assigning this permission. Without this permission, only the administrator who locks a policy can unlock it.

Procedure

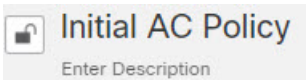
Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** ( ) next to the access control policy you want to lock or unlock.

In the access control policy list:

- The **Lock Status** column shows whether a policy is already locked, and if so, who locked it. An empty cell indicates that the policy is not locked.
- If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. Or, it is locked by another user.

Step 3 Click the lock icon next to the policy name to lock or unlock the policy.



If the policy inherits settings from a parent policy, you must choose one of these options when you click the lock icon.

- **Lock/Unlock this policy**—The locking or unlocking is for this policy only.
- **Lock/Unlock all policies in hierarchy**—This policy and all parent policies are locked or unlocked. If a parent policy is already locked by another administrator, you will see a message and you will not be able to lock that parent policy. When unlocking policies, if you have the Override Access Control Policy Lock permission, all parent policies are unlocked even if they were locked by other users.

Configure the access control default action

Configure the default action for an access control policy when connections do not match specific access control rules.

The default action for an access control policy is applied to any connection that:

- is not fast pathed by the prefilter policy

- is not on a Security Intelligence block list
- is not blocked by the decryption policy (encrypted traffic only)
- matches none of the rules in the policy (except monitor rules, which match and log—but do not handle or inspect—traffic)

Procedure

Step 1 Edit the access control policy whose inheritance settings you want to change; see Editing an access control policy, on page 1576.

Step 2 Select the **Default Action** at the bottom of the rules list.

For detailed information on what each option does, see Access control policy default actions, on page 1570.

Step 3 Click **Cog** () to configure the default action settings.

You can configure the following options. Click **OK** when finished.

- Logging options—Whether to log the connection. You can **Log at beginning of connection**, **Log at end of connection**, or both. If you select block as the default action, you can log at the beginning of the connection only.
- **Send connection events to**—If you select one of the logging options, select whether to send events to any combination of the following:
  - **Firewall Management Center**—Send events to the manager.
  - **Syslog server**—Send events to the default syslog server configured for the policy. You can configure overrides to specify a different severity level or syslog server destination.
- **SNMP trap**—If you enable logging, you can send SNMP traps to an SNMP server. Select an SNMP configuration, or click + to configure a new one.
- **Default action variable set**—If you selected one of the intrusion prevention default actions, select the variable set that should be used with the intrusion policy you selected.

Step 4 Click **Save**.

Manage access control policy inheritance

Inheritance relates to using another policy as a base policy for an access control policy. This allows you to use one policy to define some baseline characteristics that can be applied to multiple policies. To understand how inheritance works, refer to Access control policy inheritance, on page 1572.

Procedure

Step 1 Edit the access control policy whose inheritance settings you want to change; see Editing an access control policy, on page 1576.

Step 2 Manage policy inheritance:

- Change base policy — To change the base access control policy for this policy, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line and proceed as described in Choose a base access control policy, on page 1581.
- Lock settings in descendants — To enforce this policy's settings in its descendant policies, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line and proceed as described in Lock settings in descendant access control policies, on page 1581.
- Inherit settings from base policy — To inherit settings from a base access control policy, proceed as directed in Inherit access control policy settings from the base policy, on page 1582.
- Required in domains — To enforce this policy in a subdomain, click the **Targeted: x devices** link and proceed as described in Enforce an access control policy in a domain, on page 1583.

Choose a base access control policy

Choose a base access control policy to establish policy inheritance, allowing a child policy to inherit rules and settings from its parent while maintaining the ability to modify unlocked configurations.

When you change the base policy for the current access control policy, the system updates the current policy with any locked settings from the new base policy.

Procedure

Step 1 In the access control policy editor, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 2 Choose a policy from the **Select Base Policy** drop-down list.

To remove inheritance, select **None**.

Step 3 Click **OK**.

Step 4 Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Lock settings in descendant access control policies

Lock a setting in an access control policy to enforce the setting in all descendant policies.

Descendant policies can override unlocked settings. When you lock settings, the system saves overrides already made in descendant polices so that the overrides can be restored if you unlock settings again.

Procedure

Step 1 In the access control policy editor, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 2 In the Child Policy Inheritance Settings area, check the settings you want to lock.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration.

Step 3 Click **OK** to save the inheritance settings.

Step 4 Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Inherit access control policy settings from the base policy

Configure a child access control policy to inherit settings from a base policy or override them with custom configurations.

Child access control policies inherit many settings from their base policy by default. If these settings are unlocked in the base policy, you can override them.

If you later reinherit the settings from the base policy, the Firewall Management Center displays the base policy's settings and dims the controls. However, it saves the overrides you made and restores them if you disable inheritance again.

Procedure

Step 1 In the access control policy editor, click **Security Intelligence**, or select **HTTP Responses**, **Logging**, **Encrypted Visibility Engine**, or **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line

Step 2 Check the **Inherit from (*base policy*)** check box for each setting you want to inherit.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration.

Step 3 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Enforce an access control policy in a domain

Require that every device in a domain use the same base access control policy or one of its descendant policies.

This procedure is relevant in a multi-domain deployment only.

Procedure

Step 1 In the access control policy editor, click the **Targeted: x devices** link.

Step 2 Click **Required on Domains**.

Step 3 Build your domain list:

- Add — Select the domains where you want to enforce the current access control policy, then click **Add** or drag and drop into the list of selected domains.
- Delete — Click **Delete** ( ) next to a leaf domain, or right-click an ancestor domain and choose **Delete Selected**.
- Search — Type a search string in the search field. Click **Clear** ( ) to clear the search.

Step 4 Click **OK** to save the domain enforcement settings.

Step 5 Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Assign access control policy to devices

An access control policy specifies the devices that use it. Each device can be assigned to only one access control policy.

Procedure

Step 1 In the access control policy editor, click the **Targeted: x devices** link.

Step 2 Build your target list:

- Add — Select one or more **Available Devices**, then click **Add to Policy** or drag and drop into the list of **Selected Devices**.
- Delete — Click **Delete** ( ) next to a single device, or select multiple devices, right-click, then choose **Delete Selection**.
- Search — Type a search string in the search field. Click **Clear** ( ) to clear the search.

Under **Impacted Devices**, the system lists the devices whose assigned access control policies are children of the current policy. Any change to the current policy affects these devices.

Step 3 Click **OK** to save your assigned device settings.

Step 4 Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Logging settings for access control policies

Logging settings for access control policies are configuration option that allow you to configure default syslog destinations for the current access control policy. The settings are applicable to the access control policy and all the included decryption, prefilter, and intrusion policies unless the syslog destination settings are explicitly overridden with custom settings in included rules and policies.

To configure logging settings for an access control policy, select **Logging** from the **More** drop-down arrow at the end of the packet flow line.

You can configure default syslog destinations and syslog alert for the access control policy. The settings are applicable to the access control policy and all the included decryption, prefilter, and intrusion policies unless the syslog destination settings are explicitly overridden with custom settings in included rules and policies.

Logging for connections handled by the default action is initially disabled.

Intrusion settings and file and malware settings are effective only after you have selected an option at the top of the page for sending syslog messages generally.

Default syslog settings

Default syslog settings provide two destination options:

- **Send using specific syslog alert**: Events are sent based on the selected syslog alert as configured using the instructions in *Creating a Syslog alert Response* in the *Cisco Secure Firewall Management Center Administration Guide*. You can select the syslog alert from the list or add one by specifying the name, logging host, port, facility, and severity.

  When using this option, the system sends syslog messages to the server using the Management interface. Ensure there is a route from the Management interface to the syslog server, or messages will not arrive at the server.

- **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device**: Connection or intrusion events are sent with the selected severity to syslog collectors configured in Platform Settings. Using this option, you can unify the syslog configuration by configuring it in platform settings and reusing the settings in access control policy. Severity selected in this section is applied to all connection and intrusion events. The default severity is alert.

Intrusion settings

Intrusion settings include these options:

- **Send syslog messages for intrusion events**: Send intrusion events as syslog messages. The defaults set above are used unless you override them.

- **Show overrides** or **Hide overrides**: If you want to use the default syslog destination and severity, leave these options empty. Otherwise, you can set a different syslog server destination for intrusion events, and change the severity of the events.

File and malware settings

File and malware settings include these options:

- **Send syslog messages for file and malware events**: Send file and malware events as syslog messages. The defaults set above are used unless you override them.
- **Show overrides** or **Hide overrides**: If you want to use the default syslog destination and severity, leave these options empty. Otherwise, you can set a different syslog server destination for file and malware events, and change the severity of the events.

AI defense settings

Associate prefilter, decryption, and identity policies with an access control

Associate subpolicies with an access control policy to create a comprehensive security framework that handles different aspects of network traffic processing.

The easiest way to associate subpolicies to an access control policy is by clicking the policy's link in the packet flow shown at the top of an access control policy. Alternatively, you can use the policy's advanced settings to associate the subpolicy, as described in this topic. The subpolicies that you can associate with access control policy are:

- Prefilter policy—Performs early traffic handling using limited network (layer 4) outer-header criteria.
- Decryption policy—Monitors, decrypts, blocks, or allows application layer protocol traffic encrypted with Secure Socket Layer (SSL) or Transport Layer Security (TLS).
- Identity policy—Performs user identification based on the realm and authentication method associated with the traffic.

Before you begin

Before associating a decryption policy with an access control policy, review the information about TLS server identity discovery in TLS server identity discovery, on page 2173.

Procedure

Step 1 In the access control policy editor, select **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 2 Locate the policy settings area for prefilter, decryption, or identity policies.

Step 3 Click **Edit** ( ) in the corresponding policy settings area.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 4 Choose a policy from the drop-down list.

If you choose a user-created policy, you can click the edit icon that appears to edit the policy.

Step 5 Click **OK**.

Step 6 Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

View rule hit counts

Hit count indicates the number of times a policy rule or default action has been matched to a connection. The hit count is incremented only for the first packet of a connection that matches a rule. You can use this information to identify the efficacy of your rules. Hit count information is available only for access control and prefilter rules applied to Firewall Threat Defense devices.

Note

- The count persists through reboots and upgrades.
- Counts are maintained by each unit in an HA pair or cluster separately.
- You will not be able to derive the hit count information from a device when deployment or a task is in progress on the device.
- You can also see rule hit count information in the device CLI using the **show rule hits** command.
- If you have accessed the Hit Count page from the Access Control Policy page, you will not be able to view or edit prefilter rules and vice-versa.
- Hit counts are not available for rules that use the Monitor action.

Before you begin

If you use custom user roles, ensure that the roles include these privileges:

- View Device, to see the hit counts.
- Modify Device, to refresh the hit counts.

Follow these steps to view rule hit counts:

Procedure

Step 1 In the access control policy or prefilter policy editor, click **Analyze** > **Rule Hit Counts** on the top-right of the page.

Step 2 On the Hit Count page, select the device from the **Select a device** drop-down list.

If it is not the first time that you are generating hit counts for this device, the last fetched hit count information appears next to the drop-down box. Also, verify the **Last Deployed** time to confirm recent policy changes.

Step 3 If necessary, click **Refresh** ( ) to obtain current hit count data from the selected device.

In the prefilter policy, you might need to click **Fetch Current Hit Count** to get initial hit count data.

You cannot refresh the hit count while deployment to the device is in progress.

Step 4 View and analyze the data.

You can do these actions:

- Click **Prefilter** or **Access Control** to switch between the hit counts for these policies.
- Search for a specific rule by entering a search string in the **Filter** box.
- Broadly limit the list to **Hit Rules** or **Never Hit Rules** by selecting these options in the **Filter by** field. When viewing hit rules, you can further limit the list by selecting a time range in the **In Last** field (for example, in the last 1 day).
- (When viewed from the access control policy.) Clear the hit counts for one or more rule by selecting the checkbox for the rule, then clicking **Clear Hit Counts**. When confirming the action, choose **Clear and Reload** to refresh the hit count data. You can clear hit counts for up to 500 rules at a time. You cannot undo clearing hit counts.

Note Click the checkbox in the table header to select all rules visible in the list. To select a range of rules, select the first rule's checkbox, then **`Shift+click`** the last rule's checkbox; all rules in between are also selected.

- (When viewed from the access control policy.) You can do these actions with individual rules:
  - Edit the rule by clicking **Edit** from the **More** ( ) menu.
  - Delete the rule from the policy by clicking **Delete** from the **More** ( ) menu.
  - Enable or disable the rule by clicking **Enable Rule** or **Disable Rule** from the **More** ( ) menu.
  - Clear the hit count (reset it to zero) for the rule by clicking **Clear Hit Count** from the **More** ( ) menu. You cannot undo this action.
- (When viewed from the access control policy.) You can do these actions with individual rules:
  - Edit the rule by clicking **Edit** ( ).
  - Delete the rule from the policy by clicking **Delete** ( ).
  - Enable or disable the rule by clicking the **Slider** ( ).
  - Clear the hit count (reset it to zero) for the rule by clicking the **X** for the rule. You cannot undo this action.
- Change the displayed columns by clicking and selecting the columns to show. When viewed from the prefilter policy, use the **Cog** ( ) to select the columns to display.

- (When viewed from the prefilter policy.) Click on a rule name to edit it, or click **View** ( ) in the last column to view the rule details. Clicking on the rule name highlights it in the policy page where you can edit it.
- (When viewed from the prefilter policy.) Clear the hit count information (reset it to zero) for a rule by right-clicking the rule and selecting **Clear Hit Count**. You can select multiple rules by using Ctrl+click. You cannot undo this action.

Step 5 Optionally, you can generate a comma-separated values report of the details on the page by clicking **Generate CSV** on the bottom-left of the page.

Step 6 Click **Close** to return to the policy page.

Analyzing rule conflicts and warnings

View warnings and information about rule conflicts to examine the logic of your access control policy and to identify rules that need changes.

When rules overlap, you can end up with unnecessary rules in the policy, and these rules will never be matched to traffic. The analysis can help you delete unnecessary rules, or identify rules that should be moved or modified so they enforce the desired policy.

Policy warnings and errors point out things that you should understand and perhaps address to ensure that your rules provide the desired services.

Rule conflict analysis identifies these problems:

- Object overlap—An element in a field of a rule is a subset of one or more elements in the same field of the rule. For example, the source field might include a network object for 10.1.1.0/24, and another object for the host 10.1.1.1. Because 10.1.1.1 is within the network covered by 10.1.1.0/24, the object for 10.1.1.1 is redundant and can be deleted, simplifying the rule and saving device memory.
- Redundant rule—Two rules apply the same action to the same type of traffic and removing the base rule would not change the ultimate result. For example, if a rule permitting FTP traffic for a particular network were followed by a rule allowing IP traffic for that same network, and there were no rules in between denying access, then the first rule is redundant and you can delete it.
- Shadowed rule—This is the reverse of a redundant rule. In this case, one rule will match the same traffic as another rule such that the second rule will never be applied to any traffic because it comes later in the access list. If the action for both rules is the same, you can delete the shadowed rule. If the two rules specify different actions for traffic, you might need to move the shadowed rule or edit one of the two rules to implement your desired policy. For example, the base rule might deny IP traffic, and the shadowed rule might permit FTP traffic, for a given source or destination.

Before you begin

When doing the analysis:

- Only the first conflict for a given rule is identified. Once you fix the problem, the rule might be identified as having a conflict with another rule in the table. However, a rule might have multiple warnings or errors.

- Rule conflict analysis considers source/destination security zone, network, VLAN, and service/port match conditions and action only. It does not consider other match criteria, so an apparently redundant rule might not be completely redundant.
- FQDN network objects cannot be analyzed for conflict, because the IP address of an FQDN cannot be known prior to DNS lookup.
- Disabled rules are ignored.
- Time range attributes are ignored. Rules for different time periods might be marked as redundant when they are not actually redundant for the time ranges.
- Icons for warnings and errors, and rule conflicts when you enable the feature, are shown in the rules table. For a reference to the icons, see Rule and other policy warnings, on page 1573.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control** and edit an access control policy.

Step 2 Do one of these to open the rule conflicts and warnings dialog box:

- To view rule conflicts, click the **Analyze** drop-down and click **Enable Rule Conflicts**. When the analysis completes, you see a summary of the conflicts at the top of the page. Then, click **Show Rule Conflicts** from the same menu to see the specific results.

  You must re-enable rule conflict detection each time you open the policy or make a change and save the policy.
- To view rule warnings and errors, click **Analyze** > **Show Rule Warnings and Errors**.

  After you make a change to the policy, you can refresh the results by clicking the reload icon next to the **Analyze** button.
- To view policy warnings, click **Analyze** > **Show Policy Warnings**.
- If you are finished viewing rule conflicts, click **Analyze** > **Disable Rule Conflicts**.

Step 3 In the rule conflicts and warnings dialog box:

- Rule warnings and errors are shown on a separate tab from rule conflicts. There is also a separate tab for policy warnings.
- Each tab contains sub-tabs to let you examine individual types of problems, such as redundant vs. shadowed or warnings vs. errors. You can also search for an item.
- **More** (⋮) next to each rule name provides shortcuts to edit, disable, or delete the rule.

Step 4 Click **Close** when finished.

Search for rules

Use search to help you find rules, especially when you have a large number of them.

When you search for an IP address in the source or destination network (but not as a simple text search), the system returns rules that will match the address. This includes not only exact matches, but also subnet matches. For example, searching for 10.1.1.1 will include rules for 10.1.1.0/24.

Procedure

Step 1 When editing an access control policy, build the search string by clicking in the **Search** box.

- For a simple text string search, type the string. The search returns rules that have that string in any column. You cannot do a string search in conjunction with a tag search, such as combining a string search with a source networks search.
- To search on a specific column, start typing the name of the column until the system prompts you with the full name, such as Source Networks, or select the name from the list of searchable fields. When you select the search tag, you can then enter the search string for that tag. For example, **Source Networks 10.1.1.1**.
- Searches in the port field return exact match only.
- When entering mulitple values, separate the values with commas.
- When building a search string with multiple tags, do not include spaces between the tags.
- When you select a tag, you are prompted with values that appear in those columns. Select the values you want to search for.
- You can quickly filter based on some common features by clicking the filter icon to the left of the search box and selecting to show rules with any combination of the following: Allow, Block, Monitor, Intrusion Policy, Time Range, Conflicts, Warnings, Errors, Disabled rules.
- To see the rules that apply to a specific device or set of devices, click the filter icon and select the devices. Rules apply to a device if they use security zones that contain at least one interface on the device, or if they do not include security zones.

Step 2 With your cursor at the end of the search string in the search box, press Enter.

The rules that satisfy the search string are highlighted and non-matching rules are hidden. You can deselect **Show Only Matching Rules** to see the entire table, with the highlighted rules within the table. This lets you see the surrounding rules.

Beside the Show Only Matching Rules checkbox is a summary of the total number of rules in the policy compared to the number that match the search string.

Step 3 After your first search, clicking in the search box prompts you with recent searches and tags. You can quickly repeat a search by selecting it, or build similar searches by selecting previous searches or tags and building on them.

Step 4 To close the search and return to the unfiltered and unhighlighted table, click the **X** at the right of the search box. You can also put your cursor at the end of the search string and press the Esc key.

History for access control policies

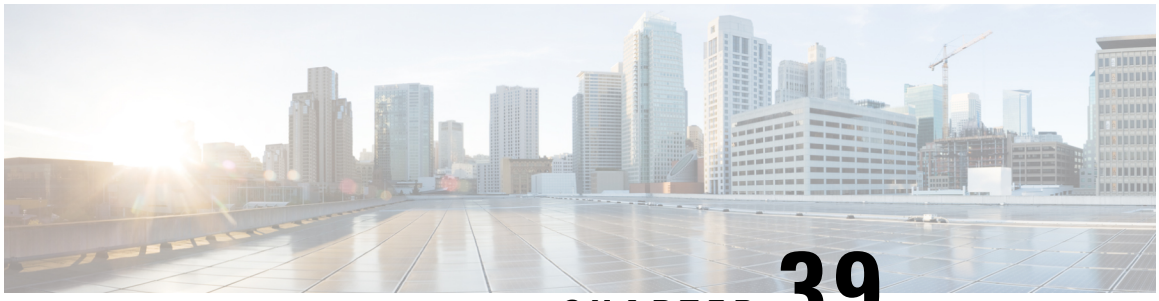
This history table provides a comprehensive history of feature changes for access control policies in Cisco Secure Firewall Management Center across releases.

Table 93: Access control policy feature history by release

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Granular permissions for modifying access control policies and rules.	7.4.0	Any	You can define custom user roles to differentiate between the intrusion configuration in access control policies and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. When defining user roles, you can select the **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** option to allow the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. You can use the **Modify Remaining Access Control Policy Configuration** to control the ability to edit all other aspects of the policy. The existing pre-defined user roles that included the Modify Access Control Policy permission continue to support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions.
New access control policy user interface and rule conflict analysis.	7.3.0	Any	The access control policy user interface introduced in 7.2 is now the default interface. You can also enable rule conflict analysis to help identify redundant rules and objects, and shadowed rules that cannot be matched due to previous rules in the policy.
Access control policy locking.	7.2.0	Any	You can lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes. Any user who has permission to modify the access control policy has permission to lock it. We added an icon to lock or unlock a policy next to the policy name while editing the policy. In addition, there is a new permission to allow users to unlock policies locked by other administrators: Override Access Control Policy Lock. This permission is enabled by default in the Administrator, Access Admin, and Network Admin roles.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Rule hit counts persist over reboot.	7.2.0	Any	Rebooting a managed device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the **show rule hits** command to see cumulative counters across the HA pair or cluster, or see the counts per node. We modified the device CLI command: **show rule hits**.
Usability improvements for the access control policy.	7.2.0	Any	There is a new user interface available for the access control policy. You can continue to use the legacy user interface, or you can try out the new user interface. The new interface has both a table and a grid view for the rules list, the ability to show or hide columns, enhanced search, infinite scroll, a clearer view of the packet flow related to policies associated with the access control policy, and a simplified add/edit dialog box for creating rules. You can freely switch back and forth between the legacy and new user interfaces while editing an access control policy.
DNS filtering	7.0.0 6.7.0 (experimental)	Any	If URL filtering is enabled and configured, a new option to enhance category and reputation filtering efficacy is enabled by default for each new access control policy. For more information, see DNS filtering, on page 1665 and subtopics. The Advanced tab of access control policy has a new option under General Settings: **Enable reputation enforcement on DNS traffic**.
TLS server identity discovery	6.7.0	Any	Enable access control policies to evaluate URL and application conditions when a client connects to a TLS 1.3-enabled server. TLS server identity discovery enables these conditions to be evaluated without decrypting traffic. Enabling this feature can impact device performance, depending on model. The Advanced tab page of access control policy has new options: • Warning is displayed on the Advanced tab; moving the slider to the right enables TLS server identity discovery. • New option on the Advanced tab page: **TLS Server Identity Discovery**.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New Security Intelligence categories	—	Any	These categories were introduced at about the time of the 6.6 release, but are not specific to 6.6: • banking_fraud • high_risk • ioc • link_sharing • malicious • newly_seen • spyware



CHAPTER 39

Security Intelligence

The following topics provide an overview of Security Intelligence, including use of lists for blocking and allowing traffic and basic configuration.

- Security intelligence, on page 1595
- License requirements for security intelligence, on page 1596
- Requirements and prerequisites for security intelligence, on page 1596
- Best practices for security intelligence, on page 1596
- Guidelines and limitations for security intelligence, on page 1597
- Security intelligence sources, on page 1598
- Configure security intelligence, on page 1599
- Security intelligence monitoring, on page 1606
- Override security intelligence blocking, on page 1606
- Troubleshooting security intelligence, on page 1607
- History for security intelligence block listing, on page 1608

Security intelligence

Security Intelligence is an early line of defense mechanism that

- uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names
- operates as the first phase of access control, before the system performs more resource-intensive evaluation, and
- improves performance by quickly excluding traffic that does not require inspection through Security Intelligence block listing.

Security intelligence features and limitations

Security Intelligence provides access to regularly updated intelligence feeds from Cisco. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations.

You can refine Security Intelligence Block listing with Do Not Block lists and monitor-only Block lists. These mechanisms exempt traffic from being blocked by a Block list, but do **not** automatically trust or fastpath

matching traffic. Traffic added to a Do Not Block list or monitored at the Security Intelligence stage is intentionally subject to further analysis with the rest of access control.

Note You cannot use a Block list to block fastpathed traffic. Prefilter evaluation occurs before Security Intelligence filtering. Fastpathed traffic bypasses all further evaluation, including Security Intelligence.

Related Topics

Security intelligence, on page 2418

License requirements for security intelligence

Threat Defense License

IPS

Classic License

Protection

Requirements and prerequisites for security intelligence

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Important You must apply the Network Discovery policy on the device for a successful application of the SI policy.

Best practices for security intelligence

Configure your access control policies to block threats detected by Cisco-provided Security Intelligence feeds. See Configuration example: Security intelligence blocking, on page 1605.

If you want to supplement the Cisco-provided Security Intelligence feeds with custom threat data, or manually block emerging threats:

- For IP addresses, use custom Security Intelligence lists and feeds, or Network objects. To create these, see Security intelligence, on page 2418 and Networks, on page 2386, and their subtopics. To use them for Security Intelligence, see Configure security intelligence, on page 1599. Network objects used in Security Intelligence policy require an IPS license.
- For URLs and domains, use custom Security Intelligence lists and feeds, *not* objects or groups. See details at Manual URL filtering options, on page 1668.
- You can also add entries to a Block list from events. See Global and domain security intelligence lists, on page 2420.

To test new feeds, or for passive deployments, set the action from block to monitor only. See Security intelligence monitoring, on page 1606.

If you need to exclude specific sites or addresses from Security Intelligence blocking, see Override security intelligence blocking, on page 1606.

If your Firepower deployment is integrated with Cisco XDR and you use custom Security Intelligence lists and feeds, be sure to update Security Services Exchange with these lists and feeds. For details, see instructions for configuring auto-promotion of events in the Security Services Exchange online help. For general information about this integration, see *Enable SecureX Integration* in the *Cisco Secure Firewall Management Center Administration Guide*.

System-provided Security Intelligence categories may change over time and without notification; you should plan to check periodically for changes, and modify your policies accordingly.

You should also configure URL filtering, a separate feature with separate licensing requirements, for further protection against malicious sites. See URL Filtering Rules, on page 1651.

To reduce latency and CPU overhead, avoid referencing a single, massive SI feed object across your entire security policy. Instead, utilize customized objects to create smaller, targeted subsets of your intelligence data.

Using URL/Domain feeds instead of IP blocklists can reduce CPU overhead because domain filtering is generally more efficient and less resource-intensive than managing massive IP blocklists.

Excluding trusted IPs by adding known good or essential partner IP addresses to an "Do Not Block" list in Security Intelligence (SI) feeds helps reduce CPU overhead as the firewall or security device bypasses unnecessary scanning and deeper inspection for these IPs.

Guidelines and limitations for security intelligence

Be aware of these limitations when configuring and using Security Intelligence:

- The Security Intelligence configuration that includes detection signatures or malware URLs might lead to false threat alerts when the Firewall Threat Defense troubleshoot files are scanned.
- If a TCP connection attempt is initiated from an IP address that is blocked due to its poor reputation, a TCP reset (RST) packet is sent. This causes the connection to be terminated instantly, preventing the establishment of the TCP session and signalling the rejection to the sender.

Security intelligence sources

Security Intelligence sources are data providers that

- supply regularly updated intelligence feeds for domains, URLs and IP addresses
- enable custom blocking and allow lists for specific sites or addresses, and
- provide global lists for immediate event-based blocking and allowing.

Types of security intelligence sources

Security Intelligence uses these source types:

- **System-provided feeds**: Cisco provides access to regularly updated intelligence feeds for domains, URLs and IP addresses. For more information, see Security intelligence, on page 2418.

  If you see a feed with "TID" in the name, this feed is *not* used by Security Intelligence. Instead, this feed is used by the feature described in Threat Intelligence Director, on page 2121.

- **Third-party feeds**: Optionally, supplement Cisco-provided feeds with third-party reputation feeds, which are dynamic lists that the Secure Firewall Management Center downloads from the internet on a regular basis. See Custom security intelligence feeds, on page 2428.

- **Custom Block lists or feeds (or objects)**: Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects.)

  For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy, as described in Custom Security Intelligence lists, on page 2430 and Configure security intelligence, on page 1599.

  For IP addresses, you can optionally use network objects rather than lists or feeds for this purpose; for information, see Networks, on page 2386. (For URLs, using lists and feeds is strongly recommended over other methods.)

- **Custom Do Not Block lists or feeds**: Override Security Intelligence blocking for specific sites or addresses. See Override security intelligence blocking, on page 1606.

- **Global Block lists (one each for Network, URL and DNS)**: While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Block List so that Security Intelligence will handle future traffic from that source. See Global and domain security intelligence lists, on page 2420.

- **Global Do Not Block lists (one each for Network, URL and DNS)**: While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Do Not Block List if you do not want Security Intelligence to block future traffic from that source. See Global and domain security intelligence lists, on page 2420.

Configure security intelligence

Configure Security Intelligence filtering to automatically block or monitor traffic based on threat intelligence feeds and custom block or allow lists. This provides an additional layer of security by filtering known malicious IP addresses, URLs, and domains before they reach your network resources.

Each access control policy has Security Intelligence options. You can add network objects, URL objects and lists, and Security Intelligence feeds and lists to a Block list or Do Not Block list, and constrain any of these by security zone. You can also associate a DNS policy with your access control policy, and add domain names to a Block or Do Not Block list.

The number of objects in the Do Not Block lists plus the number in the Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

Before you begin

- Tip: For guidance on minimum configuration recommendations, see also Configuration example: Security intelligence blocking, on page 1605.
- To ensure that ALL options are available to select, add at least one managed device to your management center.
- In passive deployments, or if you want to set Security Intelligence filtering to monitor-only, enable logging; see *Logging Connections with Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Configure a DNS policy to take Security Intelligence action for domains. For more information, see DNS Policies for Security Intelligence, on page 1993.

Follow these steps to configure Security Intelligence filtering in an access control policy:

Procedure

Step 1 In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 Choose the type of objects to configure.

- Click **Networks** to add network objects (IP addresses).

Note Network objects used in a Security Intelligence policy require a IPS license.

- Click **URLs** to add URL objects.

Step 3 Find the **Available Objects** you want to add to the Block or Do Not Block list.

- Search the available objects by typing in the **Search by name or value** field. Clear the search string by clicking **Reload** ( ) or **Clear** ( ).

- If no existing list or feed meets your needs, click **Add** (+), select **New Network List** or **New URL List**, and proceed as described in Create custom security intelligence feeds, on page 2428 or Upload new custom security intelligence lists to the Secure Firewall Management Center, on page 2431.
- If no existing object meets your needs, click **Add** (+), select **New Network Object** or **New URL Object**, and proceed as described in Create a network object, on page 2388.

Security Intelligence ignores IP address blocks using a `/0` netmask.

Step 4 Choose one or more **Available Objects** to add.

Step 5 (Optional) Choose an **Available Zone** to constrain the selected objects by zone.

You cannot constrain system-provided Security Intelligence lists by zone.

Note The **Any** zone for an SI list applies only to interfaces that are part of a security zone. However, an exception is that if a device does not have any interfaces associated with a security zone, then the **Any** zone will match any interface.

For example, if you have five interfaces on a device and none of them are associated with a security zone, any SI list that is assigned to the **Any** zone will be inspected against traffic on ALL interfaces on the device. If you add one interface to a security zone on that device, it effectively would remove SI inspection on the other four interfaces, where the zone is set to **Any** for an SI list. If you add the other four interfaces to a security zone, they will be evaluated by the SI list attached to the **Any** zone.

Step 6 Click **Add to Do Not Block list** or **Add to Block list**, or click and drag the selected objects to either list.

To remove an object from a Block or Do Not Block list, click **Delete** ( ) To remove multiple objects, choose the objects and right-click to **Delete Selected**.

Step 7 (Optional) Set objects on the Block list to monitor-only by right-clicking the object under **Block List**, then choosing **Monitor-only (do not block)**.

You cannot set system-provided global Security Intelligence lists to monitor only.

Step 8 Choose a DNS policy from the **DNS Policy** drop-down list.

Step 9 Click **Save**.

Security Intelligence filtering is now configured for your access control policy. The system will automatically block or monitor traffic based on the configured Block and Do Not Block lists, providing enhanced protection against known threats.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Related Topics

Security intelligence, on page 2418
Snort restart scenarios, on page 127

Security intelligence options

Use the Security Intelligence tab in the access control policy editor to configure network (IP address) and URL Security Intelligence, and to associate the access control policy with a DNS policy in which you have configured Security Intelligence for domains.

Available objects

Available objects include:

- Security Intelligence categories populated by the system-provided feed.

  For details, see Security intelligence categories, on page 1602.

- System-provided Global Block and Do Not Block lists.

  For descriptions, see Security intelligence sources, on page 1598.

- Security Intelligence lists and feeds that you create under Object > Object Management > Security Intelligence.

  For descriptions, see Security intelligence sources, on page 1598.

- Network and URL objects that are configured on the respective pages under Object > Object Management. These are different from the Security Intelligence objects in the previous bullet.

  For details about network objects, see Networks, on page 2386. (For URLs, use Security Intelligence lists or feeds rather than objects.)

  Note that range and group network object types are not supported in Security Intelligence policy.

Available zones

Except for the system-provided Global lists, you can constrain Security Intelligence filtering by zone.

For example, to improve performance, you might want to target enforcement to specific zones rather than all interfaces. As a more specific example, you can block spam only for a security zone that handles email traffic.

To enforce Security Intelligence filtering for an object on multiple zones, you must add the object to the Block or Do Not Block list separately for each zone.

Note that range and group network object types are not supported in Security Intelligence policy.

DNS policy

In order to match DNS traffic using Security Intelligence, you must select a DNS policy for your Security Intelligence configuration.

Using Block or Do Not Block lists, or monitoring traffic based on a DNS list or feed, also requires that you:

- Configure DNS Security Intelligence lists and feeds. See Security intelligence, on page 2418.
- Create a DNS policy. See Create basic DNS policies, on page 1997 for more information.
- Configure DNS rules that reference your DNS lists or feeds. See Create and edit DNS rules, on page 1999 for more information.
- Because you deploy the DNS policy as part of your access control policy, you must associate both policies. See Requirement: deploy DNS policy configuration changes, on page 2008 for more information.

Do not block list

See Override security intelligence blocking, on page 1606.

To select all objects in the list, right-click an object.

Block list

See Configuration example: Security intelligence blocking, on page 1605 and other topics in this chapter.

For explanations of the visual indicators in the Block list, see Block list icons, on page 1604.

To select all objects in the list, right-click an object.

Logging

Security Intelligence logging, enabled by default, logs all blocked and monitored connections handled by an access control policy's assigned devices. However, the system does not log Do Not Block list matches; logging of connections on the Do Not Block list depends on their eventual disposition. Logging must be enabled for connections on the Block list before you can set objects on that list to monitor-only.

To enable, disable, or view logging settings, right-click an object in the Block list.

Related Topics

Global and domain security intelligence lists, on page 2420
Security intelligence lists and multitenancy, on page 2421

Security intelligence categories

Security Intelligence categories are determined by the system-provided feeds described in Security intelligence, on page 2418.

These categories are used in the following locations:

- The Networks sub-tab on the Security Intelligence tab of an access control policy
- The URLs sub-tab beside the Networks tab on the Security Intelligence tab of an access control policy
- In a DNS policy on the DNS tab in the DNS rule configuration page
- In events generated when traffic matches Block or Monitor configurations in the above locations

Note If your organization is using Secure Firewall Threat Intelligence Director: When viewing events, you may see categories that indicate that the action was taken by TID, such as `TID URL Block`.

Categories are updated by Talos from the cloud, and this list may change independently of Firepower releases.

Table 94:

Security Intelligence Category	Description
Attackers	Active scanners and hosts known for outbound malicious activity

Security Intelligence Category	Description
Banking_fraud	Sites that engage in fraudulent activities that relate to electronic banking
Bogon	Bogon networks and unallocated IP addresses The Security Intelligence Bogon feed is designed to provide threat-specific intelligence. It is not intended to function as a comprehensive filtering list for all bogon traffic. Bogon traffic, including private, multicast, and unallocated address space is generally expected to be filtered by upstream network providers or through standard network security controls. Key aspects of Bogon: • **Active threat indicators**: The feed is populated only when the security intelligence identifies active threat indicators associated with bogon address space. • **Empty feed status**: An empty feed does not indicate a system malfunction or an error. It simply signifies that no active threats have been identified in the monitored bogon space at this time.
Bots	Sites that host binary malware droppers
CnC	Sites that host command-and-control servers for botnets
Cryptomining	Hosts providing remote access to pools and wallets for the purpose of mining cryptocurrency
Dga	Malware algorithms used to generate a large number of domain names acting as rendezvous points with their command-and-control servers
Exploitkit	Software kits designed to identify software vulnerabilities in clients
High_risk	Domains and hostnames that match against the OpenDNS predictive security algorithms from security graph
Ioc	Hosts that have been observed to engage in Indicators of Compromise (IOC)
Link_sharing	Websites that share copyrighted files without permission

Security Intelligence Category	Description
Malicious	Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category
Malware	Sites that host malware binaries or exploit kits
Newly_seen	Domains that have recently been registered, or not yet seen via telemetry. **Attention** Currently, this category does not have any active feed and is reserved for future use.
Open_proxy	Open proxies that allow anonymous web browsing
Open_relay	Open mail relays that are known to be used for spam
Phishing	Sites that host phishing pages
Response	IP addresses and URLs that are actively participating in malicious or suspicious activity
Spam	Mail hosts that are known for sending spam
Spyware	Sites that are known to contain, serve, or support spyware and adware activities
Suspicious	Files that appear to be suspicious and have characteristics that resemble known malware
Tor_exit_node	Hosts known to offer exit node services for the Tor Anonymizer network

Block list icons

The visual indicators may appear in the Block list on the Security Intelligence tab in an access control policy.

Icon or Visual Indicator	Description
Block ( )	The object is set to block.
Monitor ( )	The object is set to monitor-only. See Security intelligence monitoring, on page 1606
An object is displayed in strikethrough text	The same object is also on the Do Not Block list, which overrides the block.

Configuration example: Security intelligence blocking

Configure Security Intelligence blocking to protect your network from known malicious IP addresses, URLs, and domains using regularly updated threat intelligence feeds.

Configure your access control policy to block all threats detectable by the system's regularly updated Security Intelligence feeds.

The number of objects in the Block lists plus the number in the Do Not Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

Before you begin

- To ensure that all options are available to select, add at least one managed device to your management center.
- Configure a DNS policy to block all Security Intelligence threat categories for domains. For more information, see DNS Policies for Security Intelligence, on page 1993.
- If you have, or will have, custom lists of entities to block, create a Security Intelligence object of each type (URLs, DNS, Networks.) See Security intelligence, on page 2418.

Procedure

Step 1 Click **Policies** > **Access Control heading** > **Access Control**.

Step 2 Create a new access control policy or edit an existing policy.

Step 3 In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 4 Click **Networks** to add blocking criteria for IP addresses.

a) Scroll down in the Networks list and select all of the threat categories listed below the Global lists.
b) If applicable, select the security zones for which you want to block these threats.
c) Click **Add to Block List**.
d) If you have created custom lists or feeds with addresses to block, add those to the Block List using the same steps as above.

Step 5 Click **URLs** to add blocking criteria for URLs, and repeat the steps you followed for Networks.

Step 6 Choose a DNS policy from the **DNS Policy** drop-down list; see DNS policies, on page 1993.

Step 7 Click **Save**.

Your access control policy now blocks malicious IP addresses, URLs, and domains based on Security Intelligence threat feeds, providing enhanced protection against known threats.

What to do next

- Enable logging for these connections; see *Logging Connections with Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Deploy configuration changes; see Deploy configuration changes, on page 135.

- For additional protection, configure URL filtering to block malicious URLs. See URL Filtering Rules, on page 1651.

Security intelligence monitoring

Security Intelligence monitoring is a security feature that

- logs connection events for traffic that would have been blocked by Security Intelligence, but does not block the traffic,
- enables testing of feeds before implementation, and
- optimizes performance in passive deployments.

Use cases for security intelligence monitoring

Monitoring is especially useful for:

- Testing feeds before you implement them.

  Consider a scenario where you want to test a third-party feed before you implement blocking using that feed. When you set the feed to monitor-only, the system allows connections that would have been blocked to be further analyzed by the system, but also logs a record of each of those connections for your evaluation.

- Passive deployments, to optimize performance.

  Managed devices that are deployed passively cannot affect traffic flow; there is no advantage to configuring the system to block traffic. Additionally, because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

Note If configured, Secure Firewall Threat Intelligence Director may impact the action taken (Monitor or Block.) For more information, see Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

To configure Security Intelligence monitoring:

After you configure Security Intelligence blocking following the instructions in Configuration example: Security intelligence blocking, on page 1605, right-click each applicable object in the Block list and choose **Monitor-only**. You cannot set system-provided Security Intelligence lists to monitor only.

Override security intelligence blocking

Use Do Not Block lists to exempt specific domains, URLs, or IP addresses from being blocked by Security Intelligence lists or feeds.

You can use Do Not Block lists for various purposes:

- Override the occasional false-positive block in a reputable Security Intelligence feed

- Inspect specific traffic in depth instead of blocking it early based on reputation
- Exempt otherwise-restricted transactions based on zone from Security Intelligence blocking

  For example, you can add an improperly classified URL to a Do Not Block list, but then restrict the Do Not Block list object using a security zone used by those in your organization who need to access those URLs. That way, only those with a business need can access the URLs on the Do Not Block list.



Note Entries on a Do Not Block list are simply exemptions from the block list. Any connection that passes the Security Intelligence policy is subject to the access control rules. Thus, an entry in the Do Not Block list can subsequently be blocked by an access control rule or intrusion policy. Your Do Not Block entries should always be exemptions from your block lists.

Procedure

Step 1 Option 1: Add an IP address, URL, or domain from an event to the Global Do Not Block List. See Global and domain security intelligence lists, on page 2420.

Step 2 Option 2: Use a custom Security Intelligence list or feed.

a) Create the custom Security Intelligence list or feed. See Custom Security Intelligence lists, on page 2430 or Create custom security intelligence feeds, on page 2428.
b) For IP addresses (Networks) and URLs: Edit your access control policy, click the Security Intelligence tab, then click the custom list or feed in the Networks or URLs sub-tab, then click **Add to Do Not Block List**.
c) Save your changes.
d) For domains (DNS): See the "DNS Policy" section in the Security intelligence options, on page 1601 topic.
e) Deploy your changes.

The specified domains, URLs, or IP addresses are now exempted from Security Intelligence blocking and will be subject to access control rules instead.

Troubleshooting security intelligence

See the following topics for troubleshooting Security Intelligence.

Security intelligence categories missing from the Available Options List

Security Intelligence categories (such as CnC or Exploitkit) display in the Networks tab under Available Options only after you add at least one managed device to your management center.

You must add a device in order to pull all TALOS feeds that provide the Security Intelligence categories.

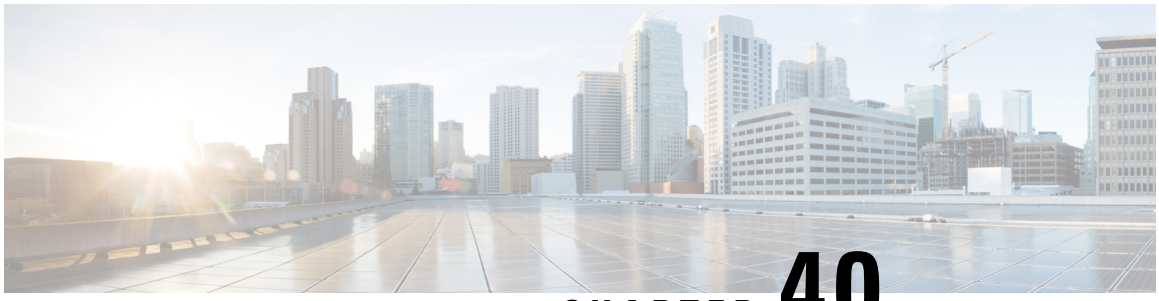
If the expected category does not appear in Security Intelligence, verify that it is not a URL filtering category, which uses a different set of categories.

To see URL filtering categories, look at the **URLs** tab in an access control rule.

History for security intelligence block listing

This reference provides a chronological history of changes and updates to Security Intelligence Block Listing features, including terminology changes and new category additions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New Security Intelligence categories	All	Any	Talos has added the new Security Intelligence categories: • banking_fraud • ioc • high_risk • link_sharing • malicious • newly_seen • spyware You should update your access control and DNS policies to address the new categories, and check periodically for future changes. New/modified pages: Security Intelligence tab, Networks and URLs sub-tabs; DNS rules in DNS policies Supported platforms: Firewall Management Center



CHAPTER 40

Access Control Rules

The following topics describe how to configure access control rules.

- Access control rules, on page 1609
- Requirements and prerequisites for access control rules, on page 1620
- Guidelines and limitations for access control rules, on page 1621
- Best practices for application control, on page 1622
- Best practices for access control rules, on page 1625
- Access control rule management, on page 1630
- Examples for access control rules, on page 1645
- History for access control rules, on page 1649

Access control rules

Within an access control policy, access control rules provide a granular method that

- handles network traffic across multiple managed devices within an access control policy
- provides conditions that match traffic in a specified order, and
- determines actions to monitor, trust, block, or allow matching traffic.

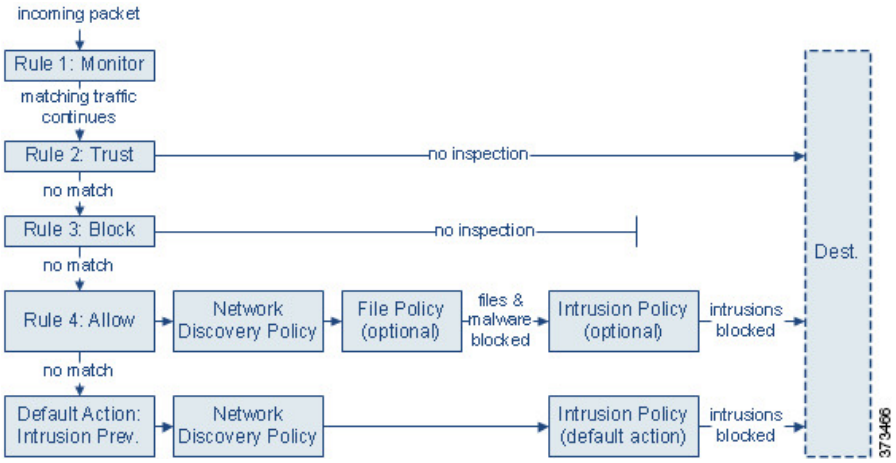
Rule evaluation and traffic handling

The system matches traffic to access control rules in the order you specify. In most cases, the system handles network traffic according to the first access control rule where all the rule's conditions match the traffic.

Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic. When you allow traffic, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network.

Note Security Intelligence filtering, decryption, user identification, and some decoding and preprocessing occur before access control rules evaluate network traffic.

This scenario summarizes the ways that traffic can be evaluated by access control rules in an inline, intrusion prevention deployment.



In this scenario, traffic is evaluated as follows:

- **Rule 1: Monitor** evaluates traffic first. Monitor rules track and log network traffic. The system continues to match traffic against additional rules to determine whether to permit or deny it. (However, see an important exception and caveat at Access control rule monitor action, on page 1614.)
- **Rule 2: Trust** evaluates traffic next. Matching traffic is allowed to pass to its destination without further inspection, though it is still subject to identity requirements and rate limiting. Traffic that does not match continues to the next rule.
- **Rule 3: Block** evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.
- **Rule 4: Allow** is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.
- **Default Action** handles all traffic that does not match any of the rules. In this scenario, the default action performs intrusion prevention before allowing non-malicious traffic to pass. In a different deployment, you might have a default action that trusts or blocks all traffic, without further inspection. (You cannot perform file or malware inspection on traffic handled by the default action.)

Traffic you allow, whether with an access control rule or the default action, is automatically eligible for inspection for host, application, and user data by the network discovery policy. You do not explicitly enable discovery, although you can enhance or disable it. However, allowing traffic does not automatically guarantee discovery data collection. The system performs discovery only for connections involving IP addresses that are explicitly monitored by your network discovery policy; additionally, application discovery is limited for encrypted sessions.

Note that access control rules handle encrypted traffic when your decryption configuration allows it to pass, or if you do not configure decryption. However, some access control rule conditions require unencrypted traffic, so encrypted traffic may match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

Access control rule management

The rules table of the access control policy editor allows you to add, edit, categorize, search, filter, move, enable, disable, delete, and otherwise manage access control rules in the current policy.

Properly creating and ordering access control rules is a complex task, but one that is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations.

Use the search bar to filter the list of access control policy rules. You can deselect the **Show Only Matching Rules** option to see all rules. Matched rules are highlighted.

For each access control rule, the policy editor displays its name, a summary of its conditions, the rule action, and icons that communicate the rule's inspection options or status.

The system provides specific icons to communicate the inspection options or status of each rule:

- **Time Range Option** ( )
- **Intrusion policy** ( )
- **File policy** ( )
- **Logging** ( )
- **Warning** ( )
- **Errors** ( )
- **Rule Conflict** ( )

Disabled rules are dimmed and marked (disabled) after the rule name.

To create or edit a rule, refer to Create and edit access control rules, on page 1631 .

Tip A right-click menu provides shortcuts to many rule management options, including editing, deleting, moving, enabling, and disabling.

Related Topics

Access control rule components, on page 1611
Best practices for access control rules, on page 1625

Access control rule components

In addition to its unique name, each access control rule has basic components that determine how the system processes and handles network traffic.

State

By default, rules are enabled. If you disable a rule, the system does not use it and stops generating warnings and errors for that rule.

Position

Rules in an access control policy are numbered, starting at 1. If you are using policy inheritance, rule 1 is the first rule in the outermost policy. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.

Rules can also belong to a section and a category, which are organizational only and do not affect rule position. Rule position goes across sections and categories.

Section and category

To help you organize access control rules, every access control policy has two system-provided rule sections, Mandatory and Default. To further organize access control rules, you can create custom rule categories inside the Mandatory and Default sections.

If you are using policy inheritance, the current policy's rules are nested between its parent policy's Mandatory and Default sections.

Conditions

Conditions specify the specific traffic the rule handles. Conditions can be simple or complex; their use often depends on license.

Traffic must meet all of the conditions specified in a rule. For example, if the Application condition specifies HTTP but not HTTPS, the URL category and reputation conditions will not apply to HTTPS traffic.

Applicable time

You can set rules to operate during specified days and times

Action

A rule's action determines how the system handles matching traffic. You can monitor, trust, block, or allow (with or without further inspection) matching traffic. The system does not perform deep inspection on trusted, blocked, or encrypted traffic.

Inspection

Deep inspection options govern how the system inspects and blocks malicious traffic you would otherwise allow. When you allow traffic with a rule, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network.

Logging

Logging settings govern records that the system keeps for handled traffic. You can log sessions at connection start, end, or both; log connections to databases, syslog, or SNMP trap servers. You can log connections to the database, as well as to a syslog or an SNMP trap server.

Comments

Each time you save changes to an access control rule, you can add comments.

Related Topics

Best practices for access control rules, on page 1625

Access control rule management, on page 1611
Create and edit access control rules, on page 1631
Access control rule actions, on page 1614
Access control rule conditions, on page 1633
Deep inspection using file and intrusion policies, on page 1617
Access control rule comments

Access control rule order

Access control rule order is a traffic processing method that

- numbers rules in an access control policy starting at 1
- matches traffic to access control rules in top-down order by ascending rule number, and
- handles network traffic according to the first access control rule where all the rule's conditions match the traffic.

In most cases, except for Monitor rules, the system does not continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule.

To help you organize access control rules, every access control policy has two system-provided rule sections, Mandatory and Default. To further organize, you can create custom rule categories inside the Mandatory or Default sections. After you create a category, you cannot move it, although you can delete it, rename it, and move rules into, out of, within, and around it. The system assigns rule numbers across sections and categories.

If you use policy inheritance, the current policy's rules are nested between its parent policy's Mandatory and Default rule sections. Rule 1 is the first rule in the outermost policy, not the current policy, and the system assigns rule numbers across policies, sections, and categories.

Any predefined user role that allows you to modify access control policies also allows you to move and modify access control rules within and among rules categories. You can, however, create custom roles that restrict users from moving and modifying rules. Any user who is allowed to modify access control policies can add rules to custom categories and modify rules in them without restriction.



Caution Failure to set up your access control rules properly can have unexpected results, including traffic being allowed that should be blocked. In general, application control rules should be lower in your access control list because it takes longer for those rules to match than rules based on IP address, for example.

Access control rules that use *specific* conditions (such as networks and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your access control rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your access control rules. For more information about the OSI model, see this Wikipedia article.

Note Proper access control rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs. For more information, refer to Best practices for ordering rules, on page 1627.

Access control rule actions

An access control rule action is a configuration setting that determines how the system handles and logs matching traffic, with options to monitor, trust, block, or allow traffic with or without further inspection.

Default action behavior

The access control policy's *default action* handles traffic that does not meet the conditions of any access control rule with an action other than Monitor.

Access control rule monitor action

The **Monitor** action is an access control rule action that forces connection logging regardless of how matching traffic is eventually handled. It does not affect traffic flow by permitting or denying traffic immediately, and allows traffic to be matched against additional rules to determine the final action.

When a connection matches a monitor rule, the next non-monitor rule that the connection matches determines traffic handling and any further inspection. If there are no additional matching rules, the Firewall Threat Defense device uses the default action.

There is an exception: If a monitor rule contains layer 7 conditions, such as an application condition, the system allows early packets to pass and the connection to be established (or the SSL handshake to complete), even if a subsequent rule would block the connection. Early packets are not evaluated against subsequent rules, so to prevent uninspected traffic, you can specify an intrusion policy for these packets in the access control policy's advanced settings. For more information, refer to Inspection of packets that pass before traffic is identified. After the system completes its layer 7 identification, it applies the appropriate action to the remaining session traffic.

Access control rule trust action

The **Trust** action is the access control rule action that allows traffic to pass without deep inspection or network discovery, still subjects trusted traffic to identity requirements and rate limiting, and bypasses additional inspection services while maintaining basic security controls.

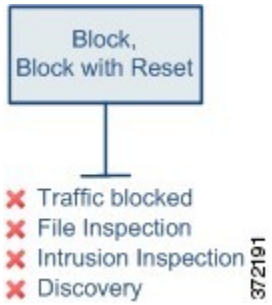


Note

- Some protocols, such as FTP and SIP, use secondary channels, which the system opens through the process of inspection. In some cases, trusted traffic can bypass all inspection, and these secondary channels cannot be opened properly. If you run into this problem, change the trust rule to **Allow**.
- For trust rules with logging options disabled, end-of-flow events are still generated in the system. However, the events are not visible on the event pages.
- Because access control rules are evaluated after other policies, such as decryption, trusting a connection does not necessarily mean it will be fast-pathed with no inspection. For example, if a connection matches both a decryption rule that requires decryption, and a trust access control rule, the connection is decrypted and inspected as needed, prior to being allowed by the trust rule. Trust simply means no additional inspection, such as intrusion inspection, will be applied. If your intention is to allow a connection uninspected, either use the prefilter policy to fast path the connection, or ensure that no other policy applies inspection services to the connection.

Access control rule blocking actions

A block action is an access control rule action that denies network traffic without further inspection and prevents the use of file, intrusion, or network discovery policies for blocked traffic.



Block and **Block with reset** actions immediately stop traffic from entering the network. Block with reset rules reset the connection except for web requests met with an HTTP response page. The HTTP response page is used to notify users when their web request is blocked, but it cannot be displayed if the connection is immediately reset.

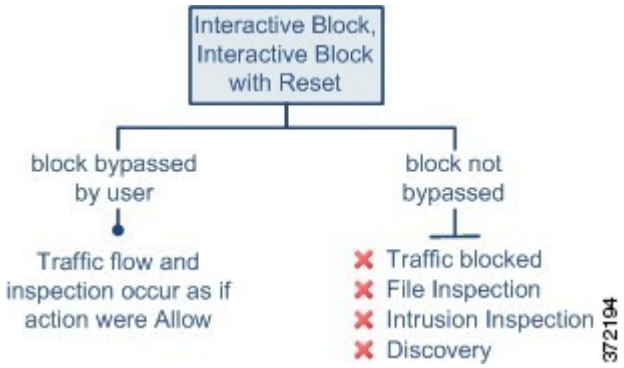
For more information, refer to HTTP response pages, on page 1669.

Related Topics

HTTP response pages, on page 1669

Access control rule interactive blocking actions

The **Interactive Block** and **Interactive Block with reset** actions are access control rule actions that give web users a choice to continue to their intended destinations.



If a user bypasses the block, the rule mimics an allow rule. Therefore, you can associate interactive block rules with file and intrusion policies, and matching traffic is also eligible for network discovery.

If a user does not (or cannot) bypass the block, the rule mimics a block rule. Matching traffic is denied without further inspection.

Note If you enable interactive blocking, you cannot reset all blocked connections. This is because the response page cannot display if the connection is immediately reset. Use the **Interactive Block with reset** action to (non-interactively) block-with-reset all non-web traffic, while still enabling interactive blocking for web requests.

For more information, refer to HTTP response pages, on page 1669.

Related Topics

Decryption rule blocking actions, on page 1779

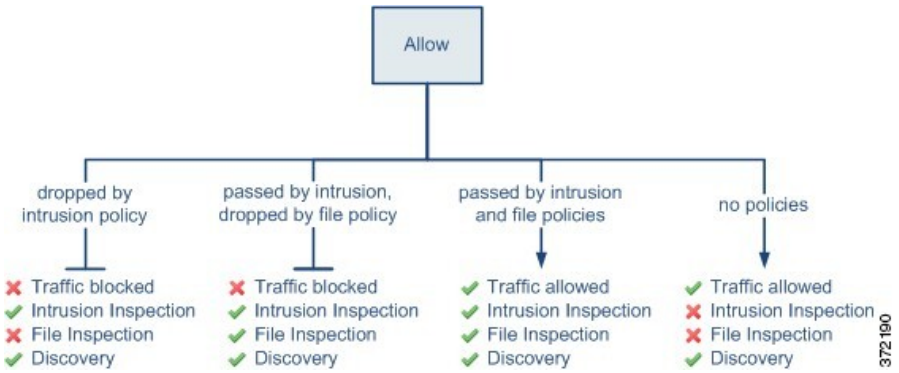
Access control rule allow action

An access control rule allow action is a rule action that allows matching traffic to pass. However, traffic is still subject to identity requirements and rate limiting.

Optionally, you can use deep inspection to further inspect and block unencrypted or decrypted traffic before it reaches its destination:

- You can use an intrusion policy to analyze network traffic according to intrusion detection and prevention configurations, and drop offending packets depending on the configuration.
- You can perform file control using a file policy. File control allows you to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
- You can perform network-based advanced malware protection (AMP), also using a file policy. malware defense can inspect files for malware, and block detected malware depending on the configuration.

This diagram illustrates the types of inspection performed on traffic that meets the conditions of an Allow rule (or a user-bypassed Interactive Block rule). Notice that file inspection occurs before intrusion inspection; blocked files are not inspected for intrusion-related exploits.



For simplicity, the diagram displays traffic flow for situations where both (or neither) an intrusion and a file policy are associated with an access control rule. You can, however, configure one without the other. Without a file policy, traffic flow is determined by the intrusion policy; without an intrusion policy, traffic flow is determined by the file policy.

Regardless of whether the traffic is inspected or dropped by an intrusion or file policy, the system can inspect it using network discovery. However, permitting traffic does not guarantee that discovery inspection occurs. The system only performs discovery for connections involving IP addresses explicitly monitored by your network discovery policy. Also, application discovery is limited for encrypted sessions.

Deep inspection using file and intrusion policies

Deep inspection is a security mechanism that uses intrusion and file policies as the last line of defense before traffic is allowed to its destination.

Policy types and capabilities

Deep inspection uses two types of policies to analyze traffic:

- *Intrusion policies* govern the system's intrusion prevention capabilities.
- *File policies* govern the system's file control and malware defense capabilities.

Access control occurs before deep inspection; access control rules and the access control default action determine which traffic is inspected by intrusion and file policies.

By associating an intrusion or file policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy, a file policy, or both.

In an access control policy, you can associate one intrusion policy with each Allow and Interactive Block rule, as well as with the default action. Every unique **pair** of intrusion policy and variable set counts as one policy.

Note By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

To associate intrusion and file policies with an access control rule, see:

- Access Control Rules: Intrusion Policy Selection
- Configure an access control rule to perform malware protection, on page 2024

For more information about intrusion policies, refer to Network Analysis and Intrusion Policy Basics.

For more information about file policies, refer to File Policies for Network Malware Protection, on page 2015.

File and intrusion inspection order

File and intrusion inspection order defines the traffic processing sequence that performs file inspection before intrusion inspection for any single connection handled by an access control rule, preventing files blocked by a file policy from being inspected for intrusions while prioritizing simple file blocking by type over malware inspection.

For a connection matching an Allow or Interactive Block rule, the system determines traffic flow based on the following configurations:

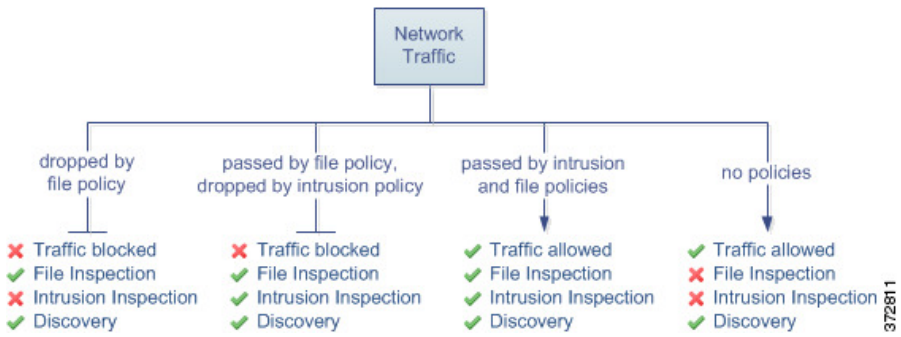
- Without a file policy, traffic flow is determined by the intrusion policy.
- Without an intrusion policy, traffic flow is determined by the file policy.
- Without either, allowed traffic is inspected by network discovery only.

In your access control policy, you can associate multiple Allow and Interactive Block rules with different intrusion and file policies to match inspection profiles to various types of traffic.

Note The system does not perform any kind of inspection on trusted traffic. Although configuring an Allow rule with neither an intrusion nor file policy passes traffic like a Trust rule, Allow rules let you perform discovery on matching traffic.

The diagram below illustrates the types of inspection you can perform on traffic that meets the conditions of either an Allow or user-bypassed Interactive Block access control rule. For simplicity, the diagram displays traffic flow for situations where both (or neither) an intrusion and a file policy are associated with a single access control rule.

Figure 409: Traffic inspection flowchart



For any single connection handled by an access control rule, file inspection occurs before intrusion inspection. That is, the system does not inspect files blocked by a file policy for intrusions. Within file inspection, simple blocking by type takes precedence over malware inspection and blocking.

For example, consider a scenario where you normally want to allow certain network traffic as defined in an access control rule. However, as a precaution, you want to block the download of executable files, examine downloaded PDFs for malware and block any instances you find, and perform intrusion inspection on the traffic.

You create an access control policy with a rule that matches the characteristics of the traffic you want to provisionally allow, and associate it with both an intrusion policy and a file policy. The file policy blocks the download of all executables, and also inspects and blocks PDFs containing malware:

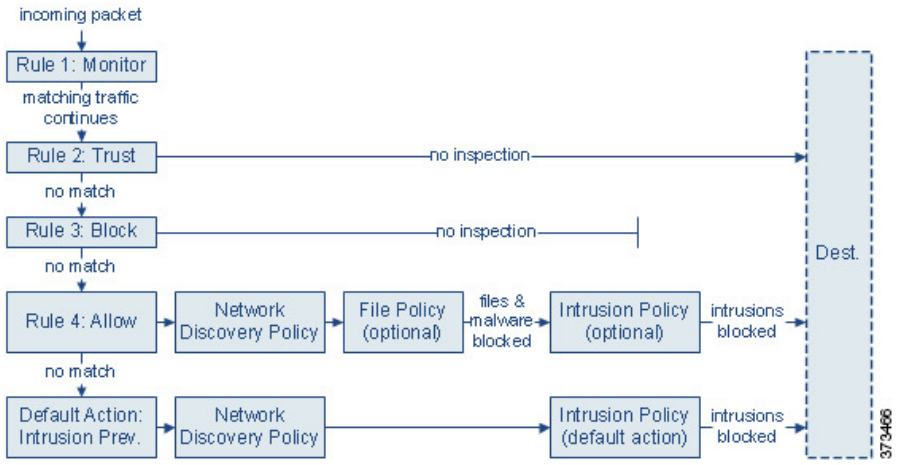
- First, the system blocks the download of all executables, based on simple type matching specified in the file policy. Because they are immediately blocked, these files are subject to neither malware nor intrusion inspection.
- Next, the system performs malware cloud lookups for PDFs downloaded to a host on your network. Any PDFs with a malware disposition are blocked, and are not subject to intrusion inspection.
- Finally, the system uses the intrusion policy associated with the access control rule to inspect any remaining traffic, including files not blocked by the file policy.

Note Until a file is detected and blocked in a session, packets from the session might be subject to intrusion inspection.

How access control traffic handling works with intrusion and file policies

Summary

This diagram shows the flow of traffic in an inline intrusion prevention and malware defense deployment, as governed by an access control policy that contains four different types of access control rules and a default action.



Workflow

In the scenario above, the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it. (However, see an important

exception and caveat at Access control rule monitor action, on page 1614.) Trust and Block rules handle matching traffic without further inspection of any kind, while traffic that does not match continues to the next access control rule.

The fourth and final rule in the policy, an Allow rule, invokes various other policies to inspect and handle matching traffic, in the following order:

1. Discovery: Network Discovery Policy—First, the network discovery policy inspects traffic for discovery data. Discovery is passive analysis and does not affect the flow of traffic. Although you do not explicitly enable discovery, you can enhance or disable it. However, allowing traffic does not automatically guarantee discovery data collection. The system performs discovery only for connections involving IP addresses that are explicitly monitored by your network discovery policy.
2. malware defense and File Control: File Policy—After traffic is inspected by discovery, the system can inspect it for prohibited files and malware. malware defense detects and optionally blocks malware in many types of files, including PDFs, Microsoft Office documents, and others. If your organization wants to block not only the transmission of malware files, but all files of a specific type (regardless of whether the files contain malware), file control allows you to monitor network traffic for transmissions of specific file types, then either block or allow the file.
3. Intrusion Prevention: Intrusion Policy—After file inspection, the system can inspect traffic for intrusions and exploits. An intrusion policy examines decoded packets for attacks based on patterns, and can block or alter malicious traffic. Intrusion policies are paired with variable sets, which allow you to use named values to accurately reflect your network environment.
4. Destination—Traffic that passes all the checks described above passes to its destination.

An Interactive Block rule (not shown in the diagram) has the same inspection options as an Allow rule. This is so you can inspect traffic for malicious content when a user bypasses a blocked website by clicking through a warning page.

Traffic that does not match any access control rules in the policy with an action other than Monitor is handled by the default action. In this scenario, the default action is an Intrusion Prevention action, which allows traffic to its final destination as long as it is passed by the intrusion policy you specify. In a different deployment, you might have a default action that trusts or blocks all traffic without further inspection. Note that the system can inspect traffic allowed by the default action for discovery data and intrusions, but not prohibited files or malware. You cannot associate a file policy with the access control default action.

Note Sometimes, when a connection is analyzed by an access control policy, the system must process the first few packets in that connection, allowing them to pass, before it can decide which access control rule (if any) will handle the traffic. However, so these packets do not reach their destination uninspected, you can specify an intrusion policy (in the advanced settings for the access control policy) to inspect these packets and generate intrusion events.

Requirements and prerequisites for access control rules

Ensure that your deployment meets these requirements before you configure access control rules.

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin
- You can define custom user roles to differentiate between the intrusion configuration in access control policy and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. The existing pre-defined user roles that included the Modify Access Control Policy permission support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions. The granular permissions are:
  - **Policies** > **Access Control heading** > **Access Control** and choose the **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** allows the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. If a user has this option only, the user can modify no other part of the policy or rule.
  - **Modify Remaining Access Control Policy Configuration** controls the ability to edit all other aspects of the policy.

Guidelines and limitations for access control rules

Consider these limitations when you configure rules in the access control policy:

- There is a limit of 1000 rules that can be shown at a time on the current page. Thus, if you have a very large number of rules, such as 3000 rules within a single category, actions like selecting all rules in a category and deleting them does not delete all of the rules. You might need to select/delete rules again to delete all the rules that you are targeting.
- If you edit an access control rule that is actively in use, the changes do not apply to established connections at deploy-time. The updated rule is used to match against future connections. However, if the system is actively inspecting a connection (for example, with an intrusion policy), it will apply changed matching or action criteria to existing connections.

  For Firewall Threat Defense, you can ensure that your changes apply to all current connections by using the Firewall Threat Defense **clear conn** CLI command to end established connections. Note that you should only do this if it is acceptable to end those connections, on the assumption that the sources for the connections will then attempt to reestablish the connection and thus be matched appropriately against the new rule.

- VLAN tags in access rules only apply to inline sets; they cannot be used in access rules applied to firewall interfaces.
- To use fully-qualified domain name (FQDN) network objects as source or destination criteria, you must also configure DNS for the data interfaces in the platform settings policy. The system does not use the management DNS server setting to do lookups for FQDN objects used in access control rules.

  Note that controlling access by FQDN is a best-effort mechanism. Consider the following points:

  - Whenever possible, use Security Intelligence or URL filtering instead of FQDN rules.
  - Because DNS replies can be spoofed, only use fully trusted DNS servers.
  - Some FQDNs, especially for very popular servers, can have hundreds if not thousands of IP addresses, and these can frequently change. Because the system uses cached DNS lookup results, users might get addresses that are not yet in the cache, and their connections will not match the FQDN rule. Rules that use FQDN network objects function effectively only for names that resolve to fewer than 100 addresses.

    We recommend that you do not create network object rules for an FQDN that resolves to more than 100 addresses, as the likelihood of the address in a connection being one that has been resolved and available in the DNS cache on the device is low. For these cases, use a URL-based rule instead of an FQDN network object rule.
  - For popular FQDNs, different DNS servers can return a different set of IP addresses. Thus, if your users use a different DNS server than the one you configure, FQDN-based access control rules might not apply to all IP addresses for the site that are used by your clients, and you will not get the intended results for your rules.
  - Some FQDN DNS entries have very short time to live (TTL) values. This can result in frequent recompilation of the lookup table, which can impact overall system performance.
  - If more than 8 FQDNs resolve to the same IP address, the system cannot reliably match traffic to the rules for those FQDN. At most 8 FQDNs per IP address can be handled.
- The maximum objects per match criteria per access control rule is 200. For example, you can have up to 200 network objects in a single access control rule.
- Block with reset can be CPU-intensive for rules that drop a high rate of TCP traffic. When the system drops TCP traffic with this action, it also generates TCP reset packets, which can affect device performance during high-volume drops. For access control rules that are expected to drop large amounts of TCP traffic, use **Block** instead of **Block with reset**, unless TCP reset behavior is required.

  If TCP reset behavior is required for denied inbound TCP traffic, you can also evaluate using a regular **Block** rule with the **service resetinbound** command through FlexConfig for the applicable interface.

Best practices for application control

These topics discuss our recommended best practices for controlling applications with access control rules.

Recommendations for application control

Ensure that adaptive profiling is enabled

If adaptive profiling is not enabled (its default state), access control rules cannot perform application control.

Enable application detectors automatically

If no detector is enabled for an application you want to detect, the system automatically enables all system-provided detectors for the application. If none exist, the system enables the most recently modified user-defined detector for the application.

Configure your policy to examine the packets that must pass before an application is identified

The system cannot perform application control before *both* of these conditions occur:

- A monitored connection is established between a client and server
- The system identifies the application in the session

This identification should occur in 3 to 5 packets, or after the server certificate exchange in the SSL handshake if the traffic is encrypted.

If early traffic matches all other criteria but application identification is incomplete, the system allows the packet to pass and the connection to be established (or the SSL handshake to complete). After the system completes its identification, the system applies the appropriate action to the remaining session traffic.

To ensure that your system examines these initial packets, select an intrusion policy in the **Intrusion Policy used before Access Control rule is determined** options in the access control policy advanced settings.

Understand limitations to identifying applications

A server must adhere to the protocol requirements of an application for the system to be able to recognize it. For example, if you have a server that sends a keep-alive packet rather than an ACK when an ACK is expected, that application might not be identified, and the connection will not match the application-based rule. Instead, it will be handled by another matching rule or the default action. This might mean that connections you want to allow can be denied instead. If you run into this problem, and you cannot fix the server to follow the protocol standards, you need to write a non-application-based rule to cover traffic for that server, for example, by matching the IP address and port number.

Create separate rules for URL and application filtering

Create separate rules for URL and application filtering whenever possible, because combining application and URL criteria can lead to unexpected results, especially for encrypted traffic.

Rules that include both application and URL criteria should come after application-only or URL-only rules, unless the application+URL rule is acting as an exception to a more general application-only or URL-only rule.

Place URL rules before application and other rules

For the most effective URL matching, place rules that include URL conditions before other rules, particularly if the URL rules are block rules and the other rules meet both of these criteria:

- They include application conditions.
- The traffic to be inspected is encrypted.

Handling application traffic packets without payloads

When performing access control, the system applies the default policy action to packets that do not have a payload in a connection where an application is identified.

Handling referred application traffic

To handle traffic referred by a web server, such as advertisement traffic, match the referred application rather than the referring application.

Controlling application traffic that uses multiple protocols

Some applications use multiple protocols. To control their traffic, make sure your access control policy covers all relevant options. These applications typically include the application name in each aspect that you can control. Also see Application-specific requirements for filtering, on page 1625.

Controlling evasive application traffic

See Application-specific requirements for filtering, on page 1625.

Best practice for choosing between application matching and port matching

In traditional firewalls, you can match traffic based on OSI layers 3 (protocol) and 4 (transport), such as IP or TCP/80. All traffic on a given port (or a whole protocol) is then either allowed or blocked based on that rule's action.

Application criteria, on the other hand, are OSI layer 7. Different applications can use the same TCP/UDP port. By using application criteria, you can selectively allow or block different applications on the same port without allowing or blocking all applications on that port.

Whether you use port-based or application-based criteria in your rule can impact rule performance. Because TCP/UDP ports are quickly identifiable in packets, the system can match the correct rule on the first packet. With application-layer criteria, it can take 3-5 packets to identify the specific application (if you do not also specify ports).

Consider these best practices:

- If you want to handle all of the traffic on a given TCP/UDP port in the same way for the specified interfaces and networks, use port-based matching. For example, to handle all SSH traffic the same way, select the SSH port (TCP/22) on the Ports tab.
- If you want to narrowly match a specific application that uses the same port as other applications, select the application on the Applications tab. This is how you can handle web applications, which all use TCP/80 or 443, so that you can selectively block or allow certain web applications without blocking or allowing all web applications.
- If you want to control application use by a user group, select the user group on the Users tab and the application on the Application tab. For example, you could block the Gaming applications category for members of the Contractor user group.
- For rules that go from a less secure network (such as the internet) to a more secure network (such as an internal protected network), use the Ports tab whenever possible. For example, you can allow/block ICMP traffic from the internet to an internal network.
- If you do have a mix of port-based and application-based rules, place the port-based rules higher in the rules list, so that connections can be matched to those rules first. Protocol and port can be more quickly identified than applications.

Application-specific requirements for filtering

Office 365 admin portal

If the access policy has logging enabled at the beginning as well as at the end of a connection, the first packet will be detected as Office 365 and the end of connection will be detected as Office 365 Admin Portal. This should not affect blocking.

Skype

To control Skype traffic, choose the **Skype** tag from the **Application Filters** list rather than selecting individual applications. This ensures that the system can detect and control all Skype traffic the same way.

GoToMeeting

In order to fully detect GoToMeeting, your rule must include all of these applications:

- GoToMeeting
- Citrix Online
- Citrix GoToMeeting Platform
- LogMeIn
- STUN

Zoho mail

To control Zoho mail, choose *both* **Zoho** and **Zoho mail** from the Available Application list.

Evasive application detection considerations

For evasive applications such as Bittorrent, Tor, Psiphon, and Ultrasurf, only the highest-confidence scenarios are detected by default. If you need to take action on this traffic (such as block or implement QoS), it may be necessary to configure more aggressive detection with better effectiveness. To do this, contact TAC to review your configurations as these changes may result in false positives.

WeChat

It is not possible to selectively block WeChat Media if you allow WeChat.

RDP file transfer

If allowing the RDP (Remote Desktop Protocol) application does not allow file transfers, ensure that the rule for RDP includes both the TCP and UDP port 3389. RDP file transfer uses UDP.

Best practices for access control rules

Configuring and ordering access control rules properly is essential to protect your network. Consider these best practices to achieve optimal results:

- Always evaluate device compatibility of access control rules before deployment.
- Ensure resources, such as physical memory and processors, can handle expanded rule criteria.



Note Ensure the system evaluates all rules together and creates a set of criteria for devices when you deploy configuration changes. You cannot deploy to a device if these criteria exceed its resources.

General best practice for access control

General best practices

- Use a prefilter policy to provide early blocking for unwanted traffic, and to fastpath traffic that does not benefit from access control inspection. For more information, refer to Best practices for fastpath prefiltering, on page 1978.
- Access control rules are deployed as access control entries (ACE) on the device. To minimize the number of access control entries created per access control rule, and improve overall performance, enable object group search for each device. Object group search is a device setting, not an access control policy setting, so you must edit each device to ensure the feature is enabled. For more information, refer to Configure object group search, on page 798.
- Whenever possible, combine multiple network objects into a single object group. The system automatically creates an object group (during deployment) when you select more than one object (for source or destination separately). Selecting existing groups can avoid object group duplication and reduce the potential impact on CPU usage when there are a large number of duplicate objects.
- Certain features, including URL filtering, application detection, and rate limiting, must allow some packets to pass in order for the system to identify the traffic.
- If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.

Licensing and feature support

- Although you can configure the system without licensing your deployment, many features require that you enable the appropriate licenses before you deploy.
- Some features are only available on certain device models. Warning icons and confirmation dialog boxes designate unsupported features.

Deployment considerations

- When you deploy an access control policy, its rules are not applied to existing connections. Traffic on an existing connection is not bound by the new policy that is deployed. In addition, the policy hit count is incremented only for the first packet of a connection that matches a policy. Thus, the traffic on an existing connection that could match a policy is omitted from the hit count. To have the policy rules effectively applied, clear the existing connection sessions, and then deploy the policy.
- For the system to affect traffic, you must deploy relevant configurations to managed devices using routed, switched, or transparent interfaces, or inline interface pairs.
- The system might prevent you from deploying inline configurations to passively deployed devices, including inline devices in tap mode. In other cases, the policy might deploy successfully, but attempts to block or alter traffic can produce unexpected results because passive devices do not enforce traffic

actions. For example, the system might report multiple beginning-of-connection events for a connection that the policy attempts to block.

Best practices for creating, ordering, and implementing access control rules are detailed in Best practices for access control rules, on page 1625 and subtopics.

Best practices for ordering rules

Access control rules are matched top down, first match wins. Thus, to get the results you expect, you must pay careful attention to proper sequencing.

- In general, place top-priority rules that must apply to all traffic near the top of the policy. Always order rules to suit your organization's needs.
- Specific rules should come before general rules, especially when the specific rules are exceptions to general rules. Otherwise, traffic will match the general rule first and never hit the applicable specific rule.
- Rules that drop traffic based on layer-3/4 criteria only (such as IP address, security zone, and port number) should come as early as possible. Rules based on these criteria do not require inspection to identify matching connections.
- Whenever possible, put specific drop rules near the top of the policy. This ensures the earliest possible decision on undesirable traffic.
- URL filtering, application-based, and geolocation-based rules and others that require inspection should come after rules that drop traffic based on layer-3/4 criteria only (such as IP address, security zone, and port number), but before rules that specify file and intrusion policies.
- For the most effective URL matching, place rules that include URL conditions before other rules, particularly if the URL rules are block rules and the other rules meet both of the following criteria:
  - They include application conditions.
  - The traffic to be inspected is encrypted.
- Put URL filtering rules above application rules, and follow application rules with micro-application rules and Common Industrial Protocol (CIP) sub-classification application filtering rules.
- In general, rules with application conditions should be lower in your access control list because it takes longer for those rules to match than rules based on IP address, for example. For more information, see Best practice for choosing between application matching and port matching, on page 1624 and Recommendations for application control, on page 1622.
- Rules that specify file policies and intrusion policies should come at the bottom of the rule order. These rules require resource-intensive deep inspection, and you should eliminate as many threats as possible using less-intensive methods first, for performance reasons, in order to minimize the number of potential threats that require deep inspection.

Application rule order

Place rules with application conditions lower in your access control list because it takes longer for those rules to match than rules based on IP address, for example.

Access control rules that use *specific* conditions (such as networks and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your access control rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your access control rules. For more information about the OSI model, see this Wikipedia article.

For more information, refer to Best practice for choosing between application matching and port matching, on page 1624 and Recommendations for application control, on page 1622.

Rule preemption

Rule preemption is a policy evaluation condition that occurs when a rule will never match traffic because a rule earlier in the evaluation order matches the traffic first. A rule's conditions govern whether it preempts other rules.

Rule preemption scenarios

Any type of rule condition can preempt a subsequent rule. This table shows common preemption scenarios:

Table 95: Rule preemption examples

Rule 1 (preempting)	Rule 2 (preempted)	Rule preemption scenario
Allow Admin users	Block Admin users	The second rule cannot block Admin traffic because the first rule allows it.
Allow Source Network VLAN 22-33	Block Source Network VLAN 27	The VLAN range in the first rule includes the VLAN in the second rule, so the first rule preempts the second. To block VLAN 27, you must move that rule above the one that allows VLAN 22-33.
Allow Source Network 10.4.0.0/16	Allow Source Network 10.4.0.0/16, VLAN 2	The VLAN range in the first rule includes the VLAN in the second rule, so the first rule preempts the second. To block VLAN 27, you must move that rule above the one that allows VLAN 22-33.
Allow Source Network 10.10.10.0/24 to URL www.netflix.com	Allow Source Network 10.10.10.0/24 to URL www.netflix.com	A rule also preempts an identical subsequent rule where all configured conditions are the same.

Best practice for rule actions and rule order

A rule's action determines how the system handles matching traffic. Improve performance by placing rules that do not perform or ensure further traffic handling before the resource-intensive rules that do. Then, the system can divert traffic that it might otherwise have inspected.

The following examples show how you might order rules in various policies, given a set of rules where none is more critical and preemption is not an issue.

If your rules include application conditions, also refer to Best practice for choosing between application matching and port matching, on page 1624.

Optimum order for access control rules

Intrusion, file, and malware inspection requires resources, especially if you use multiple custom intrusion policies and variable sets. Place access control rules that invoke deep inspection last.

1. Monitor—Rules that log matching connections, but take no other action on traffic. (However, see the important exception and caveat at Access control rule monitor action, on page 1614.)
2. Trust, Block, Block with reset—Rules that handle traffic without further inspection.
3. Allow, Interactive Block (no deep inspection)—Rules that do not inspect traffic further, but allow discovery.
4. Allow, Interactive Block (deep inspection)—Rules associated with file or intrusion policies that perform deep inspection for prohibited files, malware, and exploits.

Best practices for simplifying and focusing rules

Follow these best practices to simplify configuration and ensure optimal device performance and rule clarity:

Simplify rule conditions

Minimize individual rule criteria. Use as few elements in rule conditions as possible. For example, use IP address blocks rather than individual IP addresses when defining network conditions.

Avoid redundant conditions

If a single condition is enough to match the traffic you want to handle, do not add more. Redundant conditions can make configuration unnecessarily complex and may negatively impact device performance, especially during cluster or high-availability unit re-join.

For example:

- Use security zones that represent multiple interfaces carefully. If you specify source and destination networks as conditions, and these are enough to match the traffic you are targeting, then specifying a security zone is not required.
- If you want to match a set of internal interfaces to any destination on the Internet (for example), then simply use a source security zone that includes your internal interfaces. No network or destination interface criteria are needed.

Combine elements for organization, not performance

The use of network objects containing many individual IP addresses offers organizational benefits only. It does not improve device performance compared to listing those IP addresses individually.

For recommendations related to application detection, refer to Best practice for choosing between application matching and port matching, on page 1624.

Narrowly constrain resource-intensive rules, especially by interface

As much as possible, use rule conditions to narrowly define the traffic handled by resource-intensive rules. Focused rules are also important because rules with broad conditions can match many different types of traffic, and can preempt later, more specific rules. Examples of resource-intensive rules include:

- TLS/SSL rules that decrypt traffic—Not only the decryption, but further analysis of the decrypted traffic, requires resources. Narrow focus, and where possible, block or choose not to decrypt encrypted traffic.

Certain Firewall Threat Defense models perform TLS/SSL encryption and decryption in hardware, which improves performance significantly. For more information, refer to TLS crypto acceleration, on page 1720.

- Access control rules that invoke deep inspection—Intrusion, file, and malware inspection requires resources, especially if you use multiple custom intrusion policies and variable sets. Make sure you only invoke deep inspection where required.
- If you specify security zones in a rule, the rule is deployed only to devices that have interfaces in the specified zone. So, if you want to focus a rule on only some devices that are assigned to the policy, ensure that you select a security zone that applies to the appropriate subset of devices. This ensures that unnecessary rules are not deployed to a device.

Maximum number of access control rules and intrusion policies

The maximum number of access control rules or intrusion policies that are supported by a device depends on many factors, including policy complexity, physical memory, and the number of processors on the device.

If you exceed the maximum supported by a device, you cannot deploy the access control policy and you must reevaluate.

Guidelines for intrusion policies

Consider these guidelines when configuring intrusion policies:

- In an access control policy, you can associate one intrusion policy with each Allow and Interactive Block rule, as well as with the default action. Every unique **pair** of intrusion policy and variable set counts as one policy.
- You may want to consolidate intrusion policies or variable sets so you can associate a single intrusion policy-variable set pair with multiple access control rules. On some devices you may find you can use only a single variable set for all your intrusion policies, or even a single intrusion policy-variable set pair for the whole device.

Access control rule management

Access control rule management is a security administration process that involves procedures for creating, modifying, and maintaining access control rules.

These topics explain how to manage access control rules.

Add an access control rule category

Categories help organize rules into logical groups so you can understand and manage your policy more easily.

You can divide an access control policy's **Mandatory** and **Default** rule sections into custom categories. After you create a category, you cannot move it, although you can delete it, rename it, and move rules into, out of, within, and around it. The Firewall Management Center assigns rule numbers across sections and categories.

Procedure

Step 1 In the access control policy editor, click **Add Category**.

If your policy already contains rules, you can click a blank area in the row for an existing rule to set the position of the new category before you add it. You can also right-click an existing rule and select **Insert new category**.

Step 2 Enter a **Name**.

Step 3 From the **Insert** drop-down list, choose where you want to add the category:

- To insert a category below all existing categories in a section, choose **into Mandatory** or **into Default**.
- To insert a category above an existing category, choose **above category**, then choose a category.
- To insert a category above or below an access control rule, choose **above rule** or **below rule**, then enter an existing rule number.

Step 4 Click **Apply**.

Step 5 Click **Save** to save the policy.

What to do next

You can now:

- Drag and drop rules into, or out of, the category.
- When creating a rule, select a category it should be part of.
- When editing a rule, reposition the rule to be in the category, or to move it out of the category.

Create and edit access control rules

Use access control rules to apply actions to specific traffic classes. Rules allow you to selectively allow desirable traffic and drop unwanted traffic.

Procedure

Step 1 In the access control policy editor, you have the following options:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click **Edit** ( ).
- To start with a copy of an existing rule, choose one of the following commands from the **More** ( ) menu.
  - **Copy Rule**, to copy the rule to the clipboard, so you can use the **Paste Above/Below** commands to place it anywhere in the same policy.

- **Copy Rule to Different Policy**, to copy the rule to another access control policy. A dialog box opens so that you can select the policy and chose the rule placement.
- **Clone Rule**, to create the copy immediately below the duplicated rule.

- To edit multiple rules, use the checkboxes to select multiple rules, then select **Edit** or another action from the **Select Action/Bulk Rule Actions** list next to the search box.
- To do inline editing, where you change the configuration of an object in a rule condition, right-click the value and choose **Edit**. You can also use the right-click menu to remove a item, add it to the filter, or copy the text or value.

If **View** ( ) appears next to a rule instead, the rule belongs to an ancestor policy, or you do not have permission to modify the rule.

Step 2 If this is a new rule, enter a **Name**.

Step 3 Configure the rule components.

If you are bulk-editing multiple rules, only a subset of options are available.

Table 96: Access control rule components

Rule component	Configuration description
Position	Specify the rule position (**Insert** for new rules, the **Reposition** icon next to the rule name for existing rules); see Access control rule order, on page 1613.
Action	Choose a rule **Action**; see Access control rule actions, on page 1614.
Logging	Click **Logging** to specify options for connection logging and SNMP traps. See *Best Practices for Connection Logging* in the *Cisco Secure Firewall Management Center Administration Guide* for more information.
Time Range	(Optional.) For Firewall Threat Defense devices, choose the days and times when the rule is applicable. If you do not choose an option, the rule is always active. For details, see Create a time range object, on page 2435.
Enable Rule	Whether the rule is active. Disabled rules are not applied to connections. You can disable rules to temporarily turn them off, for example, during troubleshooting.
Security Protections (Deep inspection)	(Optional.) For Allow and Interactive Block rules, select options for **Intrusion Policy**, **Variable Set**, and **File Policy**. You can apply intrusion and file policies independently; you do not need to configure both.
Conditions	Select the objects you want to add to either source or destination, then click either **Add to Sources** or **Add to Destinations and Applications** to add matching conditions for connections. You can click a tab to restrict the list of available objects, for example, to Networks, Security Zones, Applications, and so forth. However, the sources and destination column always show all selected objects regardless of the tab you are on. See Access control rule conditions, on page 1633 for more information.
Comments	Open the comments list at the bottom of the dialog box, enter your comment, and click **Add Comment/Post** to add a comment.

Step 4 Click **Add** or **Apply** to save the rule.

Step 5 Click **Save** to save the policy.

What to do next

If you will deploy time-based rules, specify the time zone of the device to which the policy is assigned. See Configure a time zone for a device, on page 911.

Deploy configuration changes; see Deploy configuration changes, on page 135.

Related Topics

Best practices for access control rules, on page 1625

Access control rule conditions

Access control rule conditions are traffic matching criteria that define the characteristics of the connections you want to target with each rule. Use the conditions precisely to fine-tune the rule to apply to all, and only, the traffic that should be handled by the rule. The following topics explain the match conditions that you can use.

Security/tunnel zone rule conditions

Security/tunnel zone rule conditions are traffic matching mechanisms that

- use security zones and tunnel zones to select traffic for a rule
- segment your network to help you manage and classify traffic flow by grouping interfaces across multiple devices
- allow you to identify tunneled traffic, such as GRE, that should be handled as a tunnel rather than apply access control rules to the encapsulated connections within the tunnel.

You can use security zones to control traffic by its source and destination interfaces. If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones for it to match the rule. Just as all interfaces in a security zone must be of the same type (all inline, passive, switched, or routed), all zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

When using tunnel zones, ensure that you have matching rules in the prefilter policy to associate tunneled traffic with the zone. Then, you can select the tunnel zone as a source zone in a rule; tunnel zones cannot be destinations. If you do not have prefilter rules to rezone the tunnels into the tunnel zone, an access control rule for the tunnel will never apply to any connections. You can specify destination security zones to target tunnels that leave the device through specific interfaces.

Security zone considerations

Consider the following when deciding on security zone criteria:

- Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

- Access control rules generate ACL entries (ACEs) in the device configuration to provide early processing and drops whenever possible. If you specify security zones in rules, ACEs are created for each interface in the zone, which can greatly increase the size of the ACL. Excessively large ACLs generated from access control rules can impact system performance.

Network rule conditions

Network rule conditions are the network objects or geographical locations that define the network addresses or locations of the traffic.

Network criteria selection

- To match traffic from an IP address or geographical location, add the criteria to the Sources list.
- To match traffic to an IP address or geographical location, add the criteria to the Destinations list.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from these tabs:

- **Network**—Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control.

  Whenever possible, combine multiple network objects into a single object group. The system automatically creates an object group (during deployment) when you select more than one object (for source or destination separately). Selecting existing groups can avoid object group duplication and reduce the potential impact on CPU usage when there are a large number of duplicate objects.

  You can use objects that define the address using the fully-qualified domain name (FQDN); the address is determined through a DNS lookup. However, FQDN objects are not supported in these sections in access control policies: original client networks, SGT/ISE attributes, network analysis and intrusion policy, Security Intelligence, threat detection, elephant flow settings.

- **Geolocation**—Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent. Besides selecting geographical location directly in the rule, you can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.



Note To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB).

Traffic matching configuration:

- To match traffic from an IP address or geographical location, add the criteria to the Sources list.
- To match traffic to an IP address or geographical location, add the criteria to the Destinations list.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

Original client in network conditions (filtering proxied traffic)

For some rules, you can handle proxied traffic based on the originating client. Use a source network condition to specify proxy servers, then add an original client constraint to specify original client IP addresses. The system uses a packet's X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header field to determine original client IP.

Traffic matches the rule if the proxy's IP address matches the rule's source network constraint, and the original client's IP address matches the rule's original client constraint. For example, to allow traffic from a specific original client address, but only if it uses a specific proxy, create three access control rules:

Access Control Rule 1: Blocks proxied traffic from a specific IP address (209.165.201.1)

Source Networks: 209.165.201.1
Original Client Networks: none/any
Action: Block

Access Control Rule 2: Allows proxied traffic from the same IP address, but only if the proxy server for that traffic is one you choose (209.165.200.225 or 209.165.200.238)

Source Networks: 209.165.200.225 and 209.165.200.238
Original Client Networks: 209.165.201.1
Action: Allow

Access Control Rule 3: Blocks proxied traffic from the same IP address if it uses any other proxy server.

Source Networks: any
Original Client Networks: 209.165.201.1
Action: Block

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details



Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:

- Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
- Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

User rule conditions

A user rule condition is a traffic matching mechanism that

- matches traffic based on whether the user initiating the connection or the group to which they belong
- can be configured for users in Microsoft Active Directory realms only, and
- enables policy enforcement based on user identity and group membership.

Special identities users

In addition to configuring users and groups for configured realms, you can set policies for the special identities users:

- Failed Authentication: User who failed authentication with the captive portal.
- Guest: Users configured as guest users in the captive portal.
- No Authentication Required: Users that match an identity **No Authentication Required** rule action.
- Unknown: Users that cannot be identified such as users who are not downloaded by a configured realm.

For access control rules only, you must first associate an identity policy with the access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

User rule condition example

Configure a Block rule to prohibit anyone in the Finance group from accessing a network resource.

Application rule conditions

Application rule conditions are application awareness and control mechanisms that

- identify and classify applications through IP traffic analysis
- enable control with organized filters
- require one enabled detector for each condition.

Application filters and control benefits

System-provided *application filters* help perform control by organizing applications according to basic characteristics, such as type, risk, business relevance, category, and tags. You can also create reuseable, user-defined filters using combinations of system-provided filters, or custom combinations of applications.

At least one detector must be enabled for each application rule condition in the policy. If no detector is enabled, the system automatically enables all available system-provided detectors, or the most recently modified user-defined detector. For more information about application detectors, see Application detectors, on page 2284.

You can utilize both application filters and individually specified applications to ensure complete coverage. Understand the application's requirements to effectively order access control rules.

Application filters help you to quickly configure application control effectively. For example, you can easily use system-provided filters to create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the system blocks the session.

Using application filters simplifies policy creation and administration. It assures you that the system controls application traffic as expected. Because Cisco frequently updates and adds application detectors via system and vulnerability database (VDB) updates, you can ensure that the system uses up-to-date detectors to monitor application traffic. You can also create your own detectors and assign characteristics to the applications they detect, automatically adding them to existing filters.

The system characterizes detected applications using several criteria which form effective filters.

Table 97: Application characteristics

Characteristic	Description	Example
Type	Application protocols represent communications between hosts. Clients represent software running on a host. Web applications represent the content or requested URL for HTTP traffic.	HTTP and SSH are application protocols. Web browsers and email applications are clients. MPEG video and Facebook are web applications.
Risk	The likelihood that the application is being used for purposes that might be against your organization's security policy.	Peer-to-peer applications tend to have a very high risk.
Business Relevance	The likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally.	Gaming applications tend to have a very low business relevance.
Category	A general classification for the application that describes its most essential function. Each application belongs to at least one category.	Facebook is in the social networking category.
Tag	Additional information about the application. Applications can have any number of tags, including none.	Video streaming web applications often are tagged `high bandwidth` and `displays ads`.

Configure application conditions and filters

To build an application condition or filter, choose the applications whose traffic you want to control from a list of available applications. It is recommended that you constrain the available applications using filters. You can use filters and individually specified applications in the same condition.

Before you begin

- Adaptive profiling must be enabled (its default state) in the access control policy's advanced settings for access control rules to perform application control.

Follow these steps to configure application conditions and filters:

Procedure

Step 1 In the access policy rule editor, click **Applications**.

Step 2 Find and choose the applications you want to add from the **Available Applications** list.

To constrain the applications displayed in **Available Applications**, choose one or more **Application Filters** or search for individual applications.

Tip Click **Information** ( ) next to an application to display summary information and internet search links. A **lock** icon marks applications that the system can identify only in decrypted traffic.

When you choose filters, singly or in combination, the Available Applications list updates to display only the applications that meet your criteria. You can choose system-provided filters in combination, but not user-defined filters.

- Multiple filters for the same characteristic (risk, business relevance, and so on)—Application traffic must match only one of the filters. For example, if you choose both the medium and high-risk filters, the Available Applications list displays all medium and high-risk applications.
- Filters for different application characteristics—Application traffic must match both filter types. For example, if you choose both the high-risk and low business relevance filters, the Available Applications list displays only applications that meet both criteria.

Step 3 Click **Add Application** or **Add to Rule**, or drag and drop.

Tip Before you add more filters and applications, click **Clear Filters/Selection** to clear your current choices.

Step 4 Save or continue editing the rule or configuration.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

Port, protocol, and ICMP code rule conditions (concept)

A port, protocol, and ICMP code rule condition is a traffic matching criterion that

- matches traffic based on source and destination ports
- supports TCP, UDP, ICMP, and other protocols that do not use ports, and
- controls traffic flow in access control and other policy rules.

Port condition types

Port conditions match traffic based on the source and destination ports. Depending on the rule type, "port" can represent any of these types:

- TCP and UDP—Control TCP and UDP traffic based on the port. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP (6) /22.
- ICMP—Control ICMP and ICMPv6 (IPv6-ICMP) traffic based on its internet layer protocol plus an optional type and code. For example: ICMP(1):3:3.
- Protocol—Control traffic using other protocols that do not use ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Best practices for port-based rules

Specifying ports is the traditional method used to target applications. However, applications can be configured to use unique ports to bypass access control blocks. Use application filtering criteria when possible; however, note that application filtering is unavailable in prefilter rules.

Use application filtering for FTP and similar applications that open separate channels for control and data flow. Using port-based access control rules can prevent these kinds of applications from performing correctly and could result in blocking desirable connections.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as destination port conditions in a single access control rule.

Matching non-TCP traffic with port conditions

You can match non-port-based protocols. By default, if you do not specify a port condition, you are matching IP traffic. Although configuring port conditions can match non-TCP traffic, restrictions apply:

- Access control rules—For Classic devices, match GRE-encapsulated traffic with an access control rule by using the GRE (47) protocol as a destination port condition. To a GRE-constrained rule, add only network-based conditions: zone, IP address, port, and VLAN tag. The system uses outer headers to match **all** traffic in access control policies with GRE-constrained rules. For Firewall Threat Defense devices, use tunnel rules in the prefilter policy to control GRE-encapsulated traffic.

- Decryption rules—These rules support only TCP port conditions.
- IMCP echo—A destination ICMP port with the type set to 0 or a destination ICMPv6 port with the type set to 129 only matches unsolicited echo replies. ICMP echo replies, sent in response to ICMP echo requests, are ignored. To match any ICMP echo, use ICMP type 8 or ICMPv6 type 128.

Recommendation: use URL conditions for website access control

Use URL conditions to control the websites that users on your network can access.

For complete information, see URL filtering with category and reputation, on page 1652.

Dynamic attributes rule conditions

Dynamic attributes rule conditions allow you to specify access control rules based on real-time properties such as network objects, device types, locations, and security tags. Dynamic attributes can be used as source criteria and destination criteria in access control rules. These criteria help match traffic more flexibly and accurately.

Dynamic attributes configuration and behavior

You can use these types of dynamic attributes to match connections in DNS rules:

- Dynamic objects (Source or destination): The dynamic attributes connector collects data such as networks and IP addresses from cloud providers for use in access control rules. For more information, refer to About the dynamic attributes connector , on page 2061 .
- SGT objects (Source only): These contain tags defined manually or in Cisco ISE. For more information, refer to Source and destination security group tag (SGT) matching, on page 1912 and Security group tags, on page 2376 .
- Location IP objects (Source only): Defined by Cisco ISE.
- Device type objects (Source only): Defined by Cisco ISE, also referred to as endpoint profile objects.

When you configure dynamic attributes for a DNS rule, objects of the same type within a source or destination list use OR logic, while objects of different types use AND logic. For example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

When you open the **Dynamic Attributes** tab, all **Dynamic Objects** and **Security Group Tags** appear in the list. To remove objects from the list, deselect the options. To find an object, type in the search box.

Time and Day Rule Conditions

You can specify a continuous time range or a recurring time period.

For example, a rule can apply only during weekday working hours, or every weekend, or during a holiday shutdown period.

Time-based rules are applied based on the local time of the device that processes the traffic.

Time-based rules are supported only on Firewall Threat Defense devices. If you assign a policy with a time-based rule to a different type of device, the time restriction associated with the rule is ignored on that device. You will see warnings in this case.

Enable and disable access control rules

Enable or disable access control rules to control whether they are used to evaluate network traffic.

When you create an access control rule, it is enabled by default. If you disable a rule, the system does not use it to evaluate network traffic and stops generating warnings and errors for that rule. When viewing rules in an access control policy, disabled rules are grayed out but can still be modified. You can also change a rule's status in the rule editor.

Procedure

Step 1 In the access control policy editor, right-click the rule you want to change and choose a rule state.

If **View** ( ) appears next to a rule instead, the rule belongs to an ancestor policy, or you do not have permission to modify the rule.

Step 2 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Copy access control rules from one access control policy to another

You can copy access control rules from one access control policy to another. You can copy the rules either to the **Default** section or the **Mandatory** section of the access control policy.

All the settings of the copied rules, except the comments, are retained in the pasted version

Procedure

Step 1 Do one of the following:

- To copy a single rule, right-click the rule and select **Copy Rule to Different Policy**.
- To copy multiple rules, select their checkboxes, then select **Copy Rules to Different Policy** from the **Select Bulk Action** menu.

Step 2 Select the destination access control policy from the **Access Policy** drop-down list.

Step 3 From the **Place Rules** drop-down list, choose where you want to position the copied rules. You can place them at the bottom of either the Mandatory or Default sections.

Step 4 Click **Copy**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Move access control rules to a prefilter policy

You can move access control rules from an access control policy to the associated non-default prefilter policy.

You must first apply a user-defined prefilter policy to the access control policy. The access control rules cannot be moved to the default prefilter policy because the default prefilter policy cannot have rules.

Before you begin

Note these conditions before you proceed:

- When moving an access control rule to a prefilter policy the layer 7 (L7) parameters, such as application or URL filterin, in the access control rule cannot be moved. The L7 parameters are dropped during the operation.
- The comments in the access control rule configuration are lost after moving the rule. However, a new comment is added in the moved rule mentioning the source access control policy.
- You cannot move access control rules with **Monitor** set as the **Action** parameter.
- The **Action** parameter in the access control rule is changed to a suitable action in the prefilter rule when moved. To know what each action in the access control rule maps to, see this table:

Action in the access control rule	Action in the prefilter rule
Allow	Analyze
Block	Block
Block with reset	Block
Interactive Block	Block
Interactive Block with reset	Block
Trust	Fastpath

- Similarly, based on the action configured in the access control rule, the logging configuration is set to an appropriate setting after the rule is moved, as mentioned in this table.

Action in the access control rule	Enabled logging configurations in the prefilter rule
Allow	None of the check boxes are checked.
Block Block with reset Interactive Block Interactive Block with reset	• Log at Beginning of Connection • Event Viewer • Syslog Server • SNMP Trap

Action in the access control rule	Enabled logging configurations in the prefilter rule
Trust	• Log at Beginning of Connection • Log at End of Connection • Event Viewer • Syslog Server • SNMP Trap

- While moving rules from the source policy, if another user modifies those rules, you will see get a message. You may continue with the process after refreshing the page.

Procedure

Step 1 Do one of the options:

- To move a single rule, right-click the rule and select **Move Rule to Prefilter Policy**.
- To move multiple rules, select their checkboxes, then select **Move Rules to Prefilter Policy** from the **Select Bulk Action** menu.

Step 2 From the **Place Rules** drop-down list, choose where you want to position the moved rules, either **At the bottom** or **At the top**.

Step 3 Click **Move**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Position an access control rule

Position rules correctly within an access control policy to ensure the first match wins behavior produces the intended security outcomes.

You can move an existing rule within an access control policy, or insert new rules in a desired location. When you add or move a rule to a category, the system places it last in the category.

Before you begin

Review rule order guidelines in Best practices for access control rules, on page 1625.

Procedure

Step 1 Do one of these:

- New rule—Insert a new rule by hovering over the line between the existing rules, and clicking **Add Rule**. The location is selected in the **Insert** box in the Add Rule dialog box; you can select a different rule to adjust the location. You can also select **Add Rule Above** or **Add Rule Below** from the right-click menu.
- Existing rules when viewing the rule table—Click and drag the rule to the new position. This action is final, you are not prompted to confirm it.
- Existing rules when viewing the rule table—Right-click a single rule and select **Reposition Rule**. To move multiple rules as a group, select their checkboxes, then select **Reposition Rules** from the **Select Bulk Action** menu. You are prompted for where you want the rule to go.
- Existing rule when editing the rule—Click the **Reposition Rule** icon next to the rule name.

Step 2 When editing or repositioning the rule, choose where you want to move or insert the rule, then click **Move**, **Confirm**, or **Reposition** (depending on what you are doing).

- Choose **into Mandatory** or **into Default**.
- Choose a **into Category**, then choose the category.
- Choose **above rule** or **below rule**, then select the rule.

Step 3 Save the rule if you are editing it.

Step 4 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Add comments to an access control rule

Adding comments to access control rules helps you keep track of the purpose of a rule, and changes made to the rule.

When you create or edit an access control rule, you can add a comment. For example, you might summarize the overall configuration for the benefit of other users, or note when you change a rule and the reason for the change. You can display a list of all comments for a rule along with the user who added each comment and the date the comment was added.

When you save a rule, all comments made since the last save become read-only.

To search access control rule comments, use the **Search Rules** bar on the rule listing page.

Procedure

Step 1 In the access control rule editor, click **Comments**.

Step 2 Enter your comment and click **Add Comment**. You can edit or delete this comment until you save the rule.

Step 3 Save the rule.

Examples for access control rules

These topics provide examples of access control rules.

How to control access using security zones

Configure security zones and access control rules to inspect incoming traffic for intrusions and malware while allowing unrestricted internet access for internal hosts.

Consider a deployment where you want hosts to have unrestricted access to the internet, but you nevertheless want to protect them by inspecting incoming traffic for intrusions and malware.

First, create two security zones: Internal and External. Then, assign interface pairs on one or more devices to those zones, with one interface in each pair in the Internal zone and one in the External zone. Hosts connected to the network on the Internal side represent your protected assets.



Note You are not required to group all internal (or external) interfaces into a single zone. Choose the grouping that makes sense for your deployment and security policies.

Then, configure an access control rule with a destination zone condition set to Internal. This simple rule matches traffic that leaves the device from any interface in the Internal zone. To inspect matching traffic for intrusions and malware, choose a rule action of **Allow** , then associate the rule with an intrusion and a file policy.

Control application usage

Block web-based applications, particularly anonymizers or proxies, by creating access control rules that identify and restrict traffic based on application attributes

Enterprise networks increasingly rely on web-based delivery platforms and rich media applications, often using the same web protocols. Firewall Threat Defense inspects connections to determine the application, enabling access control rules targeting applications rather than just targeting specific TCP/UDP ports.

Although you can select specific applications to allow or block, you can also write rules based on type, category, tag, risk, or business relevance. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

In this use case, we will block any application that belongs to the **anonymizer/proxy** category.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control** and edit the access control policy.

Step 2 Click **Add Rule** and configure the rule for application control.

a) Name the rule (for example, Block_Anonymizers).

b) For **Action**, select **Block**.

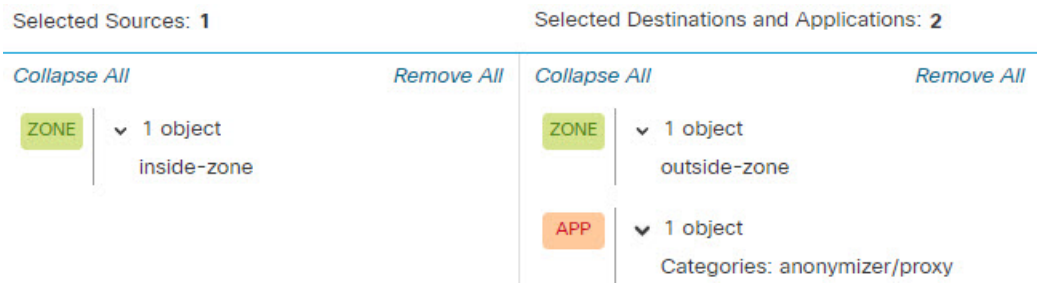


c) If you have configured security zones and want to restrict traffic from inside to outside, click the **Zones** tab, and choose your inside zone as the source zone, and the outside zone as the destination zone.

d) Click the **Applications** tab, select the applications to match, and click **Add Application**.

As you select criteria, such as category and risk level, the list to the right of the criteria updates to show exactly which applications match the criteria. The rule you are writing applies to these applications.

For purposes of this example, choose **anonymizers/proxy** from the **Categories** list and add it to **Destinations and Applications**. The match criteria should now look similar to the following graphic.



e) Click **Logging** next to the rule action, and enable logging at the start of the connection. You can select a syslog server if you use one.

You must enable logging to get information about any connections blocked by this rule.

Step 3 Move the rule so that it comes after any rules that use protocol and port criteria only, but that would not allow traffic that should be blocked by the application rule.

Matching applications requires Snort inspection. Because Snort inspection is not needed by rules that use protocol and port only, you can improve system performance by grouping these simple rules at the top of the access control policy as much as possible.

Step 4 Deploy the changes.

You can use the application rule hit counts and analysis dashboards to see how this rule is performing and how often users try these applications.

Block threats

You can implement next generation Intrusion Prevention System (IPS) filtering by adding intrusion policies to your access control rules. Intrusion policies analyze network traffic, comparing the traffic contents against known threats. If a connection matches a threat you are monitoring, the system drops the connection, thus preventing the attack.

All other traffic handling occurs before network traffic is examined for intrusions. By associating an intrusion policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy.

You can configure intrusion policies on rules that **allow** traffic only. Inspection is not performed on rules set to **trust** or **block** traffic. In addition, you can configure an intrusion policy as the default action if you do not want to use a simple block.

Security Intelligence policies allow you to preemptively block traffic to or from known bad IP addresses and URLs. This task demonstrates how to add an intrusion policy that allows traffic from the internal 192.168.1.0/24 network to external destinations, assuming block rules exist to eliminate unwanted connections, and adds Security Intelligence to block known threats.

Before you begin

- Apply the IPS license to any managed device that uses this rule.
- Ensure you have created security zones for inside and outside interfaces.
- Create the network object for the inside network.

Procedure

Step 1 Create the access control rule that applies the intrusion policy.

a) Edit the access control policy and add a new rule.

b) Name the rule (for example, Inside_Outside) and set the rule action to **Allow**.



c) Choose **Balanced Security and Connectivity** as the **Intrusion Policy**. You can either accept the default variable set or select your own if you want to customize it.

The **Balanced Security and Connectivity** policy is appropriate for most networks. It provides a good intrusion defense without being overly aggressive, which has the potential of dropping traffic that you might not want to be dropped. If you determine that too much traffic is getting dropped, you can ease up on intrusion inspection by selecting the **Connectivity over Security** policy.

If you need to be aggressive about security, try the **Security over Connectivity** policy. The **Maximum Detection** policy offers even more emphasis on network infrastructure security with the potential for even greater operational impact.

If you create your own custom policy, you can select that one instead.

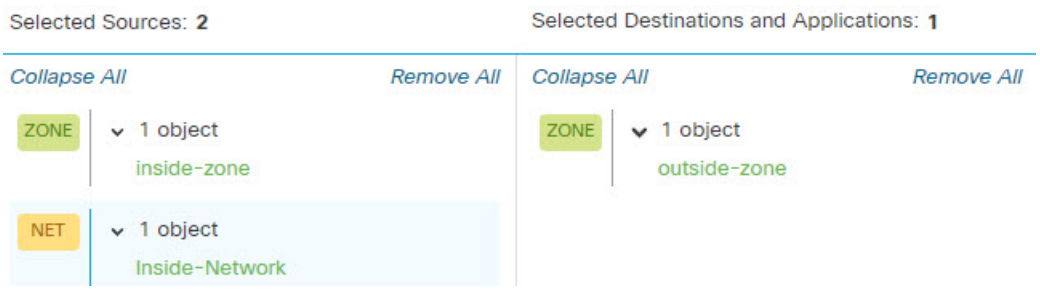
A discussion of variable sets is beyond the scope of this example. Please read the chapters on intrusion policy for detailed information about variable sets and custom policies.



d) Select the **Zones** tab, and add your inside security zone to the source criteria, and outside zone to the destination criteria.

e) Select the **Networks** tab, and add the network object that defines your inside network to the source criteria.

The match criteria should look similar to the following:



f) Click **Logging** and enable logging at the beginning or end of the connection, or both, as desired.
g) Click **Apply** to save the rule, and then **Save** to save the updated policy.
h) Move the rule to the appropriate location in the access control policy.

Step 2 Configure the Security Intelligence policy to preemptively drop connections with known bad hosts and sites.

By using Security Intelligence to block connections with hosts or sites that are known to be threats, you save your system the time needed to do deep packet inspection to identify threats in each connection. Security Intelligence provides an early block of undesirable traffic, leaving more system time to handle the traffic you really care about.

a) While editing the access control policy, click the **Security Intelligence** link in the packet path.

The link includes two policies: the DNS policy at the top, and the Security Intelligence (Network and URL) at the bottom. In this example, we are configuring the Network and URL lists. By default, these lists already include the global block and do not block lists, but these lists are empty by default until you add items to them.

b) With **Networks** selected and the **Any** security zone selected, scroll down in the Networks list until you get to the global feeds, and the first Security Intelligence category (probably Attackers). Click Attackers, then scroll to the end of the categories (probably Tor_exit_node), and Shift+Click to select all of the categories. Click **Add To Block List**.
c) Select the **URL** tab, and **Any** security zone, and use Shift+Click to select URL versions of the same categories. Click **Add To Block List**.
d) Click **Save** to save the policy.
e) As necessary, you can add network and URL objects to the block or do not block lists.

The **Do Not Block** lists are not real "allow" lists. They are exception lists. If an address or URL in the exception list also appears in the blocked list, the connection for the address or URL is allowed to pass on to the access control policy.

This way, you can block a feed, but if you later find that a desirable address or site is being blocked, you can use the exception list to override that block without needing to remove the feed entirely.

Keep in mind that these connections are subsequently evaluated by access control, and if configured, an intrusion policy. Thus, if any connections do contain threats, they can be identified and blocked during intrusion inspection.

Use the events and dashboards to determine what traffic is actually being dropped by the policy, and whether you need to add addresses or URLs to the **Do Not Block** lists.

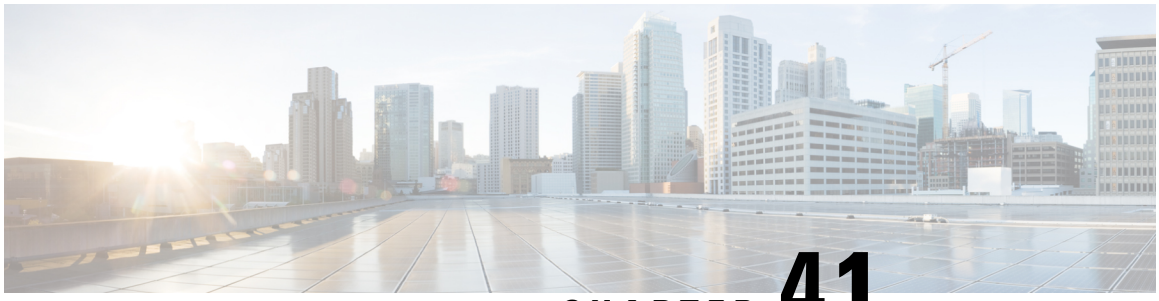
Step 3 Deploy your changes.

History for access control rules

This history table provides a summary of feature changes by release for the access control policy rules.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Maximum objects per match criteria per access control rule is 200.	7.3	Any	Previously, you could have a maximum of 50 objects per match criteria in a single access control rule. For example, you could have up to 50 network objects in a single access control rule. The limit is now 200 objects per match criteria in a single rule. We updated the access control policy to allow the increased object limit.
Search for access control rule comments	6.7	Any	The **Search Rules** bar now offers the option to search for comments. New/modified pages: Access control rules page, **Search Rules** text entry field. Supported platforms: Firewall Management Center
Copy or move rules between access control and prefilter policies	6.7	Any	You can copy access control rules from one access control policy to another. You can also move access control rules from an access control policy to the associated prefilter policy. New/modified pages: Access control policy page; the right-click menu for the selected rules provides additional options to copy and move. Supported platforms: Firewall Management Center
Bulk edit of certain settings in access control rules	6.6	Any	In the list of rules in a policy, shift-click or control-click to select multiple rules, then right-click and choose an option. Example bulk operations: You can enable or disable the rules, select a rule action, and edit most inspection and logging settings. New/modified pages: Access control rules page. Supported platforms: Firewall Management Center
Enhanced searching on configured rules	6.6	Any	Enhanced searching on configured rules. New/modified pages: Access control rules page. Supported platforms: Firewall Management Center

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Time ranges for rule application	6.6	Any	Ability to specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic. New/modified pages: • A new option on the access control Add Rule page. • A related new option on the **Devices** > **Platform Settings** > **Threat Defense** page to specify time zones for managed devices. Supported platforms: Firewall Threat Defense devices only
View object details from access control rule pages	pre-6.6	Any	To see information about an object in a list of rules or from the rule configuration dialog, right-click the object. New/modified pages: **Policies** > **Access Control** > **Access control**, and **Add Rule** page. Supported platforms: Firewall Management Center



CHAPTER 41

URL Filtering Rules

You can implement URL filtering using access control rules.

- URL filtering, on page 1651
- Best practices for URL filtering, on page 1654
- License requirements for URL filtering, on page 1659
- Requirements and prerequisites for URL filtering, on page 1660
- Configure URL filtering with category and reputation, on page 1660
- Manual URL filtering, on page 1667
- HTTP response pages, on page 1669
- Configure URL filtering health monitors, on page 1673
- Dispute URL category and reputation, on page 1673
- Take action if the URL category set changes, on page 1674
- Troubleshoot URL filtering, on page 1676
- History for URL filtering, on page 1678

URL filtering

URL filtering is a security feature that

- controls the websites that users on your network can access,
- provides category and reputation-based filtering with a URL Filtering license, and
- enables manual specification of individual URLs, groups of URLs, and URL lists with any license.

URL filtering types

Use URL filtering to control website access through these methods:

- Category and reputation-based URL filtering—With a URL Filtering license, you can control access to websites based on the URL's general classification (category) and risk level (reputation). This is the recommended option.
- Manual URL filtering—With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. For more information, see Manual URL filtering, on page 1667.

See also Security Intelligence, on page 1595, a similar but different feature for blocking malicious URLs, domains, and IP addresses.

The URL filtering feature is applicable only when you use a web browser to browse websites via the HTTP/HTTPS protocol. For other applications, you must use an FQDN-based access control rule instead of URL filtering. See Access Control Rules for more information.

URL filtering with category and reputation

URL filtering with category and reputation is a web security mechanism that

- controls access to websites based on the category and reputation of requested URLs,
- uses category classifications to group URLs by type (for example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category),
- assesses reputation levels from Unknown risk (level 0) or Untrusted (level 1) to Trusted (level 5) to determine how likely the URL is to be used for purposes that might be against the security policy for your organization, and
- allows URLs to belong to multiple categories simultaneously.

Reputation is determined by the hostname, e.g. all pages on www.cisco.com are considered to have the same reputation.

Benefits of category and reputation-based URL filtering

URL categories and reputations help you quickly configure URL filtering. For example, you can use access control to block untrusted URLs in the Hacking category. You can also use QoS to limit the rate of traffic from sites in the Streaming Video category. There are also categories for types of threats, such as a Spyware and Adware category.

Using category and reputation data simplifies policy creation and administration. It grants you assurance that the system controls web traffic as expected. Because Cisco continually updates its threat intelligence with new URLs, as well as new categories and risk levels for existing URLs, the system uses up-to-date information to filter requested URLs. Sites that (for example) represent security threats, or serve undesirable content may appear and disappear faster than you can update and deploy new policies.

These examples show how the system can adapt:

- If an access control rule blocks all gaming sites, as new domains are registered and classified as Games, the system can block those sites automatically. Similarly, if a QoS rule rate-limits traffic from all streaming video sites, the system can automatically limit traffic to new streaming video sites.
- If an access control rule blocks all malware sites and a shopping page gets infected with malware, the system can recategorize the URL from Shopping to Malware Sites and block that site.
- If an access control rule blocks untrusted social networking sites and somebody posts a link on their profile page that contains links to malicious payloads, the system can change the reputation of that page from Favorable to Untrusted and block it.

Limitations exist for category-based filtering in decryption policy Do Not Decrypt rules.

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from

its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security.

Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control, on page 1622.

For more information, refer to Use categories in URL filtering, on page 1658.

URL category and reputation descriptions

This reference lists URL category and reputation level descriptions for security management.

Category descriptions

You can find a description of each URL category at https://www.talosintelligence.com/categories.

Click **Threat Categories** to view those categories.

Reputation level descriptions

Refer to Web reputation levels for information.

URL filtering data from the Cisco cloud

URL filtering data from the Cisco cloud is a threat intelligence dataset that

- allows traffic handling based on a website's general classification, or *category*, and risk level, or *reputation*,
- is automatically enabled when a URL Filtering license is added, and
- provides real-time threat intelligence evaluation for websites not found in local cache or datasets.

URL filtering data evaluation process

By default, when users browse to a URL whose category and reputation are not in a local cache of previously accessed websites, the system submits it to the cloud for threat intelligence evaluation and adds the result to the cache.

Optionally, you can use a local URL dataset of categories and reputations, which can make web browsing faster. When you enable or re-enable URL filtering, the Firewall Management Center automatically queries Cisco for URL data and pushes the dataset to managed devices. Then, when users browse to an URL, the system checks the local dataset and the cache for category and reputation information before submitting it to the cloud for threat intelligence evaluation. To see your options for using the local dataset, including how to disable individual cloud lookups altogether, see URL filtering options, on page 1662.

Automatic updates of URL data is enabled by default. We strongly recommend that you do not disable these updates.

The set of URL categories may change periodically. When you receive a change notification, review your URL filtering configurations to make sure traffic is handled as expected. For more information, see Take action if the URL category set changes, on page 1674.

Best practices for URL filtering

Filter by category and reputation

Follow the instructions in Configure URL filtering with category and reputation, on page 1660.

Configure your policy to inspect packets that must pass before a URL can be identified

The system cannot filter URLs before:

- A monitored connection is established between a client and server.
- The system identifies the DNS, HTTP or HTTPS application in the session.
- The system identifies the requested domain or URL (for encrypted sessions, from a non-encrypted domain name, the ClientHello message or the server certificate).

This identification should occur within three to five packets, or after the server certificate exchange in the TLS/SSL handshake if the traffic is encrypted.

Important! To ensure that your system examines these initial packets that would otherwise pass, see Inspection of packets that pass before traffic is identified and subtopics.

If early traffic matches all other rule conditions but identification is incomplete, the system allows the packet to pass and the connection to be established (or the TLS/SSL handshake to complete). After the system completes its identification, the system applies the appropriate rule action to the remaining session traffic.

Block threat categories

Be sure that your policies specifically address Threat categories, which identify known malicious sites. Do this in addition to blocking sites with poor reputations.

For example, to protect your network from malicious sites, you must block all Threat categories. Additionally, Talos recommends that you block only sites with Poor category. You can block questionable reputations if you have an aggressive security posture, but this may result in a higher amount of false positives.

For specifics, see **Threat Categories** at the URL in URL category and reputation descriptions, on page 1653.

Position URL rules properly and consider rule order

Position URL rules after all other rules that *must* be hit.

URLs can belong to more than one category. It is possible to want to allow one category of websites and block another—whether explicitly or by relying on the default action. In this case, make sure you create and order URL rules so you get the desired effect, depending on whether the allow or the block should take precedence.

For additional guidelines for rules, see the following topics: Best practices for access control rules, on page 1625.

Handle uncategorized or reputationless URLs appropriately

When you build a URL rule, you first choose the category you want to match. If you explicitly choose **Uncategorized** URLs, you cannot further constrain by reputation.

Uncategorized URLs with Untrusted reputation are handled by the **Malicious Sites** category. If you want to block uncategorized sites with any other reputation level (such as Questionable), you must block all uncategorized sites.

After selecting a category and a reputation level, you can optionally select **Apply to unknown reputation**. For example, you can create a rule that applies to sites with Untrusted, Questionable, and unknown reputations.

You cannot manually assign categories and reputations to URLs, but in access control and QoS policies, you can manually block specific URLs. See Manual URL filtering, on page 1667. See also Dispute URL category and reputation, on page 1673.

URL filtering for encrypted web traffic

When performing URL filtering on encrypted web traffic, the system:

- (If DNS filtering is enabled) Checks to see if the system has previously seen the originating domain or the domain is in the local reputation database, and if so, takes action based on the reputation and category of the domain. Otherwise, the system processes the traffic based on your configurations for encrypted traffic, even if **Retry URL cache miss lookup** is enabled in the access control policy's advanced settings.
- Disregards the encryption protocol; a rule matches both HTTPS and HTTP traffic if the rule has a URL condition but not an application condition that specifies the protocol.
- Does not use URL lists. You must use URL objects and groups instead.
- Matches HTTPS traffic based on the subject common name in the public key certificate used to encrypt the traffic, and also evaluates the reputation of any other URLs presented at any time during the transaction, including the post-decryption HTTP URL.
- Disregards subdomains within the subject common name.
- Does not display an HTTP response page for encrypted connections blocked by access control rules (or any other configuration); see Limitations to HTTP response pages, on page 1669.

URL filtering and TLS server identity discovery considerations

The latest version of the Transport Layer Security (TLS) protocol 1.3, defined by RFC 8446, is the preferred protocol for many web servers to provide secure communications. Because the TLS 1.3 protocol encrypts the server's certificate for additional security, and the certificate is needed to match application and URL filtering criteria in access control rules, the Firepower System provides a way to extract the server certificate *without* decrypting the entire packet.

Access control policy advanced settings offer an **Early application detection and URL categorization** option for TLS Server Identity Discovery.

We strongly recommend enabling it for any traffic you want to match on application or URL criteria, especially if you want to perform deep inspection of that traffic. An decryption policy is not required because *traffic is not decrypted* in the process of extracting the server certificate.

Note

- TLS server identity discovery *cannot* be used with any of the following:
  - STARTTLS traffic
  - The HTTP CONNECT method
  - Traffic that is already being decrypted by another device on the network
- Because the certificate is decrypted, TLS server identity discovery can reduce performance depending on the hardware platform.
- TLS server identity discovery is not supported in inline tap mode or passive mode deployments.
- Enabling TLS server identity discovery is supported on any Secure Firewall Threat Defense Virtual version deployed in AWS. TLS server identity is incompatible with certain deployment scenarios that involve Gateway Load Balancer (GWLB). Whether the device initiates a server certificate probe depends on its deployment method with GWLB and the traffic direction.
  - Geneve single-arm flow: The probe *is not initiated* for either east–west or north–south traffic. A connection event **PROBE_FLOW_DROP_BYPASS_PROXY** increments every time the device attempts to extract the server certificate.
  - Geneve dual-arm flow: The probe *is initiated only* for north–south traffic.
- TLS Server Identity Discovery also operates on TLS 1.2 sessions.

For more information, see TLS server identity discovery, on page 2173.

HTTP/2 URL extraction limitations

The system can extract HTTP/2 URLs from TLS certificates, but not from a payload.

Use manual URL filtering effectively

- Specify URLs using a custom Security Intelligence list or feed object. Do not use a URL object or directly enter a URL into the rule. For details, see Manual URL filtering options, on page 1668.
- If you manually filter specific URLs using URL objects or by entering URLs directly into the rule, carefully consider other traffic that might be affected. To determine whether network traffic matches a URL condition, the system performs a simple substring match. If the requested URL matches any part of the string, the URLs are considered to match.
- If you use manual URL filtering to create exceptions to other rules, position the specific rule with the exceptions above the general rule that would otherwise apply.

Search query parameters in URLs are not used for matching

The system does not use search query parameters in the URL to match URL conditions. For example, consider a scenario where you block all shopping traffic. In that case, using a web search to search for amazon.com is not blocked, but browsing to amazon.com is.

Maintain default access control policy advanced settings

Unless you have good reason to change them, leave these settings on the Advanced tab of your access control policy at their defaults:

- **General Settings**:
  - **Retry URL cache miss lookup**
  - **Enable reputation enforcement on DNS traffic**

For descriptions of these settings, refer to General settings, on page 2172.

Reduce unnecessary usage of connection table space and NAT table slots

Consider a scenario in which URL filtering is enabled and any traffic that does not conform with the URL filtering rules is blocked. In such a scenario, the threat defence device analyses the initial packets in the traffic flow to extract URL information. After analysis, if the flow does not match any URL filtering rules, the flow is blocked. This means that the packets are dropped by the Threat Defense device. However, the associated connection remains in the connection table. This behaviour results in unnecessary use of connection table space and, if NAT is configured, NAT table slots, which can lead to increased consumption of network resources.

There are different ways to prevent this type of scenario. Since most of the traffic will be TCP, you can use the 'block with reset' option for TCP traffic instead of using 'block'. This approach reduces the usage of connection table space and NAT table slots.

URL filtering in high availability deployments

For guidelines for URL filtering with Firewall Management Centers in high availability, see *URL Filtering and Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide* .

Memory limitations for selected device models

Device models with less memory store less URL data locally, and the system may therefore check the cloud more frequently to determine category and reputation for sites that are not in the local database.

Lower-memory devices include

- Firepower 1010
- Firewall Threat Defense Virtual with 8 GB of RAM

HTTPS traffic filtering

HTTPS traffic filtering is a security mechanism that

- determines the requested URL based on information passed during the TLS/SSL handshake using the subject common name in the public key certificate,
- disregards subdomains within the subject common name, requiring manual filtering to use top-level domains only, and
- does not support URL lists, requiring the use of URL objects and groups instead.

HTTPS filtering characteristics

There are several key differences between HTTPS filtering and HTTP filtering:

- Do not include subdomain information when manually filtering HTTPS URLs in access control or QoS policies. For example, use example.com instead of www.example.com.
-

Tip In an decryption policies, you can handle and decrypt traffic to specific URLs by defining a distinguished name decryption policy rule condition. The common name attribute in the subject distinguished name of a certificate contains the site's URL. Decrypting HTTPS traffic allows access control rules to evaluate the decrypted session, which improves URL filtering.

Traffic control by encryption protocol:

The system disregards the encryption protocol (HTTP vs HTTPS) when performing URL filtering in access control or QoS policies. This occurs for both manual and reputation-based URL conditions. In other words, URL filtering treats traffic to these websites identically:

- http://example.com/
- https://example.com/

To configure a rule that matches only HTTP or HTTPS traffic, add an application condition to the rule. For example, you could allow HTTPS access to a site while disallowing HTTP access by constructing two access control rules, each with an application and URL condition.

Application-specific URL filtering rules

The first rule allows HTTPS traffic to the website:

- Action: Allow
- Application: HTTPS
- URL: example.com

The second rule blocks HTTP access to the same website:

- Action: Block
- Application: HTTP
- URL: example.com

Use categories in URL filtering

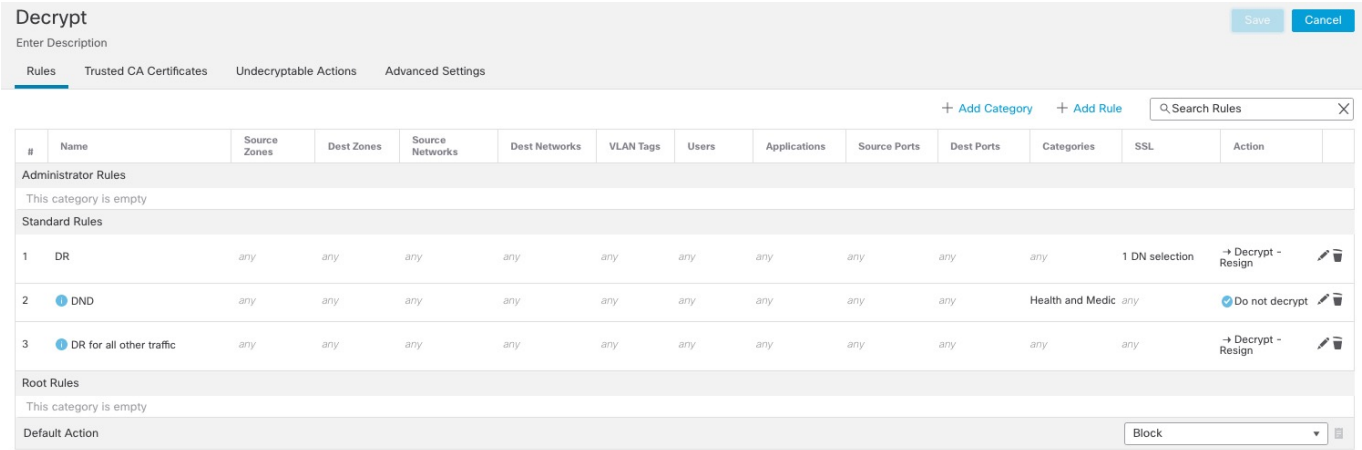
Limitations of categories in Do Not Decrypt rules

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security. While we strive to continuously update and improve URL filtering categories, it is not an exact

science. Some websites are not categorized at all and it's possible some websites might be improperly categorized.

Avoid overusing categories in do not decrypt rules to avoid decrypting traffic without a reason; for example, the Health and Medicine category includes the WebMD website, which does not threaten patient privacy.

Following is a sample decryption policy that can prevent decryption for websites in the Health and Medicine categories but allows decryption for WebMD and everything else. General information about decryption rules can be found in Guidelines for using TLS/SSL decryption, on page 1746.



Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control, on page 1622.

QUIC Fingerprinting

Snort can identify client applications in Quick UDP Internet Connections (QUIC sessions) based on EVE analysis. Refer to QUIC fingerprinting in EVE, on page 1806 for more information.

License requirements for URL filtering

This reference provides the license requirements for URL filtering functionality on Cisco Secure Firewall devices, covering both category and reputation filtering as well as manual filtering options.

Threat Defense License

- Category and reputation filtering—URL Filtering
- Manual filtering—No additional license.

Classic License

- Category and reputation filtering—URL Filtering

- Manual filtering—No additional license.

URL filtering licenses for threat defense devices

Refer to *URL Licenses* in the *Licenses* chapter in the Cisco Secure Firewall Management Center Administration Guide.

Requirements and prerequisites for URL filtering

This reference provides the requirements and prerequisites necessary for implementing URL filtering, including model support, supported domains, and required user roles.

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Configure URL filtering with category and reputation

This task enables URL filtering with category and reputation to protect your network from malicious websites and to control user access to specific website categories.

URL filtering with category and reputation provides comprehensive web security by evaluating websites based on their content categories and reputation scores. This feature helps prevent access to malicious sites while allowing administrators to control access to specific types of content.

Before you begin

- Assign the URL Filtering license to each managed device that will filter URLs.
- Ensure that the Firewall Management Center can communicate with the cloud to obtain URL filtering data. Refer to *Communication Ports and Internet Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

Follow these steps to configure URL filtering with category and reputation:

Procedure

Step 1 Review and understand limitations AND guidelines.

Best practices for URL filtering, on page 1654

Step 2 Enable the URL Filtering feature.

Enable URL filtering using category and reputation, on page 1662

Step 3 Configure rules to filter URLs by category and reputation.

Configure URL conditions, on page 1663

For the best protection against malicious sites, you must block sites by reputation and block URLs in all threat categories.

(Optional) Supplement or selectively override category and reputation-based URL filtering, on page 1668

Step 4 (Optional) Allow users to bypass a website block by clicking through a warning page.

This step is optional.

HTTP response pages, on page 1669

Step 5 Order your rules so that traffic hits the key rules first.

URL rule order, on page 1665

Step 6 (Optional) Modify advanced options related to URL filtering.

This step is optional. Generally, use the defaults unless you have a specific reason to change them.

For information about advanced options, refer to Advanced Settings for Access Control, on page 2169.

- **Maximum URL characters to store in connection events**
- **Allow an Interactive Block to bypass blocking for (seconds)**
- **Retry URL cache miss lookup**
- **Enable reputation enforcement on DNS traffic**

Step 7 Deploy your changes.

Deploy configuration changes, on page 135

Step 8 Ensure that your system receives future URL data updates as expected.

Configure URL filtering health monitors, on page 1673

Step 9 Enable other features to protect your network from malicious sites.

See Security Intelligence, on page 1595.

Enable URL filtering using category and reputation

Enable URL filtering to control and monitor web traffic based on website categories and reputation scores, providing enhanced security for your network.

You must be an Admin user to perform this task.

Before you begin

Complete prerequisites described in Configure URL filtering with category and reputation, on page 1660.

Follow these steps to enable URL filtering using category and reputation:

Procedure

Step 1 Choose **Integration** > **Other Integrations** > **Cloud Services**.

Step 2 Configure URL filtering options, on page 1662.

Step 3 Click **Save**.

URL filtering options

Adding a URL Filtering license automatically enables the URL filtering feature. With this feature, the system handles traffic based on a website's general classification (category) and risk level (reputation).

Although by default the system is configured to submit all URLs to the cloud for threat intelligence evaluation, using a local dataset of category and reputation data can make web browsing faster.When you enable or re-enable URL filtering, the Firewall Management Center automatically queries Cisco for URL data and pushes the dataset to managed devices. This process may take some time.

If you use SSL rules to handle encrypted traffic, also see Decryption Rules guidelines and limitations, on page 1746.

Enable automatic updates

If you **Enable Automatic Updates** (the default), the Firewall Management Center checks the cloud every 30 minutes for updates. If you need strict control over when the system contacts external resources, disable automatic updates and instead create a recurring task using the scheduler. See the *Cisco Secure Firewall Management Center Administration Guide*.

Update now

Click **Update Now** to perform a one-time, on demand URL data update. You cannot start an on demand update if an update is already in progress. Although daily updates tend to be small, if it has been more than five days since your last update, new URL data may take as long as 20 minutes to download, depending on your bandwidth. The update itself may take up to 30 minutes to complete.

URL query source

You can choose how the system assigns a category and reputation to the URLs that your users browse to. You can choose:

- **Local Database Only**: Uses the local dataset only. Use this option if you do not want to submit your uncategorized URLs (category and reputation not in the local dataset) to Cisco, for example, for privacy reasons. However, note that connections to uncategorized URLs do *not* match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.
- **Local Database and Cisco Cloud**: Uses the local dataset when possible, which can make web browsing faster. When users browse to an URL whose category and reputation is not in the local dataset or a cache of previously accessed websites, the system submits it to the cloud for threat intelligence evaluation and adds the result to the cache.
- **Cisco Cloud Only** (default): Does not use the local dataset. When users browse to an URL whose category and reputation is not in a local cache of previously accessed websites, the system submits it to the cloud for threat intelligence evaluation and adds the result to the cache. This option guarantees the most up-to-date category and reputation information.

  This option requires Version 7.3 on the device. If you enable this option, devices running earlier versions will use the **Local Database and Cisco Cloud** option.

Cached URLs expire

This setting is not relevant if you chose **Local Database Only** as your URL query source.

Caching category and reputation data makes web browsing faster. By default, cached data for URLs never expires, for fastest performance.

To minimize instances of URLs matching on stale data, you can set cached URLs to expire. For more accurate and current threat data, choose a shorter expiration time. A cached URL refreshes after the first time a user on the network visits it after the specified time passes. The first user does not see the refreshed result, but the next user who visits the URL does.

Configure URL conditions

Configure URL conditions to protect your network by controlling access to sites based on URL category and reputation.

URL conditions allow you to control network access based on website categories and reputations, providing protection against malicious sites and enabling security policy enforcement.

Before you begin



Attention As a prerequisite, ensure that you create at least a Monitor rule at the top of your access control policy, containing Category or Reputation parameters. This is essential to see ANY category or reputation data for ANY URLs that hit the particular access control policy.

If there is no rule in the access control policy with the category or reputation parameters configured, the **Connection Events** page in the management center shows no data for Category or Reputation for ANY URL traffic that hits the access control policy.

Follow these steps to configure URL conditions:

Procedure

Step 1 In the rule editor, click the following for URL conditions:

- Access control or QoS—Click **URLs**.
- SSL—Click **Category**.

Step 2 Find and choose the URL categories that you want to control:

In an access control or QoS rule, click **Category**.

For effective protection from malicious sites, you must block URLs in all Threat categories. Additionally, Talos recommends that you block only sites with Poor category. You can block questionable reputations if you have an aggressive security posture, but this may result in a higher amount of false positives. For a list of Threat categories, see URL category and reputation descriptions, on page 1653.

Be sure to click the arrows at the bottom of the list to see all available categories.

Step 3 (Optional) Constrain URL categories by choosing a **Reputation**.

Note that if you explicitly match **Uncategorized** URLs, you cannot further constrain by reputation. Choosing a reputation level also includes other reputations either more or less severe than the level you choose, depending on the rule action:

- Includes less severe reputations—If the rule allows or trusts web traffic. For example, if you configure an access control rule to allow Favorable (level 4), it also automatically allows Trusted (level 5) sites.
- Includes more severe reputations—If the rule rate limits, decrypts, blocks, or monitors web traffic. For example, if you configure an access control rule to block Questionable sites (level 2), it also blocks Untrusted (level 1) sites.

If you change the rule action, the system automatically changes the reputation levels in URL conditions.

Optionally, select **Apply to unknown reputation**.

Step 4 Click **Add URL** or **Add to Rule**, or drag and drop.

Step 5 (Optional) To choose predefined URL objects, or URL lists and feeds in an access control or QoS rule, click **URL**, select the objects, and add them to the destination.

These objects implement manual URL filtering rather than category-based filtering.

Step 6 Save or continue editing the rule.

URL condition in an access control rule

The following graphic shows the URL condition for an access control rule that blocks all malware sites, all untrusted sites, and all social networking sites with a reputation level of Neutral or worse.



This table summarizes how you build the condition.

Blocked URL	Category	Reputation
Malware sites, regardless of reputation	Malware Sites	ANY
Any untrusted URL (level 1)	ANY	1 - Untrusted
Social networking sites with a reputation level of Neutral or worse (levels 1 through 3)	Social Network	3 - Neutral

Rules with URL conditions

This table lists rules that support URL conditions, and the types of filtering that each rule type supports.

Rule Type	Supports Category and Reputation Filtering?	Supports Manual Filtering?
Access control	Yes	Yes
Decryption policy	Yes	No. Use distinguished name conditions instead.
QoS	Yes	Yes

To use URL filtering in a decryption policy that has **Do Not Decrypt** rule conditions, refer to Use categories in URL filtering, on page 1658.

URL rule order

For the most effective URL matching, place rules that include URL conditions before other rules, particularly if the URL rules are block rules and the other rules meet both of the following criteria:

- They include application conditions.
- The traffic to be inspected is encrypted.
- If you configure exceptions to a rule, place the exception above the other rule.

DNS filtering

DNS filtering is a URL filtering feature that

- evaluates domain category and reputation early in URL transactions, when the browser looks up the domain name to get the IP address,
- can often determine category and reputation of encrypted traffic without decryption, and
- is enabled by default through the **Enable reputation enforcement on DNS traffic** option on the **Advanced** tab of each new access control policy.

DNS filtering behavior

DNS filtering slightly modifies URL filtering behavior and is applicable only when URL filtering is enabled and configured.

If DNS filtering cannot determine the URL of encrypted traffic, that traffic is processed using your configurations for encrypted traffic.

Enable DNS filtering to identify URLs during domain lookup

DNS filtering allows you to identify and block URLs based on category and reputation during domain lookup, providing an additional layer of security by preventing access to malicious or unwanted domains before connections are established.

DNS filtering is enabled by default in new access control policies. However, additional configurations may be required in order for this setting to take effect.

Before you begin

- URL filtering using category and reputation must be licensed, enabled, and configured.

  DNS filtering does not use these settings in the URLs tab: URL groups, URL objects, URL lists and feeds, and URLs entered into the "Enter URL" text box.
- Refer to limitations at DNS filtering behavior for block actions, on page 1667.

Procedure

Step 1 In your access control policy's advanced settings, select **Enable reputation enforcement on DNS traffic**.

Step 2 In the same policy, for each access control rule that has URL category and reputation blocking configured:

- Application conditions—If the application condition is anything other than **any** (or empty), add **DNS** to that list. Other DNS-related options are not relevant for this purpose.
- Port condition—If the port/protocol condition is anything other than **any** (or empty), add **DNS_over_TCP** and **DNS_over_UDP**.

Step 3 Save your changes.

What to do next

If you are done making changes, Deploy configuration changes, on page 135.

DNS filtering behavior for block actions

Traffic that matches rules having action **Block with reset**, **Interactive Block**, or **Interactive Block with reset** will be treated as if the rule action were **Block**.

End users trying to access a blocked URL will experience this as an unexplained inability to connect to their page. The connection will spin and then time out.

DNS filtering and events

DNS filtering and events is a logging mechanism that

- generates connection events using specific fields such as DNS Query, URL Category, URL Reputation, and Destination Port,
- populates the DNS Query field with the domain name while leaving the URL field blank for DNS filtering matches, and
- sets the Destination Port to 53.

Event generation behavior

DNS filtering generates events based on the access control rule action:

- When the access control rule action is **Allow** or **Trust**, two connection events will be generated for the same traffic, one for DNS filtering (with the **DNS Query** field populated) and one for URL filtering (with the **URL** field populated).
- The first time the system encounters a particular URL, two events appear for that single session: one event showing uncategorized or reputationless for the DNS Query, and one event showing the actual category and reputation for the URL, which the system retrieves during the DNS Query and applies to the session while processing using standard URL filtering.

Manual URL filtering

Manual URL filtering is a URL filtering capability that

- supplements or selectively overrides category and reputation-based URL filtering by manually filtering individual URLs, groups of URLs, or URL lists and feeds in access control and QoS rules, and
- enables URL filtering without requiring a special license when manually permitting or blocking URLs through Allow or Block rules within an access control policy.

Manual URL filtering implementation examples

Examples:

- You might use access control to block a category of websites that are not appropriate for your organization. However, if the category contains a website that is appropriate, and to which you want to provide access, you can create a manual Allow rule for that site and place it before the Block rule for the category.
- If you prefer not to use category-based URL filtering, you can manually permit or block a URL or a group of URLs by creating an Allow or Block rule within an access control policy. You can perform this type of URL filtering without a special license.

Manual URL filtering is not supported in SSL rules. Use distinguished name conditions instead.

Caution Depending on how you implement manual URL filtering, URL matching may not be what you intend. Refer to Manual URL filtering options, on page 1668.

Manual URL filtering options

There are several ways to specify URLs for manual URL filtering.

Option	Description
(Best practice) Use custom Security Intelligence URL list or feed objects.	This is the recommended method for manual URL filtering. You can create a new list or feed, or choose an existing one in an access control or QoS rule. For more information, see Custom security intelligence lists and feeds, on page 2425 and subtopics.
Use URL objects, individually or as groups. URL objects are described at URLs, on page 2437. Or Enter URLs directly into the access control rule. (The **Enter URL** option on the rule page in the web interface.)	If you do not include a path (that is, there are no slash (/) characters in the URL), the match is based on the server's hostname only. If you include one or more / character, the entire URL string is used for a substring match. Then, a URL is considered a match if any of these are true: • The string is at the beginning of the URL. • The string follows a dot. • The string contains a dot in the beginning. • The string follows the :// characters. For example, ign.com matches ign.com or www.ign.com, but not versign.com. **Note** We recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites (that is, URL strings with / characters), as servers can be reorganized and pages moved to new paths. The **Enter URL** option does not support wildcards.

Supplement or selectively override category and reputation-based URL filtering

This task allows you to use Security Intelligence URL lists and feeds to supplement or create exceptions to your category and reputation-based URL filtering rules in access control or QoS policies.

In access control or QoS rules, you can use Security Intelligence URL lists and feeds to supplement, or to specify exceptions to, your category and reputation-based URL filtering rules.

Important! If the list or feed you are configuring in this procedure contains exceptions to category- or reputation-based rules, put this rule above those rules in the rule order.

In SSL rules, use distinguished name conditions to configure parallel behavior.

Before you begin

- Configure URL filtering using category and reputation. Refer to Configure URL conditions, on page 1663.
- Understand important best practices for manual URL filtering. Refer to Best practices for URL filtering, on page 1654 and Manual URL filtering options, on page 1668.
- Configure one or more Security Intelligence objects (lists or feeds) containing the URLs that you want to use for manual filtering. Refer to Custom security intelligence lists and feeds, on page 2425.

Follow these steps to supplement or selectively override category and reputation-based URL filtering:

Procedure

Step 1 Navigate to the access control or QoS policy in which you will define the rule.

Step 2 Create or edit the rule in which you will add the new condition:

- If you are supplementing a category- or reputation-based URL filtering rule, edit the existing rule.
- If you are overriding or creating exceptions to a category- or reputation-based URL filtering rule, create a new rule.

Step 3 Select the list or feed you created as the destination URL criteria.

Step 4 Save the rule.

HTTP response pages

An HTTP response page is a web page that displays when the system blocks web requests using either access control rules or the access control policy default action.

HTTP response page types

The response page displayed depends on how you block the session:

- **Block Response Page**: Overrides the default browser or server page that explains that the connection was denied.
- **Interactive Block Response Page**: Warns users, but also allows them to click a button (or refresh the page) to load the originally requested site. Users may have to refresh after bypassing the response page to load page elements that did not load.

If you do not choose a response page, the system blocks sessions without interaction or explanation.

Limitations to HTTP response pages

The system displays a response page only for unencrypted or decrypted HTTP/HTTPS connections blocked (or interactively blocked) either by access control rules or by the access control policy default action. The system does not display a response page for connections that are blocked by any other policy or mechanism.

The system cannot display a response page if the connection is reset (RST packet sent). If you enable response pages, the system prioritizes that configuration. Even if you choose **Block with reset** or **Interactive Block with reset** as the rule action, the system displays the response page and does not reset matching web connections. To ensure that blocked web connections are reset, you must disable response pages.

- Note that all non-web traffic that matches the rule *is* blocked with reset.

The system does not display a response page for encrypted connections that are blocked by access control rules (or any other configuration). Access control rules evaluate encrypted connections if you did not configure an SSL policy, or your SSL policy passes encrypted traffic.

-
- However, the system does display a response page for connections that are decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. In these cases, the system encrypts the response page and sends it at the end of the reencrypted SSL stream.

The system does not display a response page when web traffic is blocked because of a promoted access control rule (an early-placed blocking rule with only simple network conditions).

If a URL is entered without specifying "http" or "https", and the browser initiates the connection on port 80, and the user clicks through a response page, and the connection is subsequently redirected to port 443, the user will not see a second interactive response page because the response to this URL is already cached.

The system does not display a response page when web traffic is blocked before the system identifies the requested URL. Refer to Best practices for URL filtering, on page 1654.

The system does not display a response page if the block URL access control rule is configured after the allow application rule.

Requirements and prerequisites for HTTP response pages

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Describe the necessary conditions, user roles, and supported domains required for setting up HTTP response pages.

Choose HTTP response pages

HTTP response pages provide feedback to users when their sessions are blocked by access control policies, allowing for better user experience and network transparency.

Reliable display of HTTP response pages depends on your network configuration, traffic loads, and size of the page. Smaller pages are more likely to display successfully.

Procedure

Step 1 In the access control policy editor, select **HTTP Responses** from the **More** drop-down arrow at the end of the packet flow line.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 Choose the **Block Response Page** and **Interactive Block Response Page**:

- System-provided—Displays a generic response. Click **View** ( ) to view the code for this page.
- Custom—Create a custom response page. A pop-up window appears, prepopulated with system-provided code that you can replace or modify by clicking **Edit** ( ). A counter shows how many characters you have used.
- None—Disables the response page and blocks sessions without interaction or explanation. To quickly disable interactive blocking for the whole access control policy, choose this option.

Step 3 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Interactive blocking with HTTP response pages

Interactive blocking with HTTP response pages is a security mechanism that

- allows users to load an originally requested site after reading a warning page,
- provides user control over whether to proceed with potentially blocked traffic, and
- enables temporary bypass with configurable duration settings.

Configuration behavior and bypass settings

When you configure interactive blocking, users may have to refresh after bypassing the response page to load page elements that did not load.

Tip To quickly disable interactive blocking for the whole access control policy, display neither the system provided page nor a custom page. The system then blocks all connections without interaction.

If a user does not bypass an interactive block, matching traffic is denied without further inspection. If a user bypasses an interactive block, the access control rule allows the traffic, although the traffic may still be subject to deep inspection and blocking.

By default, a user bypass is in effect for 10 minutes (600 seconds) without displaying the warning page on subsequent visits. You can set the duration to as long as a year, or you can force the user to bypass the block every time. This limit applies to every Interactive Block rule in the policy. You cannot set the limit per rule.

Logging options for interactively blocked traffic are identical to those in allowed traffic. If a user does not bypass the interactive block, the system can log only beginning-of-connection events. When the system initially warns the user, it marks any logged beginning-of-connection event with the `Interactive Block` or `Interactive Block with reset` action. If the user bypasses the block, additional connection events logged for the session have an action of `Allow`.

Configure interactive blocking

Interactive blocking allows users to bypass URL filtering rules while maintaining security controls and logging capabilities.

This procedure describes how to allow users to bypass URL filtering rules.

Procedure

Step 1 As part of access control, configure an access control rule that matches web traffic; see Create and edit access control rules, on page 1631:

- Action—Set the rule action to **Interactive Block** or **Interactive Block with reset**; see Access control rule interactive blocking actions, on page 1615.
- Conditions—Use URL conditions to specify the web traffic to interactively block.
- Logging—Assume users will bypass the block and choose logging options accordingly; see *Logging for Allowed Connections* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Inspection—Assume users will bypass the block and choose deep inspection options accordingly; see Access control policies, on page 1569.

Step 2 (Optional) (Optional) In the access control policy **HTTP Responses**, choose a custom interactive-block HTTP response page; see Choose HTTP response pages, on page 1671.

Step 3 (Optional) (Optional) In the access control policy **Advanced** settings, change the user bypass timeout; see Set the user bypass timeout for a blocked website, on page 1673.

After a user bypasses a block, the system allows the user to browse to that page without warning until the timeout period elapses.

Step 4 Save the access control policy.

Step 5 Deploy configuration changes; see Deploy configuration changes, on page 135.

Set the user bypass timeout for a blocked website

Set the duration that users can browse after bypassing a URL filtering block before having to bypass the block again.

This procedure explains how to set the time allowed for browsing after the user bypasses a URL filtering block. When the timeout expires, the user must bypass the block again.

Procedure

Step 1 Click **Policies** > **Access Control heading** > **Access Control** and edit the policy.

Step 2 Select **Advanced Settings** from the **More** drop-down menu at the end of the packet flow line.

Step 3 Click **Edit** ( ) next to General Settings.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 4 In the **Allow an Interactive Block to bypass blocking for (seconds)** field, enter the number of seconds that must elapse before the user bypass expires.

Setting this value to 0 means the interactive block response is displayed once and the user bypass never expires.

Step 5 Click **OK**.

Step 6 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure URL filtering health monitors

The following health policies alert if the system has problems obtaining or updating URL category and reputation data.

- URL Filtering Monitor
- Threat Data Updates on Device

To ensure that these are configured the way you want them, refer to *Health Modules* and *Configuring Health Monitoring* in the *Cisco Secure Firewall Management Center Administration Guide*.

Dispute URL category and reputation

This task allows you to challenge URL categorizations or reputation scores when you disagree with the assignments made by Talos Intelligence.

If you disagree with a category or reputation assigned by Talos, you can submit a request for re-evaluation.

Before you begin

You will need your Cisco account credentials.

Procedure

Step 1 In the Firewall Management Center web interface, do one of the following:

Location of dispute option	Path to dispute option
Cloud Services configuration page	a. Navigate to the **Integration** > **Other Integrations** > **Cloud Services** page. b. Select **Dispute URL categories and reputations**.
Manual URL Lookup page	a. Navigate to the manual URL Lookup page: **Analysis** > **Advanced** > **URL**. b. Look up the URL in question. c. To see **Dispute** at the end of the table row, hover over the relevant entry in the list of results, then click **Dispute**.
URL Connection Event	a. Navigate to any page under the **Analysis** > **Connections** > **Events** menu that has a table that includes URLs. b. Right-click an item in the **URL Category** or **URL Reputation** column (show hidden columns if needed) and select an option.

The Talos web site opens in a separate browser window.

Step 2 Sign in to the Talos site with your Cisco credentials.

Step 3 Review the information and follow the instructions on the Talos page.

Step 4 On the Talos site, review how submitted disputes are handled. Check what response you can expect, if any.

The dispute process is independent of Secure Firewall products.

Take action if the URL category set changes

URL filtering categories may occasionally change to accommodate new web trends and evolving usage patterns. Taking action when these changes occur ensures that your policies continue to function properly and can be deployed successfully.

The set of URL Filtering categories may occasionally change, in order to accommodate new web trends and evolving usage patterns.

These changes affect both policies and events.

Shortly before URL category changes are scheduled to occur, and after they occur, you will see alerts in the list of rules in any access control, SSL, and QoS policy that is affected by the changes, and on URL or Category in rules that you edit.

You should take action when you see these alerts.

Note Updates to the URL category set as described in this topic are distinct from the changes that simply add new URLs to existing categories or re-classify misclassified URLs. This topic does not apply to category changes for individual URLs.

Procedure

Step 1 If you see an alert beside a rule in an access control policy, hover over the alert to see details.

Step 2 If the alert mentions changes to URL categories, edit the rule to see further details.

Step 3 Hover over the URL or Category in the rule dialog to see general information about the type of changes.

Step 4 If you see an alert beside a category, click the alert to view details.

Step 5 If you see a "More information" link in the description of a change, click it to view information about the category on the Talos web site.

Alternatively, see a list and descriptions of all categories at the link in URL category and reputation descriptions, on page 1653.

Step 6 Depending on the type of change, take appropriate action:

Type of Category Change	What The System Will Do	What You Should Do
Existing category will soon be deprecated	Nothing yet. You have a few weeks to change affected rules. If you do not take action in that time, the system eventually will not be able to redeploy the policy.	Remove this category from all rules that include it. If there is a similar new category, consider using that category instead.
New category is added	By default, the system does not use newly added categories.	Consider creating new rules for the new category.
Existing category is deleted	The category will appear in the rule in strikethrough text (that is, with a line through the category name.)	You must delete the obsolete category from the rule before you can deploy the policy.

Step 7 Check your SSL rules (Category) for these changes and take action as needed.

Step 8 Check your QoS rules (URL) for these changes and take action as needed.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

URL category and reputation changes

URL category and reputation changes are system modifications that

- affect how events are categorized and labeled in the system,
- result in different handling of events processed before and after the changes, and
- impact the display of URL reputation information in event viewers.

Effects on event processing

URL category and reputation changes affect events differently based on when they were processed:

- When URL categories change, events that the system processed before the category change will be associated with their original category names and will be labeled with **Legacy**. Events that the system processed after the category change will be associated with the new categories.

  Older, legacy events will age out of the system over time.
- If a URL does not have a reputation at the time it was processed, the URL Reputation column in the event viewer will be empty.

Troubleshoot URL filtering

This reference provides troubleshooting information for common URL filtering issues including missing categories, uninspected packets, registration failures, lookup errors, and performance problems.

Expected URL category is missing from the categories list

The URL filtering feature uses a different set of categories than the Security Intelligence feature. The category that you expect to see may be a Security Intelligence category. To see those categories, look at the **URLs** tab on the **Security Intelligence** tab in an access control policy.

Initial packets are passing uninspected

Refer to Inspection of packets that pass before traffic is identified and subtopics.

See also DNS filtering, on page 1665.

Health alert: "URL filtering registration failure"

Verify that the Firewall Management Center and any proxies can connect to the Cisco cloud. Refer to *Communication Ports and Internet Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

How can I find the category and reputation of a particular URL?

Do a manual lookup. Refer to *Finding URL Category and Reputation* in the *Cisco Secure Firewall Management Center Administration Guide*.

Error when attempting a manual lookup: "cloud lookup failure for <URL>"

Make sure the feature is properly enabled. Refer to the prerequisites in *Finding URL Category and Reputation* in the *Cisco Secure Firewall Management Center Administration Guide*.

URL appears to be incorrectly handled based on its URL category and reputation

Problem: The system does not handle the URL correctly based on its URL category and reputation.

Solutions:

- Verify that the URL category and reputation associated with the URL are what you think they are. See *Finding URL Category and Reputation* in the *Cisco Secure Firewall Management Center Administration Guide*.
- These issues may be addressed by settings described in URL filtering options, on page 1662, accessible using Enable URL filtering using category and reputation, on page 1662.
  - The URL cache may hold stale information. See information about the **Cached URLs Expire** setting in URL filtering options, on page 1662.
  - The local data set may not be updated with current information from the cloud. See information about the **Enable Automatic Updates** setting in URL filtering options, on page 1662.
  - The system may be configured to *not* check the cloud for current data. See information about the **Query Cisco cloud for unknown URLs** setting in URL filtering options, on page 1662.
- Your access control policy may be configured to pass traffic to the URL without checking the cloud. See information about the **Retry URL cache miss lookup** setting in General settings, on page 2172.
- See also Best practices for URL filtering, on page 1654.
- If the URL is processed using an SSL rule, see Decryption Rules guidelines and limitations, on page 1746 and Best practice for Decryption policy rule order
- Verify that the URL is being handled using the access control rule that you think it is being handled by, and that the rule does what you think it does. Consider rule order.
- Verify that the local URL category and reputation database on the Firewall Management Center is successfully being updated from the cloud and that managed devices are successfully being updated from the Firewall Management Center.

  Status of these processes are reported in the Health Monitor, in the **URL Filtering Monitor** module and the **Threat Data Updates on Devices** module. For details, see *Health* in the *Cisco Secure Firewall Management Center Administration Guide*.

If you want to immediately update the local URL category and reputation database, go to **Integration** > **Other Integrations** > **Cloud Services**, then click **Update Now** in the **URL Filtering** area. For more information, see URL filtering options, on page 1662.

A URL category or reputation is not correct

For access control or QoS rules: Use manual filtering, paying careful attention to rule order. See Manual URL filtering, on page 1667 and Configure URL conditions, on page 1663.

For SSL rules: Manual filtering is not supported. Instead, use distinguished name conditions.

See also Dispute URL category and reputation, on page 1673.

Web pages are slow to load

There is a tradeoff between security and performance. Some options:

- Consider modifying the **Cached URLs Expire** setting. Choose **Integration** > **Other Integrations** > **Cloud Services**. For information, see URL filtering options, on page 1662.
- Consider deselecting the **Retry URL cache miss lookup** setting in General settings, on page 2172.

Events do not include URL category and reputation

- Make sure you have included applicable URL rules in an access control policy, the rules are active, and the policies have been deployed to the relevant devices.
- URL category and reputation do not appear in an event if the connection is processed before it matches a URL rule.
- The rule that handles the connection must be configured for URL category and reputation.
- Even if you have configured URL categories in the Categories tab in an SSL rule, you must also configure the URLs tab in a rule in your access control policy.

DNS filtering is not working

Make sure you have completed all prerequisites and steps in Enable DNS filtering to identify URLs during domain lookup, on page 1666.

An end user tries to access a blocked URL and the page just spins and times out

When DNS Filtering is enabled and end users access a URL that is blocked, the page will spin but not load. End users are not notified that the page is blocked. This is currently a limitation when DNS filtering is enabled.

Refer to DNS filtering behavior for block actions, on page 1667.

Events include URL category and reputation but URL field is blank

If the DNS Query field is populated and the URL field is empty, this is expected when the DNS filtering feature is enabled.

Refer to DNS filtering and events, on page 1667.

Multiple events are generated for a single transaction

A single web transaction sometimes generates two connection events, one for DNS filtering and one for URL filtering. This is expected when DNS filtering is enabled and:

- the access control rule action for the traffic is Allow or Trust.
- the system encounters a URL for the first time.

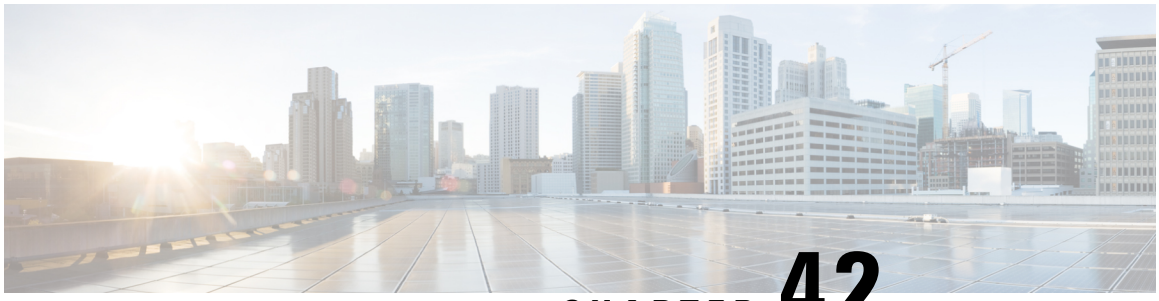
Refer to DNS filtering and events, on page 1667.

History for URL filtering

This reference provides a chronological history of URL filtering features, including release versions, supported platforms, and implementation details for each enhancement or change.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New URL category	New in release 7.0, applies to all releases	Any	New URL category: Private IP address For details, see Talosintelligence.com
DNS filtering	7.0 6.7 (Beta)	Any	A new option in the advanced settings for each access control policy allows earlier filtering of web traffic by category and reputation. By default, this feature is enabled on new installations.
Ability to specify handling for sites with unknown reputation	6.7	Any	You can now specify handling for URLs with unknown reputation. Modified screens: URL rules in access control policies and QoS policies, and category rules in SSL policies, include a new checkbox for this purpose below the reputation selection area.
New and changed URL categories New names for reputation levels	6.5	6.5	These changes apply to URL rules in access control and QoS policies and to Category rules in SSL policies: The set of URL categories has changed. There are now two pages of categories from which to select when you create a URL rule. The name associated with each reputation level has changed. For descriptions of the new categories and reputation names, see URL category and reputation descriptions, on page 1653. For complete details specific to upgrades, see also the Release Notes and upgrade instructions for version 6.5. If there are future category set changes, your rules will display icons to alert you. Modified screens: URL rules in access control policies, SSL policies, and QoS policies; event data related to URL categories.
Minor change to Classic device licensing	6.5	Any	For devices that use Classic licenses, URL filtering will not be enabled until the device is registered to the Firewall Management Center and a URL Filtering license is assigned to the device. Supported platforms: NGIPSv and ASA with FirePOWER Services devices.
Addresses for retrieving URL data from the Cisco cloud have changed	6.5	Any	Refer to *Communication Ports and Internet Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Opportunity to dispute an assigned URL category	6.5	Any	If you disagree with the category that the system assigns to a URL, you can submit a request to change the category. New and modified screens: • New menu option when right-clicking a URL category or reputation in tables of connection events under the **Analysis** menu. • New button on the URL Lookups page (**Analysis** > **Advanced** > **URL**). (Hover your pointer over the URL to display the button.) • New option on the **System** > **Integration** > **Cloud Services** page
The **Cisco CSI** tab is renamed to **Cloud Services**	6.4	Any	Modified screens and navigation: **System** > **Integration** > **Cisco CSI** is now **System** > **Integration** > **Cloud Services**
New option: Cached URLs Expire	6.3	Any	Use this new control to balance performance with freshness of URL category and reputation data in order to minimize instances of URLs matching on stale data. Modified screens: **System** > **Integration** > **Cisco CSI**.
Changed menu path	6.3	Any	The path to the manual URL Lookup page has changed from **Analysis** > **Lookup** > **URL** to **Analysis** > **Advanced** > **URL**.



CHAPTER 42

Content Restriction

The following topics describe how to configure access control policies to use content restriction features:

- About content restriction, on page 1681
- Requirements and prerequisites for content restriction, on page 1682
- Guidelines and limitations for content restriction, on page 1683
- Using access control rules to enforce content restriction, on page 1683
- Use a DNS sinkhole to enforce content restriction, on page 1684

About content restriction

Major search engines and content delivery services provide features that allow you to restrict search results and website content. For example, schools use content restriction features to comply with the Children's Internet Protection Act (CIPA).

When implemented by search engines and content delivery services, you can enforce content restriction features only for individual browsers or users. The system allows you to extend these features to your entire network.

The system allows you to enforce:

- *Safe Search*—Supported in many major search engines, this service filters out explicit and adult-oriented content that business, government, and education environments classify as objectionable. The system does not restrict a user's ability to access the home pages for supported search engines.

You can use two methods to configure the system to enforce these features:

Method: Access Control Rules
: Content restriction features communicate the restricted status of a search or content query via an element in the request URI, an associated cookie, or a custom HTTP header element. You can configure access control rules to modify these elements as the system processes traffic.

Method: DNS Sinkhole
: For Google searches, you can configure the system to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes filters for Safe Search.

The table below describes the differences between these enforcement methods.

Table 98: Comparison of content restriction methods

Attribute	Method: Access Control Rules	Method: DNS Sinkhole
Supported devices	Any	Secure Firewall Threat Defense only
Search engines supported	Any tagged `safesearch supported` in the **Applications** tab of the rule editor	Google only
YouTube Restricted Mode supported	Yes	Yes
SSL policy required	Yes	No
Hosts must be using IPv4	No	Yes
Connection event logging	Yes	Yes

When determining which method to use, consider the following limitations:

- The access control rules method requires an SSL policy, which impacts performance.
- The Google SafeSearch VIP supports IPv4 traffic only. If you configure a DNS sinkhole to manage Google searches, any hosts on the affected network must be using IPv4.

The system logs different values for the **Reason** field in connection events, depending on the method:

- Access Control Rules—`Content Restriction`
- DNS Sinkhole—`DNS Block`

Requirements and prerequisites for content restriction

Model support

Any, or as indicated in the procedure.

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Guidelines and limitations for content restriction

- Safe search is supported by Snort 2 only.
- YouTube and Google do not support the YouTubeEDU feature that was implemented in access control rules. Please remove any access control rules that configure YouTubeEDU as they are not truly functional. You can also remove associated decryption rules.

Using access control rules to enforce content restriction

The following procedure explains how to configure access control rules to restrict content."

Note When safe search is enabled in an access control rule, inline normalization is enabled automatically.

Procedure

Step 1 Create a decryption policy.

Step 2 Add rules for handling Safe Search traffic:

- Choose **Decrypt - Resign** as the **Action** for the rules.
- In **Applications**, add selections to the **Selected Applications and Filters** list:
  - Safe Search—Add the `Category: search engine` filter.

Step 3 Set rule positions for the rules you added. Click and drag, or use the right-click menu to cut and paste.

Step 4 Create or edit an access control policy, and associate the decryption policy with the access control policy.

For more information, see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 5 In the access control policy, add rules for handling Safe Search traffic:

- Choose **Allow** as the **Action** for the rules.
- In **Applications**, click the icon for **Safe search** ( ) and set related options.
  - Safe search options for access control rules, on page 1684
- In **Applications**, refine application selections in the **Selected Applications and Filters** list.

  In most cases, enabling Safe Search populates the **Selected Applications and Filters** list with the appropriate values. The system does not automatically populate the list if a Safe Search application is already present in the list when you enable the feature. If applications do not populate as expected, manually add them as follows:

- Safe Search—Add the `Category: search engine` filter.

For more information, see Configure application conditions and filters, on page 1638.

Step 6 Set rule positions for the access control rules you added. Click and drag, or use the right-click menu to cut and paste.

Step 7 Configure the HTTP response page that the system displays when it blocks restricted content; see Choose HTTP response pages, on page 1671.

Step 8 Deploy configuration changes; see Deploy configuration changes, on page 135.

Safe search options for access control rules

The system supports Safe Search filtering for specific search engines only. For a list of supported search engines, see applications tagged `safesearch supported` in the **Applications** tab of the access control rule editor. For a list of unsupported search engines, see applications tagged `safesearch unsupported`.

When enabling Safe Search for an access control rule, set the following parameters:

Enable Safe Search
Enables Safe Search filtering for traffic that matches this rule.

Unsupported Search Traffic
Specifies the action you want the system to take when it processes traffic from unsupported search engines. If you choose **Block** or **Block with Reset**, you must also configure the HTTP response page that the system displays when it blocks restricted content; see Choose HTTP response pages, on page 1671.

Use a DNS sinkhole to enforce content restriction

This task configures a DNS sinkhole to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes content filters on Google and YouTube search results.

Typically, a DNS sinkhole directs traffic away from a particular target. This procedure describes how to configure a DNS sinkhole to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes content filters on Google and YouTube search results.

Because Google SafeSearch uses a single IPv4 address for the VIP, hosts must use IPv4 addressing.

Caution If your network includes proxy servers, this content restriction method is not effective unless you position your Firewall Threat Defense devices between the proxy servers and the Internet.

This procedure enforces content restriction for Google searches only. It does not apply to any other search engine.

Before you begin

This procedure applies to Firewall Threat Defense only, and requires the IPS license.

Follow these steps to use a DNS sinkhole to enforce content restriction:

Procedure

Step 1 Obtain a list of supported Google domains via the following URL: https://www.google.com/supported_domains.

Step 2 Create a custom DNS list on your local computer, and add the following entries:

- To enforce Google SafeSearch, add an entry for each supported Google domain.
- To enforce YouTube Restricted Mode, add a "youtube.com" entry.

The custom DNS list must be in text file (.txt) format. Each line of the text file must specify an individual domain name, stripped of any leading periods. For example, the supported domain ".google.com" must appear as "google.com".

Step 3 Upload the custom DNS list to the Firewall Management Center; see Upload new custom security intelligence lists to the Secure Firewall Management Center, on page 2431.

Step 4 Determine the IPv4 address for the Google SafeSearch VIP. For example, run **nslookup** on forcesafesearch.google.com.

Step 5 Create a sinkhole object for the SafeSearch VIP; see Create a sinkhole object, on page 2432.

Use the following values for this object:

- IPv4 Address—Enter the SafeSearch VIP address.
- IPv6 Address—Enter the IPv6 loopback address (**::1**).
- Log Connections to Sinkhole—Click Log Connections.
- Type—Choose **None**.

Step 6 Create a basic DNS policy; see Create basic DNS policies, on page 1997.

Step 7 Add a DNS rule for the sinkhole; see Create and edit DNS rules, on page 1999.

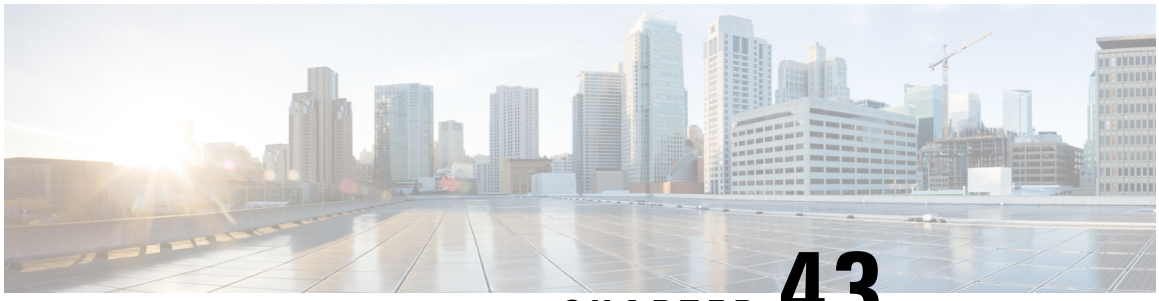
For this rule:

- Check the **Enabled** check box.
- Choose **Sinkhole** from the **Action** drop-down list.
- Choose the sinkhole object you created from the **Sinkhole** drop-down list.
- Add the custom DNS list you created to the **Selected Items** list on **DNS**.
- (Optional) Choose a network in **Networks** to limit content restriction to specific users. For example, if you want to limit content restriction to student users, assign students to a different subnet than faculty, and specify that subnet in this rule.

Step 8 Associate the DNS policy with an access control policy; see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 9 Deploy configuration changes; see Deploy configuration changes, on page 135.

The DNS sinkhole is configured to enforce content restriction by redirecting traffic to the Google SafeSearch VIP, which filters Google and YouTube search results.



CHAPTER 43

Intrusion Prevention Overview

This chapter provides an overview of the Snort 2 inspection engine, and the network analysis and intrusion policies. It also provides an insight into system-provided and custom network analysis and intrusion policies. In most cases, the system-provided policies are all you need. For advanced users with specific needs, you can create custom rules. To configure custom Snort 2 rules, see *Custom Snort 2 Intrusion Policies for Access Control*.

Note .

To configure custom Snort 3 rules, see *Custom Snort 3 Intrusion Policies for Access Control*.

- Network Analysis and Intrusion Policy Basics, on page 1687
- How Policies Examine Traffic For Intrusions, on page 1689
- System-Provided and Custom Network Analysis and Intrusion Policies, on page 1694
- License Requirements for Network Analysis and Intrusion Policies, on page 1700
- Requirements and Prerequisites for Network Analysis and Intrusion Policies, on page 1700
- Guidelines and Limitations for Network Analysis and Intrusion Policies, on page 1700
- The Navigation Panel: Network Analysis and Intrusion Policies, on page 1701
- Conflicts and Changes: Network Analysis and Intrusion Policies, on page 1702

Network Analysis and Intrusion Policy Basics

Network analysis and intrusion policies work together as part of the system's intrusion detection and prevention feature.

- The term *intrusion detection* generally refers to the process of passively monitoring and analyzing network traffic for potential intrusions and storing attack data for security analysis. This is sometimes referred to as "IDS."
- The term *intrusion prevention* includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across your network. This is sometimes referred to as "IPS."

Note

- You must configure Network Analysis Policy (NAP) in **Prevention** mode if you are using Snort 3 and SSL decryption or TLS Server Identity. The SSL functionality does not work when Snort 3 NAP is in detection mode.
- We strongly recommend that your intrusion policy (IPS) and network analysis policy (NAP) have the same settings. If IPS is in detection mode, set the NAP in detection mode, and conversely as well.

In an intrusion prevention deployment, when the system examines packets:

- A **network analysis policy** governs how traffic is *decoded* and *preprocessed* so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.
- An **intrusion policy** uses *intrusion and preprocessor rules* (sometimes referred to collectively as *intrusion rules*) to examine the decoded packets for attacks based on patterns. Intrusion policies are paired with *variable sets*, which allow you to use named values to accurately reflect your network environment.

Both network analysis and intrusion policies are invoked by a parent access control policy, but at different times. As the system analyzes traffic, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (additional preprocessing and intrusion rules) phase. Together, network analysis and intrusion policies provide broad and deep packet inspection. They can help you detect, alert on, and protect against network traffic that could threaten the availability, integrity, and confidentiality of hosts and their data.

The system is delivered with several similarly named network analysis and intrusion policies (for example, Balanced Security and Connectivity) that complement and work with each other. By using system-provided policies, you can take advantage of the experience of the Talos Intelligence Group. For these policies, Talos sets intrusion and preprocessor rule states, as well as provides the initial configurations for preprocessors and other advanced settings.

You can also create custom network analysis and intrusion policies. You can tune settings in custom policies to inspect traffic in the way that matters most to you so that you can improve both the performance of your managed devices and your ability to respond effectively to the events they generate.

You create, edit, save, and manage network analysis and intrusion policies using similar policy editors in the web interface. When you are editing either type of policy, a navigation panel appears on the left side of the web interface; the right side displays various configuration pages.

Attention

Detection mode deprecation: From management center Version 7.4.0, for a network analysis policy (NAP), the **Detection** inspection mode is deprecated and will be removed in an upcoming release.

The **Detection** mode was intended to be used as a test mode so that you can enable inspections and see how they behave in your network before setting it to drop traffic, that is, to show traffic that would be dropped.

This behavior is improved where all inspector drops are controlled by the rule state, and you can set each one to generate events. This is done to test them before configuring the rule state to drop traffic. As we now have granular control over traffic drops in Snort 3, the **Detection** mode only adds more complexity to the product and is not needed, so the detection mode is deprecated.

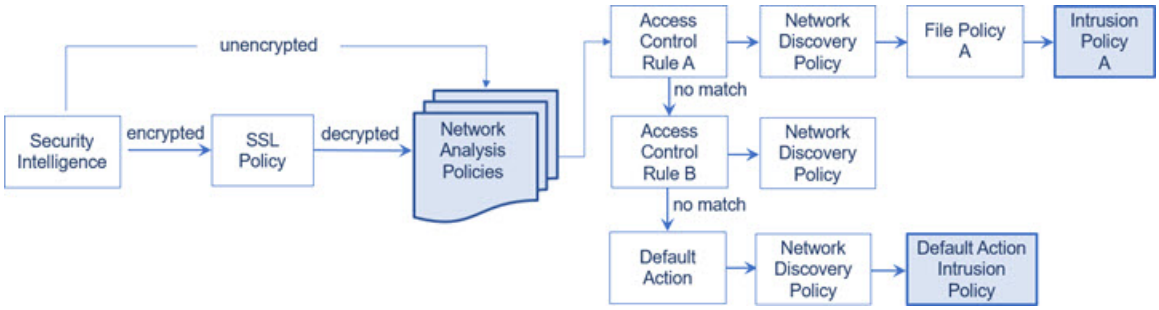
If you change a NAP in **Detection** mode to **Prevention**, the NAP that processes the traffic of intrusion events and have the result "will be dropped" will now be "dropped" and the corresponding traffic will drop the traffic from these events. This is applicable for rules whose GIDs are not 1 or 3. GIDs 1 and 3 are text/compiled rules (typically provided by Talos or from your custom/imported rules) and all other GIDs are inspections for anomalies. These are more uncommon rules to trigger in a network. Changing to **Prevention** mode is unlikely to have any impact on the traffic. You need to just disable the intrusion rule that is applicable for the dropped traffic and set it to just generate or disable.

We recommend you choose **Prevention** as the inspection mode, but if you choose **Prevention**, you cannot revert to **Detection** mode.

How Policies Examine Traffic For Intrusions

When the system analyzes traffic as part of your access control deployment, the network analysis (decoding and preprocessing) phase occurs before and separately from the intrusion prevention (intrusion rules and advanced settings) phase.

The following diagram shows, in a simplified fashion, the order of traffic analysis in an inline, intrusion prevention and malware defense deployment. It illustrates how the access control policy invokes other policies to examine traffic, and in which order those policies are invoked. The network analysis and intrusion policy selection phases are highlighted.



In an inline deployment (that is, where relevant configurations are deployed to devices using routed, switched, or transparent interfaces, or inline interface pairs), the system can block traffic without further inspection at almost any step in the illustrated process. Security Intelligence, the SSL policy, network analysis policies, file policies, and intrusion policies can all either drop or modify traffic. Only the network discovery policy, which passively inspects packets, cannot affect the flow of traffic.

Similarly, at each step of the process, a packet could cause the system to generate an event. Intrusion and preprocessor events (sometimes referred to collectively as *intrusion events*) are indications that a packet or its contents may represent a security risk.

Tip The diagram does not reflect that access control rules handle encrypted traffic when your SSL inspection configuration allows it to pass, or if you do not configure SSL inspection. By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

Note that for a single connection, although the system selects a network analysis policy before an access control rule as shown in the diagram, some preprocessing (notably application layer preprocessing) occurs after access control rule selection. This does **not** affect how you configure preprocessing in custom network analysis policies.

Decoding, Normalizing, and Preprocessing: Network Analysis Policies

Without decoding and preprocessing, the system could not appropriately evaluate traffic for intrusions because protocol differences would make pattern matching impossible. Network analysis policies govern these traffic-handling tasks:

- **after** traffic is filtered by Security Intelligence
- **after** encrypted traffic is decrypted by an optional SSL policy
- **before** traffic can be inspected by file or intrusion policies

A network analysis policy governs packet processing in phases. First the system decodes packets through the first three TCP/IP layers, then continues with normalizing, preprocessing, and detecting protocol anomalies:

- The packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and later, intrusion rules. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers. The packet decoder also detects various anomalous behaviors in packet headers.
- In inline deployments, the inline normalization preprocessor reformats (normalizes) traffic to minimize the chances of attackers evading detection. It prepares packets for examination by other preprocessors and intrusion rules, and helps ensure that the packets the system processes are the same as the packets received by the hosts on your network.

Note In a passive deployment, Cisco recommends that you enable adaptive profile updates at the access control policy level, instead of inline normalization at the network analysis level.

- Various network and transport layers preprocessors detect attacks that exploit IP fragmentation, perform checksum validation, and perform TCP and UDP session preprocessing.

  Note that some advanced transport and network preprocessor settings apply globally to all traffic handled by the target devices of an access control policy. You configure these in the access control policy rather than in a network analysis policy.

- Various application-layer protocol decoders normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently, and to obtain meaningful results.
- The Modbus, DNP3, CIP, and s7commplus SCADA preprocessors detect traffic anomalies and provide data to intrusion rules. Supervisory Control and Data Acquisition (SCADA) protocols monitor, control, and acquire data from industrial, infrastructure, and facility processes such as manufacturing, production, water treatment, electric power distribution, airport and shipping systems, and so on.
- Several preprocessors allow you to detect specific threats, such as Back Orifice, portscans, SYN floods and other rate-based attacks.

  Note that you configure the sensitive data preprocessor, which detects sensitive data such as credit card numbers and Social Security numbers in ASCII text, in intrusion policies.

In a newly created access control policy, one default network analysis policy governs preprocessing for *all* traffic for *all* intrusion policies invoked by the same parent access control policy. Initially, the system uses the Balanced Security and Connectivity network analysis policy as the default, but you can change it to another system-provided or custom network analysis policy. In a more complex deployment, advanced users can tailor traffic preprocessing options to specific security zones, networks, and VLANs by assigning different custom network analysis policies to preprocess matching traffic.

Note For an access control policy with rule action as **Trust** and a prefilter rule with action as **Fastpath** with logging options disabled, you will observe that the end-of-flow events are still generated in the system. The events are not visible on the management center event pages.

Access Control Rules: Intrusion Policy Selection

After initial preprocessing, access control rules (when present) evaluate traffic. In most cases, the first access control rule that a packet matches is the rule that handles that traffic; you can monitor, trust, block, or allow matching traffic.

When you allow traffic with an access control rule, the system can inspect the traffic for discovery data, malware, prohibited files, and intrusions, in that order. Traffic not matching any access control rule is handled by the access control policy's default action, which can also inspect for discovery data and intrusions.

Note All packets, **regardless** of which network analysis policy preprocesses them, are matched to configured access control rules—and thus are potentially subject to inspection by intrusion policies—in top-down order.

The diagram in How Policies Examine Traffic For Intrusions, on page 1689 shows the flow of traffic through a device in an inline, intrusion prevention and malware defense deployment, as follows:

- Access Control Rule A allows matching traffic to proceed. The traffic is then inspected for discovery data by the network discovery policy, for prohibited files and malware by File Policy A, and then for intrusions by Intrusion Policy A.
- Access Control Rule B also allows matching traffic. However, in this scenario, the traffic is not inspected for intrusions (or files or malware), so there are no intrusion or file policies associated with the rule. Note

that by default, traffic that you allow to proceed is inspected by the network discovery policy; you do not need to configure this.

- In this scenario, the access control policy's default action allows matching traffic. The traffic is then inspected by the network discovery policy, and then by an intrusion policy. You can (but do not have to) use a different intrusion policy when you associate intrusion policies with access control rules or the default action.

The example in the diagram does not include any blocking or trusting rules because the system does not inspect blocked or trusted traffic.

Intrusion Inspection: Intrusion Policies, Rules, and Variable Sets

You can use intrusion prevention as the system's last line of defense before traffic is allowed to proceed to its destination. Intrusion policies govern how the system inspects traffic for security violations and, in inline deployments, can block or alter malicious traffic. The main function of intrusion policies is to manage which intrusion and preprocessor rules are enabled and how they are configured.

Intrusion and Preprocessor Rules

An intrusion rule is a specified set of keywords and arguments that detects attempts to exploit vulnerabilities on your network; the system uses an intrusion rule to analyze network traffic to check if it matches the criteria in the rule. The system compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers.

The system includes the following types of rules created by Talos Intelligence Group:

- *shared object intrusion rules*, which are compiled and cannot be modified (except for rule header information such as source and destination ports and IP addresses)
- *standard text intrusion rules*, which can be saved and modified as new custom instances of the rule.
- *preprocessor rules*, which are rules associated with preprocessors and packet decoder detection options in the network analysis policy. You cannot copy or edit preprocessor rules. Most preprocessor rules are disabled by default; you must enable them to use preprocessors to generate events and, in an inline deployment, drop offending packets.

When the system processes packets according to an intrusion policy, first a rule optimizer classifies all activated rules in subsets based on criteria such as: transport layer, application protocol, direction to or from the protected network, and so on. Then, the intrusion rules engine selects the appropriate rule subsets to apply to each packet. Finally, a multi-rule search engine performs three different types of searches to determine if the traffic matches the rule:

- The protocol field search looks for matches in particular fields in an application protocol.
- The generic content search looks for ASCII or binary byte matches in the packet payload.
- The packet anomaly search looks for packet headers and payloads that, rather than containing specific content, violate well-established protocols.

In a custom intrusion policy, you can tune detection by enabling and disabling rules, as well as by writing and adding your own standard text rules. You can also use Cisco recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.

Variable Sets

Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated *variable set*. Most variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions and dynamic rule states.

The system provides a single default variable set, which is comprised of predefined default variables. Most system-provided shared object rules and standard text rules use these predefined default variables to define networks and port numbers. For example, the majority of the rules use the variable `$HOME_NET` to specify the protected network and the variable `$EXTERNAL_NET` to specify the unprotected (or outside) network. In addition, specialized rules often use other predefined variables. For example, rules that detect exploits against web servers use the `$HTTP_SERVERS` and `$HTTP_PORTS` variables.



Tip Even if you use system-provided intrusion policies, Cisco **strongly** recommends that you modify key default variables in the default set. When you use variables that accurately reflect your network environment, processing is optimized and the system can monitor relevant systems for suspicious activity. Advanced users can create and use custom variable sets for pairing with one or more custom intrusion policies.

Intrusion Event Generation

When the system identifies a possible intrusion, it generates an *intrusion or preprocessor event* (sometimes collectively called *intrusion events*). Managed devices transmit their events to the Firewall Management Center, where you can view the aggregated data and gain a greater understanding of the attacks against your network assets. In an inline deployment, managed devices can also drop or replace packets that you know to be harmful.

Each intrusion event in the database includes an event header and contains information about the event name and classification; the source and destination IP addresses; ports; the process that generated the event; and the date and time of the event, as well as contextual information about the source of the attack and its target. For packet-based events, the system also logs a copy of the decoded packet header and payload for the packet or packets that triggered the event.

The packet decoder, the preprocessors, and the intrusion rules engine can all cause the system to generate an event. For example:

- If the packet decoder (configured in the network analysis policy) receives an IP packet that is less than 20 bytes, which is the size of an IP datagram without any options or payload, the decoder interprets this as anomalous traffic. If, later, the accompanying decoder rule in the intrusion policy that examines the packet is enabled, the system generates a preprocessor event.
- If the IP defragmentation preprocessor encounters a series of overlapping IP fragments, the preprocessor interprets this as a possible attack and, when the accompanying preprocessor rule is enabled, the system generates a preprocessor event.
- Within the intrusion rules engine, most standard text rules and shared object rules are written so that they generate intrusion events when triggered by packets.

As the database accumulates intrusion events, you can begin your analysis of potential attacks. The system provides you with the tools you need to review intrusion events and evaluate whether they are important in the context of your network environment and your security policies.

System-Provided and Custom Network Analysis and Intrusion Policies

Creating a new access control policy is one of the first steps in managing traffic flow using the system. By default, a newly created access control policy invokes system-provided network analysis and intrusion policies to examine traffic.

The following diagram shows how a newly created access control policy in an inline, intrusion-prevention deployment initially handles traffic. The preprocessing and intrusion prevention phases are highlighted.

Figure 410: New Access Control Policy: Intrusion Prevention



Note how:

- A default network analysis policy governs the preprocessing of *all* traffic handled by the access control policy. Initially, the system-provided *Balanced Security and Connectivity network analysis policy* is the default.
- The default action of the access control policy allows all non-malicious traffic, as determined by the system-provided *Balanced Security and Connectivity intrusion policy*. Because the default action allows traffic to pass, the discovery feature can examine it for host, application, and user data before the intrusion policy can examine and potentially block malicious traffic.
- The policy uses default Security Intelligence options (global Block and Do Not Block lists only), does not decrypt encrypted traffic with an SSL policy, and does not perform special handling and inspection of network traffic using access control rules.

A simple step you can take to tune your intrusion prevention deployment is to use a different set of system-provided network analysis and intrusion policies as your defaults. Cisco delivers several pairs of these policies with the system.

Or, you can tailor your intrusion prevention deployment by creating and using custom policies. You may find that the preprocessor options, intrusion rule, and other advanced settings configured in those policies do not address the security needs of your network. By tuning your network analysis and intrusion policies you can configure, at a very granular level, how the system processes and inspects the traffic on your network for intrusions.

System-Provided Network Analysis and Intrusion Policies

Cisco delivers several pairs of network analysis and intrusion policies with the system. By using system-provided network analysis and intrusion policies, you can take advantage of the experience of the Talos Intelligence Group. For these policies, Talos provides intrusion and preprocessor rule states as well as initial configurations for preprocessors and other advanced settings.

No system-provided policy covers every network profile, traffic mix, or defensive posture. Each covers common cases and network setups that provide a starting point for a well-tuned defensive policy. Although you can use system-provided policies as-is, Cisco strongly recommends that you use them as the base for custom policies that you tune to suit your network.

Tip Even if you use system-provided network analysis and intrusion policies, you should configure the system's intrusion variables to accurately reflect your network environment. At a minimum, modify key default variables in the default set.

As new vulnerabilities become known, Talos releases intrusion rule updates (also known as *Snort Rule Updates*). These rule updates can modify any system-provided network analysis or intrusion policy, and can provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default policy settings. Rule updates may also delete rules from system-provided policies and provide new rule categories, as well as modify the default variable set.

If a rule update affects your deployment, the web interface marks affected intrusion and network analysis policies as out of date, as well as their parent access control policies. You must re-deploy an updated policy for its changes to take effect.

For your convenience, you can configure rule updates to automatically re-deploy affected intrusion policies, either alone or in combination with affected access control policies. This allows you to easily and automatically keep your deployment up-to-date to protect against recently discovered exploits and intrusions.

To ensure up-to-date preprocessing settings, you **must** re-deploy access control policies, which also deploys any associated SSL, network analysis, and file policies that are different from those currently running, and can also can update default values for advanced preprocessing and performance options.

Cisco delivers the following network analysis and intrusion policies with the system:

Balanced Security and Connectivity network analysis and intrusion policies

These policies are built for both speed and detection. Used together, they serve as a good starting point for most organizations and deployment types. The system uses the Balanced Security and Connectivity policies and settings as defaults in most cases.

Connectivity Over Security network analysis and intrusion policies

These policies are built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. The intrusion policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled.

Security Over Connectivity network analysis and intrusion policies

These policies are built for organizations where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.

Maximum Detection network analysis and intrusion policies

These policies are built for organizations where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact. For example, the intrusion policy enables rules in a large number of threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits.

No Rules Active intrusion policy

In the No Rules Active intrusion policy, all intrusion rules, and all advanced settings except intrusion rule thresholds, are disabled. This policy provides a starting point if you want to create your own intrusion policy instead of basing it on the enabled rules in one of the other system-provided policies.

Note Depending on the system-provided base policy that is selected, the settings of the policy vary. To view the policy settings, click the **Edit** icon next to the policy and then click the **Manage Base Policy** link.

Benefits of Custom Network Analysis and Intrusion Policies

You may find that the preprocessor options, intrusion rules, and other advanced settings configured in the system-provided network analysis and intrusion policies do not fully address the security needs of your organization.

Building custom policies can improve the performance of the system in your environment and can provide a focused view of the malicious traffic and policy violations occurring on your network. By creating and tuning custom policies you can configure, at a very granular level, how the system processes and inspects the traffic on your network for intrusions.

All custom policies have a base policy, also called a base layer, which defines the default settings for all configurations in the policy. A layer is a building block that you can use to efficiently manage multiple network analysis or intrusion policies.

In most cases, you base custom policies on system-provided policies, but you can use another custom policy. However, all custom policies have a system-provided policy as the eventual base in a policy chain. Because rule updates can modify system-provided policies, importing a rule update may affect you even if you are using a custom policy as your base. If a rule update affects your deployment, the web interface marks affected policies as out of date.

Benefits of Custom Network Analysis Policies

By default, one network analysis policy preprocessors all unencrypted traffic handled by the access control policy. That means that all packets are decoded and preprocessed according to the same settings, regardless of the intrusion policy (and therefore intrusion rule set) that later examines them.

Initially, the system-provided Balanced Security and Connectivity network analysis policy is the default. A simple way to tune preprocessing is to create and use a custom network analysis policy as the default.

Tuning options available vary by preprocessor, but some of the ways you can tune preprocessors and decoders include:

- You can disable preprocessors that do not apply to the traffic you are monitoring. For example, the HTTP Inspect preprocessor normalizes HTTP traffic. If you are confident that your network does not include any web servers using Microsoft Internet Information Services (IIS), you can disable the preprocessor option that looks for IIS-specific traffic and thereby reduce system processing overhead.

Note If you disable a preprocessor in a custom network analysis policy, but the system needs to use that preprocessor to later evaluate packets against an enabled intrusion or preprocessor rule, the system automatically enables and uses the preprocessor although the preprocessor remains disabled in the network analysis policy web interface.

- Specify ports, where appropriate, to focus the activity of certain preprocessors. For example, you can identify additional ports to monitor for DNS server responses or encrypted SSL sessions, or ports on which you decode telnet, HTTP, and RPC traffic.

For advanced users with complex deployments, you can create multiple network analysis policies, each tailored to preprocess traffic differently. Then, you can configure the system to use those policies to govern the preprocessing of traffic using different security zones, networks, or VLANs.



Note Tailoring preprocessing using custom network analysis policies—especially multiple network analysis policies—is an advanced task. Because preprocessing and intrusion inspection are so closely related, you **must** be careful to allow the network analysis and intrusion policies examining a single packet to complement each other.

Benefits of Custom Intrusion Policies

In a newly created access control policy initially configured to perform intrusion prevention, the default action allows all traffic, but first inspects it with the system-provided Balanced Security and Connectivity intrusion policy. Unless you add access control rules or change the default action, all traffic is inspected by that intrusion policy.

To customize your intrusion prevention deployment, you can create multiple intrusion policies, each tailored to inspect traffic differently. Then, configure an access control policy with rules that specify which policy inspects which traffic. Access control rules can be simple or complex, matching and inspecting traffic using multiple criteria including security zone, network or geographical location, VLAN, port, application, requested URL, or user.

The main function of intrusion policies is to manage which intrusion and preprocessor rules are enabled and how they are configured, as follows:

- Within each intrusion policy, you should verify that all rules applicable to your environment are enabled, and improve performance by disabling rules that are not applicable to your environment. In an inline deployment, you can specify which rules should drop or modify malicious packets.
- Cisco recommendations allow you to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets.
- You can modify existing rules and write new standard text rules as needed to catch new exploits or to enforce your security policies.

Other customizations you might make to an intrusion policy include:

- The sensitive data preprocessor detects sensitive data such as credit card numbers and Social Security numbers in ASCII text. Note that other preprocessors that detect specific threats (back orifice attacks, several portscan types, and rate-based attacks that attempt to overwhelm your network with excessive traffic) are configured in network analysis policies.
- Global thresholds cause the system to generate events based on how many times traffic matching an intrusion rule originates from or is targeted to a specific address or address range within a specified time period. This helps prevent the system from being overwhelmed with a large number of events.
- Suppressing intrusion event notifications and setting thresholds for individual rules or entire intrusion policies can also can prevent the system from being overwhelmed with a large number of events.

- In addition to the various views of intrusion events within the web interface, you can enable logging to syslog facilities or send event data to an SNMP trap server. Per policy, you can specify intrusion event notification limits, set up intrusion event notification to external logging facilities, and configure external responses to intrusion events. Note that in addition to these per-policy alerting configurations, you can globally enable or disable email alerting on intrusion events for each rule or rule group. Your email alert settings are used regardless of which intrusion policy processes a packet.

Limitations of custom policies

Configuration coordination requirements

You **must** be careful that your configuration allows the network analysis and intrusion policies processing and examining a single packet to complement each other because preprocessing and intrusion inspection are so closely related.

- If you disable a preprocessor in a custom network analysis policy but the system needs to evaluate preprocessed packets against an enabled intrusion or preprocessor rule, the system automatically enables and uses the preprocessor although it remains disabled in the network analysis policy web interface.
- All packets, **regardless** of which network analysis policy preprocessed them, are subsequently matched to access control rules—and thus to potential inspection by intrusion policies—in their own process. Preprocessing a packet with a particular network analysis policy does **not** guarantee that the packet will be examined with any particular intrusion policy.

Performance optimization requirements

To get the performance benefits of disabling a preprocessor, you **must** make sure that none of your intrusion policies have enabled rules that require that preprocessor.

Access control policy configuration requirements

You **must** carefully configure your access control policy so it invokes the correct network analysis and intrusion policies to evaluate a particular packet.

- Each packet's handling is governed by a network analysis policy and intrusion policy pair, but the system does **not** coordinate the pair for you.
- Tailoring preprocessing using network analysis rules and custom policies is an **advanced** task due to the complexity of ensuring proper coordination between network analysis and access control rules.

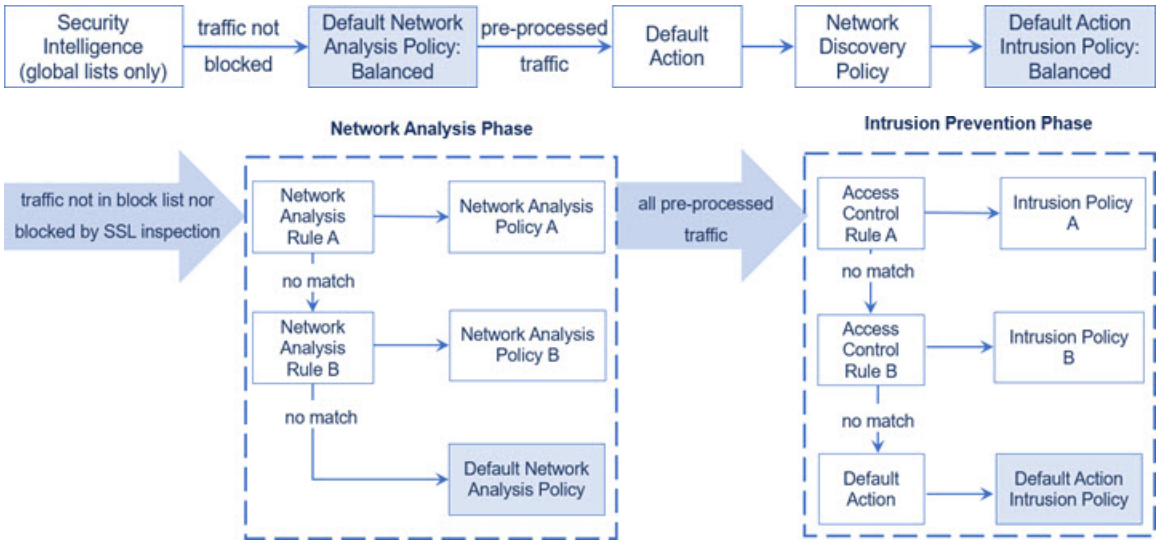
By default, the system uses one network analysis policy to preprocess all traffic handled by managed devices using a single access control policy. The system matches packets to any configured network analysis rules in top-down order by rule number. Traffic that does not match any network analysis rule is preprocessed by the default network analysis policy.

A default network analysis policy governs the preprocessing of *all* traffic handled by the access control policy. Initially, the system-provided Balanced Security and Connectivity network analysis policy is the default.

For advanced users with complex deployments, you can tailor preprocessing to specific security zones, networks, and VLANs by assigning custom network analysis policies to preprocess matching traffic. To accomplish this, you add custom *network analysis rules* to your access control policy. Each rule has an associated network analysis policy that governs the preprocessing of traffic that matches the rule.

Tip You configure network analysis rules as an advanced setting in an access control policy. Unlike other types of rules in the system, network analysis rules invoke—rather than being contained by—network analysis policies.

Figure 411: New access control policy: intrusion prevention



In this scenario, an access control policy is configured with two network analysis rules and a default network analysis policy:

- Network Analysis Rule A preprocessors matching traffic with Network Analysis Policy A. Later, you want this traffic to be inspected by Intrusion Policy A.
- Network Analysis Rule B preprocessors matching traffic with Network Analysis Policy B. Later, you want this traffic to be inspected by Intrusion Policy B.
- All remaining traffic is preprocessed with the default network analysis policy. Later, you want this traffic to be inspected by the intrusion policy associated with the access control policy's default action.

After the system preprocessors traffic, it can examine the traffic for intrusions. The diagram shows an access control policy with two access control rules and a default action:

- Access Control Rule A allows matching traffic. The traffic is then inspected by Intrusion Policy A.
- Access Control Rule B allows matching traffic. The traffic is then inspected by Intrusion Policy B.
- The access control policy's default action allows matching traffic. The traffic is then inspected by the default action's intrusion policy.

Note that for a single connection, although the system selects a network analysis policy before an access control rule, some preprocessing (notably application layer preprocessing) occurs after access control rule selection. This does **not** affect how you configure preprocessing in custom network analysis policies.

License Requirements for Network Analysis and Intrusion Policies

Threat Defense License

IPS

Classic License

Protection

Requirements and Prerequisites for Network Analysis and Intrusion Policies

Model support

Any.

Supported domains

Any

User roles

- Admin
- Intrusion Admin

Guidelines and Limitations for Network Analysis and Intrusion Policies

- A high percentage of traffic with small packets causes Snort performance to decrease. This behaviour is observed even when all the preprocessors are disabled.
- When you attempt to deploy a configuration change on a threat defense device with low memory, snort deployment is also triggered. This results in high consumption of RSS memory. Snort memory usage is also impacted if you deploy large configurations on the device, such as multiple IPS policies containing a large number of snort IPS rules, network objects, and access-control lists. You can mitigate such memory issues by optimizing the configuration. For best practices on how to configure access control rules to optimize the configuration, see Best Practices for Access Control Rules.
- If you increase the memory of a Threat Defense Virtual instance, you must redeploy the configuration for Snort 3 to utilize the additional memory.

Note The Snort 3 memory allocation is not automatically adjusted when you increase the memory of the Threat Defense Virtual instance. You must redeploy the configuration to regenerate relevant configuration files, such as `memory_allocation.lua`, which apply the updated resource limits to Snort 3.

- If an SIP stream is followed by RTP streams from the same connection, Snort inspects the initial SIP communication that is sent for connection establishment and allows SIP traffic. The RTP streams that follow the SIP communication are also trusted by default and bypass the configured rules. To prevent such scenarios, trusting the parent SIP connection or adding the parent SIP connection to a prefilter rule ensures that only the SIP stream bypasses Snort inspection and allows the subsequent RTP streams to be evaluated separately against the corresponding rules.
- If several Snort rules with the same action match a packet in the Management Center, an event is logged for each rule. However, if the matching rules have different actions, only the rule with the highest priority action generates an event. The action priority from highest to lowest is: pass, reset, block, drop, alert, log.
- When intrusion packet events are forwarded via syslog or the eStreamer fully-qualified event feed, the packet data field may be truncated due to limitations in the buffer size available for syslog generation and the eStreamer. In such scenarios, the packet length will not match the actual packet data that is sent.

The Navigation Panel: Network Analysis and Intrusion Policies

Network analysis and intrusion policies use similar web interfaces to edit and save changes to their configurations.

A navigation panel appears on the left side of the web interface when you are editing either type of policy. The following graphic shows the navigation panel for the network analysis policy (left) and the intrusion policy (right).



A dividing line separates the navigation panel into links to policy settings you can configure with (below) or without (above) direct interaction with policy layers. To navigate to any settings page, click its name in the navigation panel. Dark shading of an item in the navigation panel highlights your current settings page. For

example, in the illustration above the Policy Information page would be displayed to the right of the navigation panel.

Policy Information

The Policy Information page provides configuration options for commonly used settings. As shown in the illustration for the network analysis policy panel above, a **Policy Change icon** appears next to **Policy Information** in the navigation panel when the policy contains unsaved changes. The icon disappears when you save your changes.

Rules (intrusion policy only)

The Rules page in an intrusion policy allows you to configure rule states and other settings for shared object rules, standard text rules, and preprocessor rules.

Cisco Recommendations (intrusion policy only)

The Cisco Recommendations page in an intrusion policy allows you to associate the operating systems, servers, and client application protocols detected on your network with intrusion rules specifically written to protect those assets. This allows you to tailor your intrusion policy to the specific needs of your monitored network.

Settings (network analysis policy) and Advanced Settings (intrusion policy)

The Settings page in a network analysis policy allows you to enable or disable preprocessors and access preprocessor configuration pages. Expanding the **Settings** link displays sublinks to individual configuration pages for all enabled preprocessors in the policy.

The Advanced Settings page in an intrusion policy allows you to enable or disable advanced settings and access configuration pages for those advanced settings. Expanding the **Advanced Settings** link displays sublinks to individual configuration pages for all enabled advanced settings in the policy.

Policy Layers

The Policy Layers page displays a summary of the layers that comprise your network analysis or intrusion policy. Expanding the Policy Layers link displays sublinks to summary pages for the layers in your policy. Expanding each layer sublink displays further sublinks to the configuration pages for all rules, preprocessors, or advanced settings that are enabled in the layer.

Conflicts and Changes: Network Analysis and Intrusion Policies

When you edit a network analysis or intrusion policy, a **Policy Change icon** appears next to **Policy Information** in the navigation panel to indicate that the policy contains unsaved changes. You must save (or *commit*) your changes before the system recognizes them.



Note After you save, you must deploy the network analysis or intrusion policy for your changes to take effect. If you deploy a policy without saving, the system uses the most recently saved configuration.

Resolving Editing Conflicts

The Network Analysis Policy page (**Policies** > **Access Control heading** > **Access Control**, and then click **Network Analysis Policy** or **Policies** > **Access Control heading** > **Intrusion**, and then click **Network Analysis Policies**) and Intrusion Policy page (**Policies** > **Access Control heading** > **Intrusion**) display whether each policy has unsaved changes, as well as information about who is currently editing the policy. Cisco recommends that only one person edit a policy at a time. If you are performing simultaneous editing, the consequences are as follows:

- If you are editing a network analysis or intrusion policy at the same time another user is editing the same policy, and the other user saves their changes to the policy, you are warned when you commit the policy that you will overwrite the other user's changes.
- If you are editing the same network analysis or intrusion policy via multiple web interface instances as the same user, and you save your changes for one instance, you cannot save your changes for the other instance.

Resolving Configuration Dependencies

To perform their particular analysis, many preprocessors and intrusion rules require that traffic first be decoded or preprocessed in a certain way, or have other dependencies. When you save a network analysis or intrusion policy, the system either automatically enables required settings, or warns you that disabled settings will have no effect on traffic, as follows:

- You cannot save an intrusion policy if you added an SNMP rule alert but did not configure SNMP alerting. You must either configure SNMP alerting or disable the rule alert, then save again.
- You cannot save an intrusion policy if it includes enabled sensitive data rules but you have not enabled the sensitive data preprocessor. You must either allow the system to enable the preprocessor and save the policy, or disable the rules and save again.
- If you disable a required preprocessor in a network analysis policy, you can still save the policy. However, the system automatically uses the disabled preprocessor with its current settings, even though the preprocessor remains disabled in the web interface.
- If you disable inline mode in a network analysis policy but enable the Inline Normalization preprocessor, you can still save the policy. However, the system warns you that normalization settings will be ignored. Disabling inline mode also causes the system to ignore other settings that allow preprocessors to modify or block traffic, including checksum verification and rate-based attack prevention.

Committing, Discarding, and Caching Policy Changes

While editing a network analysis or intrusion policy, if you exit the policy editor without saving your changes, the system caches those changes. Your changes are cached even when you log out of the system or experience a system crash. The system cache can store unsaved changes for one network analysis and one intrusion policy per user; you must commit or discard your changes before editing another policy of the same type. The system discards the cached changes when you edit another policy without saving your changes to the first policy, or when you import an intrusion rule update.

You can commit or discard policy changes on the Policy Information page of either the network analysis or intrusion policy editor.

In the Secure Firewall Management Center configuration, you can control:

- whether you are prompted (or required) to comment on your network analysis or intrusion policy changes when you commit them
- whether changes and comments are recorded in the audit log

Exiting a Network Analysis or Intrusion Policy

Procedure

If you want to exit the network analysis or intrusion policy advanced editor, you have the following choices:

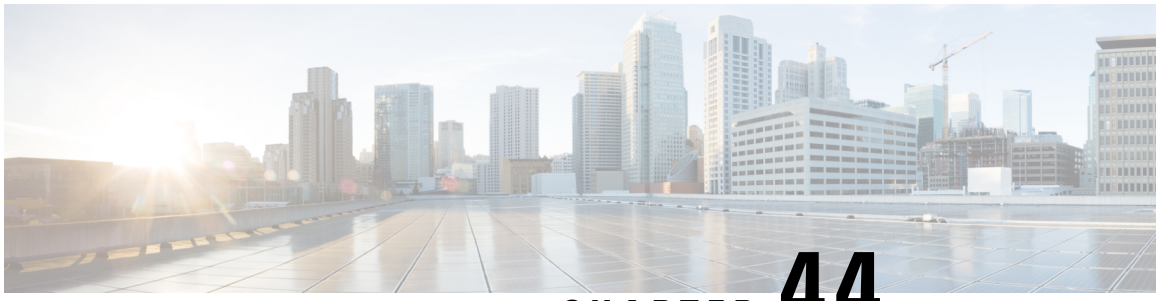
- Cache — To exit the policy and cache changes, choose any menu or other path to another page. On exiting, click **Leave page** when prompted, or click **Stay on page** to remain in the advanced editor.
- Discard — To discard unsaved changes, click **Discard Changes** on the Policy Information page, then click **OK**.
- Save — To save changes to the policy, click **Commit Changes** on the Policy Information page. If prompted, enter a comment, and then click **OK**.



PART IX

Decryption Policies and Encrypted Visibility for Access Control

- Traffic Decryption Overview, on page 1707
- Decryption Policies, on page 1727
- Decryption Rules, on page 1745
- Decryption rules and Policy Example, on page 1793
- Encrypted Visibility Engine, on page 1803



CHAPTER 44

Traffic Decryption Overview

These topics provide an overview of Transport Layer Security/Secure Sockets Layer (TLS/SSL) inspection, discuss the prerequisites for TLS/SSL inspection configuration, and detail deployment scenarios.

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

For more information about SSL and TLS protocols, see a resource such as SSL vs. TLS - What's the Difference?

- Traffic decryption, on page 1707
- How TLS/SSL handshakes work, on page 1708
- Decryption rule and policy basics, on page 1713
- TLS crypto acceleration, on page 1720
- History for decryption policy , on page 1723

Traffic decryption

Traffic decryption enables deep inspection of traffic for analysis.

Traffic handling options

Most traffic on the internet is encrypted and in most cases, you might choose not to decrypt it. You can glean some information from encrypted traffic and you can also block it from your network if desired.

Your choices are:

- Decrypt the traffic and subject it to the full array of deep inspection:
  - Advanced Malware Protection
  - Security intelligence
  - Threat Intelligence Director
  - Application detectors

    - URL and category filtering

- Leave the traffic encrypted and set up your access control and decryption policy to look for and potentially block:
    - Old protocol versions (such as Secure Sockets Layer)
    - Unsecure cipher suites
    - Applications with high risk and low business relevance
    - Untrusted issuer Distinguished Names

Access control policy integration

An access control policy is the main configuration that invokes subpolicies and other configurations, including a decryption policy. If you associate a decryption policy with access control, the system uses that decryption policy to handle encrypted sessions before it evaluates the sessions with access control rules. If you do not configure TLS/SSL inspection, or your devices do not support it, access control rules handle all encrypted traffic.

Access control rules also handle encrypted traffic when your TLS/SSL inspection configuration allows the traffic to pass. However, some access control rule conditions require unencrypted traffic, so encrypted traffic might match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improves performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.



Note As long as your managed devices have Snort 3 enabled, the system supports decrypting TLS 1.3 traffic. You can enable TLS 1.3 decryption in an decryption policy's advanced options; for more information, see Decryption policy advanced options, on page 1742.

Notes

Decryption rules require processing overhead that can impact performance. Before you decide to decrypt traffic, see Best practice for deciding when to decrypt traffic, on page 1714.

The system does not support mutual authentication; that is, you cannot upload a client certificate to the Secure Firewall Management Center and use it for **Decrypt - Resign** or **Decrypt - Known Key** decryption rule actions.

If you set the value of TCP maximum segment size (MSS) using FlexConfig, the observed MSS could be less than your setting. For more information, see TCP MSS, on page 714.

How TLS/SSL handshakes work

In this documentation, the term *TLS/SSL handshake* represents the two-way handshake that initiates encrypted sessions in both the SSL protocol and its successor protocol, TLS.

In an inline deployment, the system processes the TLS/SSL handshake, potentially modifying the ClientHello message and acting as a TCP proxy server for the session.

The figure shows an inline deployment.



Summary

The key components involved in the TLS/SSL handshake process are:

- Client: Initiates the encrypted session by sending a ClientHello message specifying multiple supported values for each encryption attribute
- Server: Responds with a ServerHello message specifying a single supported value for each encryption attribute, determining the encryption method for the secure session
- Managed device: Monitors TCP sessions for encrypted session initiation attempts and can act as a TCP proxy server
- Handshake messages: Specialized packets that communicate encryption attributes between client and server

Workflow

These stages describe how TLS/SSL handshakes establish encrypted sessions:

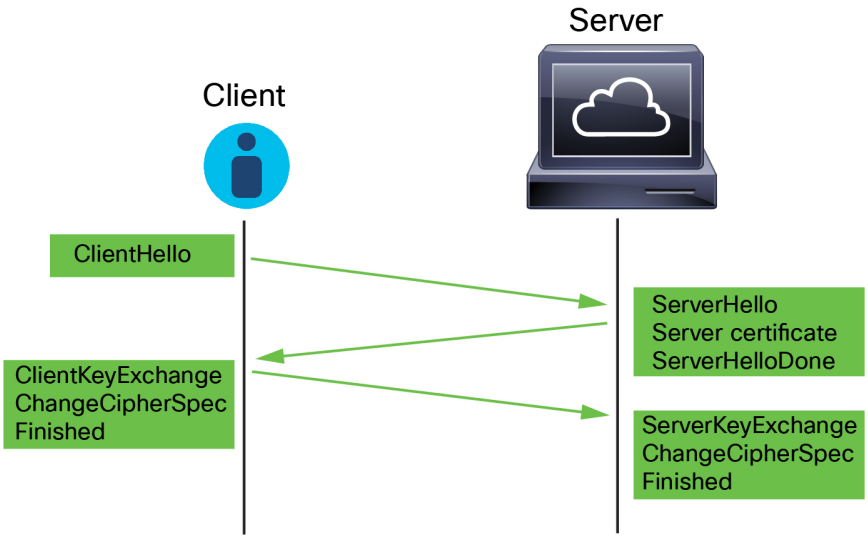
1. The client establishes a TCP connection with the server after successfully completing the TCP three-way handshake.
2. The managed device monitors the TCP session for any attempt to initiate an encrypted session.
3. The client and server exchange specialized handshake messages to establish an encrypted session.
   - ClientHello—The client specifies multiple supported values for each encryption attribute.
   - ServerHello—The server specifies a single supported value for each encryption attribute, and the ServerHello response determines which encryption method the system uses during the secure session.
4. After the TLS/SSL handshake completes, the managed device caches encrypted session data and server certificate data.

   This caching allows session resumption without requiring the full handshake and enables faster handshake processing in subsequent sessions that use the same certificate.

ClientHello message handling

The client sends the ClientHello message to the server, which acts as the packet destination, when a secure connection can be established. The client uses this message to initiate the TLS/SSL handshake to respond to a ServerHello message from the destination server.

The following figure shows an example. Also see RFC 8446, sec. 4 . You can also consult a resource such as What Happens in a TLS Handshake? at cloudflare.com.



ClientHello message process

The process consists of these steps:

1. ClientHello initiates the process.

   The ClientHello message contains the Server Name Indication (SNI), which has the server's fully qualified domain name.

2. After a managed device processes a ClientHello message and transmits it to the destination server, the server determines whether it supports the decryption attributes the client specified in the message. If it does not support those attributes, the server sends a handshake failure alert to the client. If it supports those attributes, the server sends the ServerHello message. If the agreed-upon key exchange method uses certificates for authentication, the server certificate message immediately follows the ServerHello message.

   The server certificate contains the Subject Alternative Name (SAN), which can have fully qualified domain names and IP addresses. For more information about the SAN, see Distinguished names, on page 2364.

3. When the managed device receives these messages, it attempts to match them with decryption rules configured on the system. These messages contain information that was absent from either the ClientHello message or the session data cache. Specifically, the system can potentially match these messages on decryption rules' Distinguished Names, Certificate Status, Cipher Suites, and Versions conditions.

The entire process is encrypted.

Data exchange

If you configure TLS/SSL decryption, when a managed device receives a ClientHello message, the system attempts to match the message to decryption rules that have the **Decrypt - Resign** , or **Decrypt - Known Key** action. The match relies on data from the ClientHello message and from cached server certificate data. The table lists the possible types of data available for matching conditions.

Table 99: Data Availability for Decryption rule Conditions

Decryption rule Condition	Data Present In
Zones	ClientHello
Networks	ClientHello
VLAN Tags	ClientHello
Ports	ClientHello
Users	ClientHello
Applications	ClientHello (Server Name Indicator extension)
Categories	ClientHello (Server Name Indicator extension)
Certificate	Server certificate (potentially cached)
Distinguished Names	Server certificate (potentially cached)
Certificate Status	Server certificate (potentially cached)
Cipher Suites	ServerHello
Versions	ServerHello



Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. Do not use **Cipher Suite** and **Version** with **Decrypt - Resign** or **Decrypt - Known Key** rule actions. These conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

ClientHello message modifications

If the ClientHello message matches a **Decrypt - Resign** , or **Decrypt - Known Key** rule, the system modifies the ClientHello message.

- (TLS 1.2 only; TLS 1.3 does not support compression.) Compression methods—Strips the `compression_methods` element, which specifies the compression methods the client supports. The system cannot decrypt compressed sessions.
- Cipher suites—Strips cipher suites from the `cipher_suites` element if the system does not support them. If the system does not support any of the specified cipher suites, the system transmits the original, unmodified element. This modification reduces the Unknown Cipher Suite and Unsupported Cipher Suite types of undecryptable traffic.
- Session identifiers—Strips any value from the `Session Identifier` element and the SessionTicket extension (RFC 5077, sec 3.2) that does not match cached session data. If a ClientHello value matches cached data, an interrupted session can resume without the client and server performing the full TLS/SSL handshake. This modification improves the likelihood of session resumption and reduces the Session Not Cached incidents of undecryptable traffic..

- Elliptic curves—Strips elliptic curves from the Supported Elliptic Curves extension if the system does not support them. If the system does not support any of the specified elliptic curves, the managed device removes the extension and strips any related cipher suites from the `cipher_suites` element.
- ALPN extensions—Strips any value from the Application-Layer Protocol Negotiation (ALPN) extension that is unsupported in the system (for example, the HTTP/2 protocol).
- Other Extensions—Strips the Next Protocol Negotiation (NPN) and TLS Channel IDs extensions.

  Decryption rules with a **Decrypt - Resign** , or **Decrypt - Known Key** action now natively support the Extended Master Secret (EMS) extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627 .

After the system modifies the ClientHello message, it determines whether the message passes access control evaluation (which can include deep inspection). If the message passes, the system transmits it to the destination server.

If the ClientHello message does *not* match a **Decrypt - Resign** , or **Decrypt - Known Key** rule, the system does not modify the message. It then determines whether the message passes access control evaluation (which can include deep inspection). If the message passes inspection, the system transmits it to the destination server.

ClientHello is *not* modified if traffic matches a **Monitor** rule condition.

Man-in-the-middle

Direct communication between the client and server is not possible during the TLS/SSL handshake. After the message is modified, the Message Authentication Codes (MACs) computed by the client and server no longer match. For all subsequent handshake messages (and for the encrypted session once established), the managed device acts as a man-in-the-middle. It creates two TLS/SSL sessions, one between client and managed device, one between managed device and server. Each session contains distinct cryptographic session details.

Note The cipher suites that the system can decrypt are frequently updated and do not correspond directly to the cipher suites you can use in decryption rule conditions. For the current list of decryptable cipher suites, contact Cisco TAC .

How ServerHello and server certificate messages work

Summary

The key components involved in ServerHello and server certificate message handling are:

- Managed device: Processes ServerHello and server certificate messages and performs rule matching
- decryption rules: Define actions to take when messages match specific criteria
- Server certificate data: Certificate information used for matching against internal certificate objects
- TLS/SSL handshake: The secure connection establishment process
- Certificate authority (CA): Used for re-signing certificates in decrypt-resign actions

Workflow

These stages describe how ServerHello and server certificate message handling works:

1. The managed device receives ServerHello and server certificate messages and checks for rule matches.

   If the messages do not match any decryption rules, the managed device performs the Decryption policy default actions, on page 1739.

2. When messages match a rule that belongs to a decryption policy associated with an access control policy, the managed device performs actions based on the rule configuration.

   - **Monitor**: The TLS/SSL handshake continues to completion. The managed device tracks and logs traffic but does not decrypt it.
   - **Block or Block with Reset**: The managed device blocks the TLS/SSL session and, if configured, resets the TCP connection.
   - **Do Not Decrypt**: The TLS/SSL handshake continues to completion. The managed device does not decrypt the application data exchanged during the TLS/SSL session.

3. For decrypt actions with known key or resign methods, the managed device performs certificate matching and processing.

   - **Decrypt - Known Key**: The managed device attempts to match the server certificate data to an Internal Certificate object previously imported into the Secure Firewall Management Center. Because you cannot generate an Internal Certificate object, and you must possess its private key, we assume you own the server on which you're using known key decryption.
   - **Decrypt - Resign**: The managed device processes the server certificate message and re-signs the server certificate with the previously imported or generated certificate authority (CA). The TLS/SSL handshake continues to completion. The managed device then uses the uploaded private key to decrypt and re-encrypt the application data exchanged during the TLS/SSL session.

   If the certificate matches a known certificate, the TLS/SSL handshake continues to completion. The managed device uses the uploaded private key to decrypt and re-encrypt the application data exchanged during the TLS/SSL session.

   If the server changes its certificate between the initial connection with the client and subsequent connections, you must import the new server certificate in the Secure Firewall Management Center for future connections to be decrypted.



Note The system does not support mutual authentication; that is, you cannot upload a client certificate to the Secure Firewall Management Center and use it for **Decrypt - Resign** or **Decrypt - Known Key** decryption rule actions.

Decryption rule and policy basics

This section discusses information you should keep in mind when creating your Decryption rules and policies.

Key information for decryption policy creation

Consider this information when creating your decryption policies and rules.

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

For more information about SSL and TLS protocols, refer to a resource such as SSL vs. TLS - What's the Difference?

Guidelines for traffic decryption

Traffic that is encrypted when it passes through the system can be allowed or blocked, but it *cannot* be subjected to deep inspection or the full range of policy enforcement (such as intrusion prevention).

All encrypted connections are sent through the decryption policy to determine if they should be decrypted or blocked.

You can also configure decryption rules to block encrypted traffic of types you know you do not want on your network, such as traffic that uses the nonsecure SSL protocol or traffic with an expired or invalid certificate.

If unblocked, whether or not decrypted, traffic goes through the access control policy for a final allow or block decision.

Only *decrypted* traffic takes advantage of the system's threat defense and policy enforcement features, including:

- Advanced Malware Protection
- Security intelligence
- Threat Intelligence Director
- Application detectors
- URL and category filtering

Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which can reduce overall system performance.

Encrypted traffic can be allowed or blocked by policy; encrypted traffic *cannot* be inspected.

Decrypted traffic is subject to threat defense and policy enforcement; decrypted traffic can be allowed or blocked by policy.

Detects encrypted application traffic using StartTLS (SMTPS, POPS, FTPS, TelnetS, IMAPS). Also identifies certain encrypted applications based on Server Name Indication in the TLS ClientHello message or subject distinguished name from the server certificate.

Best practice for deciding when to decrypt traffic

When not to decrypt traffic

You should not decrypt traffic if doing so is forbidden by:

- Law; for example, some jurisdictions forbid decrypting financial information
- Company policy; for example, your company might forbid decrypting privileged communications
- Privacy regulations
- Traffic that uses certificate pinning (also referred to as *TLS/SSL pinning*) must remain encrypted to prevent breaking the connection

(Snort 3.) Decryption policy is *not* bypassed for any connections that match access control rules with actions of Trust, Block, or Block with Reset, unless the traffic is prefiltered. The encrypted traffic is first evaluated by decryption policy and then proceeds to the access control policy, where a final allow or block decision is made.

Encrypted traffic can be allowed or blocked on any decryption rule condition, including, but not limited to:

- Certificate status (for example, expired or invalid certificate)
- Protocol (for example, the nonsecure SSL protocol)
- Network (security zone, IP address, VLAN tag, and so on)
- URL category and reputation
- Port
- User group

Decryption rules provide a **Do Not Decrypt** action for traffic you do not want to decrypt; for more information, see Decryption rule Do Not Decrypt action, on page 1778.

Note The related information links at the end of this topic explain how some aspects of rule evaluation work. Conditions such as URL and application filtering have limitations with respect to encrypted traffic. Make sure you understand those limitations.

For more information about using URL filtering in **Do Not Decrypt** rules, see Decryption rule Do Not Decrypt action, on page 1778.

When to decrypt traffic

All encrypted traffic must be decrypted to take advantage of the system's threat protection and policy enforcement features. If your managed device has sufficient memory and processing power to decrypt traffic, you should decrypt traffic that is not prohibited by law or regulation.

If you must decide what traffic to decrypt, base your decision on the risk of allowing the traffic on your network. The system provides a flexible framework for classifying traffic using rule conditions, which include URL reputation, cipher suite, protocol, and many other factors.

Decrypt and re-sign (outgoing traffic)

Decrypt and re-sign of traffic enables the system to act as a man in the middle, intercepting, decrypting, and (if the traffic is allowed to pass) inspecting and re-encrypting traffic. It is used with outgoing traffic where the destination server is outside your protected network and requires the client to trust the firewall's certificate to complete the connection.

How decrypt and re-sign works

The Firewall Threat Defense device negotiates with the client using an internal Certificate Authority (CA) object specified in the rule and builds a TLS/SSL tunnel between the client and the Firewall Threat Defense device. At the same time, the device connects to the destination web site and creates a TLS/SSL tunnel between the server and the Firewall Threat Defense device.

Thus, the client sees the CA certificate configured for the decryption rule instead of the certificate from the destination server. The client must trust the firewall's certificate to complete the connection. The Firewall Threat Defense device then performs decryption/re-encryption in both directions for traffic between the client and the destination server.

Prerequisite

To use the **Decrypt - Resign** rule action, you must create an internal CA object using a CA file and paired private key file. You can generate a CA and private key in the system if you don't already have them.

Note The system does not support mutual authentication; that is, you cannot upload a client certificate to the Secure Firewall Management Center and use it for **Decrypt - Resign** or **Decrypt - Known Key** decryption rule actions.

Known key decryption for incoming traffic

The **Decrypt - Known Key** decryption rule action uses a server's private key to decrypt traffic. The **Decrypt - Known Key** rule action is used with incoming traffic, where the destination server is inside your protected network.

The main purpose of decrypting with a known key is to protect your servers from external attacks.

Prerequisites and requirements

To use the **Decrypt - Known Key** rule action, you must create an internal certificate object using the server's certificate file and paired private key file.

Note The system does not support mutual authentication; that is, you cannot upload a client certificate to the Secure Firewall Management Center and use it for **Decrypt - Resign** or **Decrypt - Known Key** decryption rule actions.

Other decryption rule actions

These topics discuss other decryption rule actions.

Decryption rule components

Each decryption rule has the following components.

State

A rule can have either of two states: enabled or disabled. By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.

Position

Rules in a decryption policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number.

Conditions

Conditions specify the specific traffic the rule handles. Conditions can match traffic by security zone, network or geographical location, VLAN, port, application, requested URL category and reputation, user, certificate, certificate subject or issuer, certificate status, cipher suite, or encryption protocol version. The use of conditions can depend on target device licenses.

Action

A rule's action determines how the system handles matching traffic. You can monitor, allow, block, or decrypt encrypted matching traffic. Decrypted traffic is subject to further inspection. Note that the system does *not* inspect blocked encrypted traffic.

Logging

A rule's logging settings govern the records the system keeps of the traffic it handles. You can keep a record of traffic that matches a rule. You can log a connection when the system blocks an encrypted session or allows it to pass without decryption, according to the settings in an decryption policy. You can also force the system to log connections that it decrypts for further evaluation by access control rules, regardless of how the system later handles or inspects the traffic. You can log connections to the Secure Firewall Management Center database, as well as to the system log (syslog) or to an SNMP trap server.

For more information about logging, see Best Practices for Connection Logging in the *Cisco Secure Firewall Management Center Administration Guide*.



Tip Properly creating and ordering decryption rules is a complex task. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations. To help ensure that the system handles traffic as you expect, the decryption policy interface has a robust warning and error feedback system for rules.

Categories

For information about using decryption rule categories (such as Applications, Category, and Cert Status), see Decryption Rule conditions, on page 1758.

Decryption Rule order evaluation

Decryption Rule order evaluation determines the sequence in which the system evaluates decryption rules in a policy.

Rule evaluation process

When you create a decryption rule in a decryption policy , you specify its position using the **Insert** list in the rule editor. Decryption rules in an a decryption policy are numbered, starting at 1. The system matches traffic to decryption rules in top-down order by ascending rule number.

In most cases, the system handles network traffic according to the *first* decryption rule where *all* the rule's conditions match the traffic. Except in the case of Monitor rules (which log traffic but do not affect traffic flow), the system does *not* continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, VLAN, port, application, requested URL category and reputation, user, certificate, certificate distinguished name, certificate status, cipher suite, or encryption protocol version.

Each rule also has an *action*, which determines whether you monitor, block, or inspect matching encrypted or decrypted traffic with access control. Note that the system does *not* further inspect encrypted traffic it blocks. It does subject encrypted and undecryptable traffic to access control. However, access control rule conditions require unencrypted traffic, so encrypted traffic matches fewer rules.

Rules that use *specific* conditions (such as network and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your rules.



Note Proper decryption rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs.

In addition to ordering rules by number, you can group rules by category. By default the system provides three categories: Administrator, Standard, and Root. You can add custom categories, but you cannot delete the system-provided categories or change their order.

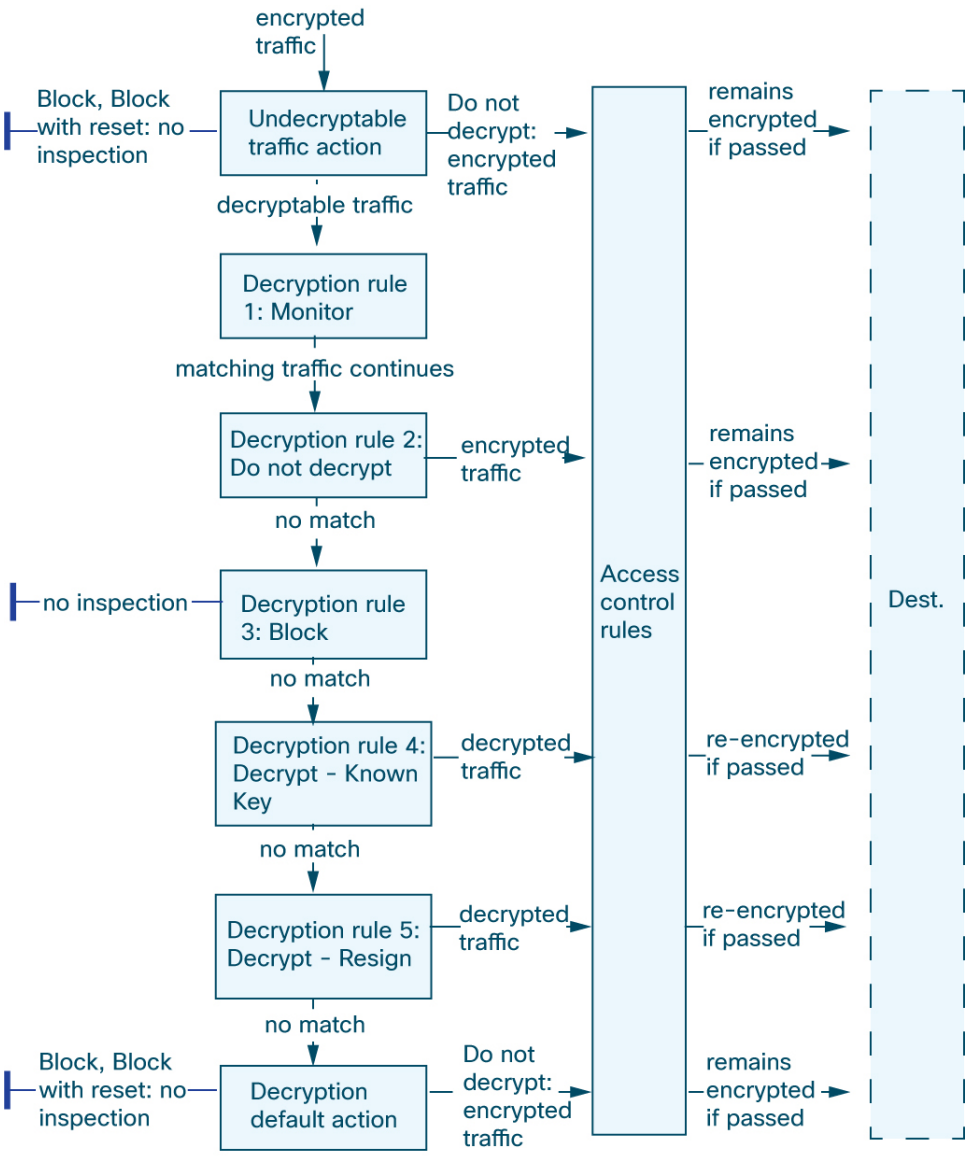
Related Topics

Best practices for access control rules, on page 1625

Multi-rule example

This reference example demonstrates how the firewall handles traffic using a decryption policy that contains multiple rules.

The following scenario summarizes the ways that decryption rules handle traffic in an inline deployment.



In this scenario, traffic is evaluated as follows:

- **Undecryptable Traffic Action** evaluates encrypted traffic first. For traffic the system cannot decrypt, the system either blocks it without further inspection or passes it for access control inspection. Encrypted traffic that does not match continues to the next rule.
- **Decryption rule 1: Monitor** evaluates encrypted traffic next. Monitor rules track and log encrypted traffic but do not affect traffic flow. The system continues to match traffic against additional rules to determine whether to permit or deny it.
- **Decryption rule 2: Do Not Decrypt** evaluates encrypted traffic third. Matching traffic is not decrypted; the system inspects this traffic with access control, but not file or intrusion inspection. Traffic that does not match continues to the next rule.

- **Decryption rule 3: Block** evaluates encrypted traffic fourth. Matching traffic is blocked without further inspection. Traffic that does not match continues to the next rule.
- **Decryption rule 4: Decrypt - Known Key** evaluates encrypted traffic fifth. Matching traffic incoming to your network is decrypted using a private key you upload. The decrypted traffic is then evaluated against access control rules. Access control rules handle decrypted and unencrypted traffic identically. The system can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the decryption rule continues to the next rule.
- **Decryption rule 5: Decrypt - Resign** is the final rule. If traffic matches, the system re-signs the server certificate with an uploaded CA certificate and decrypts traffic. The decrypted traffic is then evaluated against access control rules, which treat decrypted and unencrypted traffic the same. This additional inspection allows the system to block traffic. All remaining traffic is re-encrypted before being sent to its destination. Traffic that does not match the decryption rule rule continues to the next rule.
- **Decryption policy Default Action** handles all traffic that does not match any of the decryption rules. The default action either blocks encrypted traffic without further inspection or does not decrypt it, passing it for access control inspection.

TLS crypto acceleration

TLS crypto acceleration accelerates the following:

- TLS/SSL encryption and decryption
- VPN, including TLS/SSL and IPsec

Supported hardware and acceleration details

The following hardware models support TLS crypto acceleration:

- Secure Firewall 3100
- Secure Firewall 4200
- Firepower 2100
- Firepower 4100/9300

  For information about TLS crypto acceleration support on Firepower 4100/9300 Firewall Threat Defense container instances, see the *FXOS Configuration Guide*.

TLS crypto acceleration is *not* supported on any virtual appliances or on any hardware except for the preceding.



Note For more information about TLS crypto acceleration and the 4100/9300, see the *FXOS Configuration Guide*.

Features *not* supported by TLS crypto acceleration include:

- Managed devices where Firewall Threat Defense container instance is enabled.

- If the inspection engine is configured to preserve connections and the inspection engine fails unexpectedly, TLS/SSL traffic is dropped until the engine restarts.

  This behavior is controlled by the **configure snort preserve-connection {enable | disable}** command.

TLS crypto acceleration guidelines and limitations

HTTP-only performance

Using TLS crypto acceleration on a managed device that is not decrypting traffic can affect performance.

Federal information processing standards (FIPS)

If TLS crypto acceleration and Federal Information Processing Standards (FIPS) are both enabled, connections with the following options fail:

- RSA keys less than 2048 bytes in size
- Rivest cipher 4 (RC4)
- Single Data Encryption Standard (single DES)
- Merkle–Damgard 5 (MD5)
- SSL v3

FIPS is enabled when you configure the Firewall Management Center and managed devices to operate in a security certifications compliance mode. To allow connections when operating in those modes, you can configure web browsers to accept more secure options.

For more information:

- Ciphers supported by FIPS: Configure SSL settings, on page 885.
- Security certifications compliance modes.
- Common Criteria.

TLS heartbeat

Some applications use the *TLS heartbeat* extension to the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols defined by RFC6520. TLS heartbeat provides a way to confirm the connection is still alive—either the client or server sends a specified number of bytes of data and requests the other party echo the response. If this is successful, encrypted data is sent.

When a managed device with TLS crypto acceleration enabled encounters a packet that uses the TLS heartbeat extension, the managed device takes the action specified by the setting for **Decryption Errors** in the decryption policy's **Undecryptable Actions**:

- Block
- Block with reset

For more information, see Default handling options for undecryptable traffic, on page 1739.

To determine whether applications are using TLS heartbeat, see Troubleshoot TLS heartbeat, on page 1784.

You can configure a **Max Heartbeat Length** in a Network Analysis Policy (NAP) to determine how to handle TLS heartbeats. For more information, refer to *The SSL Preprocessor* section in the "Custom Snort 2 Intrusion Policies for Access Control" document.

TLS/SSL oversubscription

TLS/SSL oversubscription is a state where a managed device is overloaded with TLS/SSL traffic. Any managed device can experience TLS/SSL oversubscription but only managed devices that support TLS crypto acceleration provide a configurable way to handle it.

When a managed device with TLS crypto acceleration enabled is oversubscribed, any packet received by the managed device is acted on according to the setting for **Handshake Errors** in the decryption policy's **Undecryptable Actions**:

- Inherit default action
- Do not decrypt
- Block
- Block with reset

If the setting for **Handshake Errors** in the decryption policy's **Undecryptable Actions** is **Do Not decrypt** and the associated access control policy is configured to inspect the traffic, inspection occurs; decryption does *not* occur.

If a significant amount of oversubscription is occurring, you have these options:

- Upgrade your managed devices to increase TLS/SSL processing capacity.
- Change your decryption policies to add **Do Not Decrypt** rules for traffic that is not a high priority to decrypt.

Keep these guidelines in mind if your managed device has TLS crypto acceleration enabled.

View the status of TLS crypto acceleration

This task allows you to determine if TLS crypto acceleration is enabled on your managed devices.

Perform this task in the Firewall Management Center to check the TLS crypto acceleration status for your managed devices.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Devices** > **Device Management**.

Step 3 Click **Edit** ( ) to edit a managed device.

Step 4 Click **Device** page.

TLS crypto acceleration status is displayed in the General section.

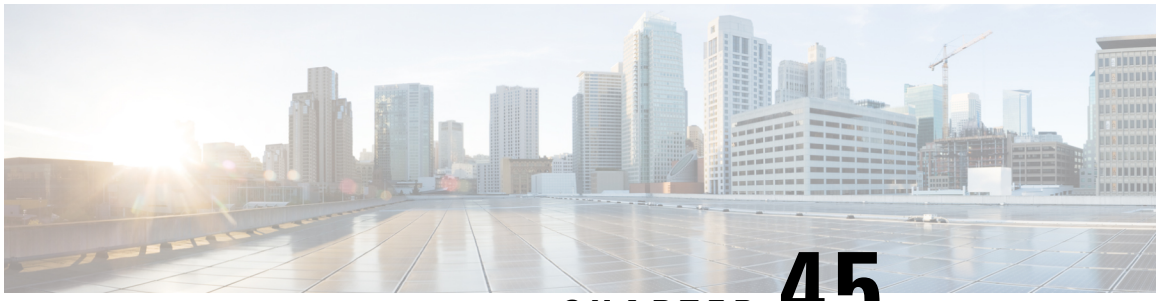
History for decryption policy

Provides a chronological overview of decryption policy features, including version support and configuration changes.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Decryption policy.	7.3.0	7.3.0	Feature renamed to *decryption policy* to better reflect what it does. We now enable you to configure a decryption policy with one or more **Decrypt - Resign** or **Decrypt - Known Key** rules at the same time. New/modified screens: • **Policies** > **Access Control heading** > **Decryption** (create new decryption policy) • The Create Decryption Policy dialog box now has two tab pages: **Outbound Connections** and **Inbound Connections** . • **Policies** > **Access Control heading** > **Decryption** (edit a decryption rule) **Advanced Settings** has new options discussed in TLS 1.3 decryption best practices, on page 1743 . • **Policies** > **Access Control Heading** > **Access Control** (edit an access control policy), click the word **Decryption** to associate a decryption policy with an access control policy.
TLS 1.3 decryption.	7.2.0	7.2.0	You can now enable TLS 1.3 decryption in an SSL policy's advanced actions. TLS 1.3 decryption requires the managed device run Snort 3. Other options are available as well; for more information, see TLS 1.3 decryption best practices, on page 1743 . New/modified screens: **SSL Policy** > **Advanced Settings**
SSL policy advanced settings.	7.2.0	7.1.0	SSL policy advanced settings New/modified screens: **SSL Policy** > **Advanced Settings**
Ability to specify handling of URLs having unknown reputation.	6.7.0	6.7.0	For details, see URL filtering with category and reputation, on page 1652 .
ClientHello modification for **Decrypt - Known** key rules.	6.7.0	6.7.0	For details, see ClientHello message handling, on page 1709 .

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Ability to extract the certificate in TLS 1.3 traffic to enable traffic to match URL and application criteria in access control rules.	6.7.0	6.7.0	New/modified screens: **Policies** > **Access Control** > **(edit an access control policy)** > **Advanced** link. For details, see Decryption policy advanced options, on page 1742 .
Changes to category and reputation-based URL Filtering.	6.7.0	6.5.0	For details, see URL filtering with category and reputation, on page 1652 .
TLS crypto acceleration cannot be disabled.	6.4.0	6.4.0	TLS crypto acceleration is enabled on all supported devices. On a managed device with native interfaces, TLS crypto acceleration cannot be disabled. Removed commands: • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Support for TLS crypto acceleration on one container instance on a Firepower 4100/9300 module/security engine.	6.4.0	6.4.0	You can now enable TLS crypto acceleration for one container instance on a module/security engine. New/modified commands: • **config hwCrypto enable** • **show crypto accelerator status**
TLS/SSL hardware acceleration is now referred to as TLS crypto acceleration .	6.4.0	6.4.0	The name change reflects that TLS/SSL encryption and decryption acceleration is supported on more devices. New/modified screens: **Devices** > **Device Management** > **Edit** > **Device** > **General** > **TLS Crypto Acceleration**
Extended Master Secret extension supported (see RFC 7627).	6.3.0.1	6.3.0.1	The TLS Extended Master Secret extension is supported for SSL policies; specifically, policies with a rule action of **Decrypt - Resign** or **Decrypt - Known Key** .
Extended Master Secret extension not supported.	6.3.0	6.3.0	The extension is stripped during ClientHello modification for **Decrypt - Resign** rules.
TLS/SSL hardware acceleration enabled by default.	6.3.0	6.3.0	TLS/SSL hardware acceleration is enabled by default on all supported devices but can be disabled if desired.
Extended Master Secret extension supported (see RFC 7627).	6.2.3.9	6.2.3.9	The TLS Extended Master Secret extension is supported for SSL policies; specifically, policies with a rule action of **Decrypt - Resign** or **Decrypt - Known Key** .

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Aggressive TLS 1.3 downgrade.	6.2.3.7	6.2.3.7	Using the **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI command, you can determine the behavior for downgrading TLS 1.3 traffic to TLS 1.2.
TLS/SSL hardware acceleration introduced.	6.2.3	6.2.3	Certain managed device models perform TLS/SSL encryption and decryption in hardware, improving performance. By default, the feature is enabled. Affected screen: To view the status of TLS/SSL hardware acceleration , **Devices** > **Device Management** > **Device** , General page.
Category and reputation conditions supported.	6.2.2	6.2.2	Access control rules or SSL rules with category/reputation conditions.
SafeSearch supported.	6.1.0	6.1.0	The system displays an HTTP response page for connections decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. SafeSearch filters objectionable content and stops people from searching adult sites.
TLS/SSL policy.	6.0.0	6.0.0	Feature introduced.



CHAPTER 45

Decryption Policies

The following topics provide an overview of decryption policy creation, configuration, management, and logging.

- About Decryption Policies, on page 1727
- Requirements and Prerequisites for Decryption Policies, on page 1728
- Create a decryption policy , on page 1728
- Decryption policy default actions, on page 1739
- Default handling options for undecryptable traffic, on page 1739
- Decryption policy advanced options, on page 1742

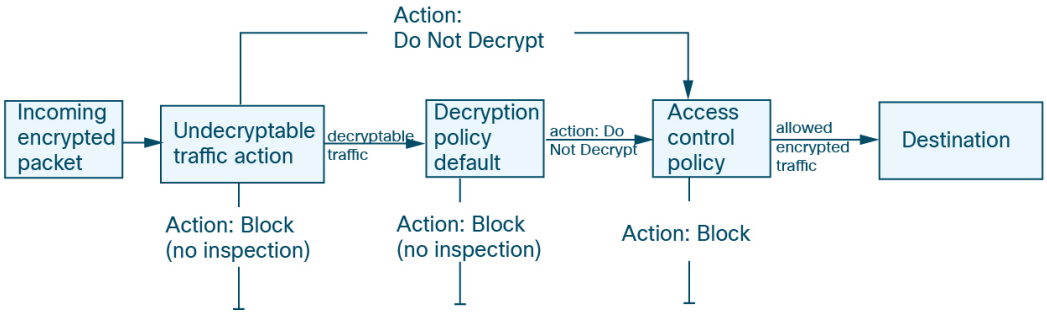
About Decryption Policies

A decryption policy determines how the system handles encrypted traffic on your network. You can configure one or more decryption policies, associate a decryption policy with an access control policy, then deploy the access control policy to a managed device. When the device detects a TCP handshake, the access control policy first handles and inspects the traffic. If it subsequently identifies a TLS/SSL-encrypted session over the TCP connection, the decryption policy takes over, handling and decrypting the encrypted traffic.

You can create multiple rules at the same time, including rules for decrypting incoming traffic (**Decrypt - Known Key** rule action) and outgoing traffic (**Decrypt - Resign** rule action). To create a rule with a **Do Not Decrypt** or other rule action (such as **Block** or **Monitor**), create an empty decryption policy and add the rule afterward.

Do Not Decrypt policy example

Following is an example decryption policy with a **Do Not Decrypt** rule action:



The simplest decryption policy, as shown in the following diagram, directs the device where it is deployed to handle encrypted traffic with a single default action. You can set the default action to block decryptable traffic without further inspection, or to inspect undecrypted decryptable traffic with access control. The system can then either allow or block the encrypted traffic. If the device detects undecryptable traffic, it either blocks the traffic without further inspection or does not decrypt it, inspecting it with access control.

Requirements and Prerequisites for Decryption Policies

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Create a decryption policy

A decryption policy is a rule-based security policy that controls how encrypted network traffic is handled.

Create decryption policy to protect outbound and inbound network connections through various rule actions.

You can create any of these types of decryption policies:

- *Outbound protection* policy with rules that protect outbound connections. The destination server is outside your protected network. This type of rule has a **Decrypt - Resign** rule action.

  Refer to Create a decryption policy with outbound connection protection, on page 1728 for guidance on creating a decryption rule with outbound connection.

- *Inbound protection* policy with a rule that protects inbound connections; that is, the destination server is inside your protected network. This type of rule has a **Decrypt - Known Key** rule action.

  Refer to Create a decryption policy with inbound connection protection, on page 1730 or guidance on creating a decryption rule with inbound connection.

- Other actions (including **Do Not Decrypt**, **Block**, and **Block with Reset**).

  See Create a decryption policy with other rule actions, on page 1737

Create a decryption policy with outbound connection protection

This task creates a decryption policy that protects outbound connections by intercepting and decrypting SSL/TLS traffic between internal clients and external servers, then re-encrypting the traffic with an internal CA certificate.

This task discusses how to create a decryption policy with a rule that protects outbound connections; that is, the destination server is outside your protected network. This type of rule has a **Decrypt - Resign** rule action.

When you create a decryption policy, you can create multiple rules at the same time, including multiple **Decrypt - Known Key** rules and multiple **Decrypt - Resign** rules.

Before you begin

You can optionally must upload or generate an internal CA certificate for your managed device before you can create a decryption policy that protects outbound connections. You can do this in any of the following ways:

- Create an internal CA certificate object by going to **Objects** > **Object Management** > **PKI** > **Internal CAs** and referring to PKI objects, on page 2389.
- At the time you create this decryption policy.

Follow these steps to create a decryption policy with outbound connection protection:

Procedure

Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Create Decryption Policy**.

Step 4 Give the policy a unique **Name** and, optionally, a **Description**.

The following characters are not supported in decryption policy names:

- Leading period
- `#,?,{,},=,$,<,>`

Step 5 Click the **Outbound Connections** tab.

Step 6 From the **Internal CA** list, upload or choose certificates for the rules.

For more information about internal certificates, see Generate an internal CA for outbound protection, on page 1735 and Upload an internal CA for outbound protection, on page 1736.

a) (Optional.) Choose networks and ports.

For more information:

- Network rule conditions, on page 1321
- Best practice: use application-based rules over port-based rules, on page 1323

What to do next

- Add rule conditions: Decryption Rule conditions, on page 1758
- Add a default policy action: Decryption policy default actions, on page 1739
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .

- Set advanced policy properties: Decryption policy advanced options, on page 1742.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Create a decryption policy with inbound connection protection

This task creates a decryption policy that protects inbound connections using either a **Decrypt - Known Key** rule action.

This task discusses how to create a decryption policy with a rule that protects inbound connections; that is, the destination server is inside your protected network. This type of rule has a **Decrypt - Known Key** rule action.

When you create a decryption policy, you can create multiple rules at the same time, including multiple **Decrypt - Known Key** rules and multiple **Decrypt - Resign** rules.

Before you begin

You must upload an internal certificate for your internal server before you can create a decryption policy that protects inbound connections. You can do this in any of the following ways:

- Create an internal certificate object by going to **Objects** > **Object Management** > **PKI** > **Internal Certs** and referring to PKI objects, on page 2389.
- At the time you create this decryption policy.

Follow these steps to create a decryption policy with inbound connection protection:

Procedure

Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Create Decryption Policy**.

Step 4 Perform these steps:

a) Give the policy a unique **Name** and, optionally, a **Description**.

The following characters are not supported in decryption policy names:

- Leading period
- `#,;,{,},=,$,<,>`

b) From the **Internal Certificates** list, upload or choose certificates for the rules.

For more information about internal CA certificates, see Internal certificate authority objects, on page 2390.

c) (Optional.) Choose networks and ports.

For more information:

- Network rule conditions, on page 1321
- Best practice: use application-based rules over port-based rules, on page 1323

d) Click **Next**.

Step 5 Continue with Configure Decryption policy exclusions, on page 1731.

Step 6 Click **Save**.

What to do next

- Add rule conditions: Decryption Rule conditions, on page 1758
- Add a default policy action: Decryption policy default actions, on page 1739
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Set advanced policy properties: Decryption policy advanced options, on page 1742.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure Decryption policy exclusions

This task helps you create exclusions in your decryption policy to prevent decryption of traffic that should remain encrypted for compliance, security, or functional reasons.

This task discusses how to exclude certain types of traffic from decryption. We create **Do Not Decrypt** rules in your decryption policy for this purpose. The rules are initially enabled only for an outbound decryption policy (a policy that uses the **Decrypt - Resign** policy action).

Before you begin

You must upload an internal CA certificate for your managed device before you can create a decryption policy that protects outbound connections. You can do this in any of the following ways:

- Create an internal CA certificate object by going to **Objects** > **Object Management** > **PKI** > **Internal CAs** and referring to PKI objects, on page 2389.
- At the time you create this decryption policy.

Follow these steps to configure decryption policy exclusions:

Procedure

Step 1 Complete the tasks discussed in:

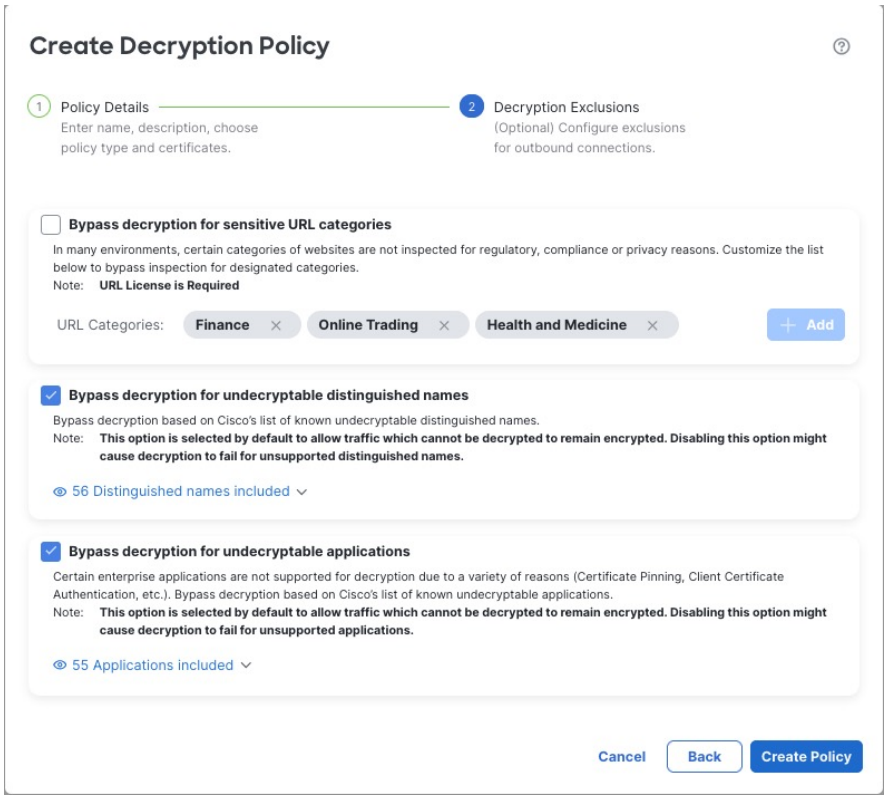
- Create a decryption policy with outbound connection protection, on page 1728
- For more information, see Create a decryption policy with inbound connection protection, on page 1730

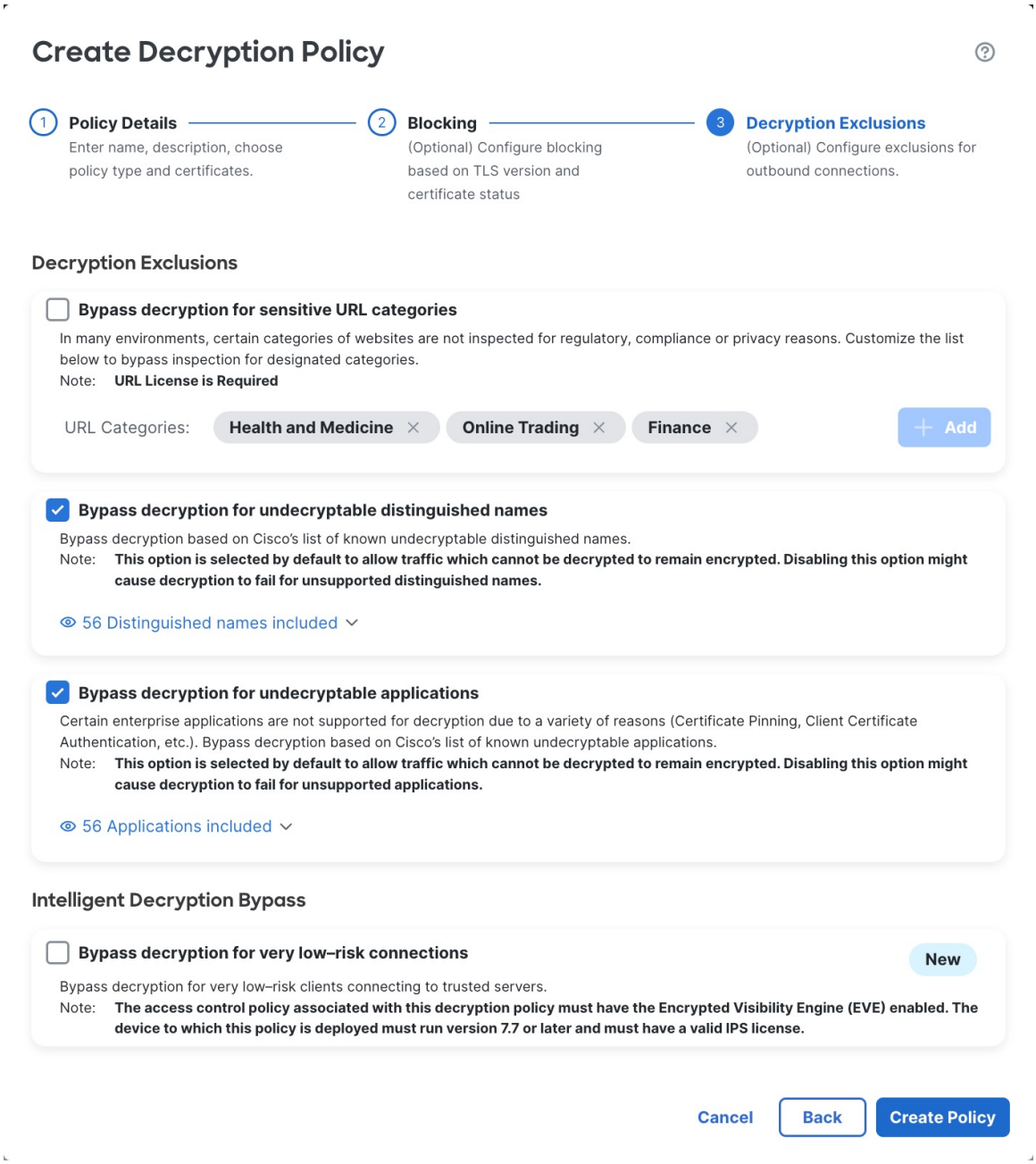
Step 2 Select the appropriate exclusion options based on your security requirements.

The exclusions page provides the following options. All options are *enabled* for an outbound protection policy (**Decrypt - Resign** rule action) and *disabled* for all other decryption policy actions.

Item	Description
Bypass decryption for sensitive URL categories	Check the box to not decrypt traffic from the indicated categories. Depending on the laws in your area, decryption certain traffic, such as finance or health-related, might be prohibited. Consult an authority in your area for more information. Click **Add** to add more categories. Click **Delete** (✕) to remove categories.
Bypass decryption for undecryptable distinguished names	Check the box to not decrypt traffic when re-signing the certificate is likely to cause the connection to fail. Typically, this behavior is associated with *certificate pinning*, which is discussed in TLS/SSL certificate pinning guidelines, on page 1752. The list of undecryptable distinguished names is maintained by Cisco.
Bypass decryption for undecryptable applications	Check the box to not decrypt traffic when re-signing the certificate is likely to cause the connection to fail. Typically, this behavior is associated with *certificate pinning*, which is discussed in TLS/SSL certificate pinning guidelines, on page 1752. Undecryptable applications are updated automatically in the Vulnerability Database (VDB). You can find a list of all applications on the Secure Firewall Application Detectors page; the **undecryptable** tag identifies applications Cisco determines are undecryptable. The list of undecryptable applications is maintained by Cisco.

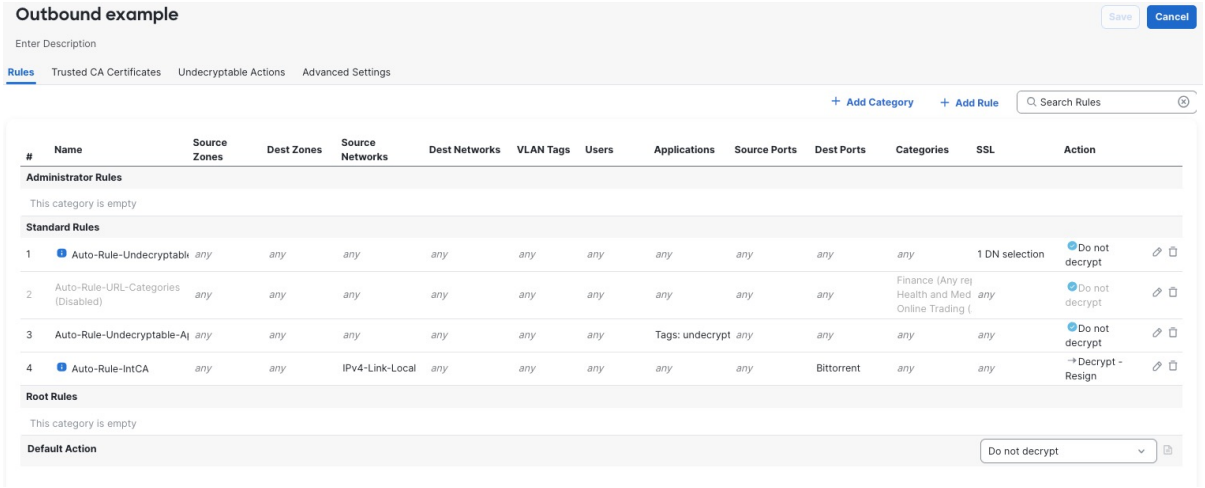
This figure shows default options.


Create Decryption Policy
1 Policy Details
Enter name, description, choose policy type and certificates.
2 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.
Bypass decryption for sensitive URL categories
In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required
URL Categories:
Finance
Online Trading
Health and Medicine
Add
Bypass decryption for undecryptable distinguished names
Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.
56 Distinguished names included
Bypass decryption for undecryptable applications
Certain enterprise applications are not supported for decryption due to a variety of reasons (Certificate Pinning, Client Certificate Authentication, etc.). Bypass decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.
55 Applications included
Cancel
Back
Create Policy



Step 3 Click **Create Policy**.

This figure shows a sample outbound protection policy.



In the preceding example, the **Do Not Decrypt** rules corresponding to your choices for rule exclusions are automatically added before the **Decrypt - Resign** rule. The rule for sensitive URL categories is disabled because, by default, that exclusion is disabled. Had you selected the **Bypass decryption for sensitive URL categories** check box, the rule would have been enabled.

What to do next

- Add rule conditions: Decryption Rule conditions, on page 1758
- Add a default policy action: Decryption policy default actions, on page 1739
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Set advanced policy properties: Decryption policy advanced options, on page 1742.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Generate an internal CA for outbound protection

This task allows you to generate an internal certificate authority object to protect outbound connections when creating a decryption rule.

This task discusses how you can optionally generate an internal certificate authority when you create a decryption rule that protects outbound connections. You can also perform these tasks using **Objects** > **Object Management** as discussed in Upload a signed certificate issued in response to a CSR, on page 2394.

Before you begin

Make sure you understand the requirements for generating an internal certificate authority object as discussed in Internal certificate authority objects, on page 2390.

Procedure

Step 1 From the **Internal CA** list, click **Create New** > **Generate CA**.

Step 2 Give the internal CA a **Name** and provide a two-letter **Country Name**.

Step 3 Click **Self-Signed** or **CSR**.

For more information about these options, see Internal certificate authority objects, on page 2390.

Step 4 Enter the requested information in the provided fields.

Step 5 Click **Save**.

Step 6 If you chose **CSR**, after the signing request has been completed, click **Install Certificate** as follows:

a) Repeat the preceding steps in this procedure.

b) Edit the CA from the **Internal CA** list as follows.



c) Click **Install Certificate**.

d) Follow the prompts on your screen to complete the task.

Step 7 Continue creating the policy as discussed in Create a decryption policy with outbound connection protection, on page 1728.

Upload an internal CA for outbound protection

Upload an internal certificate authority to create a decryption rule that protects outbound connections.

This task discusses how you can optionally upload an internal certificate authority when you create a decryption rule that protects outbound connections. You can also perform these tasks using **Objects** > **Object Management** as discussed in Upload a signed certificate issued in response to a CSR, on page 2394.

Before you begin

Make sure you understand the requirements for generating an internal certificate authority object as discussed in Internal certificate authority objects, on page 2390.

Follow these steps to upload an internal CA for outbound protection:

Procedure

Step 1 From the **Internal CA** list, click **Create New** > **Upload CA**.

Step 2 Give the internal CA a **Name**.

Step 3 Paste or browse to locate the certificate and its private key in the provided fields.

Step 4 If the CA has a password, select the **Encrypted** check box and enter the password in the adjacent field.

Step 5 Continue creating the policy as discussed in Create a decryption policy with outbound connection protection, on page 1728.

Upload an internal certificate for inbound protection

This task helps you manage certificate objects and configure decryption for secure access control by uploading an internal certificate for inbound protection.

This task discusses how to upload an internal certificate when you create a decryption rule that protects inbound connections. You can also upload the internal certificate using **Objects** > **Object Management** as discussed in Import a CA certificate and private key, on page 2391.

Before you begin

Make sure you have an internal certificate in one of the formats discussed in Internal certificate authority objects, on page 2390.

Follow these steps to upload an internal certificate for inbound protection:

Procedure

Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Create Decryption Policy**.

Step 4 Enter a name for the policy in the **Name** field and an optional description in the **Description** field.

Step 5 Click the **Inbound Connections** tab.

Step 6 From the **Internal Certificates** list, click **Add** (+).

Step 7 If an internal certificate object exists, click its name. Otherwise, click **Upload**.

a) Enter the required information.

See Add internal certificate objects, on page 2400.

Continue creating the decryption policy as discussed in Create a decryption policy with inbound connection protection, on page 1730.

Create a decryption policy with other rule actions

Create and manage decryption policies in the Secure Firewall Management Center to control encrypted traffic actions, such as **Do Not Decrypt**, **Block**, **Block With Reset**, or **Monitor**.

To create a decryption rule with a **Do Not Decrypt**, **Block**, **Block With Reset**, or **Monitor** rule action, create a decryption policy and edit the policy to add the rule.

When you create a decryption policy , you can create multiple rules at the same time, including multiple **Decrypt - Known Key** rules, and multiple **Decrypt - Resign** rules.

Procedure

Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Perform these actions:

a) Give the policy a unique **Name** and, optionally, a **Description**.

The following characters are not supported in decryption policy names:

- Leading period
- `#,;,{,},=,$,<,>`

b) Wait for the policy to be created.

Step 4 Click **Edit** ( ) next to the decryption policy name.

Step 5 Click **Add Rule**.

a) Give the rule a **Name**.

b) From the **Action** list, click a rule action and see one of the sections for more information:

- Decryption rule Do Not Decrypt action, on page 1778
- Decryption rule blocking actions, on page 1779
- Decryption rule monitor action, on page 1777

Step 6 Click **Save**.

What to do next

- Add rule conditions: Decryption Rule conditions, on page 1758
- Add a default policy action: Decryption policy default actions, on page 1739
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Set advanced policy properties: Decryption policy advanced options, on page 1742.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Decryption policy default actions

The default action for a decryption policy determines how the system handles decryptable encrypted traffic that does not match any non-monitor rule in the policy. When you deploy a decryption policy without a decryption rules, the default action determines how all decryptable traffic on your network is handled. Note that the system does not perform any kind of inspection on encrypted traffic that the default action blocks.

To set the policy default action:

1. Log in to the Secure Firewall Management Center if you haven't already done so.
2. Click **Policies** > **Access Control heading** > **Decryption**.
3. Click **Edit** ( ) next to the name of the decryption policy.
4. In the Default Action row, click one of the actions from the list.

Table 100: Decryption policy Default Actions

Default Action	Effect on Encrypted Traffic
Block	Block the TLS/SSL session without further inspection.
Block with reset	Block the TLS/SSL session without further inspection and reset the TCP connection. Choose this option if traffic uses a connectionless protocol like UDP. In that case, the connectionless protocol tries to reestablish the connection until it is reset. This action also displays a connection reset error in the browser so the users are informed that the connection is blocked.
Do not decrypt	Inspect the encrypted traffic with access control.

Default handling options for undecryptable traffic

This reference provides information about identifying and managing undecryptable TLS/SSL traffic types in decryption policies. It covers handling handshake errors, unsupported cipher suites, compressed sessions, and session caching issues, along with user-facing actions for blocking or allowing such encrypted connections.

Table 101: Undecryptable traffic types

Type	Description	Default Action	Available Action
Compressed Session	The TLS/SSL session applies a data compression method.	Inherit default action	Do not decrypt Block Block with reset Inherit default action

Type	Description	Default Action	Available Action
SSLv2 Session	The session is encrypted with SSL version 2. Note that traffic is decryptable if the ClientHello message is SSL 2.0, and the remainder of the transmitted traffic is SSL 3.0.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Unknown Cipher Suite	The system does not recognize the cipher suite.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Unsupported Cipher Suite	The system does not support decryption based on the detected cipher suite.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Session not cached	The TLS/SSL session has session reuse enabled, the client and server reestablished the session with the session identifier, and the system did not cache that session identifier.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Handshake Errors	An error occurred during TLS/SSL handshake negotiation.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Decryption Errors	An error occurred during traffic decryption.	Block	Block Block with Reset

When you first create a decryption policy, logging connections that are handled by the default action is disabled by default. Because the logging settings for the default action also apply to undecryptable traffic handling, logging connections handled by the undecryptable traffic actions is disabled by default.

Note that if your browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. For more information, see Decryption Rules guidelines and limitations, on page 1746.

If a decryption policy is associated with an access control policy that uses TCP state bypass, matching traffic is acted on based on the policy's configured **Undecryptable Actions** for **Handshake Errors**.

For example, if a decryption policy's **Handshake Errors** is set to **Block**, traffic matching the rule is blocked and the connection event's action is reported as a handshake error.

For more information about TCP state bypass, see:

- Configure TCP state bypass, on page 2200
- Bypass TCP state checks for asymmetrical routing (TCP state bypass), on page 2198

Related Topics

Set default handling for undecryptable traffic, on page 1741

Set default handling for undecryptable traffic

Set undecryptable traffic actions to handle certain types of encrypted traffic the system cannot decrypt or inspect, ensuring proper network security enforcement for encrypted connections.

You can set undecryptable traffic actions at the decryption policy level to handle certain types of encrypted traffic the system cannot decrypt or inspect. When you deploy adecryption policy that contains no decryption rules, the undecryptable traffic actions determine how all undecryptable encrypted traffic on your network is handled.

Depending on the type of undecryptable traffic, you can choose to:

- Block the connection.
- Block the connection, then reset it. This option is preferrable for connectionless protocols like UDP, which keep trying to connect until the connection is blocked.
- Inspect the encrypted traffic with access control.
- Inherit the default action from the decryption policy.

Procedure

Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** (✎) next to the name of the decryption policy.

Step 4 In the decryption policy editor, click **Undecryptable Actions**.

Step 5 For each field, choose either the decryption policy's default action or another action you want to take on the type of undecryptable traffic. See Default handling options for undecryptable traffic, on page 1739 and Decryption policy default actions, on page 1739 for more information.

Step 6 Click **Save** to save the policy.

What to do next

- Configure default logging for connections handled by the undecryptable traffic actions; see *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Decryption policy advanced options

A decryption policy 's **Advanced Settings** page contains global settings. These settings apply to all managed devices that are configured for Snort 3.

A decryption policy advanced settings are all ignored on any managed device that runs:

- A version earlier than 7.1
- Snort 2

Block flows requesting ESNI

Encrypted Server Name Indication (ESNI (link to draft proposal)) is a way for a client to tell a TLS 1.3 server what the client is requesting. Because the SNI is encrypted, the system cannot identify the server. You can choose to block these connections.

Disable HTTP/3 advertisement

This option strips HTTP/3 (RFC 9114) from the ClientHello in TCP connections. HTTP/3 is part of the QUIC transport protocol, not the TCP transport protocol. Blocking clients from advertising HTTP/3 provides protection against attacks and evasion attempts potentially burried within QUIC connections.

Propagate untrusted server certificates to clients

This setting applies only to traffic matching a **Decrypt - Resign** rule action.

Enable this option when the server certificate is untrusted. The managed device substitutes its certificate authority (CA) for the server certificate. An *untrusted* server certificate is one that is not listed as a trusted CA in the Secure Firewall Management Center. (**Objects** > **Object Management** > **PKI** > **Trusted CAs**).

Enable TLS 1.3 decryption

Whether to apply decryption rules to TLS 1.3 connections. If you do not enable this option, the decryption rules apply to TLS 1.2 or lower traffic only. See TLS 1.3 decryption best practices, on page 1743.

Enable adaptive TLS server identity probe

Automatically enabled when TLS 1.3 decryption is enabled. A *probe* is a partial TLS connection with the server, the purpose of which is to obtain the server certificate and cache it. (If the certificate is already cached, the probe is never established.)

If TLS 1.3 Server Identity Discovery is disabled on the access control policy with which the decryption policy is associated, we attempt to use the Server Name Indication (SNI), which is not as reliable.

The adaptive TLS server identity PROBE occurs on any of these conditions as opposed to on every connection as in earlier releases:

- Certificate Issuer—Matched when the value of **Issuer DNs** in a decryption rule's DN rule condition is matched.

  For more information, see Conditions for distinguished name rules in decryption policies, on page 1765.

- Certificate Status—Matched when any of the **Cert Status** conditions are matched in a decryption rule.

For more information, see Certificate Status Decryption rule conditions, on page 1771.

- Internal/External Certificate—Internal certificates can be matched by the certificate used in **Decrypt - Known Key** rule actions; external certificates can be matched in **Certificates** rule conditions.

  For more information, see Known key decryption for incoming traffic, on page 1716 and Certificate rule conditions, on page 1765.

- Application ID—Can be matched by **Applications** rule conditions in either an access control policy or a decryption policy.

  For more information, see Application rule conditions, on page 1322.

- URL Category—Can be matched by **URLs** rule conditions in an access control policy.

  For more information, see Recommendation: use URL conditions for website access control , on page 1324.



Note **Enable adaptive TLS server discovery mode** is not supported on any Secure Firewall Threat Defense Virtual deployed to AWS. If you have any such managed devices managed by the Secure Firewall Management Center, the connection event **PROBE_FLOW_DROP_BYPASS_PROXY** increments every time the device attempts to extract the server certificate.

TLS 1.3 decryption best practices

Both the decryption policy and the access control policy have advanced options that affect how traffic is handled, whether the traffic is being decrypted or not.

The advanced options are:

- Decryption policy:
  - TLS 1.3 decryption
  - TLS adaptive server identity probe
- Access control policy: TLS 1.3 Server Identity Discovery

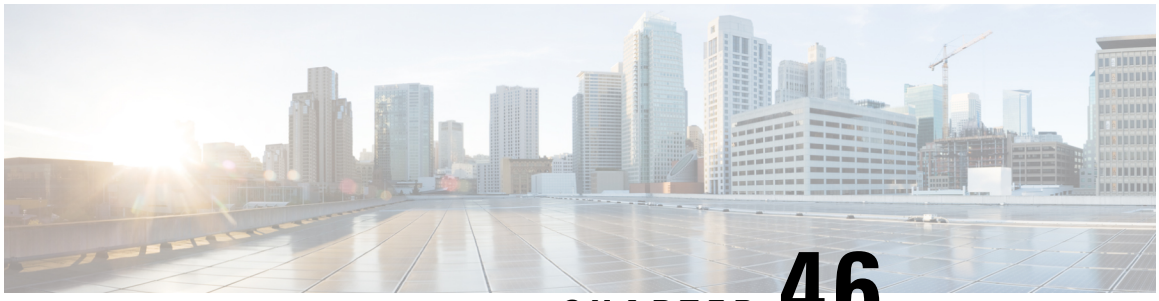
  The access control policy setting takes precedence over the decryption policy setting.

Use the following table to decide which option to enable:

TLS adaptive server identity probe setting (decryption policy)	TLS 1.3 Server Identity Discovery setting (access control policy)	Result	Recommended when
Enabled	Disabled	Adaptive probe sent if decryption policy contains *any* rule conditions specified in Decryption policy advanced options, on page 1742 *and* if the server certificate is not cached.	• You're not using application or URL conditions in access control rules • You're decrypting traffic
Enabled	Enabled	Probe is always sent if the server certificate is not cached.	Use only if your access control rules have URL or application conditions
Disabled	Enabled	Probe is always sent if the server certificate is not cached.	Not recommended.
Disabled	Disabled	Probe is never sent.	Very limited usefulness; use only if not decrypting traffic and not using application or URL conditions in the access control rule

Note A cached TLS server's certificate is available to all Snort instances on a particular Firewall Threat Defense. The cache can be cleared with a CLI command and is automatically cleared when the device is rebooted.

For more information, see the discussion of TLS server identity discovery on secure.cisco.com.



CHAPTER 46

Decryption Rules

The following topics provide an overview of creating, configuring, managing, and troubleshooting decryption rules:

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

For more information about SSL and TLS protocols, refer to a resource such as SSL vs. TLS - What's the Difference?

- Decryption Rule overview, on page 1745
- Requirements and prerequisites for Decryption Rules, on page 1745
- Decryption Rules guidelines and limitations, on page 1746
- Decryption Rule traffic handling, on page 1754
- Decryption Rule conditions, on page 1758
- Decryption Rule actions, on page 1777
- Monitor TLS/SSL hardware acceleration, on page 1780
- Troubleshoot Decryption Rules, on page 1782
- Troubleshoot using crypto archives, on page 1790

Decryption Rule overview

Decryption rules provide a granular method of handling encrypted traffic across multiple managed devices, whether blocking the traffic without further inspection, not decrypting the traffic and inspecting it with access control, or decrypting the traffic for access control analysis.

Requirements and prerequisites for Decryption Rules

This reference provides the domain support and user role requirements necessary for Decryption Rules.

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Decryption Rules guidelines and limitations

Keep these points in mind when setting up your decryption rule. Properly configuring decryption rule is a complex task, but one that is essential to building an effective deployment that handles encrypted traffic. Many factors influence how you configure rules, including certain application behavior that you cannot control.

In addition, rules can preempt each other, require additional licenses, or contain invalid configurations. Thoughtfully configured rules can also reduce the resources required to process network traffic. Creating overly complex rules and ordering rules the wrong way can adversely affect performance.

For detailed information, see Best practices for access control rules, on page 1625.

For guidelines related specifically to TLS crypto acceleration, see TLS crypto acceleration, on page 1720.

Related Topics

Rule and other policy warnings
Best practices for access control rules, on page 1625
Guidelines for using TLS/SSL decryption, on page 1746
Decryption Rules unsupported features, on page 1747
Guidelines for TLS/SSL Do Not Decrypt configuration, on page 1748
TLS/SSL Decrypt - Resign guidelines, on page 1749
TLS/SSL Decrypt - Known Key Guidelines, on page 1751
TLS/SSL block guidelines, on page 1752
TLS/SSL certificate pinning guidelines, on page 1752
TLS/SSL heartbeat guidelines, on page 1752
TLS/SSL anonymous cipher suite limitation, on page 1753
TLS/SSL normalizer guidelines, on page 1753
Other Decryption Rule guidelines, on page 1753
Best practice for Decryption policy rule order

Guidelines for using TLS/SSL decryption

General guideline

Decryption Rules require processing overhead that can impact performance. Determine which traffic must be decrypted and subjected to deep inspection before you set up any policies or rules.

- You cannot decrypt traffic on a device that uses passive interface.

- You cannot decrypt traffic on a device that uses inline tap interface.
- You cannot decrypt traffic on a device that uses TCP state bypass (only if the interfaces are in routed mode).

Guidelines for undecryptable traffic

We can determine that certain traffic is not decryptable either because the website itself is not decryptable or because the website uses TLS/SSL pinning, which effectively prevents users from accessing a decrypted site without errors in their browser.

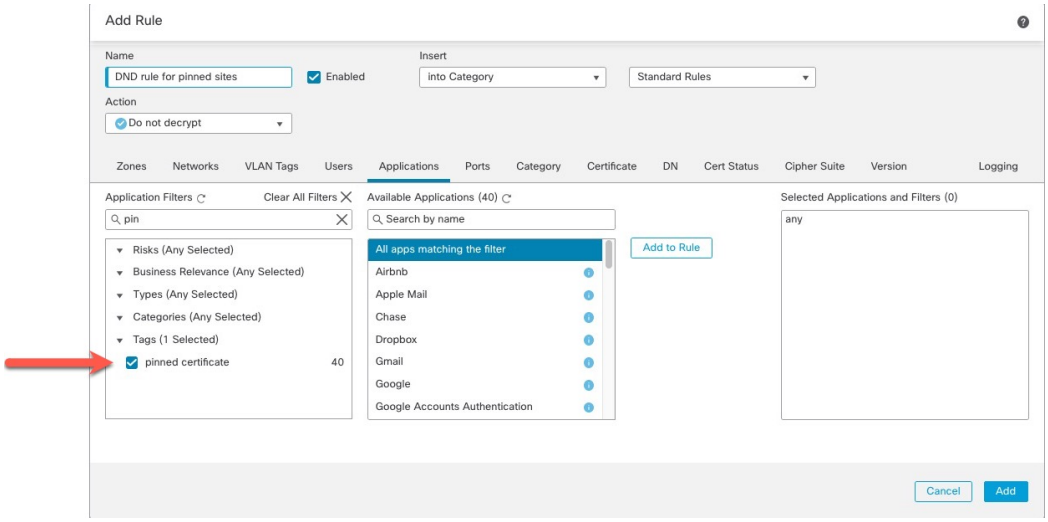
For more information about certificate pinning, see TLS/SSL pinning, on page 1784.

We maintain the list of these sites as follows:

- A Distinguished Name (DN) group named **Cisco-Undecryptable-Sites**
- The **pinned certificate** or **undecryptable** application filter

If you are decrypting traffic and you do not want users to see errors in their browsers when going to these sites, we recommend you set up a **Do Not Decrypt** rule toward the bottom of your decryption rules.

An example of setting up a **pinned certificate** application filter follows.



Decryption Rules unsupported features

This reference provides guidance for handling RC4, DES, and TLS 1.3 limitations in the Cisco Firepower System, including configuration requirements for decryption policies when dealing with unsupported cipher suites and interface types.

RC4 cipher not unsupported

The Rivest Cipher 4 (also referred to as *RC4* or *ARC4* cipher is known to have vulnerabilities and is considered unsecure.

decryption policies identify the RC4 cipher suite as unsupported; you should configure the **Unsupported Cipher Suite** action in the decryption policies policy's **Undecryptable Actions** page to match your organization's requirements. For more information, see Default handling options for undecryptable traffic, on page 1739.

Passive, inline tap mode, and SPAN interfaces not supported

TLS/SSL traffic cannot be decrypted on passive, inline tap mode, or SPAN interfaces.

Guidelines for TLS/SSL Do Not Decrypt configuration

You should not decrypt traffic if doing so is forbidden by:

- Law; for example, some jurisdictions forbid decrypting financial information
- Company policy; for example, your company might forbid decrypting privileged communications
- Privacy regulations
- Traffic that uses certificate pinning (also referred to as *TLS/SSL pinning*) must remain encrypted to prevent breaking the connection

Encrypted traffic can be allowed or blocked on any decryption rule condition, including, but not limited to:

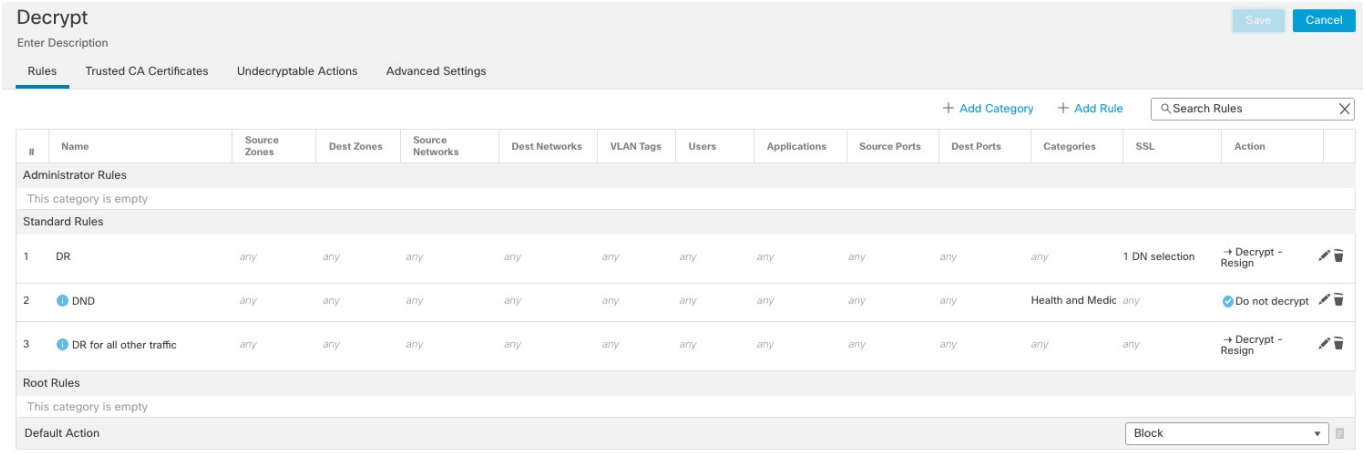
- Certificate status (for example, expired or invalid certificate)
- Protocol (for example, the nonsecure SSL protocol)
- Network (security zone, IP address, VLAN tag, and so on)
- URL category and reputation
- Port
- User group

Limitations of categories in Do Not Decrypt rules

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is not based on the declared company vertical, intent, or security. While we strive to continuously update and improve URL filtering categories, it is not an exact science. Some websites are not categorized at all and it's possible some websites might be improperly categorized.

Avoid overusing categories in do not decrypt rules to avoid decrypting traffic without a reason; for example, the Health and Medicine category includes the WebMD website, which does not threaten patient privacy.

Following is a sample decryption policy that can prevent decryption for websites in the Health and Medicine categories but allows decryption for WebMD and everything else. General information about decryption rules can be found in Guidelines for using TLS/SSL decryption, on page 1746.



Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control, on page 1622.

TLS/SSL Decrypt - Resign guidelines

You can associate one internal Certificate Authority (CA) certificate and private key with the **Decrypt - Resign** action. If traffic matches this rule, the system re-signs the server certificate with the CA certificate, then acts as a man-in-the-middle. It creates two TLS/SSL sessions, one between client and managed device, one between managed device and server. Each session contains different cryptographic session details, and allows the system to decrypt and reencrypt traffic.

- Use the **Decrypt - Resign** rule action for decrypting *outgoing* traffic, as opposed to incoming traffic for which we recommend the **Decrypt - Known Key** rule action.

  For more information about **Decrypt - Known Key**, see TLS/SSL Decrypt - Known Key Guidelines, on page 1751.

- Always check the **Replace Key Only** check box when you set up a **Decrypt - Resign** rule action.

  When a user browses to a web site that uses a *self-signed* certificate, the user sees a security warning in the web browser and is aware that they are communicating with an unsecure site.

  When a user browses to a web site that uses a trusted certificate, the user does not see a security warning.

Certificate algorithm compatibility

If you configure a rule with the **Decrypt - Resign** action, the rule matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions. Because you associate one CA certificate with a **Decrypt - Resign** action, you cannot create a decryption rule that decrypts multiple types of outgoing traffic encrypted with different signature algorithms. In addition, any external certificate objects and cipher suites you add to the rule must match the associated CA certificate encryption algorithm type.

- For example, outgoing traffic encrypted with an elliptic curve (EC) algorithm matches a **Decrypt - Resign** rule only if the action references an EC-based CA certificate; you must add EC-based external certificates and cipher suites to the rule to create certificate and cipher suite rule conditions.
- Similarly, a **Decrypt - Resign** rule that references an RSA-based CA certificate matches only outgoing traffic encrypted with an RSA algorithm; outgoing traffic encrypted with an EC algorithm does not match the rule, even if all other configured rule conditions match.

Guidelines and limitations

Anonymous cipher suite unsupported:

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

- **Do not use Version or Cipher Suite rule conditions**:



Important *Never* use either **Cipher Suite** or **Version** rule conditions in a rule with a **Decrypt - Resign** or **Decrypt - Known Key** rule action. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

- Decrypt - Resign rule action and a Certificate Signing Request: To use a **Decrypt - Resign** rule action, you should create a Certificate Signing Request (CSR) and have it signed by a trusted certificate authority. (You can use the FMC to create a CSR: **Objects** > **Object Management** > **PKI** > **Internal Certs**.)

  To be used in a **Decrypt - Resign** rule, your certificate authority (CA) must have at least one of these extensions

  - **CA: TRUE**

    For more information, see the discussion of Basic Constraints in RFC3280, section 4.2.1.10.

  - **KeyUsage=CertSign**

    For more information see RFC 5280, section 4.2.1.3.

  To verify your CSR or CA has at least one of the preceding extensions, you can use the **openssl** command as discussed in a reference such as the openssl documentation.

  This is necessary because for **Decrypt - Resign** inspection to work, the certificate that used in the decryption policy generates certificates on-the-fly and signs them so as to act as man-in-the middle and proxy all TLS/SSL connections.

- **Certificate pinning**: If the customer's browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. To allow this traffic, configure a decryption rule with the **Do Not Decrypt** action to match the server certificate common name or distinguished name.
- **Non-matching cipher suite**: This error is displayed if you attempt to save a decryption rule with a cipher suite that does not match the certificate. To resolve the issue, see Verify TLS/SSL cipher suites, on page 1789.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

- **Untrusted Certificate Authority**: If the client does not trust the Certificate Authority (CA) used to re-sign the server certificate, it warns the user that the certificate should not be trusted. To prevent this, import the CA certificate into the client trusted CA store. Alternatively, if your organization has a private PKI, you can issue an intermediate CA certificate signed by the root CA which is automatically trusted by all clients in the organization, then upload that CA certificate to the device.
- **HTTP proxy limitation**: The system cannot decrypt traffic if an HTTP proxy is positioned between a client and your managed device, and the client and server establish a tunneled TLS/SSL connection using the CONNECT HTTP method. The **Handshake Errors** undecryptable action determines how the system handles this traffic.
- **Upload signed CA**: If you create an internal CA object and choose to generate a certificate signing request (CSR), you cannot use this CA for a **Decrypt - Resign** action until you upload the signed certificate to the object.
- **Mismatched signature algorithm**: If you configure a rule with the **Decrypt - Resign** action, and mismatch signature algorithm type for one or more external certificate objects or cipher suites, the policy editor displays an **Information** ( ) next to the rule. If you mismatch signature algorithm type for all external certificate objects, or all cipher suites, the policy displays a warning icon **Warning** ( ) next to the rule, and you cannot deploy the access control policy associated with the decryption policy.

TLS/SSL Decrypt - Known Key Guidelines

When you configure the **Decrypt - Known Key** action, you can associate one or more server certificates and paired private keys with the action. If traffic matches the rule, and the certificate used to encrypt the traffic matches the certificate associated with the action, the system uses the appropriate private key to obtain the session encryption and decryption keys. Because you must have access to the private key, this action is best suited to decrypt traffic incoming to servers your organization controls.

Also note the following:

Anonymous cipher suite unsupported

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

Cannot match on Distinguished Name or Certificate

You cannot match on **Distinguished Name** or **Certificate** rule conditions when creating a decryption rule with a **Decrypt - Known Key** action. The assumption is that if this rule matches traffic, the certificate, subject DN, and issuer DN already match the certificate associated with the rule.

Do not use Version or Cipher Suite rule conditions



Important *Never* use either **Cipher Suite** or **Version** rule conditions in a rule with a **Decrypt - Resign** or **Decrypt - Known Key** rule action. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Elliptic Curve Digital Signature Algorithm (*ECDSA*) certificate results in blocked traffic
(TLS 1.3 decryption enabled only.) If you use an ECDSA certificate with a **Decrypt - Known Key** rule action, matching traffic will be blocked. To avoid this, use a certificate with another type of certificate.

TLS/SSL block guidelines

If your decryption rule is associated with an access control policy that has a rule with an action of either **Interactive Block** or **Interactive Block with reset**, the system displays a customizable response page.

If you enabled logging in your rule, two connection events are displayed (in **Analysis** > **Unified Events**): One event for the interactive block and another event to indicate whether or not the user chose to continue to the site or not.

Related Topics

HTTP response pages, on page 1669

TLS/SSL certificate pinning guidelines

Some applications use a technique referred to as *TLS/SSL pinning* or *certificate pinning*, which embeds the fingerprint of the original server certificate in the application itself. As a result, if you configured a decryption rule with a **Decrypt - Resign** action, when the application receives a resigned certificate from a managed device, validation fails and the connection is aborted.

Because TLS/SSL pinning is used to avoid man-in-the-middle attacks, there is no way to prevent or work around it. We recommend adding a **Do Not Decrypt** rule before the **Decrypt - Resign** rule so pinning traffic is excluded from being decrypted.

- Create a **Do Not Decrypt** for those applications rule ordered before **Decrypt - Resign** rules.
- Instruct users to access the applications using a web browser.

For more information about rule ordering, see Best practice for Decryption policy rule order.

To determine whether applications are using TLS/SSL pinning, see Troubleshoot TLS/SSL pinning, on page 1785.

TLS/SSL heartbeat guidelines

Some applications use the *TLS heartbeat* extension to the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols defined by RFC6520. TLS heartbeat provides a way to confirm the connection is still alive—either the client or server sends a specified number of bytes of data and requests the other party echo the response. If this is successful, encrypted data is sent.

You can configure a **Max Heartbeat Length** in a Network Analysis Policy (NAP) to determine how to handle TLS heartbeats. For more information, refer to *The SSL Preprocessor* section in the "Custom Snort 2 Intrusion Policies for Access Control" document.

For more information, refer to TLS heartbeat, on page 1783.

TLS/SSL anonymous cipher suite limitation

Anonymous cipher suites impact decryption rules.

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

You can add an anonymous cipher suite to the **Cipher Suite** condition in a decryption rule, but the system automatically strips anonymous cipher suites during ClientHello processing. For the system to use the rule, you must also configure your decryption rules in an order that prevents ClientHello processing. For more information, refer to Best practice for Decryption policy rule order

TLS/SSL normalizer guidelines

If you enable the **Normalize Excess Payload** option in the inline normalization preprocessor, when the preprocessor normalizes decrypted traffic, it might drop a packet and replace it with a trimmed packet. This does not end the TLS/SSL session. If the traffic is allowed, the trimmed packet is encrypted as part of the TLS/SSL session.

Other Decryption Rule guidelines

Consider users and groups configuration when creating decryption rules. If you add a group or user to a rule, then change your realm settings to exclude that group or user, the rule has no effect. (The same applies to disabling the realm.) For more information about realms, see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

Consider all relevant categories when configuring decryption rules. If your decryption policy has a **Decrypt - Resign** action but web sites are not being decrypted, check **Category** page on rules associated with that policy.

In some cases, a web site redirects to another site for authentication or other purposes and the redirected site might have a different URL categorization than the site you're trying to decrypt. For example, `gmail.com` (**Web based email** category) redirects to `accounts.gmail.com` (**Internet Portals** category) for authentication. Be sure to include all relevant categories in the SSL rule.



Note In order to fully process traffic based on URL category, you must also configure URL filtering. See the URL Filtering Rules, on page 1651 chapter.

Consider configuring cloud query settings for URLs not in the local database. If you create a **Decrypt - Resign** rule and users browse to a web site whose category and reputation are not in the local database, data might

not be decrypted. Some web sites are not categorized in the local database and, if not, data from those web sites is not decrypted by default.

You can control this behavior with the **Query Cisco cloud for unknown URLs** setting in **Integration** > **Other Integrations** > **Cloud Services**

Decryption Rule traffic handling

Decryption Rule traffic handling is a security mechanism that matches traffic to decryption rules in a specified order to determine appropriate actions.

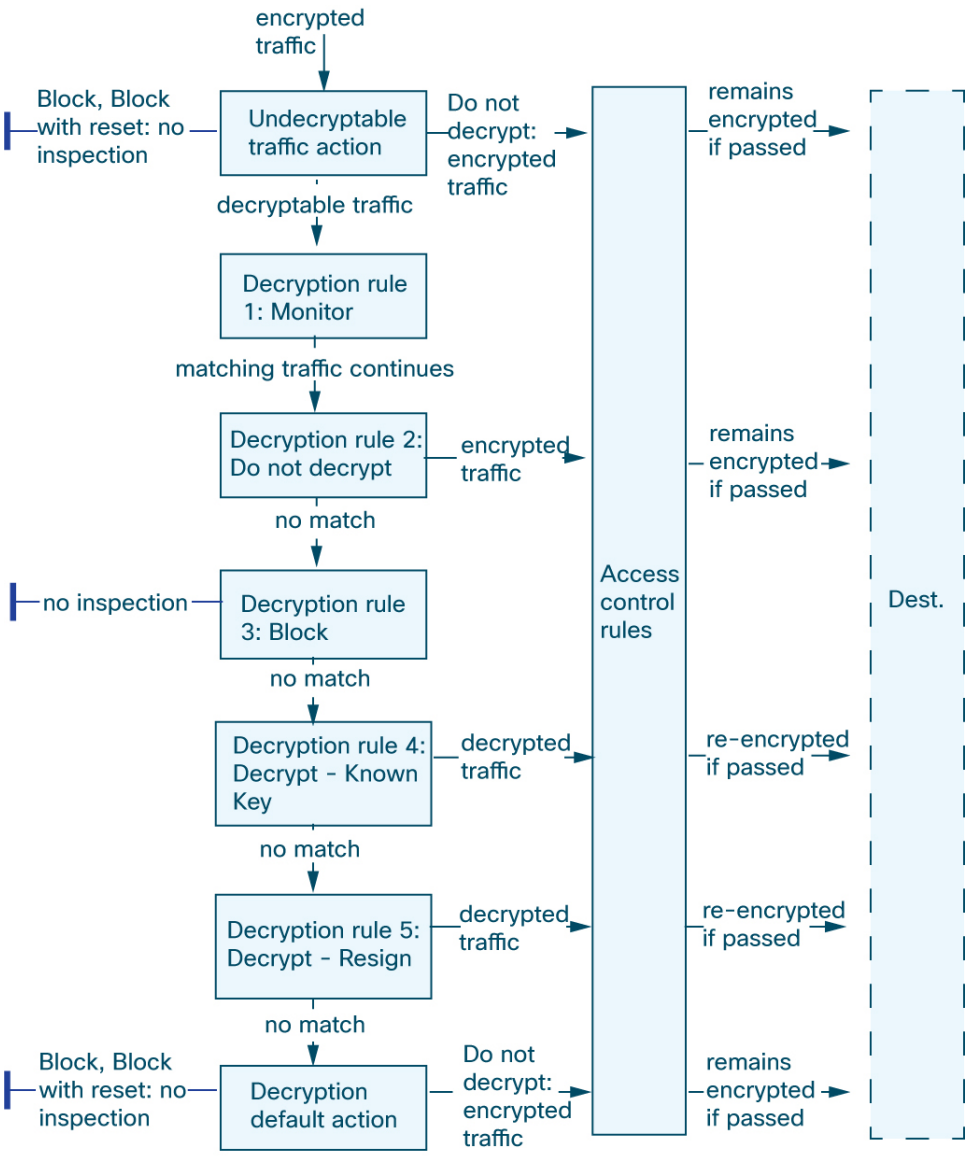
Traffic matching and processing behavior

The system matches traffic to decryption rules in the order you specify. In most cases, the system handles encrypted traffic according to the *first* decryption rule where *all* the rule's conditions match the traffic. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, VLAN, port, application, requested URL, user, certificate, certificate distinguished name, certificate status, cipher suite, or encryption protocol version.

Each rule also has an *action*, which determines whether you monitor, block, or inspect matching encrypted or decrypted traffic with access control. Note that the system does *not* further inspect encrypted traffic it blocks. It does inspect encrypted and undecryptable traffic with access control. However, some access control rule conditions require unencrypted traffic, so encrypted traffic may match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads.

Traffic handling process

This scenario summarizes the ways that Decryption Rule handle traffic in an inline deployment.



In this scenario, traffic is evaluated as follows:

- Undecryptable Traffic Action evaluates encrypted traffic first. For traffic the system cannot decrypt, the system either blocks it without further inspection or passes it for access control inspection. Encrypted traffic that does not match continues to the next rule.
- Rule 1: Monitor evaluates encrypted traffic next. Monitor rules track and log encrypted traffic but do not affect traffic flow. The system continues to match traffic against additional rules to determine whether to permit or deny it.
- Rule 2: Do Not Decrypt evaluates encrypted traffic third. Matching traffic is not decrypted; the system inspects this traffic with access control, but not file or intrusion inspection. Traffic that does not match continues to the next rule.

- Rule 3: Block evaluates encrypted traffic fourth. Matching traffic is blocked without further inspection. Traffic that does not match continues to the next rule.
- Rule 4: Decrypt - Known Key evaluates encrypted traffic fifth. Matching traffic incoming to your network is decrypted using a private key you upload. The decrypted traffic is then evaluated against access control rules. Access control rules handle decrypted and unencrypted traffic identically. The system can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the decryption rule continues to the next rule.
- Rule 5: Decrypt - Resign is the final rule. If traffic matches, the system re-signs the server certificate with an uploaded CA certificate and decrypts traffic. The decrypted traffic is then evaluated against access control rules, which treat decrypted and unencrypted traffic the same. This additional inspection allows the system to block traffic. All remaining traffic is re-encrypted before being sent to its destination. Traffic that does not match the decryption rule rule continues to the next rule.
- Default Action handles all traffic that does not match any of the decryption rule. The default action either blocks encrypted traffic without further inspection or does not decrypt it, passing it for access control inspection.

Encrypted traffic inspection configuration

You must create reusable public key infrastructure (PKI) objects to control encrypted traffic based on encrypted session characteristics and decrypt encrypted traffic. You can add this information on the fly when uploading trusted certificate authority (CA) certificates to the a decryption policy and creating decryption rule, creating the associated object in the process. However, configuring these objects ahead of time reduces the chance of improper object creation.

Decrypting encrypted traffic with certificates and paired keys

The system can decrypt incoming encrypted traffic if you configure an internal certificate object by uploading the server certificate and private key used to encrypt the session. If you reference that object in a decryption policy rule with an action of **Decrypt - Known Key** and traffic matches that rule, the system uses the uploaded private key to decrypt the session.

The system can also decrypt outgoing traffic if you configure an internal CA object by uploading a CA certificate and private key. If you reference that object in a decryption rule with an action of **Decrypt - Resign** and traffic matches that rule, the system re-signs the server certificate passed to the client browser, then acts as a man-in-the-middle to decrypt the session. You can optionally replace the self-signed certificate key only and not the entire certificate, in which case users see a self-signed certificate key notice in the browser.

Controlling traffic based on encrypted session characteristics

The system can control encrypted traffic based on the cipher suite or server certificate used to negotiate the session. You can configure one of several different reusable objects and reference the object in a decryption rule condition to match traffic. This table describes the different types of reusable objects you can configure:

If you configure...	You can control encrypted traffic based on whether...
A cipher suite list containing one or more cipher suites	The cipher suite used to negotiate the encrypted session matches a cipher suite in the cipher suite list

If you configure...	You can control encrypted traffic based on whether...
A trusted CA object by uploading a CA certificate your organization trusts	The trusted CA trusts the server certificate used to encrypt the session, whether: • The CA issued the certificate directly • The CA issued a certificate to an intermediate CA that issued the server certificate
An external certificate object by uploading a server certificate	The server certificate used to encrypt the session matches the uploaded server certificate
A distinguished name object containing a certificate subject or issuer distinguished name	The subject or issuer common name, country, organization, or organizational unit on the certificate used to encrypt the session matches the configured distinguished name

Related Topics

Cipher suite lists, on page 2359
Distinguished names, on page 2364
PKI objects, on page 2389

Decryption Rule order evaluation

Decryption Rule order evaluation determines the sequence in which the system evaluates decryption rules in a policy.

Rule evaluation process

When you create a decryption rule in a decryption policy , you specify its position using the **Insert** list in the rule editor. Decryption rules in an a decryption policy are numbered, starting at 1. The system matches traffic to decryption rules in top-down order by ascending rule number.

In most cases, the system handles network traffic according to the *first* decryption rule where *all* the rule's conditions match the traffic. Except in the case of Monitor rules (which log traffic but do not affect traffic flow), the system does *not* continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, VLAN, port, application, requested URL category and reputation, user, certificate, certificate distinguished name, certificate status, cipher suite, or encryption protocol version.

Each rule also has an *action*, which determines whether you monitor, block, or inspect matching encrypted or decrypted traffic with access control. Note that the system does *not* further inspect encrypted traffic it blocks. It does subject encrypted and undecryptable traffic to access control. However, access control rule conditions require unencrypted traffic, so encrypted traffic matches fewer rules.

Rules that use *specific* conditions (such as network and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your rules.

Note Proper decryption rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs.

In addition to ordering rules by number, you can group rules by category. By default the system provides three categories: Administrator, Standard, and Root. You can add custom categories, but you cannot delete the system-provided categories or change their order.

Related Topics

Best practices for access control rules, on page 1625

Decryption Rule conditions

A decryption rule condition identifies the type of encrypted traffic the rule handles. Conditions can be simple or complex, and you can specify more than one condition type per rule. Only if traffic meets all the conditions in a rule does the rule apply to the traffic.

Condition evaluation and rule actions

If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion. For example, a rule with a certificate condition but no version condition evaluates traffic based on the server certificate used to negotiate the session, regardless of the session SSL or TLS version.

Every decryption policy has an associated action that determines handling and logging for matching encrypted traffic:

- Handling: Most importantly, the rule action governs whether the system will monitor, trust, block, or decrypt encrypted traffic that matches the rule's conditions.
- Logging: The rule action determines when and how you can log details about matching encrypted traffic.

Your TLS/SSL inspection configuration handles, inspects, and logs decrypted traffic:

- The decryption policy's undecryptable actions handle traffic that the system cannot decrypt.
- The policy's default action handles traffic that does not meet the condition of any non-Monitor decryption rule.

You can log a connection event when the system blocks or trusts an encrypted session. You can also force the system to log connections that it decrypts for further evaluation by access control rules, regardless of how the system later handles or inspects the traffic. Connection logs for encrypted sessions contain details, such as the certificate used to encrypt that session. You can log only end-of-connection events.

- For blocked connections (Block, Block with reset), the system immediately ends the sessions and generates an event.
- For Do Not Decrypt connections, the system generates an event when the session ends.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include a decryption policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

Related Topics

Security zone rule conditions, on page 1759
Network rule conditions, on page 1321
VLAN tag rule conditions, on page 1635
User rule conditions, on page 1321
Application rule conditions, on page 1322
Best practice: use application-based rules over port-based rules, on page 1323
Category rule conditions, on page 1763
Server certificate-based rule conditions, on page 1764

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

Security zone conditions in multidomain environments

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

Network rule conditions

A network condition is a traffic matching criterion that

- controls or decrypts traffic based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Note You *cannot* use FDQN network objects in identity rules.

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details

Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

User rule conditions

A user rule condition is a traffic matching mechanism that

- matches traffic based on whether the user initiating the connection or the group to which they belong
- can be configured for users in Microsoft Active Directory realms only, and
- enables policy enforcement based on user identity and group membership.

Special identities users

In addition to configuring users and groups for configured realms, you can set policies for the special identities users:

- Failed Authentication: User who failed authentication with the captive portal.
- Guest: Users configured as guest users in the captive portal.
- No Authentication Required: Users that match an identity **No Authentication Required** rule action.
- Unknown: Users that cannot be identified such as users who are not downloaded by a configured realm.

For access control rules only, you must first associate an identity policy with the access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

User rule condition example

Configure a Block rule to prohibit anyone in the Finance group from accessing a network resource.

Application rule conditions

Application rule conditions are application awareness and control mechanisms that

- identify and classify applications through IP traffic analysis
- enable control with organized filters
- require one enabled detector for each condition.

Application filters and control benefits

System-provided *application filters* help perform control by organizing applications according to basic characteristics, such as type, risk, business relevance, category, and tags. You can also create reuseable, user-defined filters using combinations of system-provided filters, or custom combinations of applications.

At least one detector must be enabled for each application rule condition in the policy. If no detector is enabled, the system automatically enables all available system-provided detectors, or the most recently modified user-defined detector. For more information about application detectors, see Application detectors, on page 2284.

You can utilize both application filters and individually specified applications to ensure complete coverage. Understand the application's requirements to effectively order access control rules.

Application filters help you to quickly configure application control effectively. For example, you can easily use system-provided filters to create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the system blocks the session.

Using application filters simplifies policy creation and administration. It assures you that the system controls application traffic as expected. Because Cisco frequently updates and adds application detectors via system and vulnerability database (VDB) updates, you can ensure that the system uses up-to-date detectors to monitor application traffic. You can also create your own detectors and assign characteristics to the applications they detect, automatically adding them to existing filters.

The system characterizes detected applications using several criteria which form effective filters.

Table 102: Application characteristics

Characteristic	Description	Example
Type	Application protocols represent communications between hosts. Clients represent software running on a host. Web applications represent the content or requested URL for HTTP traffic.	HTTP and SSH are application protocols. Web browsers and email applications are clients. MPEG video and Facebook are web applications.
Risk	The likelihood that the application is being used for purposes that might be against your organization's security policy.	Peer-to-peer applications tend to have a very high risk.
Business Relevance	The likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally.	Gaming applications tend to have a very low business relevance.
Category	A general classification for the application that describes its most essential function. Each application belongs to at least one category.	Facebook is in the social networking category.

Characteristic	Description	Example
Tag	Additional information about the application. Applications can have any number of tags, including none.	Video streaming web applications often are tagged `high bandwidth` and `displays ads`.

Best practice: use application-based rules over port-based rules

Use application filtering criteria instead of port filtering to target traffic. Applications can be configured to use unique ports to bypass access control blocks.

Port conditions allow you to control traffic by its source and destination ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

The traditional method targets applications by using port specifications, but applications can manipulate unique ports to bypass these controls

Application filtering is recommended for applications to avoid blocking legitimate applications, like Firewall Threat Defense, that dynamically open separate channels for control and data flow. Port-based access control rules could block such applications, impacting desirable operations.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP).

- For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).
- If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

Category rule conditions

Category rule conditions are policy elements that

- enable control of web access based on Cisco Talos intelligence
- support policy creation through URL filtering without relying on company vertical, intent, or declared security, and
- can be included in decryption policies to manage encrypted traffic.

Additional information

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from

its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security.

For more information, see URL filtering, on page 1651.

If you are using category rule conditions in decryption policies in a rule with the **Do Not Decrypt** rule action, see Decryption rule Do Not Decrypt action, on page 1778.

Server certificate-based rule conditions

Server certificate-based rule conditions are decryption rules configurations that

- handle and decrypt encrypted traffic based on server certificate characteristics
- inspect traffic using certificate attributes, status, cipher suites, and session versions, and
- enhance secure traffic management and visibility through certificate validation criteria.

Server certificate attribute conditions

You can configure decryption rules based on these server certificate attributes:

- **Distinguished name conditions**: Allow you to handle and inspect encrypted traffic based on the CA that issued a server certificate, or the certificate holder. Based on the issuer distinguished name, you can handle traffic based on the CA that issued a site's server certificate.
- **Certificate conditions**: In decryption rules allow you to handle and inspect encrypted traffic based on the server certificate used to encrypt that traffic. You can configure a condition with one or more certificates; traffic matches the rule if the certificate matches any of the condition's certificates.
- **Certificate status conditions**: In decryption rules allow you to handle and inspect encrypted traffic based on the status of the server certificate used to encrypt the traffic, including whether a certificate is valid, revoked, expired, not yet valid, self-signed, signed by a trusted CA, whether the Certificate Revocation List (CRL) is valid; whether the Server Name Indication (SNI) in the certificate matches the server in the request.
- **Cipher suite conditions**: In decryption rules allow you to handle and inspect encrypted traffic based on the cipher suite used to negotiate the encrypted session.
- **Session conditions**: In decryption rules allow you to inspect encrypted traffic based on the SSL or TLS version used to encrypt the traffic.

To detect multiple cipher suites in a rule, the certificate issuer, or the certificate holder, you can create reusable cipher suite list and distinguished name objects and add them to your rule. To detect the server certificate and certain certificate statuses, you must create external certificate and external CA objects for the rule.

Related Topics

Certificate rule conditions, on page 1765
Certificate Status Decryption rule conditions, on page 1771
Trust external certificate authorities, on page 1770
Match traffic on certificate status
Cipher suite rule conditions, on page 1774
Encryption protocol version rule conditions, on page 1777

Certificate rule conditions

When you build a certificate-based decryption rule condition, you can upload a server certificate and save it as an external certificate *object* The certificate object is reusable and associates a name with a server certificate. Alternately, you can configure certificate conditions with existing external certificate objects and object groups.

You can search the **Available Certificates** field in the rule condition based for external certificate objects and object groups based on these certificate distinguished name characteristics:

- Subject or issuer common name (CN), or if the URL is contained in the certificate's Subject Alternative Name (SAN)

  The URL the user enters in the browser matches the Common Name (CN)

- Subject or issuer organization (O)
- Subject or issuer organizational unit (OU)

You can choose to match against multiple certificates in a single certificate rule condition. If the certificate used to encrypt the traffic matches any of the uploaded certificates, the encrypted traffic matches the rule.

You can add a maximum of 50 external certificate objects and external certificate object groups to the **Selected Certificates** in a single certificate condition.

Note these items:

- You cannot configure a certificate condition if you also select the **Decrypt - Known Key** action. That action requires you to select a server certificate to decrypt traffic. Therefore, the certificate already matches the traffic.
- If you configure a certificate condition with an external certificate object, any cipher suites you add to a cipher suite condition or internal CA objects you associate with the **Decrypt - Resign** action, must match the external certificate's signature algorithm type. For example, if your rule's certificate condition references an EC-based server certificate, any cipher suites you add or CA certificates you associate with the **Decrypt - Resign** action, must also be EC-based. If you mismatch signature algorithm types in this case, the policy editor displays a warning next to the rule.
- When the system first detects an encrypted session to a new server, it does not have certificate data for ClientHello processing. As a result, the first session may not be decrypted. After the initial session, the managed device caches data from the server Certificate message. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with certificate conditions and process the message to maximize decryption potential.

Conditions for distinguished name rules in decryption policies

Learn to use distinguished name conditions in a decryption rule. If you're not sure, you can find a certificate's Subject Alternative Name (SAN) and Common Name using a web browser. You can then you can add those values to a decryption rule as distinguished name conditions.

For detailed information about SANs, see RFC 5280, section 4.2.1.6.

Overview

Distinguished name (DN) conditions allow you to specify certificate field values in decryption rules. This helps control which encrypted traffic is decrypted or excluded from decryption based on the certificate's Common Name (CN) and Subject Alternative Name (SAN)

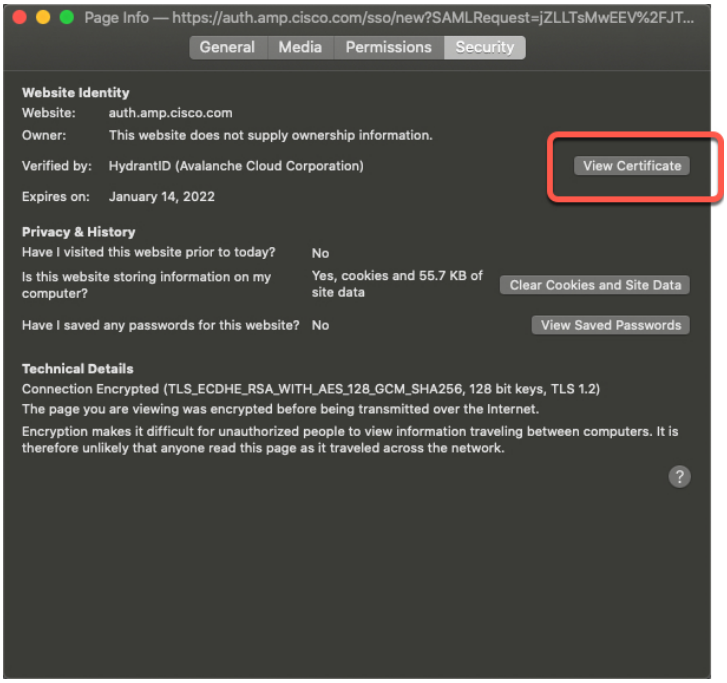
Identifying Certificate Values

Use these steps to find a certificate's Common Name. These steps also work to find the Common Name and SANs for a self-signed certificate.

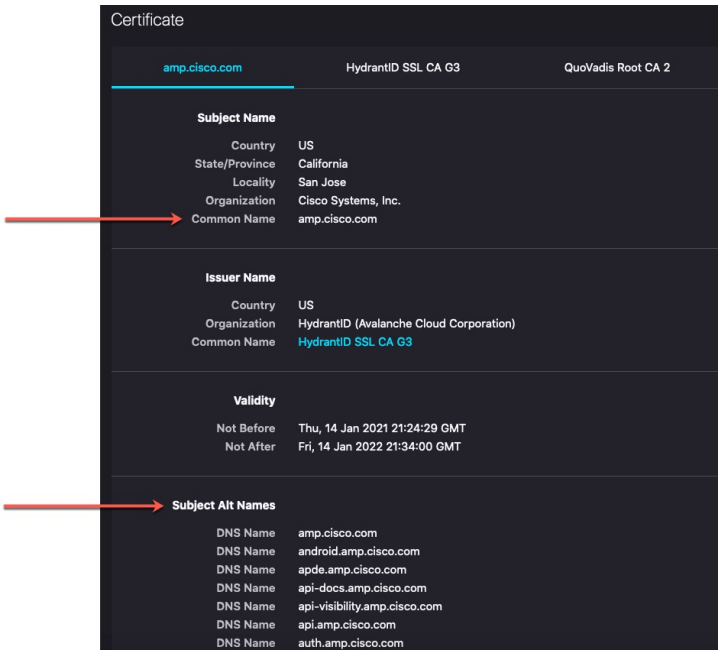
These instructions use Firefox as an example, but other browsers work similarly. The following procedure uses `amp.cisco.com` as an example.

1. Browse to `amp.cisco.com` in Firefox.
2. In the browser's location bar, to the left of the URL, click .
3. Click **Connection secure** > **More Information**.

   (For a non-secure or self-signed certificate, click **Connection not secure** > **More Information**.)
4. On the Page Info dialog box, click **View Certificate**.



5. The next page shows certificate details.



Note the following:

- `CN=auth.amp.cisco.com`, if used as a DN rule condition, would match ONLY that host name (that is, SNI). The SNI `amp.cisco.com` would NOT match.
- Wildcards can be used in DNs to match multiple domains.

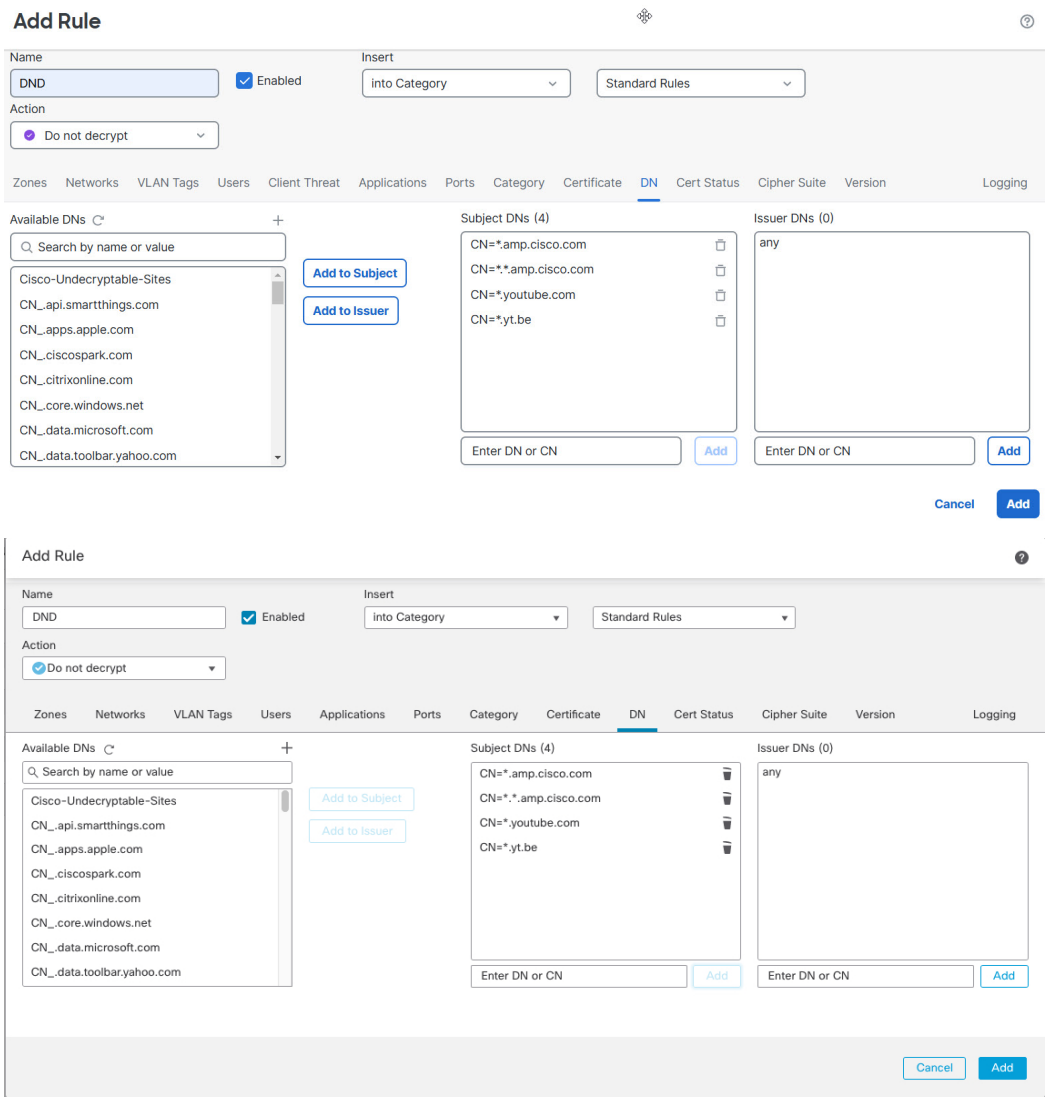
  For example, to match `auth.amp.cisco.com`, use `CN=*.amp.cisco.com`. To match `auth.us.amp.cisco.com`, use `CN=*.*.amp.cisco.com`.

  A DN like `CN=*.example.com` matches `www.example.com` but NOT `example.com`. To match both SNIs, use two DNs in the rule condition.
- Avoid overly broad wildcards like `CN=*.google.com` matches a very large number of SANs. Instead of `CN=*.google.com`, use a DN object like `CN=*.youtube.com` as the DN object so it matches names like `www.youtube.com`.

  You can also use variations of the SNI that match SANs like `CN=*.youtube.com`, `CN=youtu.be`, `CN=*.yt.be`, and so on.
- A self-signed certificate should work the same way. You can confirm it's a self-signed certificate by the fact the issuer DN is the same as the subject DN.

Example: DN rule matching

Suppose you want to prevent decryption for traffic going to `amp.cisco.com` or YouTube. Configure DN rule conditions such as:



These DN conditions would match URLs like:

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

These DN conditions would not match any of the URLs listed, so the traffic would not match the Do Not Decrypt rule. However, it might match another decryption rules in the same decryption policy .

- amp.cisco.com
- youtube.com

- yt.be

To match any of the preceding host names, add more CNs to the rule (for example, adding `CN=yt.be` would match that URL.)

System behavior: SNI and SANs usage

The host name in the client request is called the Server Name Indication (SNI). During the TLS handshake, the client specifies which hostname they want to connect to (for example, `auth.amp.cisco.com`) using the SNI extension. The server then selects the corresponding private key and certificate chain that are required to establish the connection while hosting all certificates on a single IP address.

If the SNI matches the CN or a SAN in the certificate, the SNI is used for DN rule matching.

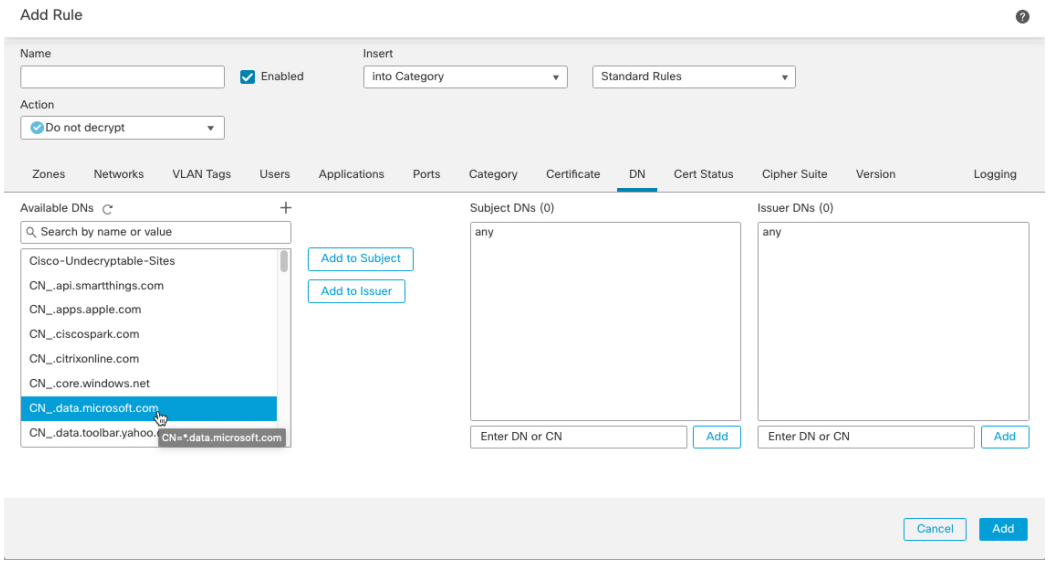
If there is no SNI, or the SNI does not match the certificate, the CN is used for DN rule matching.

Add a DN rule condition

After you identify the CN you want to match,, edit the decryption rule by using an existing DN, creating a new DN object, or adding the DN directly.

- Use an existing DN.

  Click the name of a DN and then click either **Add to Subject** or **Add to Issuer**. (**Add to Subject** is much more common.) To view the value of a DN object, hover the mouse pointer over it.)

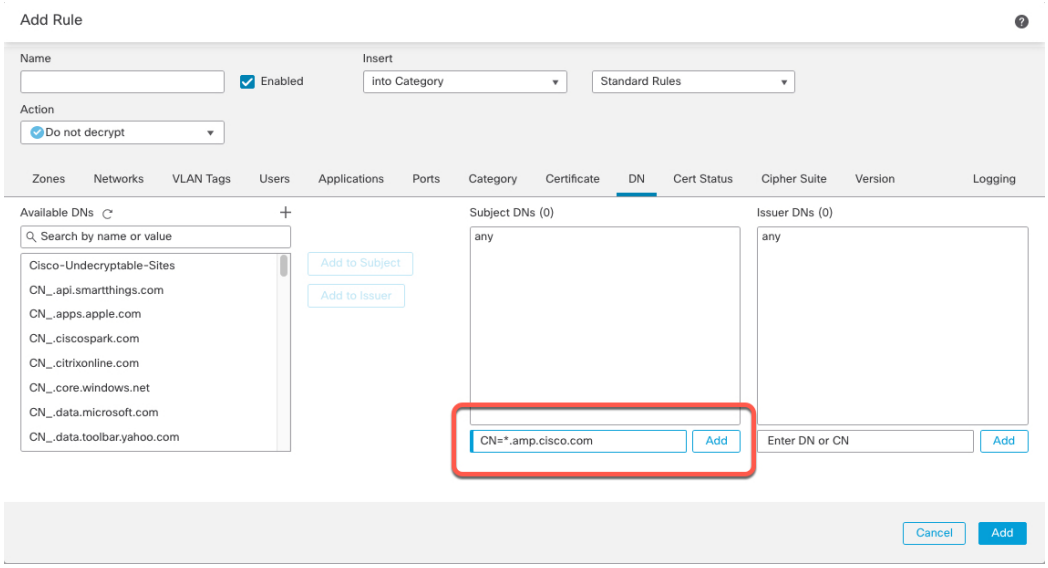


- Create a new DN object.

  Click **Add** (+) to the right of Available DNs. The DN object must consist of a name and a value.

- Add the DN directly.

  Enter the DN in the field at the bottom of the **Subject DNs** field or the **Issuer DNs** field. (**Subject DNs** is more common.) After you enter the DN, click **Add**.



Related Topics

Distinguished names, on page 2364

Trust external certificate authorities

Trust CAs by adding root and intermediate CA certificates to your decryption policy, then use these trusted CAs to verify server certificates used to encrypt traffic.

If a trusted CA certificate contains an uploaded certificate revocation list (CRL), you can also verify whether a trusted CA revoked the encryption certificate.

Tip Upload all certificates in a root CA's chain of trust to the list of trusted CA certificates, including the root CA certificate and all intermediate CA certificates. Otherwise, it is more difficult to detect trusted certificates issued by intermediate CAs. Also, if you configure certificate status conditions to trust traffic based on the root issuer CA, all traffic within a trusted CA's chain of trust can be allowed without decryption, rather than unnecessarily decrypting it.

For more information, see Trusted CA objects, on page 2396.

Note When you create a decryption policy, the policy's **Trusted CA Certificate** tab page is populated with several trusted CA certificates, including the **Cisco-Trusted-Authorities** group, which is added to the **Select Trusted CAs** list.

Procedure

Step 1 Log in to the Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** ( ) next to the decryption policy to edit.

Step 4 Click **Add Rule** to add a new decryption rule or click **Edit** ( ) to edit an existing rule.

Step 5 Click the **Certificates** tab.

Step 6 Find the trusted CAs you want to add from the **Available Certificates**, as follows:

- To add a trusted CA object on the fly, which you can then add to the condition, click **Add** ( ) above the **Available Certificates** list.
- To search for trusted CA objects and groups to add, click the **Search by name or value** prompt above the **Available Certificates** list, then enter either the name of the object, or a value in the object. The list updates as you type to display matching objects.

Step 7 To select an object, click it. To select all objects, right-click and then **Select All**.

Step 8 Click **Add to Rule**.

Tip You can also drag and drop selected objects.

Step 9 Add or continue editing the rule.

The trusted CA certificates are configured in your decryption policy and can be used to verify server certificates for secure traffic inspection.

What to do next

- Add a certificate status decryption rule condition to your SSL rule.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Certificate Status Decryption rule conditions

For each certificate status decryption rule you configure, you can match traffic against the presence or absence of a given status. You can select several statuses in one rule condition. If the certificate matches any of the selected statuses, the rule matches the traffic.

You can choose to match against the presence or absence of multiple certificate statuses in a single certificate status rule condition. The certificate needs to match only one of the criteria to match the rule.

You should consider, when setting this parameter, whether you're configuring a decrypt rule or a block rule. Typically, you should click **Yes** for a block rule and **No** for a decrypt rule. Examples:

- If you're configuring a **Decrypt - Resign** rule, the default behavior is to decrypt traffic with an expired certificate. To change that behavior, click **No** for **Expired** so traffic with an expired certificate is not decrypted and resigned.
- If you're configuring a **Block** rule, the default behavior is to allow traffic with an expired certificate. To change that behavior click **Yes** for **Expired** so traffic with an expired certificate is blocked.

This table describes how the system evaluates encrypted traffic based on the status of the encrypting server's certificate.

Table 103: Certificate status rule condition criteria

Status Check	Status Set to Yes	Status Set to No
Revoked	The policy trusts the CA that issued the server certificate, and the CA certificate uploaded to the policy contains a CRL that revokes the server certificate.	The policy trusts the CA that issued the ser certificate, and the CA certificate uploaded policy does not contain a CRL that revoke certificate.
Self-signed	The detected server certificate contains the same subject and issuer distinguished name.	The detected server certificate contains dif subject and issuer distinguished names.
Valid	All of these are true: • The policy trusts the CA that issued the certificate. • The signature is valid. • The issuer is valid. • None of the policy's trusted CAs revoked the certificate. • The current date is between the certificate Valid From and Valid To date.	At least one of these is true: • The policy does not trust the CA that certificate. • The signature is invalid. • The issuer is invalid. • A trusted CA in the policy revoked th certificate. • The current date is before the certifica From date. • The current date is after the certificate date.
Invalid signature	The certificate's signature cannot be properly validated against the certificate's content.	The certificate's signature is properly validat the certificate's content.
Invalid issuer	The issuer CA certificate is not stored in the policy's list of trusted CA certificates.	The issuer CA certificate is stored in the po of trusted CA certificates.
Expired	The current date is after the certificate Valid To date.	The current date is before or on the certific To date.
Not yet valid	The current date is before the certificate Valid From date.	The current date is after or on the certificat From date.

Status Check	Status Set to Yes	Status Set to No
Invalid certificate	The certificate is not valid. At least one of these is true: • Invalid or inconsistent certificate extension; that is, a certificate extension had an invalid value (for example, an incorrect encoding) or some value inconsistent with other extensions. • The certificate cannot be used for the specified purpose. • The Basic Constraints path length parameter has been exceeded. For more information, see RFC 5280, section 4.2.1.9. • The certificate's value for Not Before or Not After is invalid. These dates can be encoded as UTCTime or GeneralizedTime For more information, see RFC 5280 section 4.1.2.5. • The format of the name constraint is not recognized; for example, an email address format of a form not mentioned in RFC 5280, section 4.2.1.10. This could be caused by an improper extension or some new feature not currently supported. An unsupported name constraint type was encountered. OpenSSL currently supports only directory name, DNS name, email, and URI types. • The root certificate authority is not trusted for the specified purpose. • The root certificate authority rejects the specified purpose.	The certificate is valid. All of these are • Valid certificate extension. • The certificate can be used for the purpose. • Valid Basic Constraints path lengt • Valid values for Not Before and N • Valid name constraint. • The root certificate is trusted for t purpose. • The root certificate accepts the spec

Status Check	Status Set to Yes	Status Set to No
Invalid CRL	The Certificate Revocation List (CRL) digital signature is not valid. At least one of these is true: • The value of the CRL's Next Update or Last Update field is invalid. • The CRL is not yet valid. • The CRL has expired. • An error occurred when attempting to verify the CRL path. This error occurs only if extended CRL checking is enabled. • CRL could not be found. • The only CRLs that could be found did not match the scope of the certificate.	The CRL is valid. All of these are true: • Next Update and Last Update fields a • The CRL's date is valid. • The path is valid. • The CRL was found. • The CRL matches the certificate's sco
Server mismatch	The server name does not match the server's Server Name Indication (SNI) name, which could indicate an attempt to spoof the server name.	The server name matches the SNI name of to which the client is requesting access.

Note that even though a certificate might match more than one status, the rule causes an action to be taken on the traffic only once.

Checking whether a CA issued or revoked a certificate requires uploading root and intermediate CA certificates and associated CRLs as objects. You then add these trusted CA objects to an decryption policy's list of trusted CA certificates.

Cipher suite rule conditions

The system provides predefined cipher suites you can add to a cipher suite rule condition for Block or Block WITH Reset rule actions. You can also add cipher suite list objects containing multiple cipher suites.

Important Cipher suite rule conditions should be used only to *block* traffic, they should not be used to *decrypt* traffic.

Note You cannot add new cipher suites. You can neither modify nor delete predefined cipher suites.

You can add a maximum of 50 cipher suites and cipher suite lists to the **Selected Cipher Suites** in a single cipher suite condition. The system supports adding these cipher suites to a cipher suite condition:

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

Note these considerations:

- If you add cipher suites not supported for your deployment, you cannot deploy your configuration. For example, passive deployments do not support decrypting traffic with the any of the ephemeral Diffie-Hellman (DHE) or ephemeral elliptic curve Diffie-Hellman (ECDHE) cipher suites. Creating a rule with these cipher suites prevents you from deploying your access control policy.
- You can add an anonymous cipher suite to the **Cipher Suite** condition in decryption policy. To use the rule, you must also configure your settings in an order that prevents ClientHello processing. For more information, refer to Best practice for Decryption policy rule order.
- When you specify a cipher suite as a rule condition, the rule matches the negotiated cipher suite in the ServerHello message, not the entire list from the ClientHello message. During ClientHello processing, the managed device removes unsupported cipher suites from the ClientHello message. If all specified cipher suites are removed, the system retains the original list. If the system keeps unsupported cipher suites, it cannot decrypt the session during subsequent evaluation.

Encryption protocol version rule conditions

You can choose to match against traffic encrypted with SSL version 3.0, or TLS version 1.0, 1.1, or 1.2. By default, all protocol versions are selected when you create a rule; if you select multiple versions, encrypted traffic that matches any of the selected versions matches the rule. You must select at least one protocol version when saving the rule condition.

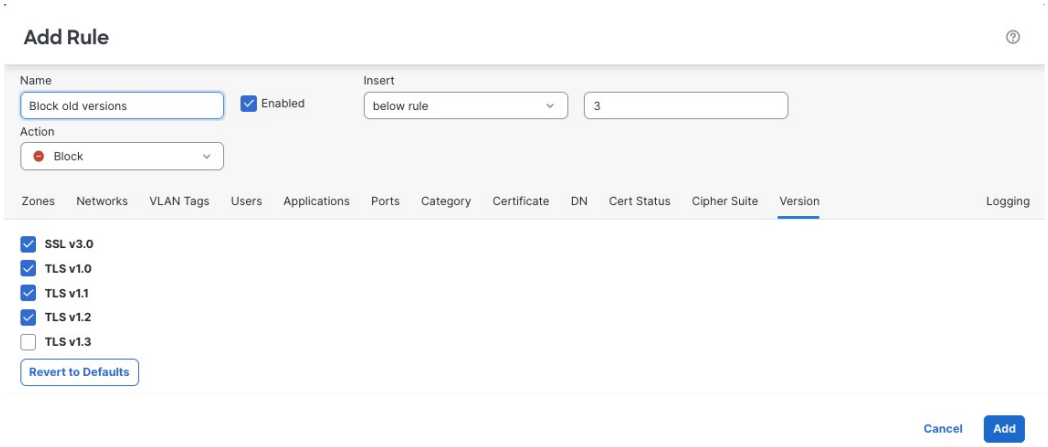
You can use SSL 3.0 in a Do Not Decrypt, Block, or Block with Reset rule action.

You *cannot* select SSL v2.0 in a version rule condition; the system does not support decrypting traffic encrypted with SSL version 2.0. You can configure an undecryptable action to allow or block this traffic without further inspection. For more information, see Set default handling for undecryptable traffic, on page 1741.

Important Protocol version rule conditions should be used *only* to *block* traffic, they should not be used to *decrypt* traffic.

For example, to block all SSL v3.0, TLS v1.0, TLS v1.1, and TLS v1.2 traffic, set the options as follows:

Figure 412: Block all SSL v3.0, TLS v1.0, TLS v1.1, and TLS 1.2 traffic



Decryption Rule actions

Decryption Rule actions are operational functions that define how the system processes SSL/TLS traffic based on configured decryption rules.

Available actions

The system provides various actions for decryption rule.

Decryption rule monitor action

The **Monitor** action is not designed to permit or deny traffic. Rather, its primary purpose is to force connection logging, regardless of how matching traffic is eventually handled. The ClientHello message is not modified if traffic matches a **Monitor** rule condition.

Monitor action traffic handling

Traffic that matches a **Monitor** rule is processed in this sequence:

1. Traffic matches the Monitor rule condition and connection logging is forced.
2. Traffic is then matched against additional rules, if present, to determine whether to trust, block, or decrypt it.
3. The first non-Monitor rule matched determines traffic flow and any further inspection.
4. If there are no additional matching rules, the system uses the default action.

The system automatically logs end-of connection events for monitored traffic to the Secure Firewall Management Center database, regardless of the logging configuration of the rule or default action that later handles the connection.

Decryption rule Do Not Decrypt action

The Do Not Decrypt action passes encrypted traffic for evaluation by the access control policy's rules and default action. Because some access control rule conditions require unencrypted traffic, this traffic might match fewer rules. The system cannot perform deep inspection on encrypted traffic, such as intrusion or file inspection.

Typical use cases for do not decrypt rules

Typical reasons for a **Do Not Decrypt** rule action include:

- When decrypting TLS/SSL traffic is prohibited by law.
- Sites you know you can trust.
- Sites you can disrupt by inspecting traffic (such as Windows Update).
- To view the values of TLS/SSL fields using connection events. (You do not need to decrypt traffic to view connection event fields.) For more information, see *Requirements for Populating Connection Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide*.

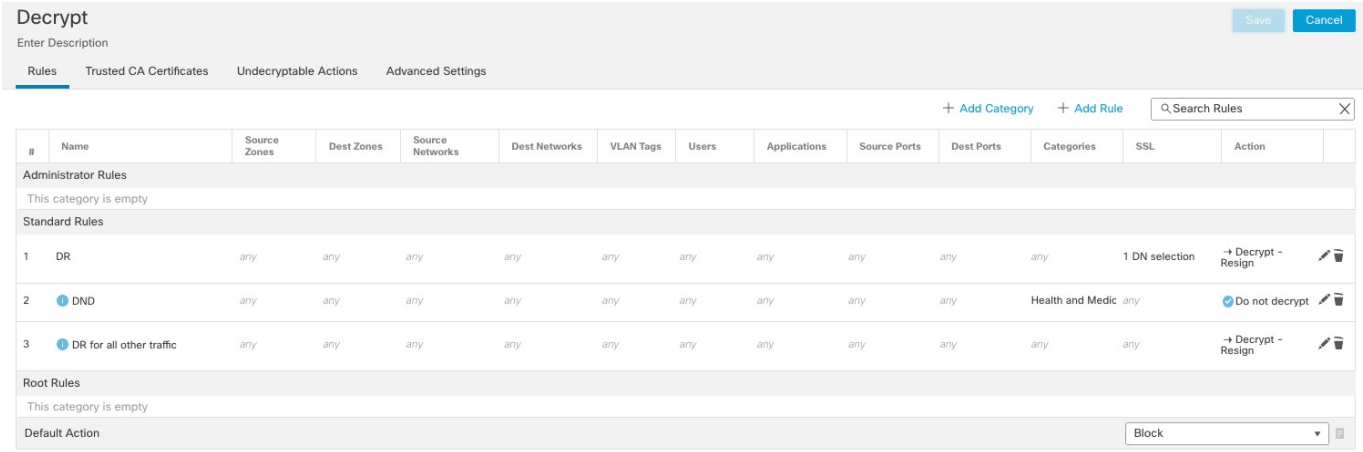
For more information, see Default handling options for undecryptable traffic, on page 1739

Limitations of categories in Do Not Decrypt rules

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security. While we strive to continuously update and improve URL filtering categories, it is not an exact science. Some websites are not categorized at all and it's possible some websites might be improperly categorized.

Avoid overusing categories in do not decrypt rules to avoid decrypting traffic without a reason; for example, the Health and Medicine category includes the WebMD website, which does not threaten patient privacy.

Following is a sample decryption policy that can prevent decryption for websites in the Health and Medicine categories but allows decryption for WebMD and everything else. General information about decryption rules can be found in Guidelines for using TLS/SSL decryption, on page 1746.



Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control, on page 1622.

Decryption rule blocking actions

Decryption rule blocking actions provide different termination methods to control connection handling.

Available blocking actions

The system provides these decryption rule actions for traffic you do not want to pass through the system:

- **Block**: Terminates the connection, resulting in an error in the client browser. The error message does not indicate the site was blocked due to policy. Instead, errors might indicate that there are no common encryption algorithms. It is not obvious from this message that you blocked the connection on purpose.
- **Block with reset**: Terminates and resets the connection, resulting in an error in the client browser. The error indicates the connection was reset but does not indicate why.

Tip You cannot use the **Block** or **Block with reset** action in a passive or inline (tap mode) deployment because the device does not directly inspect the traffic. If you create a rule with the **Block** or **Block with reset** action that contains passive or inline (tap mode) interfaces within a security zone condition, the policy editor displays a warning (⚠) next to the rule.

Decryption rule decrypt actions

Decrypt - Known Key, and **Decrypt - Resign** are rule actions that decrypt encrypted traffic. The system inspects decrypted traffic with access control. Access control rules handle decrypted and unencrypted traffic

identically — you can inspect it for discovery data as well as detect and block intrusions, prohibited files, and malware. The system reencrypts allowed traffic before passing it to its destination.

Certificate authority recommendations

We recommend you use a certificate from a trusted Certificate Authority (CA) to decrypt traffic. This prevents **Invalid Issuer** from being displayed in the SSL Certificate Status column in connection events.

For more information about adding trusted objects, see Trusted certificate authority objects, on page 2395.

Related topic: TLS 1.3 decryption best practices, on page 1743.

Related Topics

TLS 1.3 decryption best practices, on page 1743

Monitor TLS/SSL hardware acceleration

TLS/SSL hardware acceleration monitoring is a set of topics that discuss how to monitor the status of TLS/SSL hardware acceleration.

Informational counters

Monitor TLS/SSL hardware acceleration performance and interpret KEY counter values, such as PRIV_KEY_RECV and SECU_PARAM_RECV, to assess system load and connection activity using the **show counters** command.

If a system under load is working well, you should see large counts for the following counters. Because there are two sides to the tracker process per connection, you can see these counters increase by two per connection. The PRIV_KEY_RECV and SECU_PARAM_RECV counters are the most important, and are highlighted. The CONTEXT_CREATED and CONTEXT_DESTROYED counters relate to the allocation of cryptographic chip memory.

```
> show counters
Protocol     Counter                          Value   Context
SSLENC       CONTEXT_CREATED                 258225   Summary
SSLENC       CONTEXT_DESTROYED               258225   Summary
TLS_TRK      OPEN_SERVER_SESSION             258225   Summary
TLS_TRK      OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK      UPSTREAM_CLOSE                  516450   Summary
TLS_TRK      DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK      FREE_SESSION                    516450   Summary
TLS_TRK      CACHE_FREE                      516450   Summary
TLS_TRK      PRIV_KEY_RECV                   258225   Summary
TLS_TRK      NO_KEY_ENABLE                   258225   Summary
TLS_TRK      SECU_PARAM_RECV                 516446   Summary
TLS_TRK      DECRYPTED_ALERT                 258222   Summary
TLS_TRK      DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK      ALERT_RX_CNT                    258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX      OPEN_SESSION                    516450   Summary
TCP_PRX      FREE_SESSION                    516450   Summary
TCP_PRX      UPSTREAM_CLOSE                  516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX      FREE_CONN                       258222   Summary
```

```
TCP_PRX      SERVER_CLEAN_UP                 258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                 258222   Summary
```

Alert counters

Alert counters identify potential issues based on standardized alert types.

These counters are based on the TLS 1.2 specification. FATAL or BAD alerts could indicate issues. However, ALERT_RX_CLOSE_NOTIFY is normal.

For details, see RFC 5246 section 7.2.

```
TLS_TRK      ALERT_RX_CNT                       311   Summary
TLS_TRK      ALERT_TX_CNT                         2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT             308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                 3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                 2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY              308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE             1   Summary
```

Error counters

Error counters help you interpret system performance data to identify potential issues and optimize performance using the show counters command.

Fatal counters

Monitor and interpret TLS/SSL hardware acceleration fatal counters to identify serious errors, assess system health, and troubleshoot persistent crypto acceleration issues on Cisco devices. Reset or review counters for proactive system maintenance and support.

Fatal counters indicate serious errors. These counters should be at or near 0 on a healthy system. This is an example list of the fatal counters.

```
> show counters
Protocol     Counter                         Value   Context
CRYPTO       RING_FULL                           1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT            1   Summary
CRYPTO       ACCELERATOR_RESET                   1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED          1   Summary
```

The RING_FULL counter is not a fatal counter, but indicates how often the system overloaded the cryptographic chip. The ACCELERATOR_RESET counter is the number of times the TLS crypto acceleration process failed unexpectedly, which also causes the failure of pending operations, which are the numbers you see in ACCELERATOR_CORE_TIMEOUT and RSA_PRIVATE_DECRYPT_FAILED.

If you have persistent problems, disable TLS crypto acceleration (or **config hwCrypto disable**) and work with Cisco TAC to resolve the issues.

Note You can do additional troubleshooting using the **show snort tls-offload** and **debug snort tls-offload** commands. Use the **clear snort tls-offload** command to reset the counters displayed in the **show snort tls-offload** command to zero.

Troubleshoot Decryption Rules

This topic discusses how to troubleshoot decryption rules.

TLS/SSL oversubscription

TLS/SSL oversubscription is a state where a managed device is overloaded with TLS/SSL traffic. Any managed device can experience TLS/SSL oversubscription but only managed devices that support TLS crypto acceleration provide a configurable way to handle it.

TLS/SSL oversubscription details

When a managed device with TLS crypto acceleration enabled is oversubscribed, any packet received by the managed device is acted on according to the setting for **Handshake Errors** in the decryption policy's **Undecryptable Actions**:

- Inherit default action
- Do not decrypt
- Block
- Block with reset

If the setting for **Handshake Errors** in the decryption policy's **Undecryptable Actions** is **Do Not decrypt** and the associated access control policy is configured to inspect the traffic, inspection occurs; decryption does *not* occur.

Troubleshoot TLS/SSL oversubscription

Monitor and troubleshoot TLS/SSL oversubscription by configuring decryption policies, enabling logging, and adding SSL Flow Flags to connection event views in Firewall Management Center.

If your managed device has TLS crypto acceleration enabled, you can view connection events to determine whether or not the devices are experiencing SSL oversubscription. You must add at least the **SSL Flow Flags** event to the table view of connection events.

Before you begin

- Configure a decryption policy with a setting for **Handshake Errors** on **Undecryptable Actions** page.

  For more information, see Set default handling for undecryptable traffic, on page 1741.

- Enable logging for your SSL rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Follow these steps to troubleshoot TLS/SSL oversubscription:

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Analysis** > **Connections** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.

Step 5 Click **Apply**.
TLS/SSL oversubscription is indicated by the values of `ERROR_EVENT_TRIGGERED` and `OVER_SUBSCRIBED` in the **SSL Flow Flags** column.

Step 6 If TLS/SSL oversubscription is occurring, log in to the managed device and enter any of the following commands:

Command	Result
show counters	If the value of **TCP_PRX BYPASS_NOT_ENOUGH_MEM** is large, consider upgrading your device to one with a larger capacity for SSL traffic or use **Do NOT Decrypt** rules for lower priority encrypted traffic.
show snort TLS-offload	If the value of **BYPASS_NOT_ENOUGH_MEM** is large, consider upgrading your device to one with a larger capacity for SSL traffic or use **Do NOT Decrypt** rules for lower priority encrypted traffic.

TLS heartbeat

A TLS heartbeat extension enables applications to confirm active TLS or DTLS connections.

TLS heartbeat handling

Some applications use the *TLS heartbeat* extension to the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols defined by RFC6520. TLS heartbeat provides a way to confirm the connection is still alive—either the client or server sends a specified number of bytes of data and requests the other party echo the response. If this is successful, encrypted data is sent.

When a managed device with TLS crypto acceleration enabled encounters a packet that uses the TLS heartbeat extension, the managed device takes the action specified by the setting for **Decryption Errors** in the decryption policy's **Undecryptable Actions**:

- Block
- Block with reset

Related Topics

Troubleshoot TLS heartbeat, on page 1784

Troubleshoot TLS heartbeat

This task helps you identify TLS heartbeat activity in your network to determine if applications are using the TLS heartbeat extension.

If your managed device has TLS crypto acceleration enabled, you can view connection events to determine whether or not the devices are seeing traffic with the TLS heartbeat extension. You must add at least the **SSL Flow Messages** event to the table view of connection events.

TLS heartbeat is indicated by the value of `HEARTBEAT` in the **SSL Flow Messages** column in the table view of connection events.

Before you begin

To determine if applications in your network use TLS heartbeat, first perform these tasks:

- Configure an decryption policy with a setting for **Decryption Errors** on **Undecryptable Actions** page.

  For more information, refer to Set default handling for undecryptable traffic, on page 1741.

- Enable logging for your SSL rules as discussed in Secure Firewall Management Center and Threat Defense Management Network Administration.

Follow these steps to troubleshoot TLS heartbeat:

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Analysis** > **Connections** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.

Step 5 Click **Apply**.
TLS heartbeat is indicated by the value of `HEARTBEAT` in the **SSL Flow Messages** column.

Step 6 If applications in your network use TLS heartbeat, refer to Decryption Rules guidelines and limitations, on page 1746.

TLS/SSL pinning

TLS/SSL pinning is a security mechanism that

- validates server certificates against a predetermined set of trusted certificates or keys
- prevents man-in-the-middle attacks by rejecting connections to servers with unexpected certificates, and
- requires applications to maintain a local store of trusted certificate information for validation.

TLS/SSL pinning implementation details

Some applications use a technique referred to as *TLS/SSL pinning* or *certificate pinning*, which embeds the fingerprint of the original server certificate in the application itself. As a result, if you configured a decryption rule with a **Decrypt - Resign** action, when the application receives a resigned certificate from a managed device, validation fails and the connection is aborted.

To confirm that TLS/SSL pinning is occurring, attempt to log in to a mobile application like Facebook. If a network connection error is displayed, log in using a web browser. (For example, you *cannot* log in to a Facebook mobile application but *can* log in to Facebook using Safari or Chrome.) You can use Firepower Management Center connection events as further proof of TLS/SSL pinning

Note TLS/SSL pinning is not limited to mobile applications.

If applications in your network use SSL pinning, see TLS/SSL certificate pinning guidelines, on page 1752.

Related Topics

Troubleshoot TLS/SSL pinning, on page 1785

Troubleshoot TLS/SSL pinning

This task helps you identify and confirm whether applications in your network are using TLS/SSL pinning by analyzing SSL connection events and flow DATA.

You can view connection events to determine whether or not the devices are experiencing TLS/SSL pinning. You must add at least the **SSL Flow Flags** and **SSL Flow Messages** columns to the table view of connection events.

Before you begin

- Enable logging for your decryption rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.
- Log in to a mobile application like Facebook. If a network connection error displays, log in to Facebook using Chrome or Safari. If you *can* log in using a web browser but not the native application, TLS/SSL pinning is likely occurring.

Follow these steps to troubleshoot TLS/SSL pinning:

Procedure

Step 1 If you haven't DONE so already, log in to the Firewall Management Center.

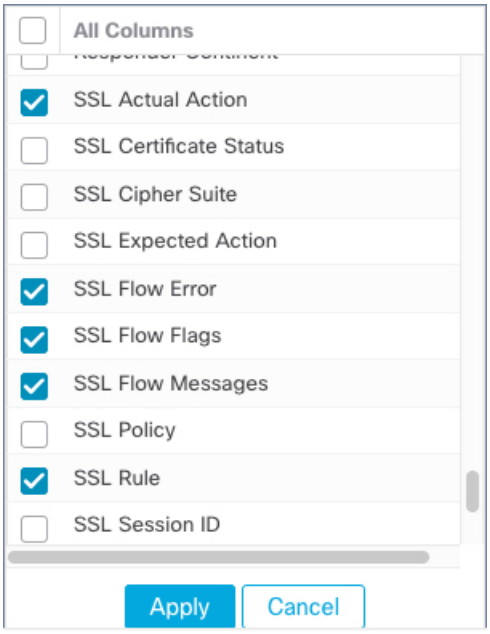
Step 2 Click **Analysis** > **Connections** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events.



The columns are added in the order discussed in the section on connection and security intelligence event fields in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Step 5 Click **Apply**.

Step 6 Analyze the SSL flow DATA to identify SSL pinning behavior.

Step 7 If you determine that applications in your network use SSL pinning, see Decryption Rules guidelines and limitations, on page 1746.

What to do next

You can use TLS/SSL connection events to confirm TLS/SSL pinning is occurring by looking for any of the following:

- Applications that send an SSL ALERT Message as soon as the CLIENT receives the SERVER_HELLO, SERVER_CERTIFICATE, SERVER_HELLO_DONE message from the SERVER, followed by a TCP Reset, exhibit the following symptoms. (The ALERT, `Unknown CA (48)`, can be viewed using a packet capture.)
  - The SSL Flow Flags column displays `ALERT_SEEN` but *not* `APP_DATA_C2S` or `APP_DATA_S2C`.

- If your managed device has SSL hardware acceleration enabled, the SSL Flow Messages column typically displays: `CLIENT_ALERT`, `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`.
- If your managed device doesn't support SSL hardware acceleration or if the feature is disabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`.
- `Success` is displayed in the SSL Flow Error column.

- Applications that send no alerts but instead send TCP Reset after the SSL handshake is FINISHED exhibit the following symptoms:
  - The SSL Flow Flags column does *not* display `ALERT_SEEN`, `APP_DATA_C2S`, or `APP_DATA_S2C`.
  - If your managed device has SSL hardware acceleration enabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`, `SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`.
  - If your managed device doesn't support SSL hardware acceleration or if the feature is disabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`,`SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`.
  - `Success` is displayed in the SSL Flow Error column.

Related Topics

Troubleshoot unknown or bad certificates or certificate authorities, on page 1787

Troubleshoot unknown or bad certificates or certificate authorities

Enable logging for TLS/SSL decryption rules to monitor connection events and identify certificate-related issues. This helps you diagnose problems with certificate authorities, bad certificates, or unknown certificates in your TLS/SSL connections.

You can view connection events to determine whether or not the devices are experiencing unknown certificate authorities, bad certificates, or unknown certificates. This procedure can also be used if a TLS/SSL certificate has been pinned. You must add at least the **SSL Flow Flags** and **SSL Flow Messages** columns to the table view of connection events.

Before you begin

- Set up a decryption rule.
- Enable logging for your decryption rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Follow these steps to troubleshoot unknown or bad certificates or certificate authorities:

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

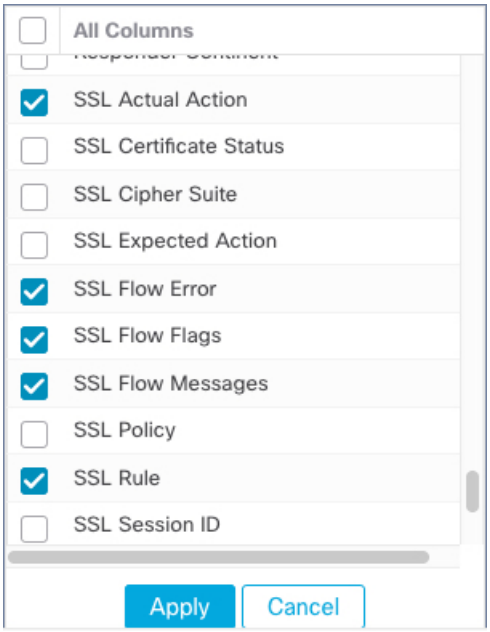
Step 2 Click **Analysis** > **Connections** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events.



The columns are added in the order discussed in the section on connection and security intelligence event fields in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Step 5 Click **Apply**.

Step 6 Review the SSL flow flags to determine if a certificate or certificate authority is bad or missing.

SSL flow flag	Meaning
CLIENT_ALERT_SEEN_UNKNOWN_CA	Indicates a valid certificate chain or partial chain was received by an SSL client application, but the certificate was not accepted because the CA certificate could not be located or could not be matched with a known, trusted CA. This message always indicates an unrecoverable error.
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	A certificate was corrupt, contained signatures that did not verify correctly, or had other problems.
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	Some other (unspecified) issue arose in processing the certificate, rendering it unacceptable.

Verify TLS/SSL cipher suites

This task helps you resolve cipher suite incompatibility errors that occur when saving a decryption rule that has cipher suite conditions. The error indicates that one or more of the cipher suites you chose for the decryption rule condition are incompatible with the certificate used in the decryption rule.

This topic discusses actions you must take if you see the following error when saving a decryption rule that has cipher suite conditions:

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that matches the resigning CA's signature algorithm
```

Before you begin

To resolve the issue, you must have access to the certificate you're using.

Note The tasks in this topic assume knowledge of how TLS/SSL encryption works.

Follow these steps to verify TLS/SSL cipher suites:

Procedure

Step 1 When you attempt to save a decryption rule rule with either **Decrypt - Resign** or **Decrypt - Known Key** with specified cipher suites, the following error is displayed:

Example:

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

Step 2 Locate the certificate you're using to decrypt traffic and, if necessary, copy the certificate to a system that can run openssl commands.

Step 3 Run the following command to display the signature algorithm used by the certificate:

Example:

openssl x509 -in *CertificateName* **-text -noout**

The first few lines of output are displayed similar to the following:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

Step 4 The **Signature algorithm** tells you the following:

- The cryptographic function used (in the preceding example, **ECDSA** means Elliptic Curve Digital Signature Algorithm).
- The hash function used to create a digest of the encrypted message (in the preceding example, **SHA256**).

Step 5 Search a resource such as *OpenSSL at University of Utah* for cipher suites that match those values. The cipher suite must be in RFC format.
You can also search a variety of other sites, such as Server Side TLS at the Mozilla wiki or Appendix C of RFC 5246. Cipher Suites in TLS/SSL (Schannel SSP) in Microsoft documentation has a detailed explanation of cipher suites.

Step 6 If necessary, translate the OpenSSL name to an RFC name that the Firepower Management System uses. See the RFC mapping list on the on the `https://testssl.sh` site.

Step 7 The previous example, **ECDSA-with-SHA256**, can be found in the Modern Compatibility List on the Mozilla wiki.

Choose only cipher suites that have **ECDSA** and **SHA-256** in the name. These cipher suites follow:

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

Find the corresponding RFC cipher suite on RFC mapping list. These cipher suites follow:

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

Step 8 Add the preceding cipher suites to your decryption rule.

Troubleshoot using crypto archives

Crypto issues are difficult to triage. Crypto archives help you to troubleshoot these issues. A crypto archive contains crypto session information about the crypto request, peer information, the component that sent the crypto request, and the timed-out crypto session information.

About crypto archives

Threat defense does not save keys and initialization vectors (IVs) for the session. For SSL and IPsec, you can also view these information:

- For SSL: Session SSL version, source, destination IP addresses, and ports.
- For IPsec: IPsec security association information.

A ring can hold 2000 crypto command entries. Threat defense pushes the crypto command in one of the rings and pulls out the result after completing the crypto request. Crypto archive files now have the timed-out crypto request's ring and entry index. The ring and its entry index help in troubleshooting problematic crypto commands.

The crypto archive has two formats: a text file and a binary file. You can use the **debug menu ctm 103** command to decode the binary file. The crypto archive files are available at disk0:/crypto_archive.

For example:

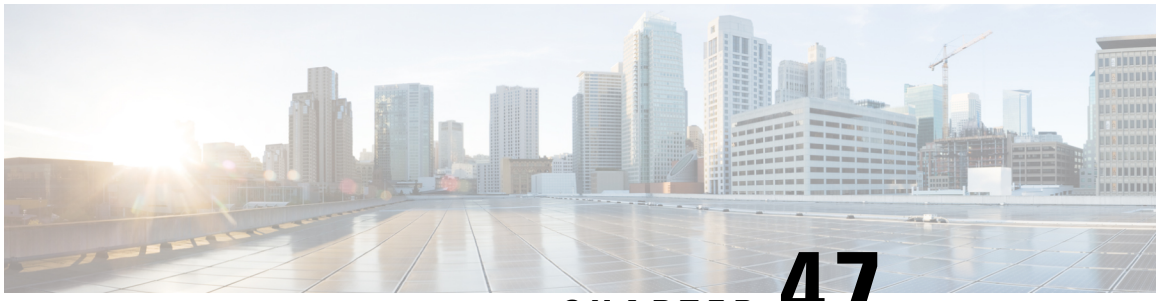
```
FTD# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443
```

In this example, the highlighted information shows the timeout ring, the crash time (timeout entry), and SSL session information.

Supported devices for crypto archives

These devices with Nitrox V crypto accelerator support crypto archives:

- Cisco Firepower 3105, 3110, 3120, 3130, 3140
- Cisco Firepower 4112, 4115, 4125, 4145
- Cisco Firepower 9300 SM-40, SM-48 and SM-56
- Cisco Secure Firewall 4200



CHAPTER 47

Decryption rules and Policy Example

This chapter builds on concepts discussed in this guide to provide a specific example of an SSL policy with decryption rules that follow our best practices and recommendations. You should be able to apply this example to your situation, adapting it to the needs of your organization.

In short:

- For trusted traffic (such as transferring a large compressed server backup), bypass inspection entirely, using prefiltering and flow offload.
- Put *first* any decryption rules that can be evaluated quickly, such as those that apply to specific IP addresses.
- Put *last* any decryption rules that require processing, **Decrypt - Resign**, and rules that block unsecure protocol versions and cipher suites.

- Decryption rule Examples, on page 1793
- , on page 1793
- : Decrypt Specific Test Traffic, on page 1794
- Decryption rules: Block or Monitor Certificates and Protocol Versions, on page 1794
- Associate the Decryption policy with an Access Control Policy and Advanced Settings, on page 1798
- Traffic to Prefilter, on page 1800
- Decryption rule Settings, on page 1801

Decryption rule Examples

This section provides an example of decryption rule that illustrate our best practices.

See one of the following sections for more information.

The first decryption rule in the example does not decrypt traffic that goes to an internal network (defined as **intranet**). **Do Not Decrypt** rule actions are matched during ClientHello so they are processed very fast.

Note If you have traffic going from internal DNS servers to internal DNS resolvers (such as Cisco Umbrella Virtual Appliances), you can add **Do Not Decrypt** rules for them as well. You can even add those to prefiltering policies if the internal DNS servers do their own logging.

However, we strongly recommend you *do not* use **Do Not Decrypt** rules or prefiltering for DNS traffic that goes to the internet, such as internet root servers (for example, Microsoft internal DNS resolvers built into Active Directory). In those cases, you should fully inspect the traffic or even consider blocking it.

Rule detail:

: Decrypt Specific Test Traffic

The next rule is *optional* in the example; use it to decrypt and monitor limited types of traffic before determining whether or not to allow it on your network.

Rule detail:

Decryption rules: Block or Monitor Certificates and Protocol Versions

The last decryption rules, because they are the most specific and require the most processing, are rules that either monitor or block bad certificates and unsecure protocol versions.

Rule details:

Example: Decryption rule to Monitor or Block Certificate Status

The last decryption rules, because they are the most specific and require the most processing, are rules that either monitor or block bad certificates and unsecure protocol versions. The example in this section shows how to monitor or block traffic by certificate status.

Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. Do not use **Cipher Suite** and **Version** with **Decrypt - Resign** or **Decrypt - Known Key** rule actions. These conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** ( ) next to your decryption policy.

Step 4 Click **Edit** ( ) next to a decryption rule.

Step 5 Click **Add Rule**.

Step 6 n the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 Click **Cert Status**.

Step 8 For each certificate status, you have the following options:

- Click **Yes** to match against the *presence* of that certificate status.
- Click **No** to match against the *absence* of that certificate status.
- Click **Any** to skip the condition when matching the rule. In other words, choosing **Any** means the rule matches whether the certificate status is present or absent.

Step 9 From the **Action** list, click either **Monitor** to only monitor and log traffic that matches the rule or click **Block** or **Block with Reset** to block the traffic and optionally reset the connection.

Step 10 To save changes to the rule, at the bottom of the page, click **Add**.

Step 11 To save changes to the policy, at the top of the page, click **Save**.

Example

The organization trusts the Verified Authority certificate authority. The organization does not trust the Spammer Authority certificate authority. The system administrator uploads the Verified Authority certificate and an intermediate CA certificate issued by Verified Authority to the system. Because Verified Authority revoked a certificate it previously issued, the system administrator uploads the CRL that Verified Authority provided.

The following figure shows a certificate status rule condition checking for valid certificates, those issued by a Verified Authority, are not on the CRL, and still within the Valid From and Valid To date. Because of the configuration, traffic encrypted with these certificates is not decrypted and inspected with access control.

The following figure shows a certificate status rule condition checking for the absence of a status. In this case, because of the configuration, it matches against traffic encrypted with a certificate that has not expired.

In the following example, traffic would match this rule condition if the incoming traffic is using a certificate that has an invalid issuer, is self-signed, expired, and it is an invalid certificate.

The following graphic illustrates a certificate status rule condition that matches if the SNI of the request matches the server name or if the CRL is not valid.

Example: Decryption rule to Monitor or Block Protocol Versions

This example shows how to block TLS and SSL protocols on your network that are no longer considered secure, such as TLS 1.0, TLS 1.1, and SSLv3. It's included to give you a little more detail about how protocol version rules work.

You should exclude nonsecure protocols from your network because they are all exploitable. In this example:

- You can block some protocols using **Version** page on the decryption rule.

- Because the system considers SSLv2 as undecryptable, you can block it using the **Undecryptable Actions** on the decryption policy.
- Similarly, because compressed TLS/SSL is not supported, you should block it as well.

Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. Do not use **Cipher Suite** and **Version** with **Decrypt - Resign** or **Decrypt - Known Key** rule actions. These conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** (✎) next to your decryption policy.

Step 4 Click **Edit** (✎) next to a decryption rule.

Step 5 Click **Add Rule**.

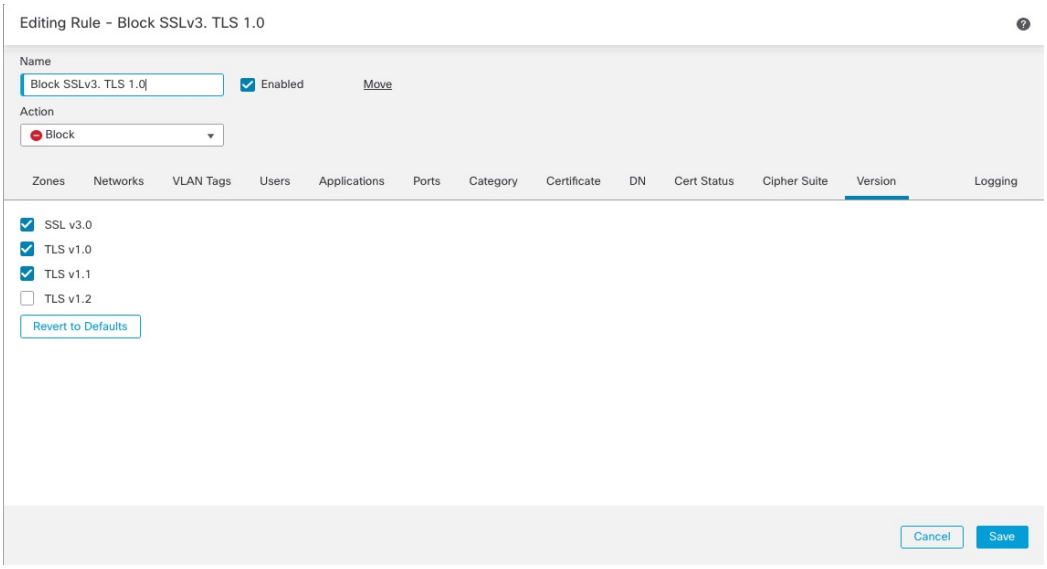
Step 6 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 From the **Action** list, click **Block** or **Block with reset**.

Step 8 Click **Version** page.

Step 9 Check the check boxes for protocols that are no longer secure, such as **SSL v3.0**, **TLS 1.0**, and **TLS 1.1**. Clear the check boxes for any protocols that are still considered secure.

The following figure shows an example.



Step 10 Choose other rule conditions as needed.

Step 11 Click **Add**.

Optional Example: Manual Decryption rule to Monitor or Block Certificate Distinguished Name

This rule is included to give you an idea about how to monitor or block traffic based on the server certificate's distinguishedname. It's included to give you a little more detail.

The distinguished name can consist of country code, common name, organization, and organizational unit, but typically consists of a common name only. For example, the common name in the certificate for `https://www.cisco.com` is `cisco.com`. (However, it's not always this simple; Conditions for distinguished name rules in decryption policies, on page 1765 shows how to find common names.)

The host name portion of the URL in the client request is the Server Name Indication (SNI). The client specifies which hostname they want to connect to (for example, `auth.amp.cisco.com`) using the SNI extension in the TLS handshake. The server then selects the corresponding private key and certificate chain that are required to establish the connection while hosting all certificates on a single IP address.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** ( ) next to your decryption policy.

Step 4 Click **Edit** ( ) next to a decryption rule.

Step 5 Click **Add Rule**.

Step 6 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 From the **Action** list, click **Block** or **Block with reset**.

Step 8 Click **DN**.

Step 9 Find the distinguished names you want to add from the **Available DNs**, as follows:

- To add a distinguished name object on the fly, which you can then add to the condition, click **Add** ( ) above the **Available DNs** list.
- To search for distinguished name objects and groups to add, click the **Search by name or value** prompt above the **Available DNs** list, then type either the name of the object, or a value in the object. The list updates as you type to display matching objects.

Step 10 To select an object, click it. To select all objects, right-click and then **Select All**.

Step 11 Click **Add to Subject** or **Add to Issuer**.

Tip You can also drag and drop selected objects.

Step 12 Add any literal common names or distinguished names that you want to specify manually. Click the **Enter DN or CN** prompt below the **Subject DNs** or **Issuer DNs** list; then type a common name or distinguished name and click **Add**.

Although you can add a CN or DN to either list, it's more common to add them to the **Subject DNs** list.

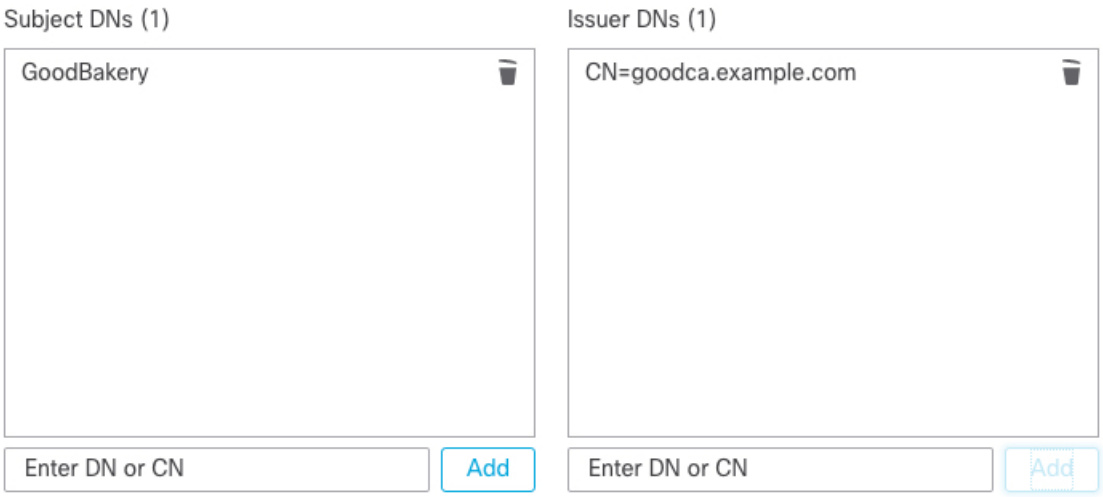
Step 13 Add or continue editing the rule.

Step 14 When you're done, to save changes to the rule, click **Add** at the bottom of the page.

Step 15 To save changes to the policy, click **Save** at the top of the page.

Example

The following figure shows a distinguished name rule condition searching for certificates issued to goodbakery.example.com or issued by goodca.example.com. Traffic encrypted with these certificates is allowed, subject to access control.



Associate the Decryption policy with an Access Control Policy and Advanced Settings

This task discusses how to associate the decryption policy with an access control policy and setting recommended advanced settings for the access control policy.

For your decryption policy to be used by the system, you *must* associate it with an access control policy.

Before you begin

Create the sample decryption policy as discussed in this guide.

For more information about decryption policy advanced options, see Decryption policy advanced options, on page 1742.

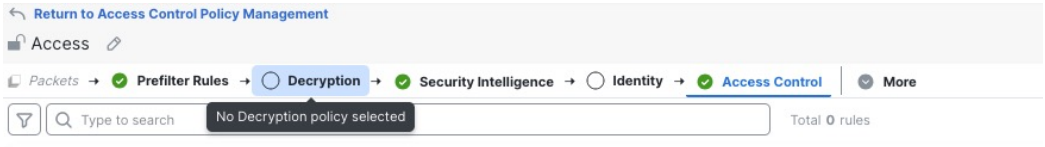
Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

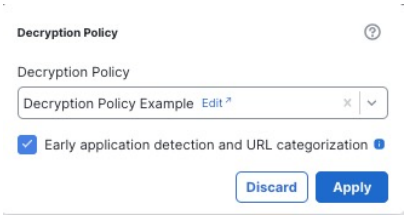
Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

Step 3 Either create a new access control policy or click **Edit** (✎) to edit an existing one.

Step 4 Click the word Decryption as the following figure shows.

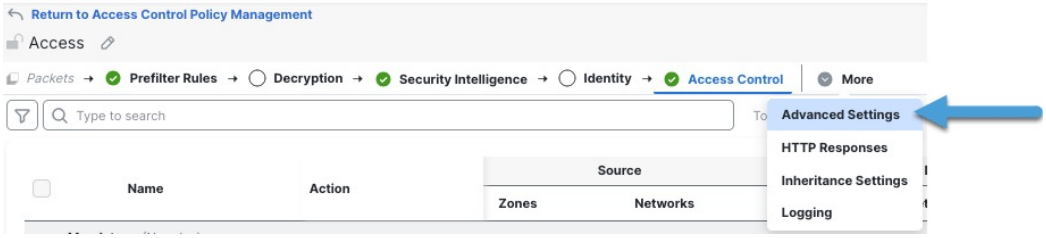


Step 5 From the list, click the name of your decryption policy and also check **Early application detection and URL categorization** as the following figure shows.



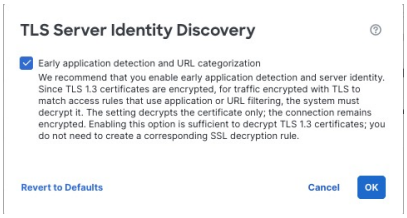
Step 6 Click **Apply**.

Step 7 Click **More** > **Advanced Settings** as the following figure shows.



Step 8 Click **Edit** (✎) next to **TLS Server Identity Discovery**.

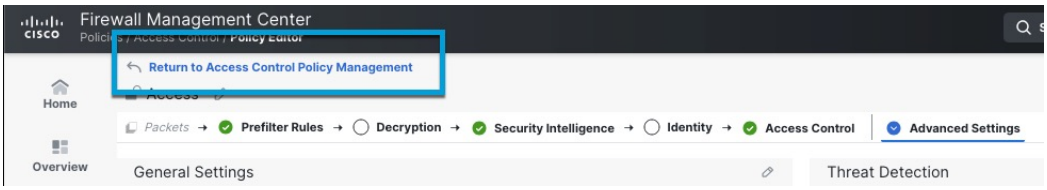
Step 9 Select the check box as the following figure shows.



Step 10 Click **OK**.

Step 11 At the top of the page, click **Save**.

Step 12 At the top of the page, click **Return to Access Control Policy Management**, as the following figure shows



Step 13 Click **Edit** ( ) to edit the access control rule.

Step 14 At the bottom of the page, next to the default action, click (Default Logging and Inspection).

Step 15 Check **Log at beginning of connection** and any other options you choose.

For more information, see Logging settings for access control policies, on page 1584Logging Settings for Access Control Policies in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 16 Click **Apply**.

Step 17 At the top of the page, click **Save**.

What to do next

- Add rule conditions: Decryption Rule conditions, on page 1758.
- Add a default policy action: Decryption policy default actions, on page 1739.
- Configure logging options for the default action as described in *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* .
- Set advanced policy properties: Decryption policy advanced options, on page 1742.
- Associate the decryption policy with an access control policy as described in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Traffic to Prefilter

Prefiltering is the first phase of access control, before the system performs more resource-intensive evaluation. Prefiltering is simple, fast, and early compared to subsequent evaluation, which uses inner headers and has more robust inspection capabilities.

Based on your security needs and traffic profile, you should consider prefiltering and therefore excluding from any policy and inspection the following:

- Common intraoffice applications such as Microsoft Outlook 365
- Elephant flows, such as server backups

Decryption rule Settings

How to configure recommended best practice settings for your decryption rules.

Decryption rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)

Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **Edit** ( ) next to your decryption policy.

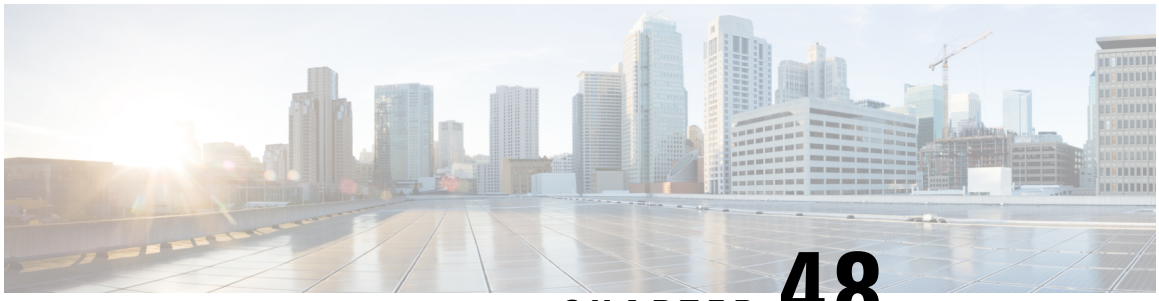
Step 4 Click **Edit** ( ) next to a decryption rule.

Step 5 Click the **Logging** tab.

Step 6 Click **Log at End of Connection**.

Step 7 Click **Save**.

Step 8 Click **Save** at the top of the page.



CHAPTER 48

Encrypted Visibility Engine

Encrypted Visibility Engine (EVE) is used to identify client applications and processes utilizing Transport Layer Security (TLS) encryption. It enables visibility and allows administrators to take actions and enforce policy within their environments. The EVE technology can also be used to identify and stop malware.

- Encrypted Visibility Engine, on page 1803
- How EVE works, on page 1804
- Indications of compromise events, on page 1805
- QUIC fingerprinting in EVE, on page 1806
- Configure EVE, on page 1806
- Configure EVE Exception Rules, on page 1809
- Use case - Block Traffic Based on the EVE Threat Confidence Score, on page 1810

Encrypted Visibility Engine

The encrypted visibility engine (EVE) is used to provide more visibility into the encrypted sessions without the need to decrypt them. These insights into encrypted sessions are obtained by Cisco's open-source library that is packaged in Cisco's vulnerability database (VDB). The library fingerprints and analyzes incoming encrypted sessions and matches it against a set of known fingerprints. This database of known fingerprints is also available in the Cisco VDB.

Key capabilities

Important features of Encrypted Visibility Engine (EVE) include the following:

- Access control policy actions on traffic using information derived from EVE
- Vulnerability Database (VDB) integration with Cisco Secure Firewall for assigning applications to EVE-detected processes with high confidence values
- Custom application detector creation for mapping EVE-detected processes to user-defined applications and overriding built-in process confidence values
- Detection of the operating system type and version of clients that create Client Hello packets in encrypted traffic
- Quick UDP Internet Connections (QUIC) traffic fingerprinting and analysis with server name display in the URL field of the **Connection Events** page

For custom application detector configuration, see the **Configuring Custom Application Detectors** and **Specifying EVE Process Assignments** sections in the **Application Detection** chapter of the Cisco Secure Firewall Management Center Device Configuration Guide.

Note The encrypted visibility engine feature is supported only on Firewall Management Center-managed devices running Snort 3. This feature is not supported on Snort 2 devices and Firewall Device Manager-managed devices.

Attention To use EVE on Firewall Management Center, you must have a valid IPS license on your device. In the absence of a IPS license, the policy displays a warning and deployment is not allowed.

Note

- EVE can detect the operating system type and version of SSL sessions. Normal usage of the operating system, such as running applications and package management software, can trigger OS detection. To view client OS detection, in addition to enabling the EVE toggle button, you must enable **Hosts** under **Policies** > **Network Discovery**. To view a list of possible operating systems on the host IP address, click **Analysis** > **Hosts heading** > **Network Map**, and then choose the required host.
- After enabling EVE for your access control policy, ensure that you have turned on logging for the access control rules within that policy to display the expected results on the EVE dashboard whenever any specific rule conditions are met. For more information on how to turn on logging, see Create and Edit Access Control Rules.
- EVE will not provide visibility or insights for encapsulated traffic.

How EVE works

Encrypted Visibility Engine (EVE) provides the ability to identify and control applications without enabling TLS decryption. By using fingerprints of known malicious processes, EVE technology can also be used to identify and block encrypted malicious traffic without outbound decryption.

Summary

The key components involved in how EVE works are:

- Client Hello inspection: EVE examines the initial TLS handshake packet to create client fingerprints
- Fingerprint database: Contains over 5,000 identified client processes mapped to applications
- Machine learning technology: Processes over one billion TLS fingerprints and over 10,000 malware samples daily
- Cisco Vulnerability Database (VDB): Delivers updated fingerprints to customers

Workflow

These stages describe how EVE identifies and processes client applications:

1. EVE inspects the Client Hello portion of the TLS handshake to identify client processes. The Client Hello is the initial data packet that is sent to the server. This gives a good indication of the client process on the host.
2. The system combines the fingerprint with other data such as destination IP address to provide the basis for EVE's application identification. By identifying specific application fingerprints during the TLS session establishment, the system can identify the client process and take appropriate action, such as allowing or blocking it.
3. If EVE does not recognize a fingerprint, it identifies the client application and estimates the threat score of the first flow using the destination details, such as IP address, port, and server name. At this point, the status of the fingerprints are randomized and the status can be viewed in the debug logs. For subsequent flows with the same fingerprint, EVE skips reanalysis and marks the fingerprint status as unlabeled. If you intend to block traffic based on EVE's Low or Very Low score thresholds, the initial flow is blocked. Future flows are allowed once the application's fingerprint is cached.
4. Through machine learning (ML) technology, Cisco processes over one billion TLS fingerprints and over 10000 malware samples daily to create and update EVE fingerprints. These updates are then delivered to customers using Cisco Vulnerability Database (VDB) package.

Indications of compromise events

An Indication of Compromise (IoC) event is a security detection mechanism that

- identifies connection events with a very high malware confidence level, as reported by EVE,
- triggers for encrypted sessions generated from a host using a malicious client, and
- provides information such as the IP address, MAC address, operating system information of the malicious host, and timestamp of the suspicious activity.

A session with an Encrypted Visibility Threat Confidence score of 'Very High' as seen in connection events generates an IoC event. You must enable **Hosts** from **Policies** > **Network Discovery**. In the Firewall Management Center, view the IoC event existence from here:

- **Analysis** > **Hosts heading** > **Indications of Compromise**, and then **Analysis** > **Indications of Compromise**.
- **Analysis** > **Hosts heading** > **Network Map** > Choose the host that must be checked.

  You can view the process information of the session that generated the IoC on the **Connection Events** page. Click **Analysis** > **Connections** > **Events** to access the **Connection Events** page. Note that you must manually select the Encrypted Visibility fields and IoC field from the **Table View of Connection Events** tab.
- Click **Analysis** > **Unified Events** and choose the Encrypted Visibility fields and IoC field from the column picker option.

QUIC fingerprinting in EVE

QUIC fingerprinting in EVE is a Snort identification mechanism that

- detects applications over QUIC without enabling decryption,
- identifies malware without enabling decryption, and
- detects service applications for access control rule assignment based on the service detected over the QUIC protocol.

Configure EVE

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** ( ) next to the access control policy you want to edit.

Step 3 Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 Click **Edit** ( ) next to **Encrypted Visibility Engine**.

Step 5 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 6 **Use EVE for Application Detection**—This toggle button is enabled by default, which means that EVE is allowed to assign client applications to processes.

EVE's fingerprint information is added in the **Encrypted Visibility Fingerprint** column header of the connection events or unified events. For further analysis of the EVE data collected, you can right-click the fingerprint information to open a dropdown menu. In the menu, click **View Encrypted Visibility Engine Process Analysis** to go to the Secure Firewall Application Detectors site and view details, such as the fingerprint, VDB version, and so on. Different rows with the same fingerprint string and potential process names associated with them and their prevalence are displayed. Prevalence indicates the frequency of a process associated with a particular fingerprint in the data collection system. You can choose the process names and click **Submit Request** to give feedback about any discrepancy in EVE's process detection. For example, you can submit requests if the process name that is detected does not match with the traffic that is being sent or if the process name is not detected at all for a particular fingerprint.

Access to view additional details on the Secure Firewall Application Detectors page is currently not available to users with non-Cisco email addresses.

If you disable the **Use EVE for Application Detection** toggle button:

- AppID-identified clients are assigned to processes and you can see the EVE process and score, but there is no mapping of EVE-detected processes to applications and no action is taken. You can see the details of the events under **Connection Events** or **Unified Events**. To see the difference in connection events (with and without application assignment), see the **Client Application** column header.
- The **Encrypted Visibility Fingerprint** field in the connection events or unified events is empty.

Step 7 Enable the **Block Malware Processes Based on Threat Confidence Level** toggle button to block malicious client processes with the prefix *malware_* based on EVE's threat confidence level.

The default block threshold is 99 percent, which means:

- If EVE detects the traffic to be malware with 99 percent confidence or more, the traffic is blocked.
- If EVE detects the traffic to be malware with less than 99 percent confidence, EVE takes no action.

Note If EVE has blocked the traffic, the **Reason** column header on the **Connection Events** page displays **Encrypted Visiblity Block**.

Step 8 Use the slider to adjust the threshold for blocking based on EVE's threat confidence, which ranges from **Very Low** to **Very High**.

Step 9 For further granular control, enable the **Advanced Mode** toggle button. Now, you can assign a specific EVE Threat Confidence Level for blocking traffic. The default block threshold is 99 percent.

Caution We recommend that you do not set a threshold below 50 percent to ensure optimal performance.

Step 10 Click **OK**.

Step 11 Click **Save**.

What to do next

Deploy configuration changes.

View Encrypted Visibility Engine events

This task allows you to access and view connection events generated by the Encrypted Visibility Engine (EVE) in the Firewall Management Center.

After enabling the **Encrypted Visibility Engine** and deploying your access control policy, you can start sending live traffic through your system. You can view the logged connection events in the **Unified Events** page.

Perform this procedure to access the connection events in the Firewall Management Center.

Procedure

Step 1 Click **Analysis** > **Unified Events**.

Additionally, you can use the **Security-Related Connection Events** page (**Analysis** > **Connections** > **Security-Related Events**) to view the connections that are blocked by Encrypted Visibility Engine, as well as malicious connections with medium, high, and very high threat confidence levels.

The Encrypted Visibility Engine can identify the client process that initiated a connection and the operating system in the client, and indicate if the process contains malware or not.

Step 2 In the **Unified Events** page, explicitly enable these columns that are added for the Encrypted Visibility Engine:

- **Encrypted Visibility Fingerprint**
- **Encrypted Visibility Process Name**
- **Encrypted Visibility Process Confidence Score**
- **Encrypted Visibility Threat Confidence**
- **Encrypted Visibility Threat Confidence Score**
- **Detection Type**

For information about these fields, refer to Connection and Security-Related Connection Event Fields in the *Cisco Secure Firewall Management Center Administration Guide*.

Note On the **Connection Events** page, if processes are assigned applications, the **Detection Type** column displays **Encrypted Visibility Engine**, indicating that the client application was identified by the Encrypted Visibility Engine. Without application assignments to process names, the **Detection Type** column displays **AppID**, indicating that the engine that identified the client application was AppID.

View EVE dashboard

You can use the EVE dashboard to monitor encrypted visibility data, view threat confidence levels, and analyze process identification results across your network.

Before you begin

- In an access control policy, the **Encrypted Visibility Engine (EVE)** must be enabled under **Advanced Settings**.

Follow these steps to view the EVE dashboards:

Procedure

Step 1 Go to **Overview** > **Dashboards heading** > **Dashboard**.

Step 2 In the **Summary Dashboard** window, click the **switch dashboard** link and choose **Application Statistics** from the dropdown box.

Step 3 Choose the **Encrypted Visibility Engine** tab to view the following two dashboards:

- **Top Encrypted Visibility Engine Discovered Processes**—Displays top client processes used in your network and the connection count. Click the process name in the table to view the **Connection Events** page, filtered by the process name.

- **Connections by Encrypted Visibility Engine Threat Confidence**—Displays connections by the confidence levels (Very High, Very Low, and so on). Click the Threat confidence level in the table to view the **Connection Events** page, filtered by the confidence level.

Configure EVE Exception Rules

You can create an encrypted visibility engine (EVE) exception rule to ensure the continuity of trusted connections and services by bypassing the EVE's block action. You can add attributes such as process names and destination IP address to the exception rule. For example, you may want to bypass EVE's block verdict for trusted networks. All the connections in the bypassed networks are exempted from EVE's block verdict based on the threat confidence level.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** ( ) next to the access control policy you want to edit.

Step 3 From the **More** drop-down arrow at the end of the packet flow line, choose **Advanced Settings**.

Step 4 Next to **Encrypted Visibility Engine (EVE)**, click **Edit** ( ).

Step 5 On the **Encrypted Visibility Engine** page, click the **Encrypted Visibility Engine (EVE)** toggle button to enable EVE.

Step 6 Enable the **Block Traffic Based on EVE Score** toggle button to block traffic based on EVE's threat confidence level.

Step 7 Click **Add Exception Rule** and add one or more of the following attributes.

a) Under the **Process Name** tab, enter an EVE-identified process name, and click **Add to Process** on the right side of the window.

You can add multiple process names to the same exception rule. EVE exception list based on process names works only with EVE-identified process names, which are case- and space-sensitive.

b) Under the **Network Objects** tab, perform one of the following:

- Choose one or more IP addresses from the list and add to the **Selected Networks** list.
- Under **Selected Networks**, manually enter the IP address and click the **+** icon to add it to the list of selected networks.

c) (Optional) In the **Comment** field available on all the tabs, you can enter a reason for adding the required attributes to the EVE exception rule.

Step 8 Click **Save** to save the EVE exception rule.

Step 9 Save and deploy the access control policy on the devices.

Note When a connection matches an exception rule, it bypasses the EVE's block verdict. You can view EVE's action in the **Connection Events** or **Unified Events** page. The **Reason** column header displays **EVE Exempted** for identification of such EVE-bypassed traffic.

Add exception rule from unified events

Add exception rules for connections that are blocked by EVE using the information in the Unified Events page.

Use the **Unified Events** page to add exception rules for connections that are blocked by EVE.

Before you begin

Exception list is supported only from threat defense version 7.6.0 or later.

Follow these steps to add exception rules for connections that are blocked by EVE:

Procedure

Step 1 Click **Analysis** > **Unified Events**.

Step 2 In the **Reason** column with **Encrypted Visibility Block** as the reason, click the **Ellipsis**(⋮) icon inside the cell.

Step 3 Choose **Add EVE Exception Rule** from the drop-down list.

Step 4 In the **Encrypted Visibility Engine** window that is displayed, the rule is automatically added to the bottom of the exception list. You can review and make changes to the added rule before saving and deploying the configuration.

Use case - Block Traffic Based on the EVE Threat Confidence Score

About Encrypted Visibility Engine

You can use the Encrypted Visibility Engine (EVE) to identify client applications and processes using Transport Layer Security (TLS) encryption. EVE provides more visibility into the encrypted sessions without decryption. Based on EVE's findings, administrators can enforce policy actions on the traffic within their environments. You can also use the EVE to identify and stop malware.

Benefits

Administrators can leverage and adjust EVE's threat score to block malicious encrypted traffic. If the probability that the incoming traffic is malicious, then based on the threat score, you can configure EVE to block the connection.

Sample Business Scenario

A large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, adoption of robust network security measures is necessary and important. The security team uses EVE to enhance encrypted traffic inspection without the need to implement full man-in-the-middle (MITM) decryption. The EVE technology uses fingerprints of known malicious processes to identify and stop malware. Network administrators must have the flexibility to configure EVE's block traffic thresholds to block potentially malicious connections, which are based on their configured block thresholds.

Prerequisites

- You must be running management center 7.4.0 or later, and the managed threat defense must also be 7.4.0 or later.
- Ensure that you have a valid Intrusion Prevention System (IPS) license and Snort 3 is the detection engine.

High-Level Workflow

1. EVE analyzes the incoming traffic and gives a verdict on the probability of incoming traffic being malware or not.
2. If EVE detects incoming traffic to be malware with a certain level of confidence, you can configure EVE to block that traffic.
3. The packets are first checked for malware probability or threat score, and the threat score is compared with the block threshold that you have set.
4. If the threat score is higher than the configured threshold, EVE blocks the traffic.
5. If the threat score is lesser than the configured threshold, EVE takes no action.

Configure Block Thresholds in EVE

This procedure shows how to block potentially malicious traffic, based on the EVE threat confidence score of 90 percent or higher.

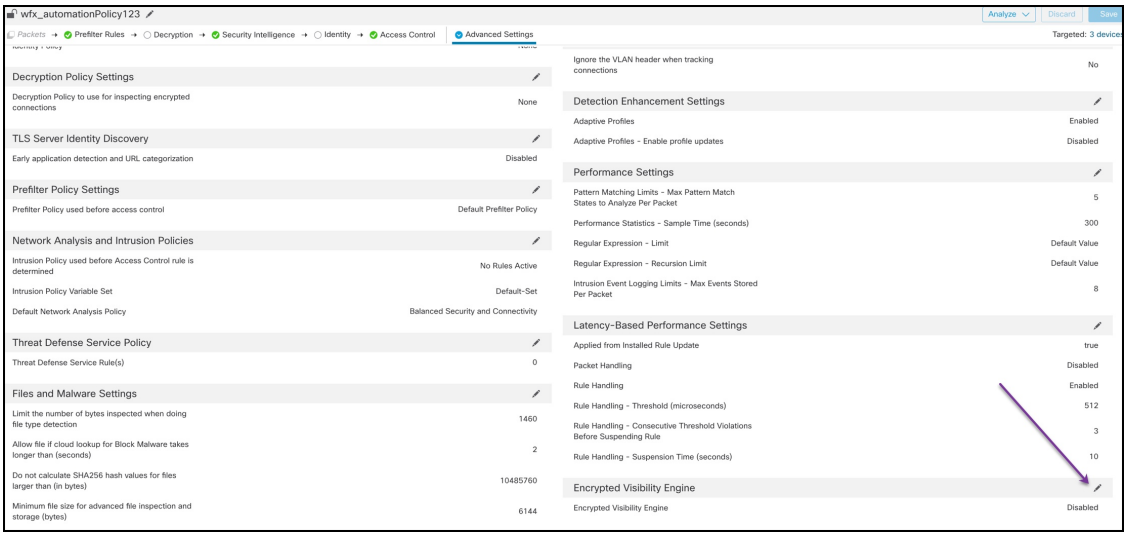
Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

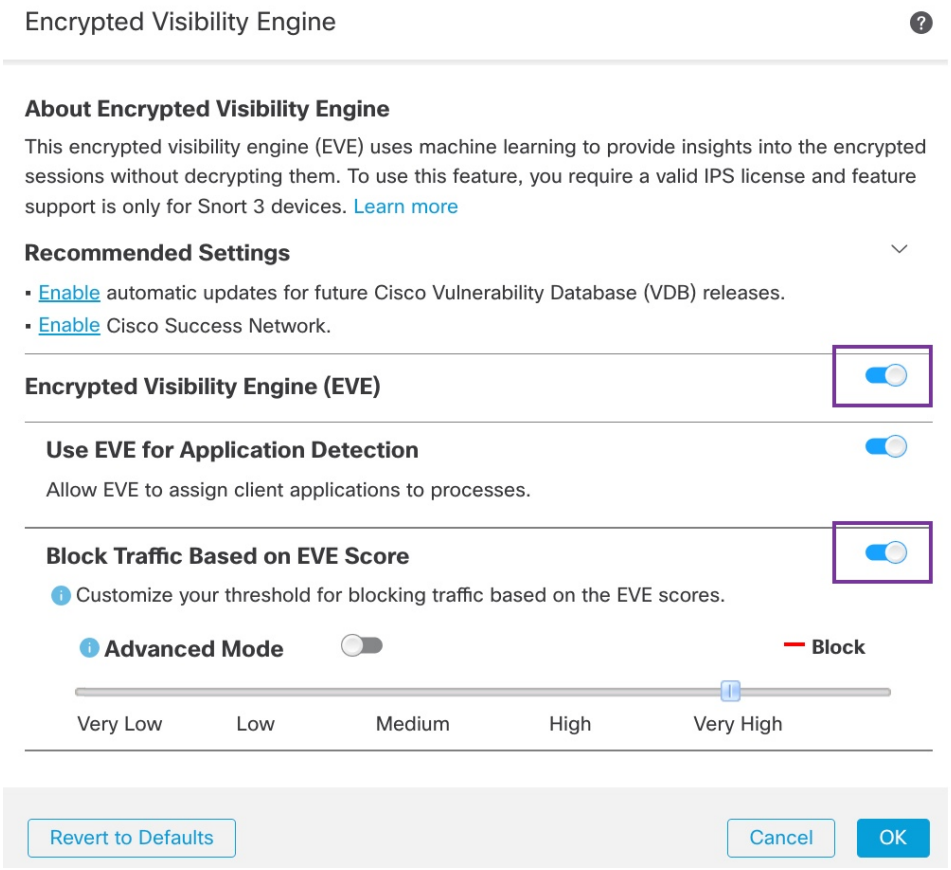
Step 3 Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 Click **Edit** (✎) next to **Encrypted Visibility Engine**.



Step 5 In the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

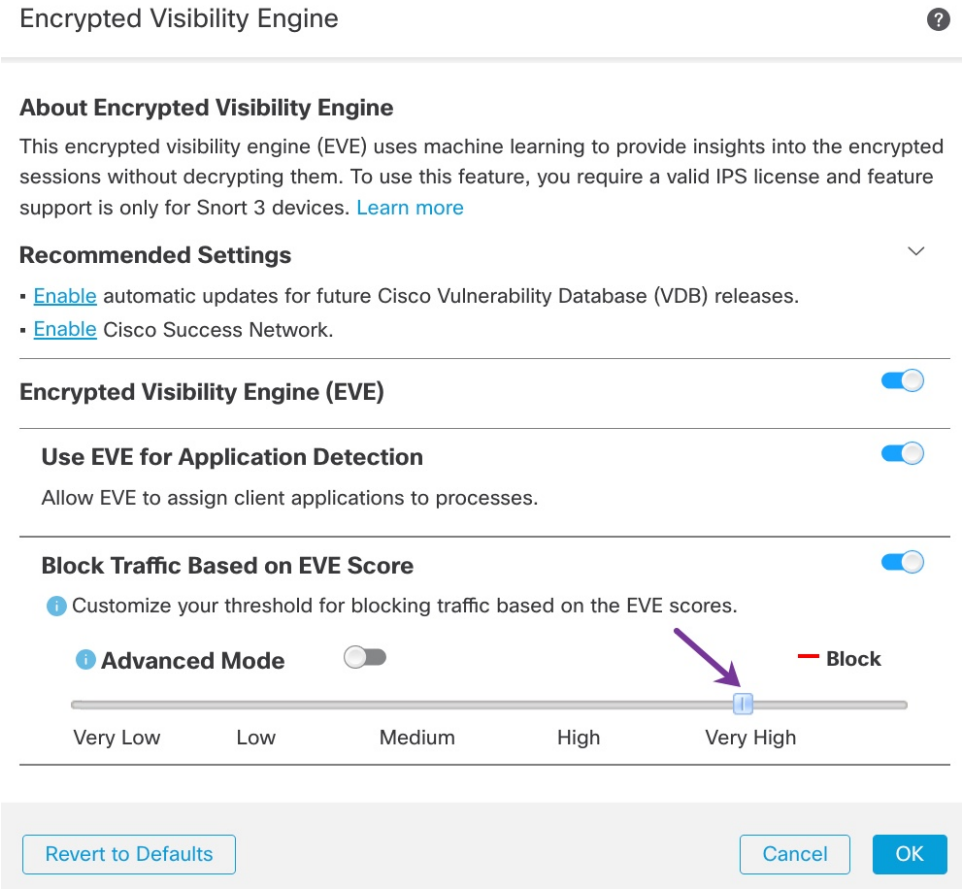
Step 6 Enable the **Block Traffic Based on EVE Score** toggle button. Any incoming traffic that is a potential threat is blocked by default.



Note By default, the threshold at which malware is blocked is 99 percent, which means:

- If EVE detects the traffic to be malware with 99 percent confidence or higher, EVE blocks the traffic.
- If EVE detects the traffic to be malware with less than 99 percent confidence, EVE takes no action.

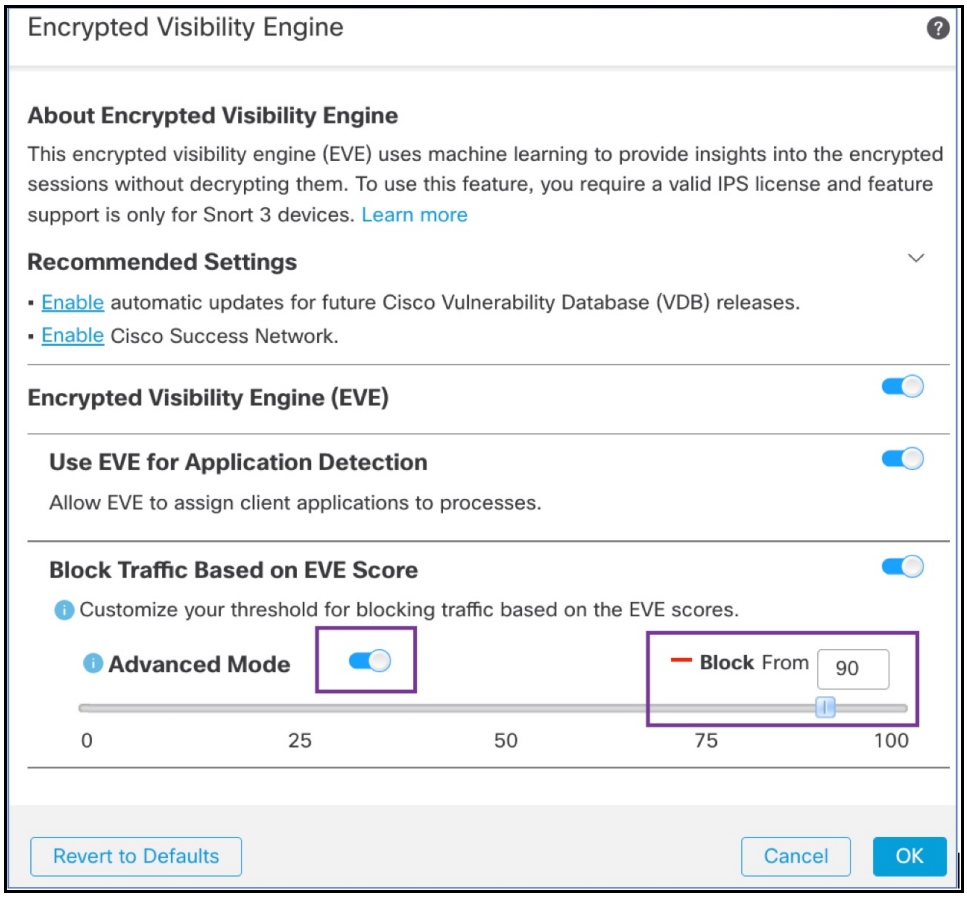
Step 7 Use the slider to adjust the threshold for blocking based on EVE threat confidence. This ranges from **Very Low** to **Very High**. In this example, the slider is set to **Very High**.



Step 8 For further granular control, enable the **Advanced Mode** toggle button. Now, you can assign a specific EVE Threat Confidence Score for blocking traffic. The default threshold is 99 percent.

Step 9 In this example, change the block threshold to **90** percent.

Attention As a best practice, we recommend that you do not set the block threshold to below 50 percent to ensure optimum performance.



Step 10 Click **OK**.

Step 11 Click **Save**.

What to do next

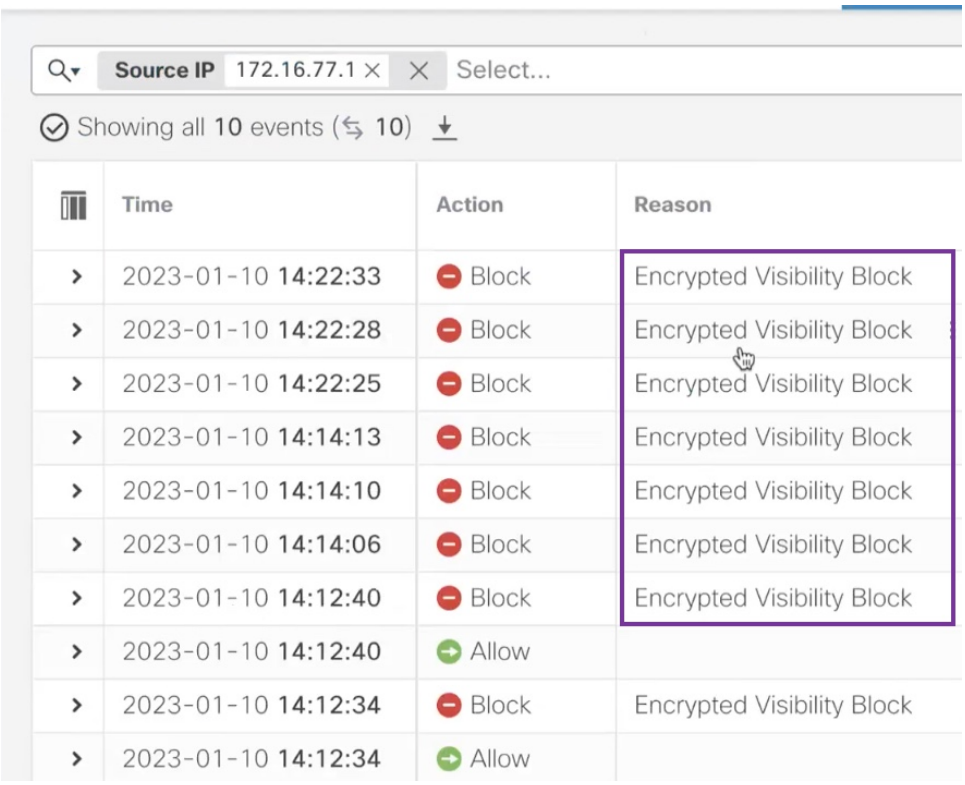
Deploy configuration changes.

View EVE Events

Procedure

Step 1 To verify the block action, choose **Analysis** > **Connections** > **Events**. You can also view the events from the **Unified Events** viewer.

Step 2 If you have configured EVE to block traffic, the **Reason** field shows **Encrypted Visibility Block**.



Step 3 The following is an example of the **Encrypted Visibility Process Name** as **test_malware**, **Encrypted Visibility Threat Confidence** as **Very High**, and **Encrypted Visibility Threat Confidence Score** as **90** percent.



Additional References

For detailed conceptual information, see the Encrypted Visibility Engine for Snort 3 chapter in this guide or the content in the following link:

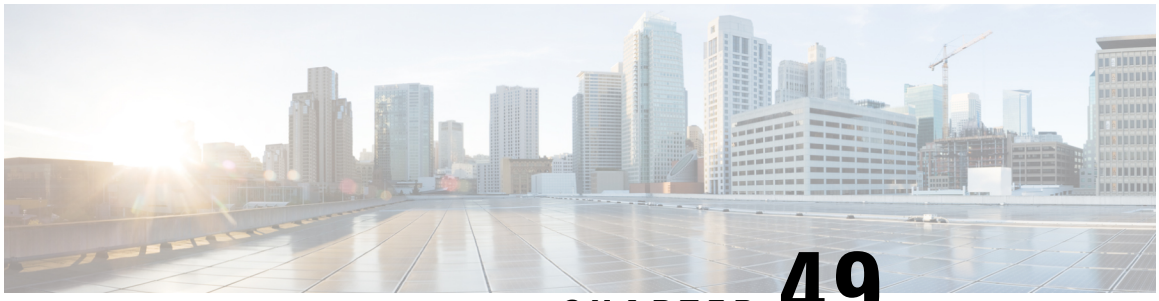
Encrypted Visibility Engine



PART X

Identity Policies for Access Control

- Identity Overview, on page 1819
- Realms, on page 1835
- Identity Source: Captive Portal, on page 1887
- Identity Source: ISE/ISE-PIC, on page 1911
- Identity Source: Remote Access VPN, on page 1931
- Identity source: TS agent, on page 1937
- Identity Policies, on page 1941



CHAPTER 49

Identity Overview

The following topics discuss user identity:

- User identity, on page 1819
- Host and user limits, on page 1830
- Recommendation: identity realm limit, on page 1833
- User limits for microsoft azure active directory realms, on page 1833

User identity

User identity information can help you to identify the source of policy breaches, attacks, or network vulnerabilities, and trace them to specific users.

User identity information can help you determine:

- Who owns the host targeted by an intrusion event that has a Vulnerable (level 1: red) impact level.
- Who initiated an internal attack or portscan.
- Who is attempting unauthorized access to a specified host.
- Who is consuming an unreasonable amount of bandwidth.
- Who has not applied critical operating system updates.
- Who is using instant messaging software or peer-to-peer file-sharing applications in violation of company policy.
- Who is associated with each indication of compromise on your network.

Armed with this information, you can use other features of the system to mitigate risk, perform access control, and take action to protect others from disruption. These capabilities also significantly improve audit controls and enhance regulatory compliance.

After you configure user identity sources to gather user data, you can perform user awareness and user control.

For more information about identity sources, see About user identity sources, on page 1820.

Identity terminology

Identity terminology is a set of concepts that

- identifies users on networks using identity sources
- enables user awareness from authoritative and non-authoritative sources, and
- manages user access using identity policies.

Key identity terminology

This topic discusses common terminology for user identity and user control.

- **User awareness**: Identifying users on your network using *identity sources* (such as, TS Agent, or Cisco ISE). User awareness enables you to identify users from both *authoritative* (such as Active Directory) and *non-authoritative* (application-based) sources. To use Active Directory as an identity source, you must configure a realm and directory. For more information, see About user identity sources, on page 1820.
- **User control**: Configuring an *identity policy* that you associate with an *access control policy*. (The identity policy is then referred to as an access control *subpolicy*.) The identity policy specifies the identity source and, optionally, users and groups belonging to that source. By associating the identity policy with an access control policy, you determine whether to monitor, trust, block, or allow users or user activity in traffic on your network. For more information, see Access Control Policies, on page 1569.
- **Authoritative identity source**: a trusted server that validates user logins (for example, Active Directory). You can use the data obtained from authoritative logins to perform user awareness and user control. Authoritative user logins are obtained from passive and active authentications:
  - *Passive authentications* occur when a user authenticates through an external repository. ISE/ISE-PIC, the TS Agent, Microsoft Active Directory, and Microsoft Azure Active Directory are passive authentication user repositories supported by the system.
  - *Active authentications* occur when a user authenticates through preconfigured managed devices. Captive portal is another name for active authentication. Active authentication generally uses the same user repositories as passive authentication (the exceptions being ISE/ISE-PIC, and TS Agent, which are passive only).
- **Non-authoritative identity source**: an unknown or untrusted server that validates the user login. Traffic-based detection is the only non-authoritative identity source supported by the system. You can use the data obtained from non-authoritative logins to perform user awareness.

About user identity sources

Learn how to select and configure user identity sources for the firewall to enable user awareness and access control policies. This overview covers supported identity sources, authentication types, and key considerations for optimizing user identity management.

The table provides a brief overview of the user identity sources supported by the system. Each identity source provides a store of users for user awareness. These users can then be controlled with identity and access control policies.

User Identity Source	Server Requirements	Login Type	Authentication Type	User Control	For more, see...
Captive portal	OpenLDAP Microsoft Active Directory	Authoritative	Active	Yes	Captive portal identity source, on page 1887
Passive authentication	OpenLDAP Microsoft Active Directory	Non-authoritative	Active	Yes	Create an LDAP realm or an Active Directory realm and realm directory, on page 1860
Passive authentication with the TS Agent	Microsoft Windows Terminal Server	Authoritative	Passive	Yes	Terminal services agent identity source, on page 1937
Remote Access VPN	OpenLDAP or Microsoft Active Directory	Authoritative	Active	Yes	Remote access VPN identity sources, on page 1931
	RADIUS	Authoritative	Active	No, awareness only	
ISE/ISE-PIC	Microsoft Active Directory	Authoritative	Passive	Yes	The ISE/ISE-PIC identity source, on page 1911
Traffic-based detection (Configured in the network discovery policy.)	—	Non-authoritative	—	No, awareness only	Traffic-based detection identity sources, on page 2314

Consider the information when selecting identity sources to deploy:

- You must use traffic-based detection for non-LDAP user logins.
- You must use traffic-based detection or captive portal to record failed login or authentication activity. A failed login or authentication attempt does not add a new user to the list of users in the database.
- The captive portal identity source requires a managed device with a routed interface. You *cannot* use an inline (also referred to as tap mode) interface with captive portal.

Data from those identity sources is stored in the Secure Firewall Management Center's users database and the user activity database. You can configure Secure Firewall Management Center-server user downloads to automatically and regularly download new user data to your databases.

After you configure identity rules using the desired identity source, you must associate each rule with an access control policy and deploy the policy to managed devices for the policy to have any effect. For more information about access control policies and deployment, see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

For general information about user identity, see User identity, on page 1819.

Best practices for user identity

General recommendations for identity policy setup

Review the following recommendations before you set up identity policies.

- Know user limits
- Health monitor
- Use latest version of ISE/ISE-PIC, two types of remediation
- User agent support drops in 6.7
- Captive portal requires routed interface, several individual tasks

Microsoft active directory and LDAP

Create one realm per LDAP server or Active Directory domain. The system supports Active Directory, LDAP, and other user repositories for user awareness and control. The association between an Active Directory or LDAP repository and the Secure Firewall Management Center is referred to as a *realm*. For details about which versions are supported, see Supported servers for realms, on page 1841.

- The only user identity source supported by LDAP is captive portal. To use other identity sources (with the exception of ISE/ISE-PIC), you must use Active Directory.
- For Active Directory only: Create one *directory* per domain controller. For details, see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860
- Users and groups in trust relationships between two domains are supported provided you add all Active Directory domains and domain controllers as realms and directories, respectively. For more information, see Realms and trusted domains, on page 1837.

Passive Identity Agent identity source
pxGrid Cloud Identity Source
Proxy sequence
Health monitor

The Secure Firewall Management Center health monitor provides valuable information about the status of various Secure Firewall Management Center functions, including user/realm mismatches, Snort memory usage, and ISE connection status.

- For more information about health modules, see *Health Modules* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To set up policies to monitor health modules, see *Creating Health Policies* in the *Cisco Secure Firewall Management Center Administration Guide*.

Device-specific user limits

Every physical or virtual Firewall Management Center device has limits to the number of users that can be downloaded. When the user limit is reached, the Firewall Management Center can run out of memory and can function unreliably as a result.

- User limits are discussed in User limits for microsoft active directory, on page 1831.

- If you use the ISE/ISE-PIC identity source, you can optionally limit the subnets the Firewall Management Center monitors to reduce memory usage using identity mapping filters as discussed in Create an identity policy, on page 1943.

Use the latest version of ISE/ISE-PIC

If you expect to use the ISE/ISE-PIC identity source, we strongly recommend you always use the latest version to make sure you get the latest features and bug fixes.

- pxGrid 2.0 (which is used by version 2.6 patch 6 or later; or 2.7 patch 2 or later) also changes the remediation used by ISE/ISE-PIC from Endpoint Protection Service (EPS) to Adaptive Network Control (ANC). If you upgrade ISE/ISE-PIC, you must migrate your mediation policies from EPS to ANC.
- More information about using ISE/ISE-PIC can be found in Best practices for ISE/ISE-PIC integration, on page 1914.
- To set up the ISE/ISE-PIC identity source, see ISE/ISE-PIC configurations for user control , on page 1916.

Captive portal information

Captive portal is the only identity source that supports LDAP in addition to Active Directory. The captive portal identity source is triggered when a user tries to access network resources using the managed device in AWS, using either an IP address or host name. Captive portal gets user information from LDAP or Active Directory using the proxy sequence and sends user information to Secure Firewall Management Center.

- For more information about the captive portal identity source, see Captive portal identity source, on page 1887.

TS agent information

The TS Agent user identity source is required to identify user sessions on a Windows Terminal Server. The TS Agent software must be installed on the Terminal Server machine as discussed in the *Cisco Terminal Services (TS) Agent Guide*. In addition, you must synchronize the time on your TS Agent server with the time on the Secure Firewall Management Center.

- TS Agent data is visible in the Users, User Activity, and Connection Event tables and can be used for user awareness and user control.
- For more information, see Best practices for TS agent configuration, on page 1938.

Associate the identity policy with an access control policy

After you configure your realm, directory, and user identity source, you must set up identity rules in an identity policy. To make the policy effective, you must associate the identity policy with an access control policy.

- For more information about creating an identity policy, see Create an identity policy, on page 1943.
- For more information about creating identity rules, see Create an identity rule, on page 1952.
- To associate an identity policy with an access control policy, see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Identity deployments

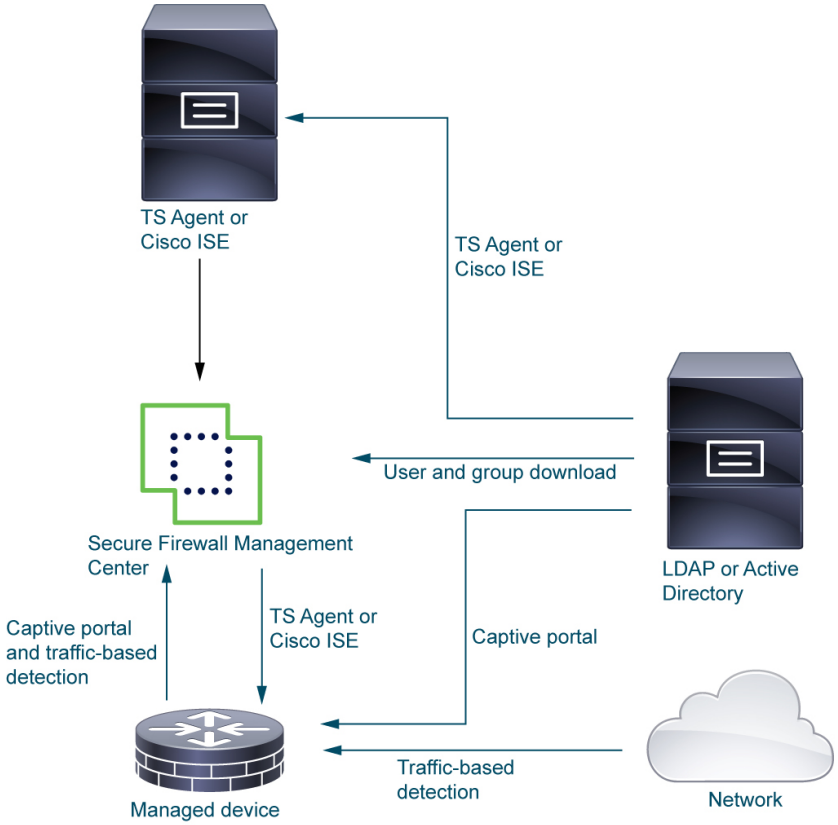
The Secure Firewall Management Center uses various identity sources, such as TS Agent, ISE/ISE-PIC, pxGrid Cloud, passive identity agent, and captive portal, to collect and manage user and group data for access control and user awareness.

User data collection and storage

When the system detects user data from a user login, from any identity source, the user from the login is checked against the list of users in the Secure Firewall Management Center user database. If the login user matches an existing user, the data from the login is assigned to the user. Logins that do not match existing users cause a new user to be created, unless the login is in SMTP traffic. Non-matching logins in SMTP traffic are discarded.

The group to which the user belongs is associated with the user as soon as the user is seen by the Secure Firewall Management Center.

This diagram illustrates how the system collects and stores user data:



Here are examples of identity deployments.

In the preceding figure, Secure Firewall Management Center and one managed device are deployed to AWS and the other devices are located on premises. These devices can be either physical or virtual; they just need to be able to communicate with each other.

LDAP or Active Directory are required only for TS Agent and captive portal, as the following paragraphs explain.

For more information about setting up a system like this, see Set up an identity policy, on page 1825.

ISE/ISE-PIC identity source

When you deploy the ISE/ISE-PIC identity source, the ISE/ISE-PIC server sends users, groups, and subscriptions to the Secure Firewall Management Center.

You can optionally have an LDAP server in an ISE/ISE-PIC deployment but because it's optional, it isn't shown in this figure.

For more information about ISE/ISE-PIC, see The ISE/ISE-PIC identity source, on page 1911.

TS Agent identity source

The Terminal Services (TS) Agent software runs on a Microsoft Server and sends Secure Firewall Management Center user information based on the port range the users log in to the server with. TS Agent gets user identity information from LDAP or Active Directory and sends it to Secure Firewall Management Center.

For more information about the TS Agent identity source, see Terminal services agent identity source, on page 1937.

Captive portal

Captive portal is the only identity source that supports LDAP in addition to Active Directory. The captive portal identity source is triggered when a user tries to access network resources using the managed device in AWS—using either an IP address or host name. Captive portal gets user information from LDAP or Active Directory using the proxy sequence and sends user information to Secure Firewall Management Center.

For more information about the captive portal identity source, see Captive portal identity source, on page 1887.

Set up an identity policy

Set up an identity policy to control user access and filter network traffic using various user identity sources such as TS Agent, ISE/ISE-PIC, captive portal.

An identity policy is not required if all these conditions are true:

- You use the ISE or ISE-PIC identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies.

This topic provides a high-level overview of setting up an identity policy using any available user identity source: TS Agent, ISE/ISE-PIC, captive portal.

Procedure

	Command or Action	Purpose
Step 1	(Optional.) Create a realm and directory, one realm for every domain in the forest that contain users you want to use in user control. Also	Creating a realm, realm directory is optional if any of these are true:

	Command or Action	Purpose
	create one directory for every domain controller. Only users and groups that have corresponding Firewall Management Center realms and directories can be used in identity policies.	• You use SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions. • You are using an identity policy only to filter network traffic. The *realm* is a trusted user and group store, typically a Microsoft Active Directory repository. The Firewall Management Center downloads users and groups at intervals you specify. You can include or exclude users and groups from being downloaded. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860. For details about the options to create a realm, see Realm fields, on page 1844. A *directory* is an Active Directory domain controller that organizes information about a computer network's users and network shares. An Active Directory controller provides Directory Services for the realm. Active Directory distributes user and group objects across multiple domain controllers, which are peers that propagate local changes between each other by the use of Directory Services. For more information, see the Active Directory technical specification glossary on MSDN. You can specify more than one directory for a realm, in which case each domain controller is queried in the order listed on the realm's **Directory** tab page to match user and group credentials for user control. **Note** Configuring a realm or realm se not user, group, realm, Endpoint
Step 2	Synchronize users and groups from the realm.	To be able to control users and groups, you must synchronize them with the Firewall Management Center. You can synchronize them with users and groups whenever you want or you can configure the system to synchronize them at a specified interval. When you synchronize users and groups, you can specify exceptions; for example, you can exclude the Engineering group from all user

	Command or Action	Purpose
		control for that realm, or you can exclude the user `joe.smith` from user controls that apply to the Engineering group. See Synchronize users and groups, on page 1865
Step 3	(Optional.) Create a realm sequence.	A realm sequence is an ordered list of realms that, when used in an identity policy, causes the system to search the realms in the specified order to find users to match the rule. See Create a realm sequence, on page 1867.
Step 4	Create a method to retrieve user and group data (the *identity source*).	Set up an identity source with its unique configuration to be able to control users and groups using data stored in the realm. Identity sources include TS Agent, captive portal, or Remote VPN. See one of these: • Configure the captive portal for user control, on page 1891 • Configure Remote Access VPN for AD-authenticated users, on page 1932
Step 5	Create an identity policy.	An identity policy contains one or more identity rules, optionally organized in categories. See Create an identity policy, on page 1943. **Note** Configuring a realm or realm not user, group, realm, Endp only to filter network traffic.
Step 6	Create one or more identity rules.	Identity rules enable you to specify a number of matching criteria, including the type of authentication, network zones, networks or geolocation, realms, realm sequences, and so on. See Create an identity rule, on page 1952.
Step 7	Associate your identity policy with an access control policy.	An access control policy filters and optionally inspects traffic. An identity policy must be associated with an access control policy to have any effect. See Associate prefilter, decryption, and identity policies with an access control, on page 1585.

What to do next

1. Deploy the access control policy to at least one managed device.

To use your policy to control user activity, the policy must be deployed to the managed devices to which clients connect. See Deploy configuration changes, on page 135.

2. Monitor user activity.

   View a list of active sessions collected by user identity sources or a list of user information collected by user identity sources. See *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide* .

User activity database

The user activity database on the Secure Firewall Management Center is a logging system that contains records of user activity on your network detected or reported by all of your configured identity sources.

User activity logging events

The system logs events in these circumstances:

- When it detects individual logins or logoffs.
- When it detects a new user.
- When a system administrator manually delete a user.
- When the system detects a user that is not in the database, but cannot add the user because you have reached your user limit.
- When you resolve an indication of compromise associated with a user, or enable or disable indication of compromise rules for a user.

Note If the TS Agent monitors the same users as another passive authentication identity source (such as the ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive source report identical activity from the same IP address, only the TS Agent data is logged to the Firewall Management Center.

You can view user activity detected by the system using the Secure Firewall Management Center. (**Analysis** > **Users heading** > **User Activity**.)

Users database

A users database on the Secure Firewall Management Center is a system component that

- contains a record for each user detected or reported by all configured identity sources
- stores data obtained from authoritative sources for user control, and
- prioritizes user data based on identity source type when user limits are reached.

User database management and limitations

For more information about the supported non-authoritative and authoritative identity sources, refer to About user identity sources, on page 1820.

The total number of users the Secure Firewall Management Center can store depends on the Secure Firewall Management Center model, as described in User limits for microsoft active directory, on page 1831. After the user limit is reached, the system prioritizes previously-undetected user data based on its identity source, as described in this list:

- Non-authoritative identity source: If the new user is from a non-authoritative identity source, the system does not add the user to the database. To allow new users to be added, you must delete users manually or with a database purge.
- Authoritative identity source: If the new user is from an authoritative identity source, the system deletes the non-authoritative user who has remained inactive for the longest period and adds the new user to the database.

If an identity source is configured to exclude specific user names, user activity data for those user names are not reported to the Secure Firewall Management Center. These excluded user names remain in the database, but are not associated with IP addresses. For more information about the type of data stored by the system, refer to *User Data* in the *Cisco Secure Firewall Management Center Administration Guide*.

If you have Firewall Management Center high availability configured and the primary fails, no logins reported by a captive portal, ISE/ISE-PIC, TS Agent, or Remote Access VPN device can be identified during failover downtime, even if the users were previously seen and downloaded to the Firewall Management Center. The unidentified users are logged as Unknown users on the Firewall Management Center. After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.

Note If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive source report identical activity from the same IP address, only the TS Agent data is logged to the Firewall Management Center.

When the system detects a new user session, the user session data remains in the users database until one of these conditions occurs:

- A user on the Firewall Management Center manually deletes the user session.
- An identity source reports the logoff of that user session.
- A realm ends the user session as specified by the realm's **User Session Timeout: Authenticated Users**, **User Session Timeout: Failed Authentication Users**, or **User Session Timeout: Guest Users** setting.

Note In deployments that use multitenancy with Firewall Management Center domains, passive identity sessions apply to all managed Firewall Threat Defense devices, regardless of domain.

Host and user limits

Host and user limits are deployment restrictions that determine how many individual hosts you can monitor with your deployment, as well as how many users you can monitor and use to perform user control.

Host limits

The system adds a host to the network map when it detects activity associated with an IP address in your monitored network (as defined in your network discovery policy). The number of hosts a Secure Firewall Management Center can monitor, and therefore store in the network map, depends on its model.

Table 104: Host Limits by Secure Firewall Management Center Model

Firewall Management Center Model	Hosts
MC1600	50,000
MC1700	50,000
MC2600	150,000
MC2700	150,000
MC4600	600,000
MC4700	600,000
virtual	50,000

You cannot view contextual data for hosts not in the network map. However, you can perform access control. For example, you can perform application control on traffic to and from a host not in the network map, even though you cannot use a compliance allow list to monitor the host's network compliance.

Note The system counts MAC-only hosts separately from hosts identified by both IP addresses and MAC addresses. All IP addresses associated with a host are counted together as one host.

Reaching the host limit and deleting hosts

The network discovery policy controls what happens when you detect a new host after reaching the host limit. You can drop the new host, or replace the host that has been inactive for the longest time. You can also set the period after which the system removes a host from the network map due to inactivity. Although you can manually delete a host, an entire subnet, or all of your hosts from the network map, if the system detects activity associated with a deleted host, it re-adds the host.

User limits for microsoft active directory

User limits impact monitoring and login capacity in Secure Firewall Management Center and Secure Firewall Threat Defense models for Microsoft Active Directory realms. These limits include maximum downloaded users and concurrent session limits. User prioritization, session management, and troubleshooting information help manage user database constraints.

About user limits

Your Firewall Management Center model determines how many individual users you can monitor. The user is added to the Firewall Management Center user database when:

- The user is downloaded from a realm.
- A captive portal or RA-VPN user logs in.
- A user is detected from any identity source (for example, TS Agent).

Only authoritative users are available for user control with access control policies.

Note the following:

- The maximum number of *downloaded* users depends on your Firewall Management Center model.
- The maximum number of *concurrent* user sessions (that is, logins) depends on your managed device model. A single user can have multiple sessions from different unique IP addresses.



Note The system downloads all user sessions to all Firewall Threat Defense devices. If you have devices with different user concurrent user session limits, the Firewall Threat Defense with the smallest limit reports health warnings when its memory reaches the configured limit. (For example, if your Firewall Management Center manages a Firepower 2110 and a 4125, the 2110 reports health warnings when the number of concurrent user sessions approaches its maximum of 64,000.)

User limits for microsoft active directory

Table 105: Maximum Concurrent User Login Limits by Firewall Threat Defense

Firewall Threat Defense Model	Maximum Concurrent User Logins per Realm
Firewall Threat Defense Virtual 5, 10, 20, 30, 50 (any supported hypervisor)	64,000
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130 Secure Firewall 3105, 3110, 3120	64,000

Firewall Threat Defense Model	Maximum Concurrent User Logins per Realm
Firepower 2140 Secure Firewall 3130, 3140 Firepower 4112, 4115, 4125	150,000
Firepower 4145 Firepower 9300	300,000
Secure Firewall 4215	300,000
Secure Firewall 4225, 4245, 4250	315,000

User limits are applied per Microsoft Active Directory realm. That is, if you attempt to download more than the maximum users in a *single* realm, the download stops after that many users and a health alert is displayed. If, however, you attempt to download more than the maximum number of users spread across *different* realms, the download succeeds (unless any one realm has more than 150,000 users, in which case the download fails for that realm).

Table 106: Maximum Downloaded Users by Firewall Management Center Model

Firewall Management Center Model	Maximum Downloaded Users
FMC 1600	50,000
FMC 1700	50,000
FMC 2600	150,000
FMC 2700	150,000
FMC 2800	150,000
FMC 4600	600,000
FMC 4700	600,000
Firewall Management Center Virtual (any supported hypervisor)	50,000
Firewall Management Center Virtual 300 (any supported hypervisor)	150,000

When the system detects a new, previously-undetected user after the limit has been reached, it prioritizes user data based on their identity source:

- If the new user is from a non-authoritative source, the system does not add the non-authoritative user to the database. To allow new users to be added, you must delete users manually or purge the database.
- If the new user is from an authoritative identity source, the system deletes the non-authoritative user who has remained inactive for the longest period and adds the new authoritative user to the database.

  If there are only authoritative users, the system deletes the authoritative user who has remained inactive for the longest period of time and adds the new user to the database.

Troubleshooting information can be found in Troubleshoot user control, on page 1962.

Tip Note that if you are using traffic-based detection, you can restrict user logging by protocol to help minimize username clutter and preserve space in the database. For example, you could prevent the system from adding users discovered in AIM, POP3, and IMAP traffic because you know it is traffic from specific contractors or visitors you do not want to monitor.

Recommendation: identity realm limit

We limit you to a maximum of 25 realms regardless of Firewall Threat Defense model; the same limit applies to the Cloud-Delivered Firewall Management Center.

The number of *users* you can download to a system is limited according to the information provided in:

User limits for microsoft active directory, on page 1831

User limits for microsoft azure active directory realms

This reference provides user limit information for Microsoft Azure Active Directory realms, showing how different device models handle user monitoring and login capacity.

Microsoft azure active directory user limits

About user limits

Your Firewall Management Center model determines how many individual users you can monitor.

Note the following:

- The maximum number of *downloaded* users depends on your Firewall Management Center model.
- The maximum number of *concurrent* user sessions (that is, logins) depends on your managed device model. A single user can have multiple sessions from different unique IP addresses.

Note The system downloads all user sessions to all Firewall Threat Defense devices. If you have devices with different user concurrent user session limits, the Firewall Threat Defense with the smallest limit reports health warnings when its memory reaches the configured limit. (For example, if your Firewall Management Center manages a Firepower 2110 and a 4125, the 2110 reports health warnings when the number of concurrent user sessions approaches its maximum of 64,000.)

Refer to these tables.

Table 107: Maximum Downloaded Users by Firewall Management Center Model[1]

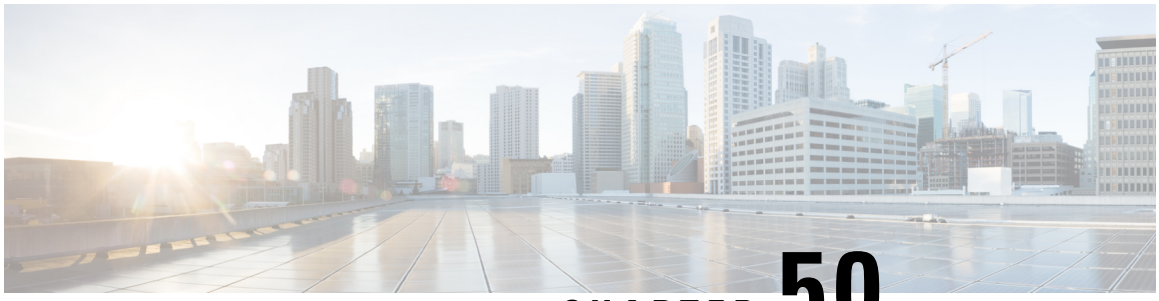
Firewall Management Center Model	Number of Dynamic Attributes Connector Connectors	Maximum Downloaded Users
FMC1600, FMC1700	10	50,000
FMC2600, FMC2700	20	150,000
FMC4600, FMC4700	30	600,000
Firewall Management Center Virtual (any supported hypervisor)	10	50,000
Firewall Management Center Virtual 300 (any supported hypervisor)	20	150,000

[1]—Firewall Management Center models are subject to end of life and end of sale. For more information, see End-Of-Life and End-Of-Sale Notices.

Table 108: Maximum Concurrent User Login Limits by Firewall Threat Defense

Firewall Threat Defense Model	Maximum Concurrent User Logins
Firewall Threat Defense Virtual 5, 10, 20, 30, 50 (any supported hypervisor)	50,000
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130 Secure Firewall 3110, 3120, 3130, 3140	50,000
Firepower 2140 Secure Firewall 3130, 3140	150,000
Firepower 4140, 4145, 4150 Firepower 9300 Secure Firewall 4215	225,000
Secure Firewall 4225, 4245	300,000

Note The Secure Firewall 200 series can download a *cumulative total* of 10,000 user IPs, SXP/SGT mappings, endpoint profiles, and dynamic objects. After a total of 10,000 have been downloaded, the Secure Firewall 200 stops downloading any objects until some previously downloaded objects have been removed. (For example, if users log out, the memory is free for other objects.)



CHAPTER 50

Realms

The following topics describe realms and identity policies:

- Realms and realm sequences, on page 1835
- License requirements for realms, on page 1843
- Requirements and prerequisites for realms, on page 1843
- Prerequisites for kerberos authentication, on page 1843
- Realm fields, on page 1844
- Realm directory and synchronize fields, on page 1848
- Create a Microsoft Azure AD Realm, on page 1850
- Create an LDAP realm or an Active Directory realm and realm directory, on page 1860
- Create a realm sequence, on page 1867
- Cross-domain trust setups with Firewall Management Center, on page 1868
- Manage a realm, on page 1876
- Compare realms, on page 1877
- Troubleshoot realms and user downloads, on page 1877
- History for realms, on page 1885

Realms and realm sequences

Realms are connections between the Secure Firewall Management Center and the user accounts on the servers you monitor that

- specify the connection settings and authentication filter settings for the server,
- specify the users and user groups whose activity you want to monitor, and
- query the user repository for user metadata on authoritative users, as well as some non-authoritative users: POP3 and IMAP users detected by traffic-based detection and users detected by traffic-based detection, a TS Agent, or ISE/ISE-PIC.

(Microsoft AD realm only.) A *realm sequence* is an ordered list of two or more Active Directory realms to use in identity policy. When you associate a realm sequence with an identity rule, the system searches the Active Directory domains in order from first to last as specified in the realm sequence.

Realm configuration requirements

You can add multiple domain controllers as directories in a realm, but they must share the same basic realm information. The directories in a realm must be exclusively LDAP or exclusively Active Directory (AD) servers. After you enable a realm, your saved changes take effect next time the Secure Firewall Management Center queries the server.

To perform user awareness, you must configure a realm for any of the supported server types. The system uses these connections to query the servers for data associated with POP3 and IMAP users, and to collect data about LDAP users discovered through traffic-based detection.

The system uses the email addresses in POP3 and IMAP logins to correlate with LDAP users on an Active Directory, Microsoft Azure Active Directory, or OpenLDAP. For example, if a managed device detects a POP3 login for a user with the same email address as an LDAP user, the system associates the LDAP user's metadata with that user.

To perform user control, you can configure any of these:

- A realm or realm sequence for an Active Directory, Microsoft Azure Active Directory, server, or for ISE/ISE-PIC



Note Configuring a Microsoft AD realm or realm sequence is optional if you plan to configure SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions; or if you use your identity policy only to filter network traffic.

Realm sequence is not available for Microsoft Azure AD realms.

- A realm or realm sequence for a Microsoft AD server for the TS Agent.
- For captive portal, an LDAP realm.

  A realm sequence is not supported for LDAP.

You can nest Microsoft AD groups and the Firewall Management Center downloads those groups and the users they contain. You can optionally restrict which groups and users get downloaded as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

User synchronization

You can configure a realm or realm sequence to establish a connection between the Firewall Management Center and an LDAP or Microsoft AD server to retrieve user and user group metadata for certain detected users:

- LDAP and Microsoft AD users authenticated by captive portal or reported by ISE/ISE-PIC. This metadata can be used for user awareness and user control.
- POP3 and IMAP user logins detected by traffic-based detection, if those users have the same email address as an LDAP or AD user. This metadata can be used for user awareness.

The Firewall Management Center obtains this information and metadata about each user:

- LDAP user name
- First and last names

- Email address
- Department
- Telephone number



Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

User activity data

User activity data is stored in the user activity database and user identity data is stored in the users database. The maximum number of users you can store and use in access control depends on your Firewall Management Center model. When choosing which users and groups to include, make sure the total number of users is less than your model limit. If your access control parameters are too broad, the Firewall Management Center obtains information on as many users as it can and reports the number of users it failed to retrieve in the Tasks tab page of the Message Center.

To optionally limit the subnets on which a managed device watches for user awareness data, you can use the **configure identity-subnet-filter** command as discussed in the *Cisco Secure Firewall Threat Defense Command Reference*.



Note If you remove a user that has been detected by the system from your user repository, the Firewall Management Center does *not* remove that user from its users database; you must manually delete it. However, your LDAP changes *are* reflected in access control rules when the Firewall Management Center next updates its list of authoritative users.

Realms and trusted domains

When you configure a Microsoft Active Directory (AD) *realm* in the Firewall Management Center, it is associated with a Microsoft Active Directory or LDAP *domain*.

Microsoft active directory forests and trust relationships

A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a *forest*. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined in domain B.



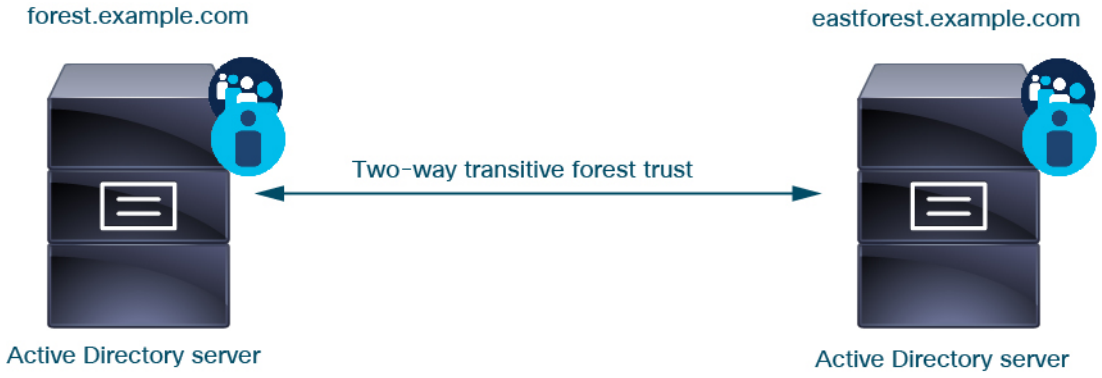
Note Trusted domains apply to Microsoft Active Directory domains only. They do *not* apply to either Microsoft Azure Active Directory or LDAP domains.

The system supports AD forests that are configured in a trust relationship. There are several types of trust relationships; this guide discusses two-way, transitive forest trust relationships. This simple example shows two forests: **forest.example.com** and **eastforest.example.com**. Users and groups in each forest can be authenticated by AD in the other forest, provided you configure the forests that way.

If you set up the system with one realm for each domain and one directory for each domain controller, the system can discover up to 100,000 foreign security principals (users and groups). If these foreign security principals match a user downloaded in another realm, then they can be used in access control policy.

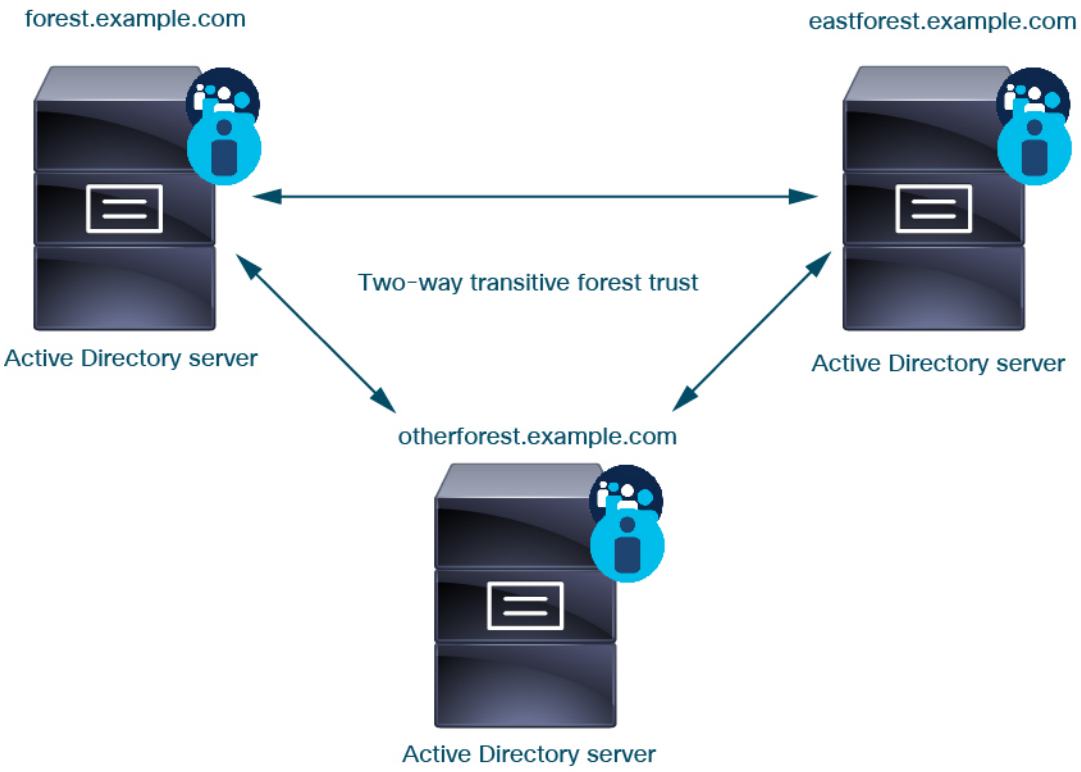
You need not configure a realm for any domain that has no users you wish to use in access control policies.

Figure 413: Two-forest configuration with two-way transitive trust



To continue the example, suppose you have three AD forests (one of which could be a subdomain or an independent forest), all set up as two-way transitive forest relationships, all users and groups are available in all three forests as well as in the system. (As in the preceding example, all three AD domains must be set up as realms and all domain controllers must be configured as directories in those realms.)

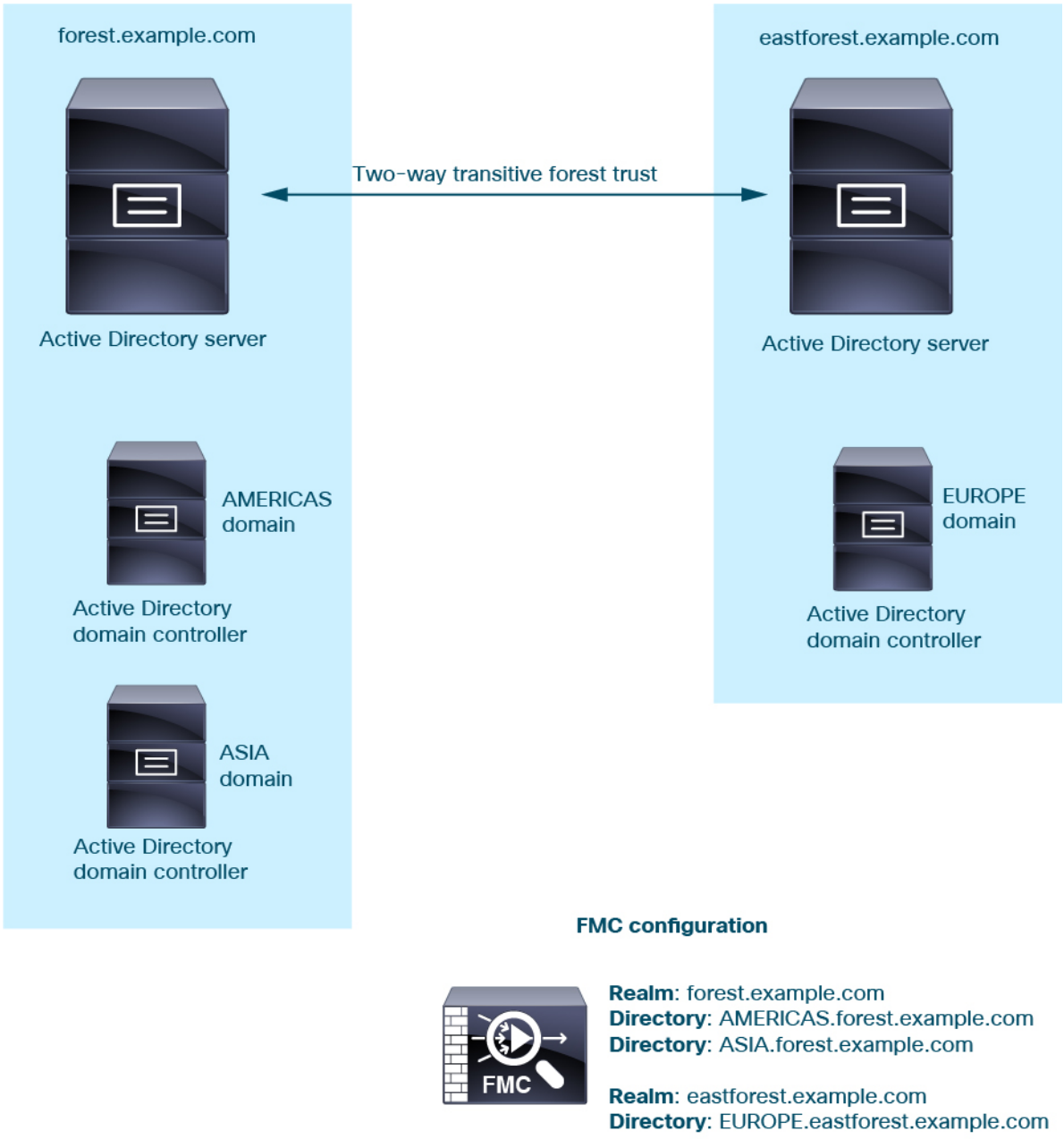
Figure 414: Three-forest configuration with two-way transitive trust



Finally, you can set up the Firewall Management Center to be able to enforce identity policies on users and groups in a two-forest system with two-way transitive forest trust. Suppose each forest has at least one domain controller, each of which authenticates different users and groups. For the Firewall Management Center to be able to enforce identity policies on those users and groups, you must set up each domain containing relevant users as Firewall Management Center realm and each domain controller as Firewall Management Center directory in the respective realm.

Failure to properly configure the Firewall Management Center prevents some of the users and groups from being able to be used in policies. You will see warnings when you try to synchronize users and groups in that case.

Figure 415: Multi-domain forest configuration



Using the preceding example, set up the Firewall Management Center as follows:

- Realm for any domain in **forest.example.com** that contains users you want to control with access control policies
  - Directory in the realm for **AMERICAS.forest.example.com**
  - Directory in the realm for **ASIA.forest.example.com**

- Realm for any domain in **eastforest.example.com** that contains users you want to control with access control policies
  - Directory in the realm for **EUROPE.eastforest.example.com**

Note The Firewall Management Center uses the AD field **msDS-PrincipalName** to resolve references to find user and group names in each domain controller. **msDS-PrincipalName** returns a NetBIOS name.

Supported servers for realms

You can configure realms to connect to the following types of servers, providing they have TCP/IP access from the Firewall Management Center:

Server Type	Supported for ISE/ISE-PIC data retrieval?	Supported for TS Agent data retrieval?	Supported for captive portal data retrieval?
Microsoft Active Directory on Windows Server 2012, 2016, and 2019	Yes	Yes	Yes
Microsoft Azure AD	Yes	No	No
OpenLDAP on Linux	No	No	Yes

An Active Directory Global Catalog server is *not supported* as a realm directory. For more information about the Global Catalog Server, refer to Global Catalog on learn.microsoft.com.

Note If the TS Agent is installed on a Microsoft Active Directory Windows Server shared with another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and a passive identity source report activity by the same IP address, only the TS Agent data is logged to the Firewall Management Center.

Note the following about your server group configurations:

- To perform user control on user groups or on users in groups, you must configure user groups on the LDAP or Active Directory server.
- Group names cannot start with `S-` because it is used internally by LDAP.

  Neither group names nor organizational unit names can contain special characters like asterisk (*), equals (=), or backslash (\); otherwise, users in those groups or organizational units are not downloaded and are not available for identity policies.

- To configure an Active Directory realm that includes or excludes users who are members of a sub-group on your server, note that Microsoft recommends that Active Directory has no more than 5000 users per group in Windows Server 2012. For more information, see Active Directory Maximum Limits—Scalability on MSDN.

  If necessary, you can modify your Active Directory server configuration to increase this default limit and accommodate more users.

- To uniquely identify the users reported by a server in your Remote Desktop Services environment, you must configure the Cisco Terminal Services (TS) Agent. When installed and configured, the TS Agent assigns unique ports to individual users so the system can uniquely identify those users. (Microsoft changed the name *Terminal Services* to *Remote Desktop Services*.)

  For more information about the TS Agent, see the *Cisco Terminal Services (TS) Agent Guide*.

Supported server object class and attribute names

Map user metadata attributes from your LDAP servers to the correct firewall fields to ensure user information is accurately retrieved and populated in the firewall.

The servers in your realms *must* use the attribute names listed in the following table for the Secure Firewall Management Center to retrieve user metadata from the servers. If the attribute names are incorrect on your server, the Secure Firewall Management Center cannot populate its database with the information in that attribute.

Table 109: Map of attribute names to Secure Firewall Management Center fields

Metadata	Firewall Management Center Attribute	LDAP ObjectClass	Active Directory Attribute	OpenLDAP Attribute
LDAP user name	Username	• user • inetOrgPerson	samaccountname	cn uid
first name	First Name		givenname	givenname
last name	Last Name		sn	sn
email address	Email		mail userprincipalname (if mail has no value)	mail
department	Department		department distinguishedname (if department has no value)	ou
telephone number	Phone		telephonenumber	telephonenumber

Note The LDAP ObjectClass for groups is `group`, `groupOfNames`, (`group-of-names` for Active Directory) or `groupOfUniqueNames`.

For more information about ObjectClasses and attributes, see these references:

- Microsoft Active Directory:
  - ObjectClasses: All Classes on MSDN
  - Attributes: All Attributes on MSDN
- OpenLDAP: RFC 4512

License requirements for realms

This topic outlines the specific license requirements necessary to enable and manage realms.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for realms

Model support

Any.

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Prerequisites for kerberos authentication

If you're using Kerberos to authentication captive portal users, keep the following in mind.

Hostname character limit

If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

DNS response character limit

DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.

Realm fields

Configure a realm to manage user authentication, directory access, and session timeouts for Active Directory, LDAP, or LOCAL user repositories in the Secure Firewall Management Center. Learn how to set realm type, credentials, supported characters, and session duration for identity policies and RA-VPN configurations.

Realm configuration fields

These settings apply to all Active Directory servers or domain controllers (also referred to as *directories*) in a realm.

Name

A unique name for the realm.

- To use the realm in identity policies, the system supports alphanumeric and special characters.
- To use the realm in RA VPN configurations, the system supports alphanumeric, hyphen (-), underscore (_), and plus (+) characters.

Description

(Optional.) Enter a description of the realm.

Type

The type of realm, **AD** for Microsoft Active Directory, **LDAP** for other supported LDAP repositories, or **LOCAL**. For a list of supported LDAP repositories, see Supported servers for realms, on page 1841. You can authenticate captive portal users with an LDAP repository; all others require Active Directory.

Note Only captive portal supports an LDAP realm.

The realm type **LOCAL** is used for configuring LOCAL user settings. The LOCAL realm is used in remote access user authentication.

Add the following LOCAL User Information for the LOCAL realm:

- **Username**—Name of the LOCAL user.
- **Password**—LOCAL user password.
- **Confirm Password**—Confirm the LOCAL user password.



Note **Click Add another LOCAL user** to add more users to the LOCAL realm.

You can add more users after creating the realm and update password for the LOCAL users. You can also create multiple LOCAL realms but cannot disable them.

AD Primary Domain

For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.



Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

AD Join Username and AD Join Password
(Available on the **Realm Configuration** tab page when you edit a realm.)

For Microsoft Active Directory realms intended for Kerberos captive portal active authentication, the distinguished username and password of any Active Directory user with appropriate rights to create a Domain Computer account in the Active Directory domain.

Keep the following in mind:

- DNS must be able to resolve the domain name to an Active Directory domain controller's IP address.
- The user you specify must be able to join computers to the Active Directory domain.
- The user name must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).

If you choose **`Kerberos`** (or **`HTTP Negotiate`**, if you want Kerberos as an option) as the **Authentication Protocol** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.



Note The SHA-1 hash algorithm is not secure for storing passwords on your Active Directory server and should not be used. For more information, consult a reference such as Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet or Password Storage Cheat Sheet on the Open Web Application Security Project website.

We recommend SHA-256 for communicating with Active Directory.

Group Attribute
(Available on the **Realm Configuration** tab page.)

These group attributes are available for Microsoft Active Directory or LDAP realms.

- Member: A user attribute that indicates the groups to which a user belongs. Each user entry contains a Member attribute that lists the groups the user is part of, rather than each group listing its members.
- Unique Member: A group attribute that lists the distinguished names (DNs) of the members of the group.

Directory Username and Directory Password

The distinguished username and password for a user with appropriate access to the user information you want to retrieve.

Note the following:

- For OpenLDAP, the user's access privileges are determined by the `<level>` parameter discussed in section 8 of the OpenLDAP specification. The user's `<level>` should be `auth` or better.
- The user name must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).

Note The SHA-1 hash algorithm is not secure for storing passwords on your Active Directory server and should not be used. For more information, consult a reference such as Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet or Password Storage Cheat Sheet on the Open Web Application Security Project website.

We recommend SHA-256 for communicating with Active Directory.

Base DN

(Optional.)The directory tree on the server where the Secure Firewall Management Center should begin searching for user data. If you don't specify a **Base DN**, the system retrieves the top-level DN provided you can connect to the server.

Typically, the base distinguished name (DN) has a basic structure indicating the company domain name and operational unit. For example, the Security organization of the Example company might have a base DN of **`ou=security,dc=example,dc=com`**.

Group DN

(Optional.)The directory tree on the server where the Secure Firewall Management Center should search for users with the group attribute. A list of supported group attributes is shown in Supported server object class and attribute names, on page 1842. If you don't specify a **Group DN**, the system retrieves the top-level DN provided you can connect to the server.

Note The following is the list of characters the system *supports* in users, groups, DNS in your directory server. Using any characters other than these could result in the system failing to download users and groups.

Entity	Supported characters
User name	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
Group name	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
Base DN and Group DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

A space is not supported anywhere in a user name, including at the end.

These fields are available when you edit an existing realm.

User Session Timeout

(Available on the **Realm Configuration** tab page when you edit a realm.)

Enter the number of minutes before user sessions time out. The default is 1440 (24 hours) after the user's login event. After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the Secure Firewall Management Center as Unknown (except for **Failed Captive Portal Users**).

In addition, if you set up ISE/ISE-PIC without a realm and the timeout is exceeded, a workaround is required. For more information, contact Cisco TAC.

You can set timeout values for the following:

- **User Agent and ISE/ISE-PIC Users**: Timeout for users tracked by the user agent or by ISE/ISE-PIC, which are types of passive authentication.

  The timeout value you specify does *not* apply to pxGrid SXP session topic subscriptions (for example, destination SGT mappings). Instead, session topic mappings are preserved as long as there is no delete or update message for a given mapping from ISE.

  For more information about ISE/ISE-PIC, see The ISE/ISE-PIC identity source, on page 1911.

- **Terminal Services Agent Users**: Timeout for users tracked by the TS Agent, which is a type of passive authentication. For more information, see Terminal services agent identity source, on page 1937.

- **Captive Portal Users**: Timeout for users who successfully log in using the captive portal, which is a type of active authentication. For more information, see Captive portal identity source, on page 1887.

- **Failed Captive Portal Users**: Timeout for users who do not successfully log in using the captive portal. You can configure the **Maximum login attempts** before the user is seen by the Secure Firewall Management Center as Failed Auth User. A Failed Auth User can optionally be granted access to the network using access control policy and, if so, this timeout value applies to those users.

  For more information about failed captive portal logins, see Captive portal fields, on page 1903.

- **Guest Captive Portal Users**: Timeout for users who log in to the captive portal as a guest user. For more information, see Captive portal identity source, on page 1887.

Realm directory and synchronize fields

Configure Active Directory realm directory and user synchronization fields to enable secure authentication, user data lookup, and group management in the Secure Firewall Management Center. Learn how to specify server, encryption, domain, and group settings for optimized user awareness and access control.

Realm directory fields

These settings apply to individual servers (such as Active Directory domain controllers) in a realm.

Hostname / IP Address

Fully qualified host name of the Active Directory domain controller machine. To find the fully qualified name, see Find the active directory server's name, on page 1863.

If you're using Kerberos for authenticating captive portal, also make sure you understand these considerations:

If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.

Port

The server's port.

Encryption

(Strongly recommended.) The encryption method to use:

- **`STARTTLS`**—encrypted LDAP connection
- **`LDAPS`**—encrypted LDAP connection
- **`None`**—unencrypted LDAP connection (unsecured traffic)

To communicate securely with an Active Directory server, see Connect securely to Active Directory or LDAP, on page 1862.

CA Certificate

The TLS/SSL certificate to use for authentication to the server. You must configure **`STARTTLS`** or **`LDAPS`** as the **Encryption** type to use a TLS/SSL certificate.

If you are using a certificate to authenticate, the name of the server in the certificate must match the server **Hostname / IP Address**. For example, if you use 10.10.10.250 as the IP address but **`computer1.example.com`** in the certificate, the connection fails.

Interface used to connect to Directory server

Required only for RA VPN authentication so the Secure Firewall Threat Defense can connect securely to your Active Directory server. This interface is not used for downloading users and groups, however.

You can choose only a routed interface group. For more information, see Interfaces, on page 2383.

Click one of these options:

- **Resolve via route lookup**: Use routing to connect to the Active Directory server.
- **Choose an interface**: Choose a specific managed device interface group to connect to the Active Directory server.

User synchronize fields

AD Primary Domain

For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.



Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

Enter query to look for users and groups

Base DN:

(Optional.) The directory tree on the server where the Firewall Management Center should begin searching for user data.

Typically, the base distinguished name (DN) has a basic structure indicating the company domain name and operational unit. For example, the Security organization of the Example company might have a base DN of `ou=security,dc=example,dc=com`.

Group DN:

(Optional.) The directory tree on the server where the Firewall Management Center should search for users with the group attribute. A list of supported group attributes is shown in Supported server object class and attribute names, on page 1842.



Note Neither the group name nor the organizational unit name can contain special characters like asterisk (*), equals (=), backslash (\) because users in those groups are not downloaded and cannot be used in identity policies.

Load Groups

Enables you to download users and groups for user awareness and user control.

Available Groups, Add to Include, Add to Exclude

Limits the groups that can be used in policy.

- Groups that are displayed in the **Available Groups** field are available for policy unless you move groups to the **Included Groups and Users** or **Excluded Groups and Users** field.
- If you move groups to the **Included Groups and Users** field, only those groups and users they contain are downloaded and user data is available for user awareness and user control.
- If you move groups to the **Excluded Groups and Users** field, all groups and users they contain *except* these are downloaded and available for user awareness and user control.
- To include users from groups that are not included, enter the user name in the field below **User Inclusion** and click **Add**.
- To exclude users from groups that are not excluded, enter the user name in the field below **User Exclusion** and click **Add**.



Note The users that are downloaded to the Firewall Management Center is calculated using the formula **R = I - (E+e) + i**, where

- R is list of downloaded users
- I is included groups
- E is excluded groups
- e is excluded users
- i is included users

Synchronize Now
Click to synchronize groups and users with AD.

Begin automatic synchronization at
Enter the time and time interval at which to download users and groups from AD.

Create a Microsoft Azure AD Realm

You can use a Microsoft Azure Active Directory (AD) realm with Cisco ISE to authenticate users and get user sessions for user control. We get groups from Azure AD and logged-in user session data from Cisco ISE.

Authentication options

You have two authentication options:

- Resource owned password credentials (ROPC): Enables users to log in with a client like AnyConnect using a user name and password. ISE sends user sessions to the Secure Firewall Management Center. For more information, see How Entra ID and Cisco ISE authentication with resource owned password credentials works, on page 1851.

  Additional resource: Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials on learn.microsoft.com.

- Extensible Authentication Protocol (EAP) Chaining with Tunnel-based Extensible Authentication Protocol (TEAP) and Transport Layer Security (TLS), abbreviated EAP/TEAP-TLS: TEAP is a tunnel-based EAP

method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel. ISE is used to validate user credentials and to send user sessions to the Secure Firewall Management Center. For more information, see How Entra ID and Cisco ISE authentication works with TEAP/EAP-TLS, on page 1852.

Note Before deploying policies related to a Microsoft Azure AD realm, see User limits for microsoft azure active directory realms, on page 1833.

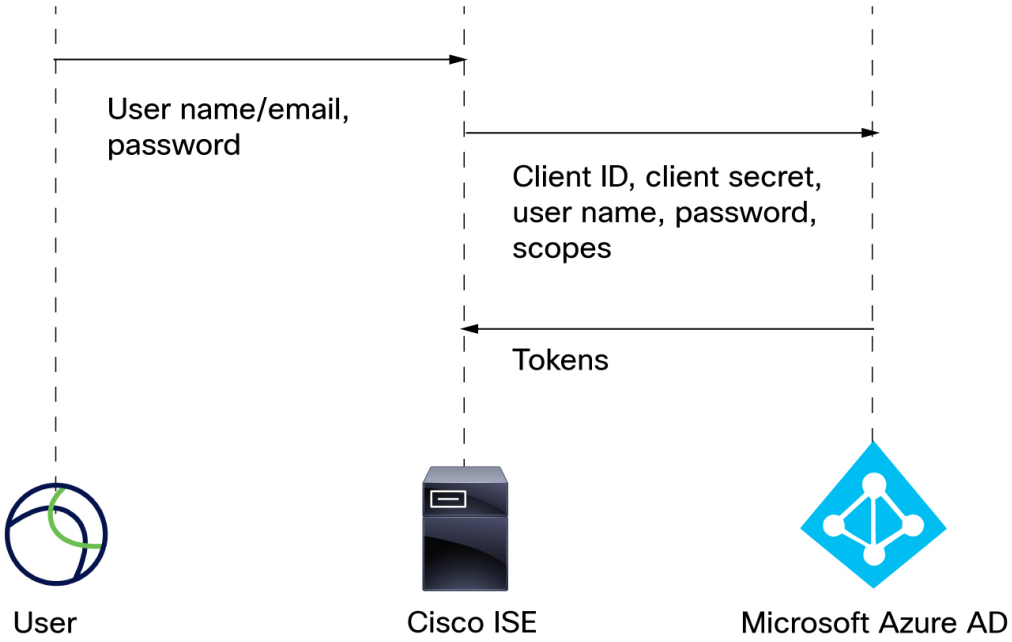
How Entra ID and Cisco ISE authentication with resource owned password credentials works

Summary

The key components involved in the Entra ID authentication with resource owned password credentials process are:

- User: Logs in with credentials using a VPN client
- Cisco Secure Client: VPN client that sends user credentials
- Entra ID (formerly Azure AD): Validates credentials and issues tokens
- Cisco ISE: Receives tokens and manages user sessions
- Secure Firewall Management Center: Receives user sessions from ISE

Workflow



These stages describe how Entra ID and Cisco ISE authentication with resource owned password credentials works:

1. The user logs in with a user name (or email address) and password using a VPN client like Cisco Secure Client.
2. The client ID, client secret, user name, password, and scopes are sent to Entra ID.
3. Tokens are sent from Entra ID to Cisco ISE, which sends user sessions to the Secure Firewall Management Center.

   For details about configuring Cisco ISE, see Configure ISE 3.0 REST ID with Azure Active Directory.

   Additional resource: Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials on learn.microsoft.com.

How Entra ID and Cisco ISE authentication works with TEAP/EAP-TLS

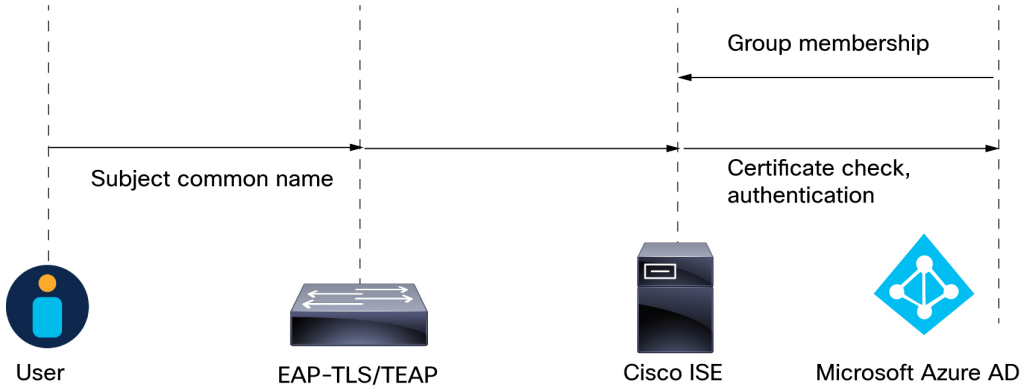
Tunnel Extensible Authentication Protocol (TEAP), defined by RFC7170, can be used with ISE and the Secure Firewall Management Center for secure authentication.

Summary

The key components involved in this authentication process are:

- User device: Provides certificate through EAP-TLS or TEAP protocol
- ISE: Validates certificate and performs user lookup through Azure Graph API
- Entra ID: Provides user attributes and group information for authorization

Workflow



These stages describe how the authentication process works and are based on Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory:

1. The user's certificate is sent to ISE through EAP-TLS or TEAP with EAP-TLS as the inner method.
2. ISE evaluates the user's certificate (validity period, trusted certificate authority, certificate revocation list, and so on).

3. ISE takes the certificate subject name (CN) and performs a look-up to the Azure Graph API to fetch the user's groups and other attributes. This is referred to by Azure as User Principal name (UPN).
4. ISE authorization policies are evaluated against the user's attributes returned from Azure.

Create a Microsoft Azure AD realm

Create and configure a (now called *Entra ID*) realm for passive authentication use with the Secure Firewall Management Center.

This configuration enables passive authentication between Microsoft Entra ID and your firewall system through proper realm setup and access control policy integration.

Procedure

Step 1 Enable the Dynamic Attributes Connector.

The Dynamic Attributes Connector is required to use a realm. You can do it first or you can enable it when you create the realm. For more information, see Enable the dynamic attributes connector, on page 2063.

Step 2 Configure Microsoft Entra ID.

Several configuration tasks are required, including setting up an event hub, giving your application permission to the Microsoft Graph API, and enabling the audit log.

See Configure Microsoft Entra ID, on page 1854.

Step 3 Configure Cisco ISE.

The way you configure ISE depends on how users authenticate with your system. For more information, see Configure Cisco ISE for Microsoft Azure AD, on page 1855.

Step 4 Create a Cisco ISE identity source.

The identity source enables ISE to communicate with the Secure Firewall Management Center.

Step 5 Get the information required to configure your Microsoft Azure AD realm.

This information includes client and tenant IDs, client secret, and other information store in Microsoft Entra ID.

Step 6 Configure and verify your realm.

Test the realm's configuration before you start to use it in access control policies.

Step 7 Create access control policies and rules using your Microsoft Azure AD (SAML) realm.

Unlike other types of realms, you do not need to create an identity policy or associate the identity policy with an access control policy.

See Creating a basic access control policy, on page 1575 and Create and edit access control rules, on page 1631.

What to do next

See How Entra ID and Cisco ISE authentication with resource owned password credentials works, on page 1851.

Configure Microsoft Entra ID

Configure Microsoft Entra ID to enable passive authentication and user group synchronization with the Secure Firewall Management Center.

This task provides basic information about how to set up a Microsoft Entra ID (formerly called *Microsoft Azure Active Directory (AD)*) as a realm you can use with the Secure Firewall Management Center. We expect you to already be familiar with Entra ID; if not, consult documentation or a support resource before you get started.

Procedure

Step 1 Grant your Entra ID application the Microsoft Graph permissions.

Grant your Entra ID application the following permissions to Microsoft Graph as discussed in Authorization and the Microsoft Graph Security API on the Microsoft site:

- Reader role
- User.Read.All permission
- Group.Read.All permission

This permission enables the Secure Firewall Management Center to download users and groups from Entra ID the first time.

Required information from this step for setting up the Entra ID realm in the Secure Firewall Management Center:

- Name of the app you registered
- **Application (client) ID**
- **Client secret**
- **Directory (tenant) ID**

Step 2 Set up an event hub.

Set up the event hub as discussed in Quickstart: Create an event hub using Azure portal on the Microsoft site. The Secure Firewall Management Center uses the event hub audit log to download periodic updates to users and groups.

More information: Features and terminology in Azure Event Hubs.



Important You must choose the **Standard** pricing tier or better. If you choose **Basic**, the realm cannot be used.

Required information from this step for setting up the Entra ID realm in the Secure Firewall Management Center:

- Namespace **Name**
- **Connection string—primary key**
- Event Hub **Name**
- Consumer group **Name**

Step 3 Enable the audit log.

Enable the audit log as discussed in Tutorial: Stream Azure Active Directory logs to an Azure event hub on the Microsoft site.

Step 4 Configure Cisco ISE for Entra ID.

To send user session information to the Secure Firewall Management Center, configure Cisco ISE for Entra ID as discussed in Configure ISE 3.0 REST ID with Azure Active Directory.

What to do next

See Configure Cisco ISE for Microsoft Azure AD, on page 1855.

Configure Cisco ISE for Microsoft Azure AD

In a Microsoft Azure AD (now called *Entra ID*) realm, it's the responsibility of ISE to send user sessions (login, logout) to the Secure Firewall Management Center. This topic discusses how to set up ISE for use with an Azure AD realm.

Resource owned password credentials authentication

To use ISE with Microsoft Azure ADMicrosoft Azure AD implemented through Representational State Transfer (REST) Identity (ID) service with the help of Resource Owner Password Credentials (ROPC), see Configure ISE 3.0 REST ID with Azure Active Directory.

TEAP/EAP-TLS

To use ISE with authorization policies based on Azure AD group membership and other user attributes with EAP-TLS or TEAP as the authentication protocols, see Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory.

What to do next

Get required information For Your Microsoft Azure AD realm, on page 1855

Get required information For Your Microsoft Azure AD realm

This task enables you to collect the necessary credentials and configuration information from Microsoft Entra ID (formerly Azure AD) and Event Hubs to establish a SAML authentication realm in your Secure Firewall Management Center.

This task explains how to get the information required to set up a Microsoft Azure AD (now called *Entra ID*) realm in the Secure Firewall Management Center. You might have already obtained this information when you set up Microsoft Entra ID as discussed in Configure Microsoft Entra ID, on page 1854.

Procedure

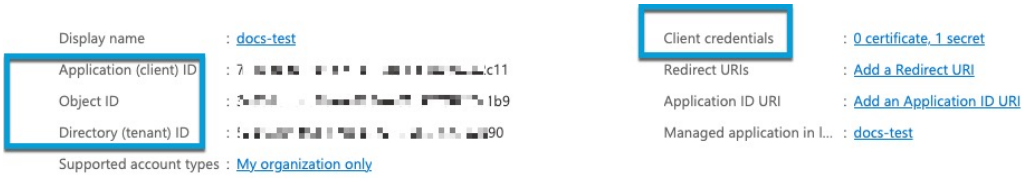
Step 1 Log in to https://portal.azure.com/ as a user with at least the Product Designer role.

Step 2 At the top of the page, click **Microsoft Entra ID**.

Step 3 In the left column, click **App Registrations**.

a) If necessary, filter the list of displayed apps to show the one you want to use.

b) Click the name of your app.



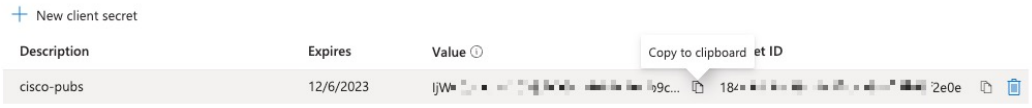
c) Click **Copy** ( ) next to the following values on this page and paste those values to a text file.

- **Application (Client) ID**
- **Directory (tenant) ID**

d) Click **Client Credentials**.

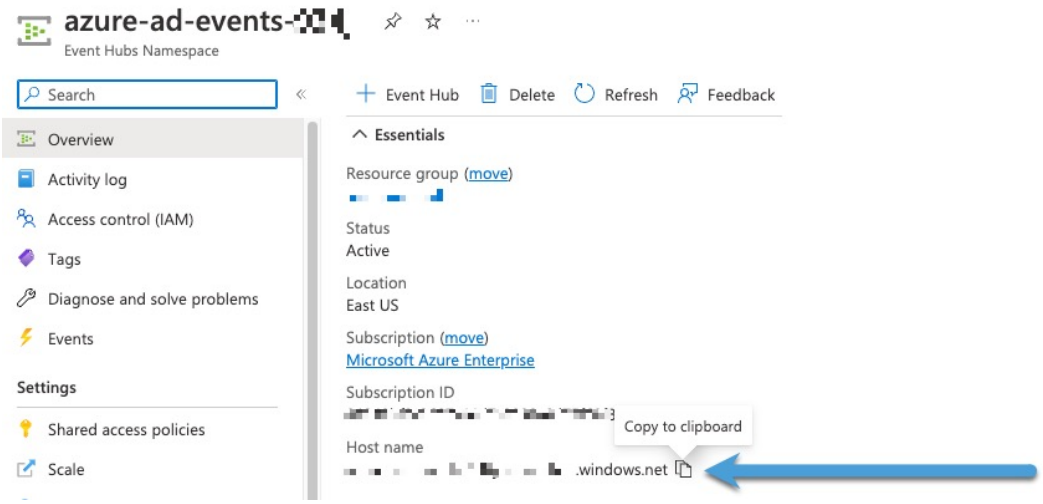
e) Unless you already know the client secret *value* (as opposed to the client *secret ID*), you must create a new client secret as follows:

1. Click **New Client Secret**.
2. Enter the required information in the provided fields.
3. Click **Add**.
4. Click **Copy** ( ) next to Value as the following figure shows.



Step 4 From https://portal.azure.com/, click **Event Hubs** > **(name of an event hub)**.

a) In the right pane, click **Copy** ( ) next to the value of **Host name** and paste the value to the clipboard. This is your event hub host name.

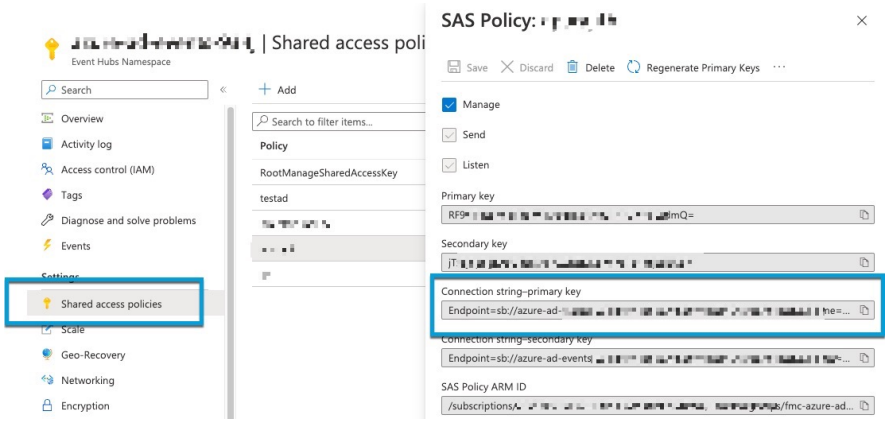


b) Write down or copy to a text file the name of the event hub (same as the **Event Hubs Namespace** at the top of the page).

c) In the left pane, under Settings, click **Shared access policies**.

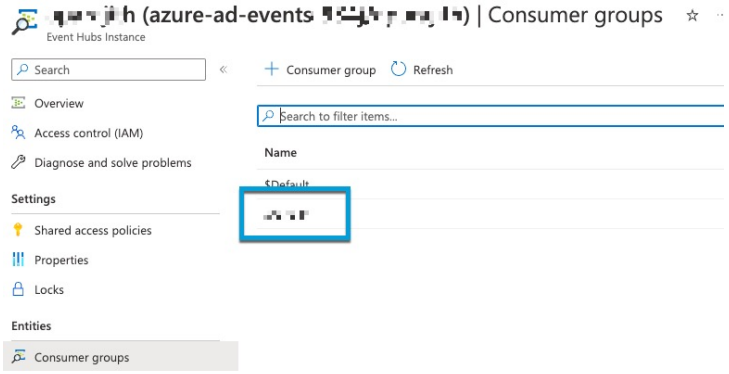
d) Click the name of a policy.

e) Click **Copy** ( ) next to **Connection string-primary key**.



Step 5 Click **Overview** > **Entities** > **Event Hubs** > **(name of an event hub)** > **Entities** > **Consumer Groups**.

Write down this value or copy it to the clipboard. This is your consumer group name.



Step 6 In the left pane, click **Overview**.

Step 7 Click **Copy** ( ) next to **Namespace**.



This is your event hubs topic name.

Create an Azure AD realm

This task creates a *realm* (a connection between the Firewall Management Center and a Microsoft Azure AD realm) to enable user and identity control through access control policies.

Note To perform user and identity control with an Azure AD realm, you need only an access control policy with an associated Azure AD realm. You do not need to create an identity policy.

Before you begin

Complete all of the following tasks:

- Configure ISE as discussed in Configure Cisco ISE for Microsoft Azure AD, on page 1855
- Create an ISE identity source as discussed in ISE/ISE-PIC configuration, on page 1919
- Enable the Dynamic Attributes Connector as discussed in Enable the dynamic attributes connector, on page 2063 .
- Get values required for the Azure AD realm as discussed in Get required information For Your Microsoft Azure AD realm, on page 1855.
- Configure Azure AD as discussed in Configure Microsoft Entra ID, on page 1854

Follow these steps to create an Azure AD realm:

Procedure

Step 1 Log in to Secure Firewall Management Center .

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 To create a new realm, click **Add Realm** > **Azure AD**.

Step 4 Enter the required information.

Item	Description
Name	
(Optional.) **Description**	
Client ID	Enter the information you found as discussed in Get required information For Your Microsoft Azure AD realm, on page 1855.
Client Secret	
Tenant ID	
Event Hubs Host Name	
Event Hub Name	
Event Hub Connection String	
(Optional.) **Excluded User Groups**	Enter one or more groups from which to *not* download users for identity control. Users in these groups will not be available for use in access control policies. Enter one group name per line followed by a line break. Group names are case-sensitive.

Step 5 Enter the values you found as discussed in Get required information For Your Microsoft Azure AD realm, on page 1855.

Step 6 Click **Test**.

Step 7 Fix any errors that are displayed in the test.

Step 8 Click **Save**.

What to do next

Create an access control policy and rule as discussed in Creating a basic access control policy, on page 1575.

Note Before deploying policies related to a Microsoft Azure AD realm, see User limits for microsoft azure active directory realms, on page 1833.

Azure AD user session timeout

Set the Entra ID user session timeout for ISE or ISE-PIC to define how long users stay authenticated, ensuring network access control after timeout via the User Session Timeout page when editing an Entra ID realm.

The Azure AD user session timeout for ISE/ISE-PIC is available on the **User Session Timeout** page when you edit an Azure AD realm.

The default value 1440 minutes (24 hours). After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the Firewall Management Center as Unknown (except for **Failed Captive Portal Users**).

Create an LDAP realm or an Active Directory realm and realm directory

Before you begin

If you're using Kerberos authentication for captive portal, see the following section before you begin: Prerequisites for kerberos authentication, on page 1843 .



Note Microsoft Azure Active Directory is not supported for captive portal.



Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

If you're setting up ISE/ISE-PIC without a realm, be aware there is a user session timeout that affects how users are seen by the Firewall Management Center.

The following procedure enables you to create a *realm* (a connection between the Firewall Management Center and an Active Directory realm) and a *directory* (a connection between the Firewall Management Center and an LDAP server or an Active Directory domain controller).

(Recommended.) To connect securely from the Firewall Management Center to your Active Directory server, first perform the following tasks:

- Export the active directory server's root certificate, on page 1863
- Find the active directory server's name, on page 1863

Microsoft has announced that Active Directory servers will start enforcing LDAP binding and LDAP signing in 2020. Microsoft is making these a requirement because when using default settings, an elevation of privilege vulnerability exists in Microsoft Windows that could allow a man-in-the-middle attacker to successfully forward an authentication request to a Windows LDAP server. For more information, refer to 2020 LDAP channel binding and LDAP signing requirement for Windows on the Microsoft support site.

For more information about realm and directory configuration fields, see Realm fields, on page 1844 and Realm directory and synchronize fields, on page 1848 .

A step-by-step example of setting up a realm with cross-domain trust is shown in Cross-domain trust setups with Firewall Management Center, on page 1868 .

An Active Directory Global Catalog server is *not supported* as a realm directory. For more information about the Global Catalog Server, refer to Global Catalog on learn.microsoft.com.

Note You must specify a unique **AD Primary Domain** for every Microsoft Active Directory (AD) realm. Although the system allows you to specify the same **AD Primary Domain** for different Microsoft AD realms, the system won't function properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group. The system prevents you from specifying more than one realm with the same **AD Primary Domain** because users and groups won't be identified properly. This happens because system assigns a unique ID to every user and group in each *realm*; therefore, the system cannot definitively identify any particular user or group.

Procedure

Step 1 Log in to the Secure Firewall Management Center. Click **Integration** > **Other Integrations** > **Realms** > **Realms**

Step 2 To create a new realm, choose from **Add Realm** drop-down list.

Step 3 To perform other tasks (such as enable, disable, or delete a realm), see Manage a realm, on page 1876 .

Step 4 Enter realm information as discussed in Realm fields, on page 1844 .

Step 5 In the Directory Server Configuration section, enter directory information as discussed in Realm directory and synchronize fields, on page 1848 .

Step 6 (Optional.) To configure another domain for this realm, click **Add another directory** .

Step 7 Click **Configure Groups and Users** .

Information	Description
AD Primary Domain	Domain for the Active Directory server where users should be authenticated. For additional information, see Realm fields, on page 1844 . You must create the realm with the original domain name of the domain and not any alternative user principal name (UPN) suffixes of the domain. Otherwise, users and groups fail to download and identity policies will not be enforced. For example, if the original domain is `domain.example.com` and the alternative UPN name is`domain2.mydomain.com`, you must configure the realm to use `domain.example.com`. For more information about configuring an alternative UPN suffix, see a resource like Configuring Alternate Login ID on learn.microsoft.com.
Base DN	The directory tree on the server where the Firewall Management Center should begin searching for user data.
Group DN	The directory tree on the server where the Firewall Management Center should begin searching for group data.

Information	Description
Load Groups	Click to load groups from the Active Directory server. If no groups are displayed, enter or edit information in the **AD Primary Domain** , **Base DN** , and **Group DN** fields and click **Load Groups** . For more information about those fields, see Realm fields, on page 1844 .
Available Groups section	Limit the groups to use in policy by moving them to either the **Included Groups and Users** or **Excluded Groups and Users** list. Moving one group to the **Included Groups and Users** list, for example, allows that group only to be used in policy but excludes all other groups. Groups in the **Excluded Groups and Users** and the users they contain are excluded from user awareness and control. All other groups and users *are* available. For more information, see Realm directory and synchronize fields, on page 1848 .

Configure the Realm

Before you begin

You must have created a new realm and its groups and users, as described in the prior procedure.

Procedure

Step 1 Click the **Realm Configuration** tab.

Step 2 Enter **Group Attribute** , and (if you use Kerberos authentication for captive portal) enter **AD Join Username** and **AD Join Password** . For more information, see Realm directory and synchronize fields, on page 1848 .

Step 3 If you use Kerberos authentication, click **Test** . If the test fails, wait a short time and try again.

Step 4 Enter user session timeout values, in minutes, for **ISE/ISE-PIC Users** , **Terminal Server Agent Users** , **Captive Portal Users** , **Failed Captive Portal Users** , and **Guest Captive Portal Users** .

Step 5 When you're finished configuring the realm, click **Save** .

Connect securely to Active Directory or LDAP

To create a secure connection between an Active Directory or LDAP server and the Secure Firewall Management Center (which we strongly recommend), you must perform all of the following tasks:

- Export the server's *root* certificate.
- Import the root certificate into the Secure Firewall Management Center as a trusted CA certificate (**Objects** > **Object Management** > **PKI** > **Trusted CAs**).
- Find the server's fully qualified name.

- Create the realm directory.

Related Topics

Export the active directory server's root certificate, on page 1863
Find the active directory server's name, on page 1863
Create an LDAP realm or an Active Directory realm and realm directory, on page 1860

Find the active directory server's name

Find the fully qualified server name in Microsoft Active Directory that you need to configure a realm directory.

To configure a realm directory in the Firewall Management Center, you must know the fully qualified server name, which you can find as discussed in the procedure that follows.

These tasks apply to Microsoft Active Directory only. If you use LDAP, consult an appropriate reference for the procedure.

Before you begin

You must log in to the Active Directory server as a user with sufficient privileges to view the computer's name.

Follow these steps to find the Active Directory server's name:

Procedure

Step 1 Log in to the Active Directory server.

Step 2 Click **Start**.

Step 3 Right-click **This PC**.

Step 4 Click **Properties**.

Step 5 Click **Advanced System Settings**.

Step 6 Click the **Computer Name** tab.

Step 7 Note the value of **Full computer name**.
You must enter this exact name when you configure the realm directory in the Firewall Management Center.

What to do next

Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

Related Topics

Export the active directory server's root certificate, on page 1863

Export the active directory server's root certificate

Export the Active Directory server's root certificate to enable secure connection to the Firewall Management Center for obtaining user identity information and authentication purposes.

The task that follows discusses how to export the Active Directory server's root certificate, which is required to connect securely to the Firewall Management Center to obtain user identity information.

These tasks apply to Microsoft Active Directory only. If you use LDAP, consult an appropriate reference for the procedure.

Before you begin

You must know the name of your Active Directory server's root certificate. The root certificate might have the same name as the domain or the certificate might have a different name. The procedure that follows shows one way you can find the name; there could be other ways, however.

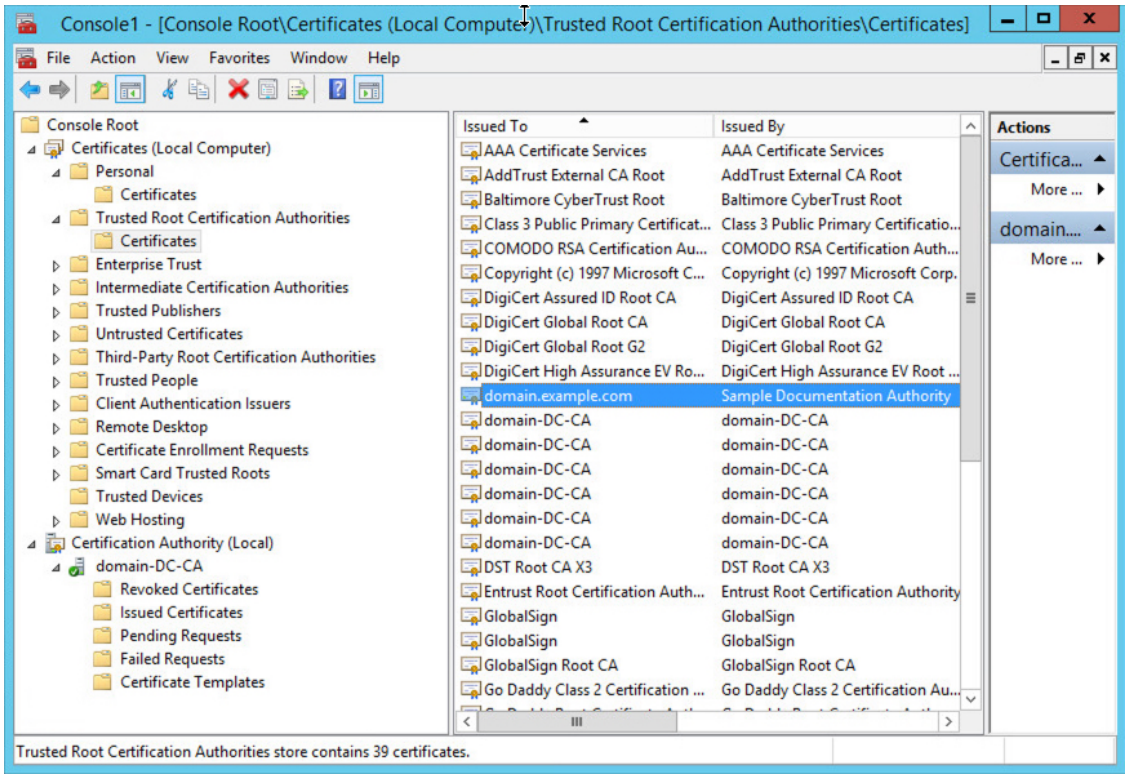
Follow these steps to export the Active Directory server's root certificate:

Procedure

Step 1 Find the name of the Active Directory Server's root certificate using the Microsoft Management Console.

This is one way to find the name of the Active Directory Server's root certificate; consult Microsoft documentation for more information:

a) Log in to the Active Directory server as a user with privileges to run the Microsoft Management Console.
b) Click **Start** and enter **mmc**.
c) Click **File** > **Add/Remove Snap-in**
d) From the Available Snap-ins list in the left pane, click **Certificates (local)**.
e) Click **Add**.
f) At the Certificates snap-in dialog box, click **Computer Account** and click **Next**.
g) At the Select Computer dialog box, click **Local Computer** and click **Finish**.
h) *Windows Server 2012 only*. Repeat the preceding steps to add the Certification Authority snap-in.
i) Click **Console Root** > **Trusted Certification Authorities** > **Certificates**.
The server's trusted certificates are displayed in the right pane. The following figure is only an example for Windows Server 2012; yours will probably look different.



Step 2 Export the certificate using the **certutil** command.

This is only one way to export the certificate. It is a convenient way to export the certificate, especially if you can run a web browser and connect to the Firewall Management Center from the Active Directory server.

a) Click **Start** and enter **cmd**.
b) Enter the command **certutil -CA.cert** *certificate-name*.
The server's certificate is displayed on the screen.
c) Copy the entire certificate to the clipboard, starting with **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----** (including those strings).

What to do next

Import the Active Directory server's certificate into the Firewall Management Center as a trusted CA certificate as discussed in Add a trusted CA object, on page 2396.

Related Topics

Find the active directory server's name, on page 1863

Synchronize users and groups

This task synchronizes users and groups from Active Directory domains to enable their use in identity policies.

Synchronizing users and groups means the Firewall Management Center queries the realms and directories you configured for groups and users in those groups. All users the Firewall Management Center finds can be used in identity policies.

If issues are found, you most likely need to add a realm that contains users and groups the Firewall Management Center cannot load. For details, see Realms and trusted domains, on page 1837.

Before you begin

Create a Secure Firewall Management Center *realm* for each Active Directory domain and a Firewall Management Center *directory* for each Active Director domain controller in each forest. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

Note Synchronizing users and groups is not necessary for Microsoft Azure AD realms.

You must create a realm only for domains that have users you want to use in user control.

You can nest Microsoft AD groups and the Firewall Management Center downloads those groups and the users they contain. You can optionally restrict which groups and users get downloaded as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

You must create the realm with the original domain name of the domain and not any alternative user principal name (UPN) suffixes of the domain. Otherwise, users and groups fail to download and identity policies will not be enforced. For example, if the original domain is `domain.example.com` and the alternative UPN name is`domain2.mydomain.com`, you must configure the realm to use `domain.example.com`. For more information about configuring an alternative UPN suffix, see a resource like Configuring Alternate Login ID on learn.microsoft.com.

Follow these steps to synchronize users and groups:

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 Next to each realm, click **Download** ( ).

Step 4 To see the results, click the **Sync Results** tab.
The Realms column indicates whether or not there were issues synchronizing users and groups in Active Directory forests. Look for the following indicators next to each realm.

Indicator in Realms column	Meaning
(nothing)	All users and groups synchronized without error. No action is necessary.

Indicator in Realms column	Meaning
Yellow Triangle ( )	There were issues synchronizing users and groups. Make sure you added a realm for each Active Directory domain and a directory for each Active Directory domain controller. For more details, see Troubleshoot cross-domain trust, on page 1882.

Create a realm sequence

Creating a realm sequence provides an ordered list of realms the system searches when it applies identity policy, allowing you to specify the priority order for user authentication across multiple Active Directory servers.

The following procedure enables you to create a realm sequence, which is an ordered list of realms the system searches when it applies identity policy. You add a realm sequence to an identity rule exactly the same way as you add a realm; the difference is that the system searches all the realms in the order specified in the realm sequence when applying an identity policy.

Before you begin

You must create and enable at least two realms, each corresponding to a connection with an Active Directory server. You cannot create realm sequences for LDAP realms.

Create a realm as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

Follow these steps to create a realm sequence:

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so and click **Integration** > **Other Integrations** > **Realms** > **Realm Sequences**.

Step 2 Under the **Realm Sequences** tab, click **Add Sequence**.

Step 3 In the **Name** field, enter a name to identify the realm sequence.

Step 4 (Optional.) In the **Description** field, enter a description for the realm sequence.

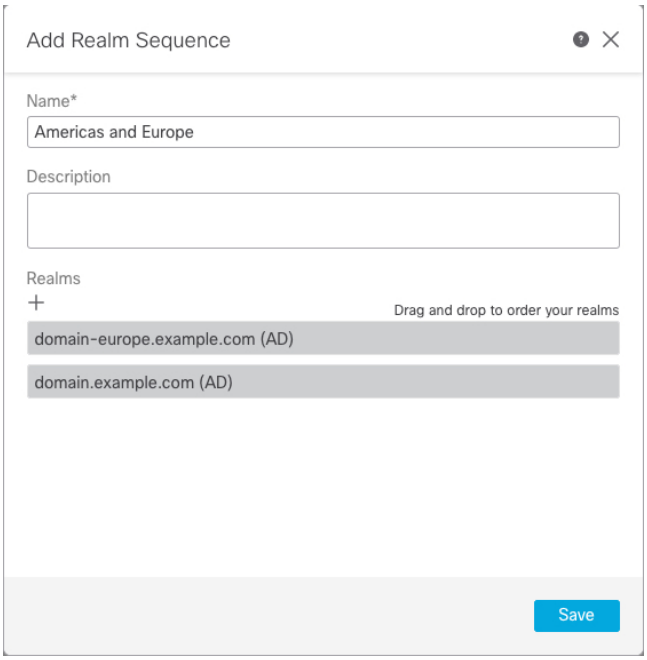
Step 5 Under Realms, click **Add** ( ).

Step 6 Click the name of each realm to add to the sequence.

To narrow your search, enter all or part of a realm name in **Filter** field.

Click **OK**.

Step 7 In the Add Realm Sequence dialog box, drag and drop the realms in the order in which you want the system to search for them.
The following figure shows an example of a realm sequence consisting of two realms. The **domain-europe.example.com** realm will be searched for users before the **domain.example.com** realm.



Step 8 Click **Save**.

What to do next

See Create an identity policy, on page 1943.

Cross-domain trust setups with Firewall Management Center

A cross-domain trust setup allows discovery and use of users and groups from multiple domains in access control policies.

This is an introduction to several topics that walk you through configuring the Firewall Management Center with two realms having cross-domain trust.

Example setup configuration

This step-by-step example involves two forests: **forest.example.com** and **eastforest.example.com**. The forests are configured so that certain users and groups in each forest can be authenticated by Microsoft AD in the other forest.

Note This topic applies to Microsoft AD realms only. It does *not* apply to Microsoft Azure AD realms.

The example setup uses this configuration:



Using this example, you would set up the Firewall Management Center with these components:

- Realm and directory for any domain in **forest.example.com** that contains users you want to control with access control policy
- Realm and directory for any domain in **eastforest.example.com** that contains users you want to control with access control policy

Each realm in the example has one domain controller, which is configured in the Firewall Management Center as a directory. The directories in this example are configured as follows:

- **forest.example.com**
  - Base distinguished name (DN) for users: **ou=UsersWest,dc=forest,dc=example,dc=com**
  - Base DN for groups: **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - Base DN for users: **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - Base DN for groups: **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

Related Topics

Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories, on page 1869

Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories

This task configures the Firewall Management Center to recognize Active Directory servers in a cross-domain trust relationship, enabling the discovery and use of users and groups from multiple domains in access control policies.

This is the first task in a step-by-step procedure that explains how to configure the Firewall Management Center to recognize Active Directory servers configured in a cross-domain trust relationship, which is an increasingly common configuration for enterprise organizations. For an overview of this sample configuration, see Cross-domain trust setups with Firewall Management Center, on page 1868.

If you set up the system with one realm for each domain and one directory for each domain controller, the system can discover up to 100,000 foreign security principals (users and groups). If these foreign security principals match a user downloaded in another realm, then they can be used in access control policy.

Before you begin

You must configure Microsoft Active Directory servers in a cross-domain trust relationship; see Realms and trusted domains, on page 1837 for more information.

If you authenticate users with LDAP or Microsoft Azure AD, you *cannot* use this procedure.

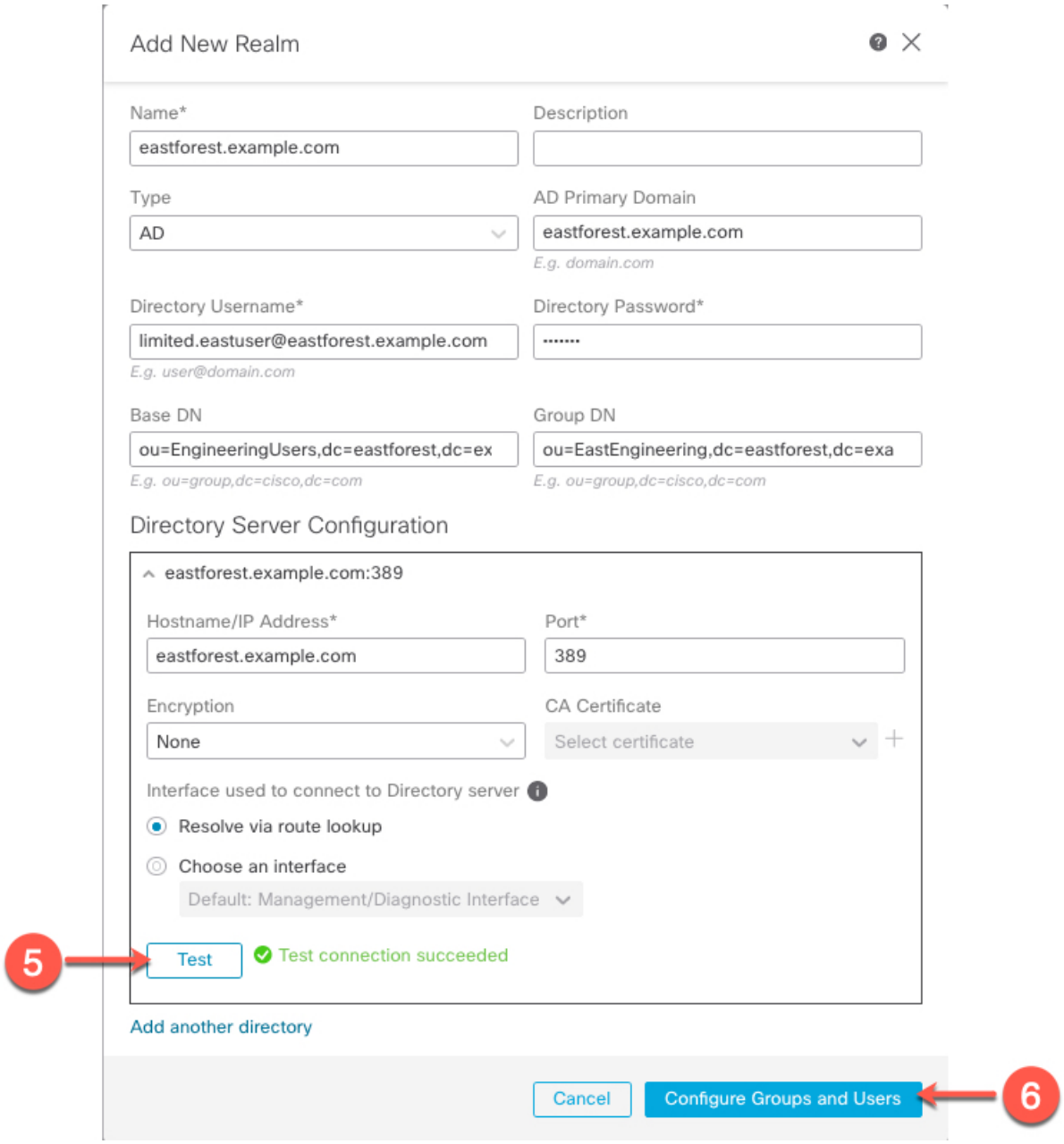
Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 Click **Add Realm** > **Active Directory/LDAP**.

Step 4 Enter the following information to configure **forest.example.com**.



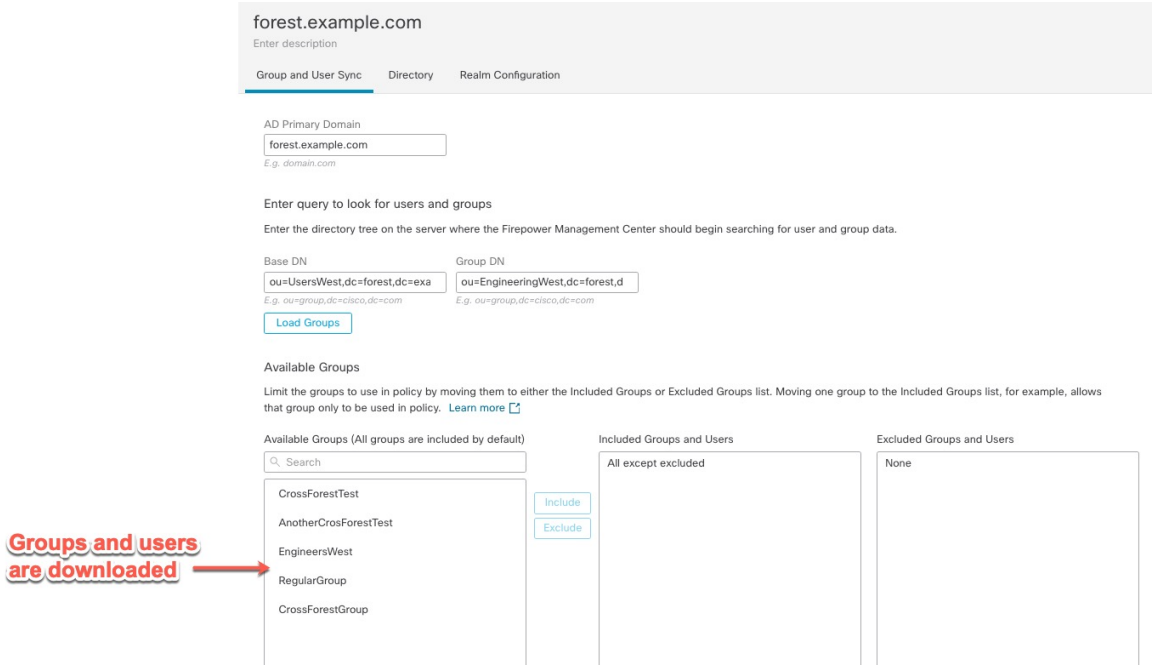
Note The **Directory Username** can be any user in the Active Directory domain; no special permissions are required.

The **Interface used to connect to Directory server** can be any interface that can connect to the Active Directory server.

Step 5 Click **Test** and make sure the test succeeds before you continue.

Step 6 Click **Configure Groups and Users**.

Step 7 Verify your configuration was successful by checking that the next page is displayed similar to the following.



Note If groups and users were not downloaded, verify the values in the **Base DN** and **Groups DN** fields and click **Load Groups**.

There are other optional configurations available on this page; for more information about them, see Realm fields, on page 1844 and Realm directory and synchronize fields, on page 1848.

Step 8 If you made changes on this page or tab pages, click **Save**.

Create another realm

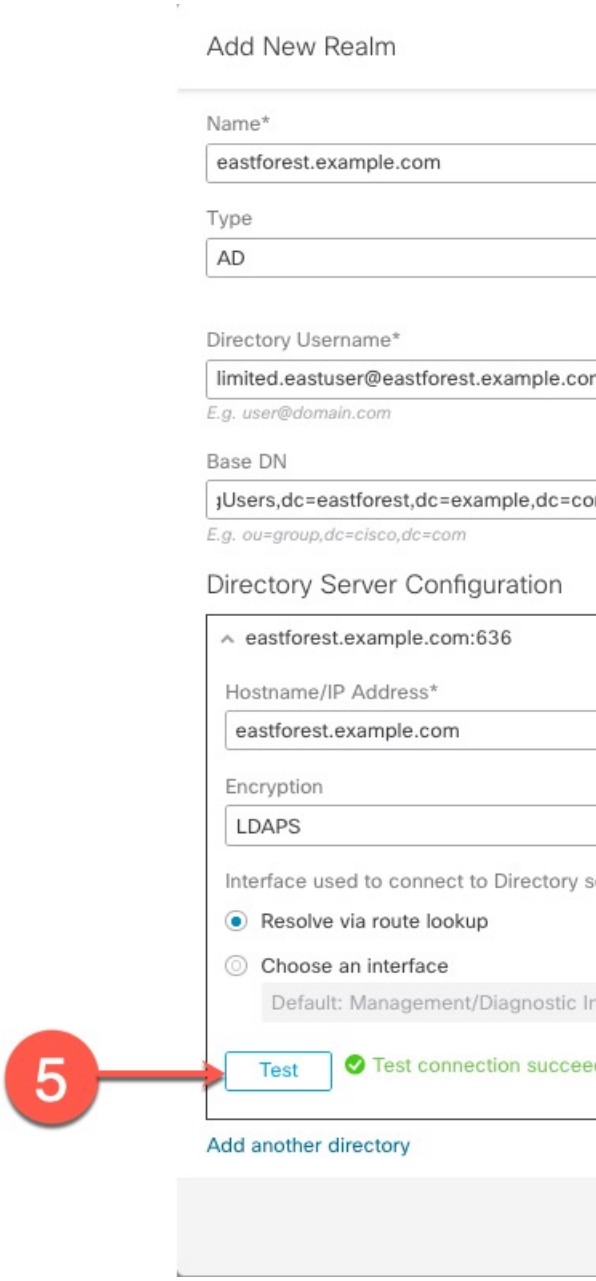
Before you begin

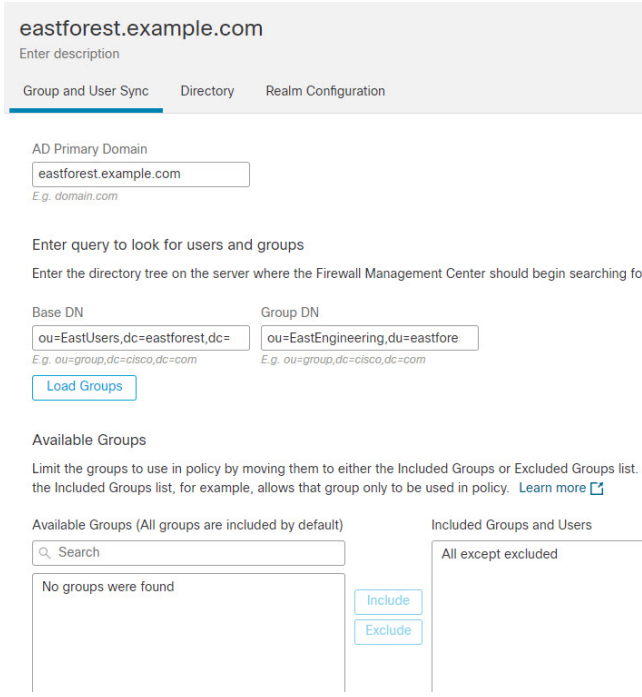
Complete the configuration of your first realm as in the prior task.

Follow these steps to create another realm.

Procedure

	Command or Action	Purpose
Step 1	Click **Integration** > **Other Integrations** > **Realms** > **Realms**.	
Step 2	Click **Add Realm**.	

	Command or Action	Purpose
Step 3	Enter the following information to configure **eastforest.example.com**.	
Step 4	Click **Test** and make sure the test succeeds before you continue.	
Step 5	Click **Configure Groups and Users**.	

	Command or Action	Purpose
Step 6	Verify your configuration was successful by checking that the next page is displayed similar to the following.	

You have successfully configured two realms (**forest.example.com** and **eastforest.example.com**) with their respective directories.

Configure the Secure Firewall Management Center for cross-domain trust Step 2: Synchronize users and groups

This task allows you to download users and groups from Active Directory servers with cross-domain trust relationships to synchronize identity data in the Secure Firewall Management Center and resolve download issues by verifying directory setup and device communication.

After you configure two or more Active Directory servers that have a cross-domain trust relationship, you must download users and groups. That process exposes possible issues with the Active Directory configuration (for example, groups or users downloaded for one Active Directory domain but not the other).

Before you begin

Make sure you have performed the tasks discussed in Configure Secure Firewall Management Center for cross-domain-trust step 1: Configure realms and directories, on page 1869.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 3 At the end of the row of any realm in the cross-domain trust, click **Download Now**( ), then click **Yes**.

Step 4 Click **Check Mark** ( ) (Notifications) > **Tasks**.

If groups and users fail to download, try again. If subsequent attempts fail, review your realm and directory setup as discussed in Realm fields, on page 1844 and Realm directory and synchronize fields, on page 1848.

Step 5 Click **Integration** > **Other Integrations** > **Realms** > **Sync Results**.

Related Topics

Configure the Secure Firewall Management Center for cross-domain trust step 3: Resolve issues, on page 1875

Configure the Secure Firewall Management Center for cross-domain trust step 3: Resolve issues

This task enables you to make sure users and groups are downloaded without errors during cross-domain trust setup.

The final step in setting up cross-domain trust in the Firewall Management Center is to make sure users and groups are downloaded without errors. A typical reason why users and groups do not download properly is that the realms to which they belong have not been downloaded to the Firewall Management Center.

This topic discusses how to diagnose that a group referred in one forest to cannot be downloaded because the realm is not configured to find the group in the domain controller hierarchy.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

In the Realms column, if **Yellow Triangle** ( ) is displayed next to the name of a realm, you have issues that must be resolved. If not, your results are configured properly and you can quit.

Step 3 Download users and groups again from the realms that display issues.

a) Click the **Realms** tab.

b) Click (Download Now), then click **Yes**.

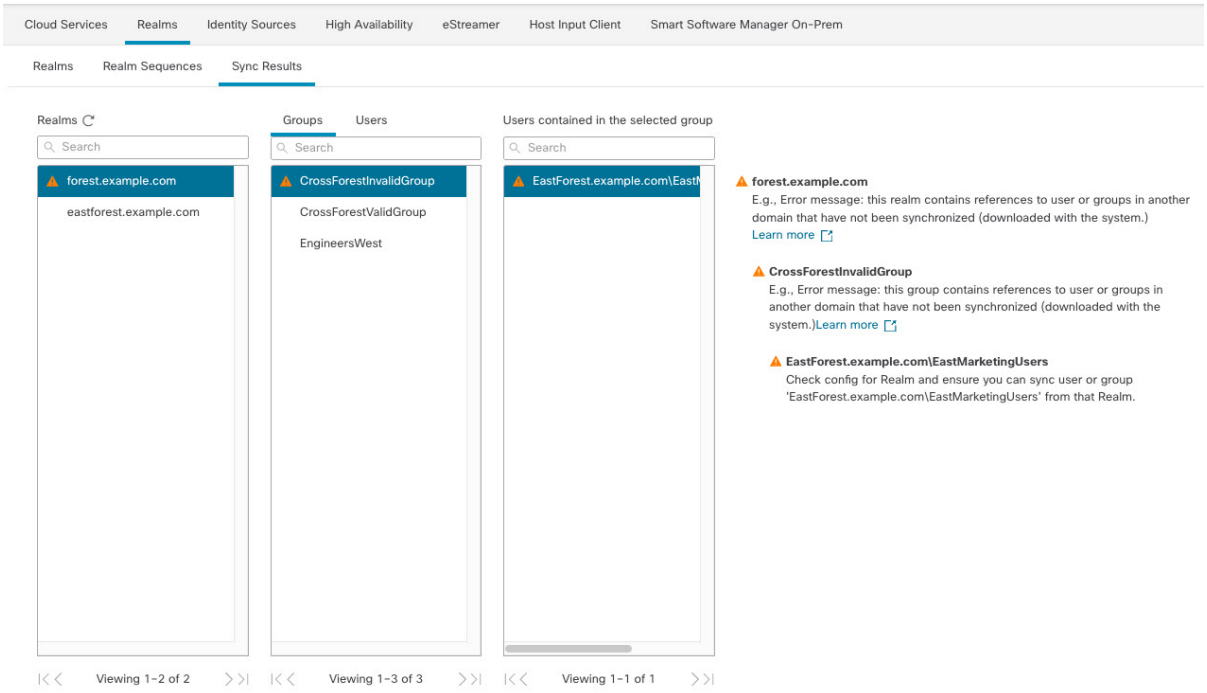
Step 4 Click the **Sync Results** tab page.

If the **Yellow Triangle** ( ) is displayed in the Realms column, click **Yellow Triangle** ( ) next to the realm that has issues.

Step 5 In the middle column, click either **Groups** or **Users** to find more information.

Step 6 In the Groups or Users tab page, click **Yellow Triangle** ( ) to display more information.

The right column should display enough information you can isolate the source of the issue.



In the preceding example, **forest.example.com** includes a cross-domain group **CrossForestInvalidGroup** that contains another group **EastMarketingUsers** that was not downloaded by the Firewall Management Center. If, after synchronizing the **eastforest.example.com** realm again, the error does not resolve, it likely means that the Active Directory domain controller does not include **EastMarketingUsers**.

To resolve this issue, you can:

- Remove the **EastMarketingUsers** from **CrossForestInvalidGroup**, synchronize the **forest.example.com** realm again, and recheck.
- Remove the **ou=EastEngineering** value from the **Group DN** of the **eastforest.example.com** realm, which causes the Firewall Management Center to retrieve groups from the highest level in the Active Directory hierarchy, synchronize **eastforest.example.com**, and recheck.

Manage a realm

This task enables you to perform various maintenance operations on realms to manage authentication and user access control.

This section discusses how to perform various maintenance tasks for a realm using controls on the Realms page:

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 2 To delete a realm, click **Delete** ( ).

Step 3 To edit a realm, click **Edit** ( ) next to the realm and make changes as described in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

Step 4 To enable a realm, slide **State** to the right; to disable a realm, slide it to the left.

Step 5 To download users and user groups, click **Download** ( ).

Step 6 To copy a realm, click **Copy** ( ).

Step 7 To compare realms, see Compare realms, on page 1877.

Compare realms

Use this task to compare identity realms in the Secure Firewall Management Center to review differences between selected realms, generate comparison reports, and analyze changes to support identity integration management.

You must be an Admin, Access Admin, Network Admin, or Security Approver to perform this task.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.

Step 2 Click **Compare Realms**.

Step 3 Choose **Compare Realm** from the **Compare Against** list.

Step 4 Choose the realms you want to compare from the **Realm A** and **Realm B** lists.

Step 5 Click **OK**.

Step 6 To navigate individually through changes, click **Previous** or **Next** above the title bar.

Step 7 (Optional.) Click **Comparison Report** to generate the realm comparison report.

Step 8 (Optional.) Click **New Comparison** to generate a new realm comparison view.

Troubleshoot realms and user downloads

If you notice unexpected server connection behavior, consider tuning your realm configuration, device settings, or server settings. For other related troubleshooting information, see:

- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues, on page 1927
- Troubleshoot the TS agent identity source, on page 1938
- Troubleshoot the captive portal identity source, on page 1906
- Troubleshooting guidelines for remote access VPN identity source, on page 1934
- Troubleshoot user control, on page 1962

Realms and groups reported but not downloaded

The Secure Firewall Management Center's health monitor informs you of user or realm mismatches, which are defined as:

- User mismatch: A user is reported to the Secure Firewall Management Center without being downloaded.

  A typical reason for a user mismatch is that the user belongs to a group you have excluded from being downloaded to the Secure Firewall Management Center. Review the information discussed in *Cisco Secure Firewall Management Center Device Configuration Guide*.

- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firewall Management Center.

For example, if you defined a realm that corresponds to a domain named **domain.example.com** in the Firewall Management Center but a login is reported from a domain named **another-domain.example.com**, this is a *realm mismatch*. Users in this domain are identified by the Firewall Management Center as Unknown.

You set the mismatch threshold as a percentage, above which a health warning is triggered. Examples:

- If you use the default mismatch threshold of 50%, and there are two mismatched realms in eight incoming sessions, the mismatch percentage is 25% and no warning is triggered.
- If you set the mismatch threshold to 30% and there are three mismatched realms in five incoming sessions, the mismatch percentage is 60% and a warning is triggered.

Unknown users that do not match identity rules have no policies applied to them. (Although you can set up identity rules for Unknown users, we recommend keeping the number of rules to a minimum by identifying users and realms correctly.)

For more information, see Detect realm or user mismatches, on page 1881.

Users are not downloaded

Possible causes include:

- If you have the realm **Type** configured incorrectly, users and groups cannot be downloaded because of a mismatch between the attribute the system expects and what the repository provides. For example, if you configure **Type** as **LDAP** for a Microsoft Active Directory realm, the system expects the `uid` attribute, which is set to `none` on Active Directory. (Active Directory repositories use `sAMAccountName` for the user ID.)

  Solution: Set the realm **Type** field appropriately: **AD** for Microsoft Active Directory or **LDAP** for another supported LDAP repository.

- Users in Active Directory groups that have special characters in the group or organizational unit name might not be available for identity policy rules. For example, if a group or organizational unit name

contains the characters asterisk (*), equals (=), or backslash (\), users in those groups are not downloaded and can't be used for identity policies.

Solution: Remove special characters from the group or organizational unit name.



Important To reduce latency between the Firewall Management Center and your Active Directory domain controller, we strongly recommend you configure a realm directory (that is, domain controller) that is as close as possible geographically to the Firewall Management Center.

For example, if your Firewall Management Center is in North America, configure a realm directory that is also in North America. Failure to do so can cause problems such as timeout downloading users and groups.

Not all users in a realm are downloaded

Possible causes include:

- If you attempt to download more than the maximum number of users in any one realm, the download stops at the maximum number of users and a health alert is displayed. User download limits are set per Secure Firewall Management Center model. For more information, see User limits for microsoft active directory, on page 1831.
- Every user must be a member of a group. Users that are members of no groups do not get downloaded.

Access control policy doesn't match group membership

This solution applies to an AD domain that is in a trust relationship with other AD domains. In this discussion, *external domain* means a domain other than the one to which the user logs in.

If a user belongs to a group defined in a trusted external domain, the Secure Firewall Management Center doesn't track membership in the external domain. For example, consider this scenario:

- Domain controllers 1 and 2 trust each other
- Group A is defined on domain controller 2
- User `mparvinder` in controller 1 is a member of Group A

Even though user `mparvinder` is in Group A, the Secure Firewall Management Center access control policy rules specifying membership Group A don't match.

Solution: Create a similar group in domain controller 1 that contains has all domain 1 accounts that belong to group A. Change the access control policy rule to match any member of Group A or Group B.

Access control policy doesn't match child domain membership

If a user belongs to a domain that is child of parent domain, Firepower doesn't track the parent/child relationships between domains. For example, consider this scenario:

- Domain `child.parent.com` is child of domain `parent.com`
- User `mparvinder` is defined in `child.parent.com`

Even though user `mparvinder` is in a child domain, the Firepower access control policy matching the `parent.com` don't match `mparvinder` in the `child.parent.com` domain.

Solution: Change the access control policy rule to match membership in either `parent.com` or `child.parent.com`.

Realm or realm directory test fails

The **Test** button on the directory page sends an LDAP query to the hostname or IP address you entered. If it fails, check these items:

- The **Hostname** you entered resolves to the IP address of an LDAP server or Active Directory domain controller.
- The **IP Address** you entered is valid.

The **Test AD Join** button on the realm configuration page verifies these items:

- DNS resolves the **AD Primary Domain** to an LDAP server or Active Directory domain controller's IP address.
- The **AD Join Username** and **AD Join Password** are correct.

  AD Join Username must be fully qualified (for example, **`administrator@mydomain.com`**, *not* **`administrator`**).
- The user has sufficient privileges to create a computer in the domain and join the Secure Firewall Management Center to the domain as a Domain Computer.

User timeouts are occurring at unexpected times

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your ISE/ISE-PIC server is synchronized with the time on the Secure Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your ISE/ISE-PIC, or TS Agent server is synchronized with the time on the Secure Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

User data for previously-unseen ISE/ISE-PIC users is not displaying in the web interface

After the system detects activity from an ISE/ISE-PIC or TS Agent user whose data is not yet in the database, the system retrieves information about them from the server. In some cases, the system requires additional time to successfully retrieve this information from Microsoft Windows servers. Until the data retrieval succeeds, activity seen by the ISE/ISE-PIC, or TS Agent user is *not* displayed in the web interface.

Note that this can also prevent the system from handling the user's traffic using access control rules.

User data in events is unexpected

If you notice user or user activity events contain unexpected IP addresses, check your realms. The system does not support configuring multiple realms with the same **AD Primary Domain** value.

Users originating from terminal server logins are not uniquely identified by the system

If your deployment includes a terminal server and you have a realm configured for one or more servers connected to the terminal server, you must deploy the Cisco Terminal Services (TS) Agent to accurately report user logins in terminal server environments. When installed and configured, the TS Agent assigns unique ports to individual users so the system can uniquely identify those users in the web interface.

For more information about the TS Agent, see the *Cisco Terminal Services (TS) Agent Guide*.

Detect realm or user mismatches

Detection of realm or user mismatches helps ensure accurate user identification and proper policy application in the Cisco Secure Firewall Management Center.

This section discusses how to detect realm or user *mismatches*, which are defined as:

- User mismatch: A user is reported to the Secure Firewall Management Center without being downloaded.

  A typical reason for a user mismatch is that the user belongs to a group you have excluded from being downloaded to the Secure Firewall Management Center. Review the information discussed in *Cisco Secure Firewall Management Center Device Configuration Guide*.

- Realm mismatch: A user logs into a domain that corresponds to a realm not known to the Firewall Management Center.

For additional details, see Troubleshoot realms and user downloads, on page 1877.

Unknown users that do not match identity rules have no policies applied to them. (Although you can set up identity rules for Unknown users, we recommend keeping the number of rules to a minimum by identifying users and realms correctly.)

Procedure

Step 1 Enable detection of realm or user mismatches:

a. Log in to the Firewall Management Center if you have not already done so.

b. Click **System** (⚙) > **Health** > **Policy**.

c. Create a new health policy or edit an existing one.

d. On the Editing Policy page, set a **Policy Runtime Interval**.

This is the frequency at which all health monitor tasks run.

e. In the left pane, click **Realm**.

f. Enter the following information:

- **Enabled**: Click **On**
- **Warning Users match threshold %**: The percentage of either realm mismatches or user mismatches that triggers a warning in the Health Monitor. For more information, see Troubleshoot realms and user downloads, on page 1877.

g. At the bottom of the page, click **Save Policy & Exit**.

h. Apply the health policy to managed devices as discussed in *Applying Health Policies* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 2 View user and realm mismatches in any of the following ways:

- If the warning threshold is exceeded, click **Warning** > **Health** in the top navigation of the Firewall Management Center. This opens the Health Monitor.
- Click **System** (⚙) > **Health** > **Monitor**.

Step 3 On the Health Monitor page, in the Display column, expand **Realm: Domain** or **Realm: User** to view details about the mismatch.

Troubleshoot cross-domain trust

Troubleshoot user and group synchronization issues in the Secure Firewall Management Center configuration for cross-domain trust. This reference provides information on typical issues, error interpretation, and resolution steps for Active Directory forest synchronization problems.

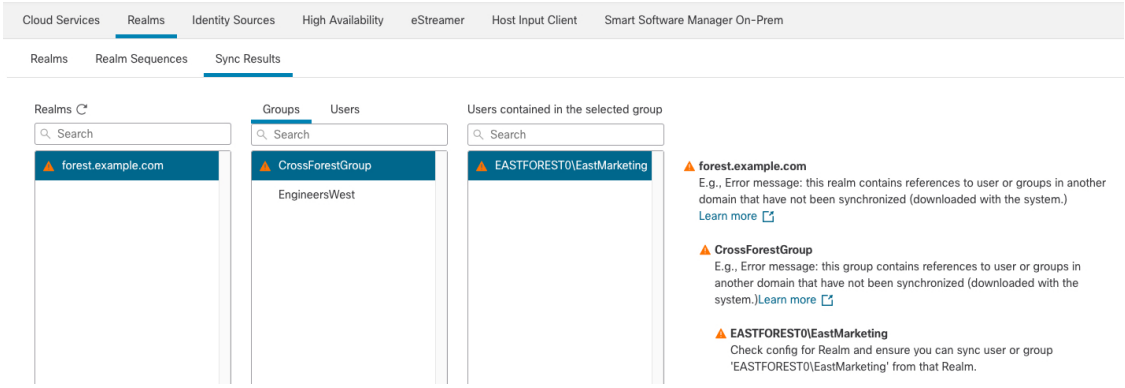
Typical issues

Typical issues with troubleshooting the Secure Firewall Management Center configuration for cross-domain trust include these items:

- Not adding realms or directories for all forests that have shared groups.
- Configure a realm to exclude users from being downloaded and those users are referenced in a group in a different realm.
- Certain temporary issues.

Understand the issues

If there are issues with the Firewall Management Center being able to synchronize users and groups with your Active Directory forests, the Sync Results tab page is displayed similar to this.



This table explains how to interpret the information.

Column	Meaning
Realms	Displays all realms configured in the system. Click **Refresh** ( ) to update the list of realms. **Yellow Triangle** ( ) is displayed to indicate issues in the realm. Nothing is displayed next to a realm if all users and groups synchronized successfully.
Groups	Click **Groups** to display all groups in the realm. As with realms, **Yellow Triangle** ( ) is displayed to indicate issues. Click **Yellow Triangle** ( ) to see more detail about the issue.
Users	Click **Users** to display all users, sorted by group.
Users contained in the selected group	Displays all users in the group you selected in the Groups column. Clicking **Yellow Triangle** ( ) displays more information to the right of the table.
Groups that contain selected user	Displays all groups the selected user belongs to. Clicking **Yellow Triangle** ( ) displays more information to the right of the table.
Error detail information (displayed to the right of the table).	The system displays the NetBIOS forest name and group name it could not synchronize. Typical reasons the system cannot synchronize these users and groups follow: • **Problem**: The forest containing the groups and users do not have corresponding realms configured in the Firewall Management Center. **Solution**: Add a realm for the forest that contains the group as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860. • **Problem**: You excluded groups from being downloaded to the Firewall Management Center. **Solution**: Click the **Realms** tab page, click **Edit** ( ), then move the indicated group or user from the **Excluded Groups and Users** list.

Try downloading users and groups again

If there is a possibility the issues are temporary, download users and groups for all realms.

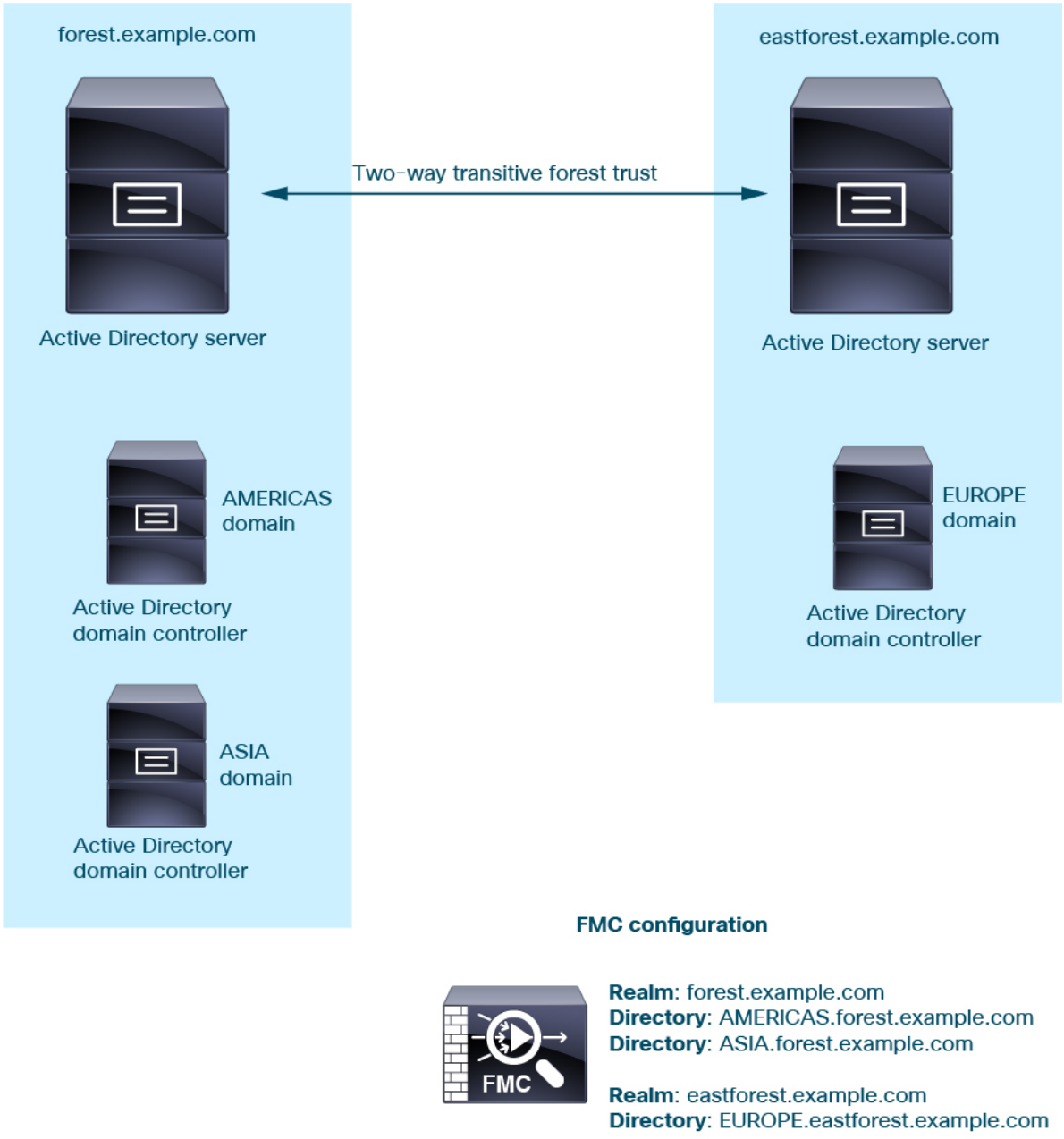
1. If you haven't done so already, log in to the Firewall Management Center.
2. Click **Integration** > **Other Integrations** > **Realms** > **Realms**.
3. Click **Download** ( ).
4. Click the **Sync Results** tab page.
5. If no indicator is displayed for entries in the Realms column, the issues have been resolved.

Add a realm for all forests

Make sure you configured:

- Firewall Management Center realm for each forest that has users you want to use in identity policies.
- Firewall Management Center directory for each domain controller in that forest with users you want to use in identity polices.

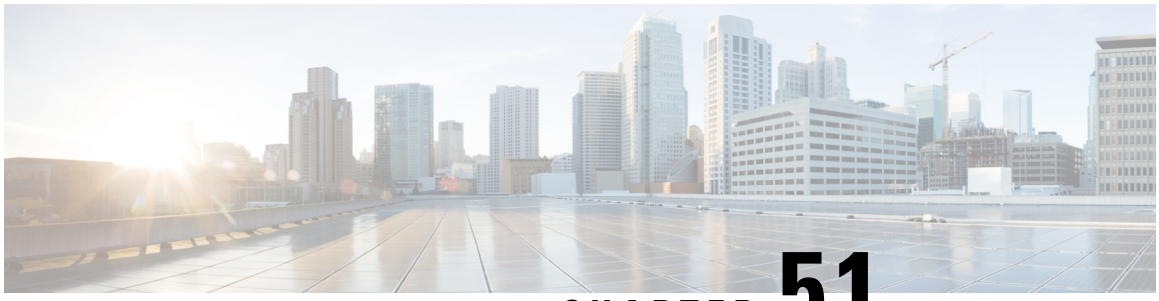
This figure shows an example.



History for realms

This reference provides the version history and implementation details for realm-related features across different versions of the Cisco security platform.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Microsoft Azure Active Directory (AD) realms.	7.4.0	7.4.0	You can use a Microsoft Azure Active Directory (AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: **System** > **Integration** > **Realms** > **Add Realm** > **Azure AD**
Proxy sequences.	7.2.0	7.2.0	Similar to a realm sequence, a proxy sequence is one or more managed devices that can communicate with Security Cloud Control in the event Security Cloud Control cannot communicate with the LDAP or Active Directory server. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Proxy Sequence**
Cross-domain trust for Active Directory domains.	7.2.0	7.0.0	A grouping of Microsoft Active Directory (AD) domains that trust each other is commonly referred to as a *forest*. This trust relationship can enable domains to access each other's resources in different ways. For example, a user account defined in domain A can be marked as a member of a group defined in domain B. The Firewall Management Center can get users from Active Directory forests for identity rules.
Realm sequences.	7.2.0	6.7.0	A *realm sequence* is an ordered list of two or more realms to which to apply identity rules. When you associate a realm sequence with an identity policy, the Firepower System searches the Active Directory domains in order from first to last as specified in the realm sequence. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Realm SequencesSystem** > **Integration** > **Realms** > **Realm Sequences**
Realms for user control.	7.2.0	Any	A realm is a connection between the Firewall Management Center either an Active Directory or LDAP user repository.



CHAPTER 51

Identity Source: Captive Portal

- Captive portal identity source, on page 1887
- License requirements for captive portal, on page 1888
- Requirements and prerequisites for captive portal, on page 1888
- Best practices for captive portal guidelines and limitations, on page 1889
- Configure the captive portal for user control, on page 1891
- Troubleshoot the captive portal identity source, on page 1906
- History for captive portal, on page 1907

Captive portal identity source

A captive portal identity source is an active authentication method that

- presents a login page to users and authenticates HTTP and HTTPS traffic to enable secure access to network resources
- requires authentication to access the internet or to access restricted internal resources
- differs from passive authentication by presenting users with a login page on the managed device rather than querying the authentication realm.

You typically use captive portal to require authentication to access the internet or to access restricted internal resources; you can optionally configure guest access to resources. After the system authenticates captive portal users, it handles their user traffic according to access control rules. Captive portal performs authentication on HTTP and HTTPS traffic only.

Captive portal authentication details

Captive portal is one of the authoritative identity sources supported by the system. Active authentication differs from passive authentication in that the user is presented with a login page by the managed device, whereas passive authentication queries the authentication realm (for example, Microsoft AD) to authenticate the user.

After the system authenticates captive portal users, it handles their user traffic according to access control rules. Captive portal performs authentication on HTTP and HTTPS traffic only. You can optionally configure guest access to resources.

Note HTTPS traffic must be decrypted before captive portal can perform authentication.

Captive portal also records failed authentication attempts. A failed attempt does not add a new user to the list of users in the database. The user activity type for failed authentication activity reported by captive portal is **Failed Auth User**.

The authentication data gained from captive portal can be used for user awareness and user control.

Hostname redirect

A hostname redirect uses the managed device's fully-qualified domain name (FQDN) instead of an IP address for authentication redirections.

(Snort 3 only) An active authentication identity rule redirects to the captive portal port using its configured interface. Because the redirect is typically done to an IP address, the user gets an untrusted certificate error. As this behavior is similar to a man-in-the-middle attack, users might be reluctant to accept the untrusted certificate.

To avoid this problem, you can configure the captive portal to use the managed device's fully-qualified domain name (FQDN). With a properly configured certificate, users will not get an untrusted certificate error, and the authentication will be more seamless and appear to be more secure.

License requirements for captive portal

This reference provides the license requirements for captive portal functionality.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for captive portal

This reference provides the requirements and prerequisites for captive portal implementation.

Supported domains

Any

User roles

- Admin
- Access Admin

- Network Admin

Best practices for captive portal guidelines and limitations

Captive portal and policies

You configure captive portal in your identity policy and invoke active authentication in your identity rules. Identity policies are associated with access control policies and access control policies define access to resources in the network. For example, you might exclude users in the US-West/Finance group to access Engineering servers or you can prohibit users from accessing nonsecure applications on the network.

You configure some captive portal identity policy settings on the identity policy's **Active Authentication** tab page and configure the rest in the identity rule associated with the access control policy.

An active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected. In each case the system transparently enables or disables TLS/SSL decryption, which restarts the Snort process.



Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include a decryption policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

When the captive portal authenticates users that match an identity rule, any user in a Microsoft Active Directory or LDAP group that has not been downloaded is identified as Unknown. To avoid users being identified as Unknown, configure the realm or realm sequence to download users in all groups you expect to authenticate with captive portal. Unknown users are handled according to the associated access control policy; if the access control policy is configured to block Unknown users, these users are blocked.

To make sure the system downloads all users in a realm or realm sequence, make sure the groups are in the Available Groups list in the realm's configuration.

Microsoft Azure AD SAML realm configuration

To use a Microsoft Azure AD (SAML) realm as a captive portal, see Create a Microsoft Azure AD (SAML) realm for active authentication (captive portal).

Routed interface requirements

Ensure that captive portal active authentication is performed only by a device with a routed interface configured. If you are configuring an identity rule for captive portal and your captive portal device contains inline and routed interfaces, you must configure interface rule conditions in the access control policy to target only the routed interfaces on the device.

If the identity policy associated with your access control policy contains one or more captive portal identity rules and you deploy the policy on the Secure Firewall Management Center that manages one or more devices with routed interfaces configured, the policy deployment succeeds and the routed interfaces perform active authentication.

For more information about synchronizing users and groups, see Synchronize users and groups, on page 1865.

Required certificates and certificate authorities

Before you can use the captive portal for user control and awareness, you must have all of the following:

- To authenticate with Microsoft AD, export the server's root certificate and import it into the Secure Firewall Management Center as a trusted CA certificate.
- An internal certificate object for authenticating with the managed device to which the identity policy is deployed.
- An internal certificate authority for the required decryption rule.

Captive portal requirements and limitations

Note the requirements and limitations when configuring captive portal:

- Captive portal does not support HTTP/3 QUIC connections.
- The system supports up to 20 captive portal logins per second.
- A failed login attempt is counted toward the maximum login attempts only if it occurs within five minutes of the previous failed attempt. The five minute limit is not configurable.

  Connection events show the number of maximum login attempts. To view connection events, click **Analysis** > **Unified Events**.

  If more than five minutes elapse between failed logins, the user is redirected to captive portal for authentication and will not be designated a failed login user or a guest user, and will not be reported to the Secure Firewall Management Center.
- Captive portal does not negotiate TLS v1.0 connections. Only TLS v1.1, v1.2, and TLS 1.3 connections are supported.
- To securely log a user out of captive portal and prevent the user from logging in again, an administrator can close their session: **Analysis** > **Users heading** > **Active Sessions**. If the user closes their browser, the browser does not reauthenticate automatically.
- If a realm is created for a parent domain and the managed device detects a login to a child of that parent domain, the user's subsequent logout is not detected by the managed device.
- To limit the amount of non-HTTP or HTTPS traffic that is allowed through the managed device, you should enter typical HTTP and HTTPS ports in the identity policy's **Ports** tab page.
- Your access control rule must allow traffic destined for the IP address and port of the device you plan to use for captive portal.
- To perform captive portal active authentication on HTTPS traffic, you must use a decryption policy to decrypt the traffic from the users you want to authenticate. You cannot decrypt the traffic in the connection between a captive portal user's web browser and the captive portal daemon on the managed device; this connection is used to authenticate the captive portal user.
- The managed device changes a previously unseen user from **`Pending`** to **`Unknown`** when it determines that the incoming request does not use the HTTP or HTTPS protocol. As soon as the managed device changes a user from **`Pending`** to another state, access control, Quality of Service, and decryption policies can be applied to that traffic. If your other policies don't permit non-HTTP or HTTPS traffic, configuring ports on the captive portal identity policy can prevent undesired traffic from being allowed through the managed device.

Kerberos prerequisites

If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.

Configure the captive portal for user control

Configure captive portal active authentication to enable user authentication through the portal by setting up the necessary components and associating them with access control policies.

To use the captive portal for active authentication, you must set up an LDAP realm; or a Microsoft AD realm or realm sequence; Microsoft Azure AD (SAML) realm; access control policy; an identity policy; a decryption policy; and associate the identity and decryption policies with the same access control policy. Finally, you must deploy the policies to managed devices. This topic provides a high-level summary of those tasks.

Note Microsoft Azure Active Directory is not supported for captive portal.

Before you begin

Perform these tasks first:

- Confirm that your Secure Firewall Management Center manages one or more devices with a *routed* interface configured.
- To use encrypted authentication with the captive portal, either create a PKI object for the authenticating managed device or have your certificate data and key available on the machine from which you're accessing the Secure Firewall Management Center. To create a PKI object, see PKI objects, on page 2389.

Follow these steps to configure the captive portal for user control:

Procedure

Step 1 Create and enable an LDAP realm; or a Microsoft AD realm and optionally realm sequence as discussed in these topics:

- Create an LDAP realm or an Active Directory realm and realm directory, on page 1860
- Synchronize users and groups, on page 1865

To make sure the system downloads all users in a realm or realm sequence, make sure the groups are in the Available Groups list in the realm's configuration.

For more information, see Synchronize users and groups, on page 1865.

Step 2 Get required certificates and certificate authorities.

You must have all of these:

- To authenticate with Microsoft AD, export the server's root certificate and import it into the Secure Firewall Management Center as a trusted CA certificate.
- An internal certificate object for authenticating with the managed device to which the identity policy is deployed.
- An internal certificate authority for the required decryption rule.

Step 3 Create a network object with an associated trusted certificate authority.

See Create a network object, on page 1892.

Step 4 Create identity policy with an active authentication rule.

The identity policy enables selected users in your realm access resources after authenticating with the captive portal.

For more information, see Create an identity policy and active authentication rule, on page 1894.

Step 5 Configure an access control rule for the captive portal that allows traffic on the captive portal port (by default, TCP 885).

You can choose any available TCP port for the captive portal to use. Whatever your choice, you must create a rule that allows traffic on that port.

For more information, see Create a TCP port access control rule, on page 1896.

Step 6 Add another access control rule to allow users in the selected realm or realm sequence to access resources using the captive portal.

For more information, see Create a user access control rule, on page 1898.

Step 7 Configure a decryption policy with a **Decrypt - Resign** rule for the **Unknown** user so captive portal users can access web pages using the HTTPS protocol.

The captive portal can authenticate users only if the HTTPS traffic is decrypted before the traffic is sent to the captive portal. The captive portal itself is seen by the system as the **Unknown** user.

Create a decryption policy with an outbound rule, on page 1899

Step 8 Associate the identity and decryption policies with the access control policy from step 3.

This final step enables the system to authenticate users with the captive portal.

For more information, see Associate Identity and decryption policies with the access control policy, on page 1903.

What to do next

See Create a network object, on page 1892.

Create a network object

Create a network object to enable access using a fully qualified domain name for captive portal authentication.

This task discusses how to start configuring the captive portal as an identity source.

Before you begin

(Snort 3 only.) Create a fully-qualified host name (FQDN) using your DNS server and upload the Firewall Threat Defense's internal certificate to the Firewall Management Center. You can consult a resource such as this one if you've never done it before. Specify the IP address of a routed interface on one of the devices managed by your Firewall Management Center.

For more information about the network object, see Redirect to host name network rule conditions, on page 1946.

Procedure

Step 1 If you haven't already done so, log in to your Firewall Management Center and click **Objects** > **Object Management**..

Step 2 Expand **PKI**.

Step 3 Click **Internal Certs**.

Step 4 Click **Add Internal Cert**.

a) In the **Name** field, enter a name to identify the internal cert (for example, **`MyCaptivePortal`**).

b) In the **Certificate Data** field, either paste the certificate or use the **Browse** button to locate it.

The certificate Common Name must exactly match the FDQN with which you want captive portal users to authenticate.

c) In the **Key** field, either paste the certificate's private key or use the **Browse** button to locate it.

d) If the certificate is encrypted, select the **Encrypted** check box and enter the password in the adjacent field.

e) Click **Save**.

Step 5 Click **Network**.

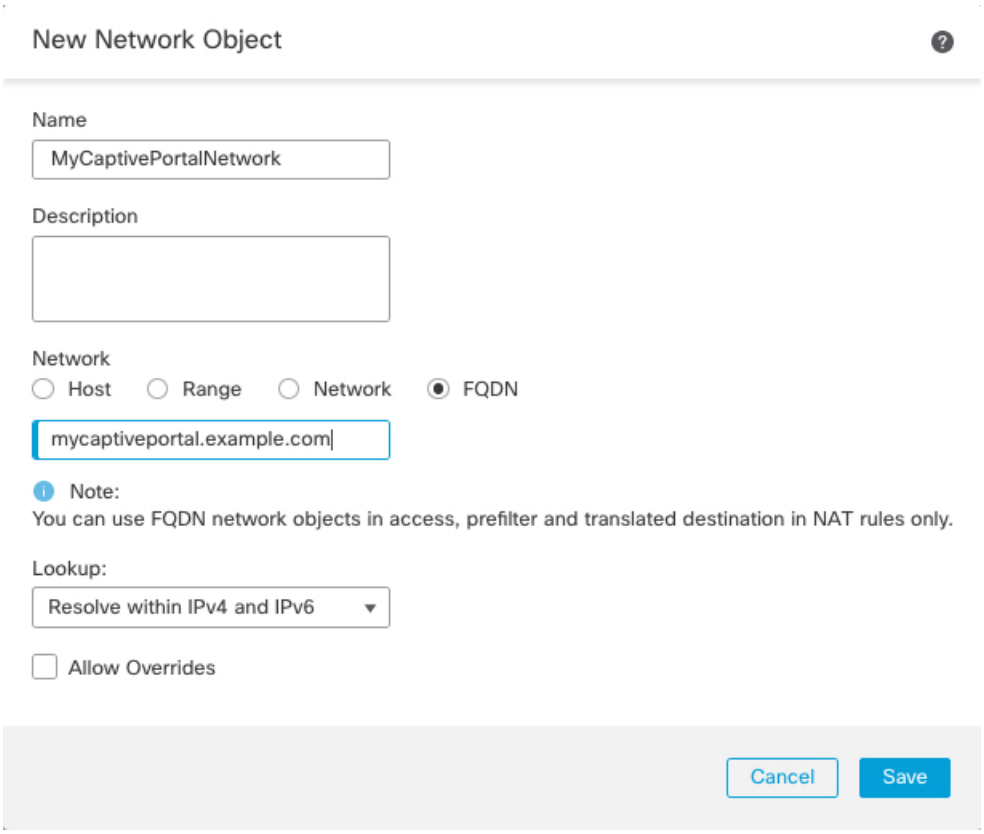
Step 6 Click **Add Network** > **Add Object**.

a) In the **Name** field, enter a name to identify the object (for example, **`MyCaptivePortalNetwork`**).

b) Click **FDQN** and, in the field, enter the name of the captive portal's FDQN.

c) Click an option for **Lookup**.

The following figure shows an example.



d) Click **Save**.

What to do next

Create an identity policy and active authentication rule, on page 1894.

Create an identity policy and active authentication rule

This procedure enables captive portal to perform active authentication for users in your domains using the Secure Firewall Management Center.

This multi-part procedure shows how to set up the captive portal using the default TCP port 885 and using a Secure Firewall Management Center server certificate for both the captive portal and for TLS/SSL decryption. Each part of this example explains one task required to enable the captive portal to perform active authentication.

If you follow all the steps in this procedure, you can configure captive portal to work for users in your domains. You can optionally perform additional tasks, which are discussed in each part of the procedure.

For an overview of the entire procedure, see Configure the captive portal for user control, on page 1891.

Procedure

Step 1 In the Firewall Management Center, click **Policies** > **Access Control heading** > **Identity** and create or edit an identity policy.

Step 2 (Optional.) Click **Add Category** to add a category for the captive portal identity rules and enter a **Name** for the category.

Step 3 Click the **Active Authentication** tab.

a) Choose the appropriate *root* **Server Certificate** from the list or click **Add** (+) to add a certificate.

For more information, see Connect securely to Active Directory or LDAP, on page 1862.

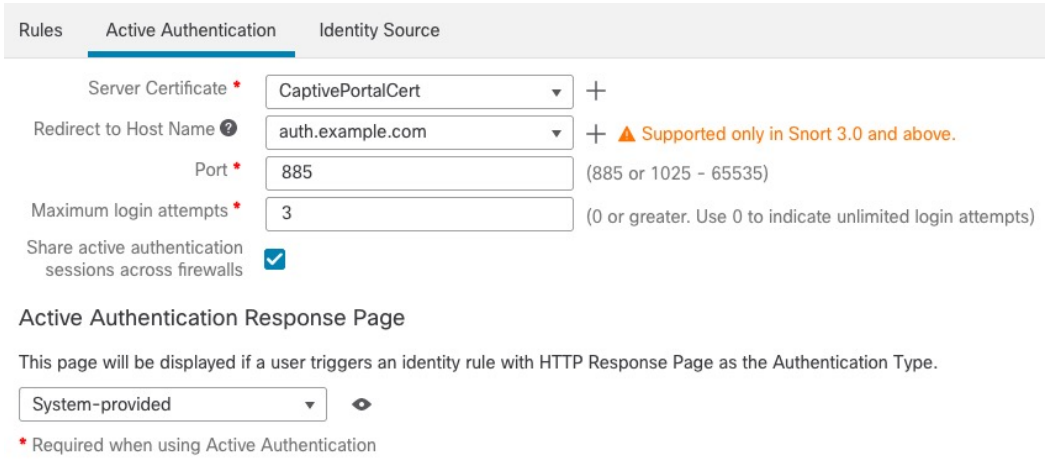
Note Captive portal does *not* support the use of Digital Signature Algorithm (DSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates.

b) From the **Redirect to Host Name** field, click the network object you previously created or click **Add** (+).

c) Enter **885** in the **Port** field and specify the **Maximum login attempts**.

d) Uncheck **Share active authentication across firewalls** to enable the Firewall Management Center to require users to reauthenticate every time they access your network using a different managed device than the last time.
For more information about this option, see Captive portal fields, on page 1903.

e) (Optional.) Choose an **Active Authentication Response Page** as described in Captive portal fields, on page 1903.



f) (If you upgraded to version 7.4.1 from an earlier version only and you authenticate users with a realm sequence.) Click **Edit** (✎) and see Update a custom authentication form, on page 1896.

Step 4 Click **Save**.

Step 5 Click the **Rules** tab.

Step 6 Click **Add Rule** to add a new captive portal identity policy rule, or click **Edit** (✎) to edit an existing rule.

In the **Add Rule** page,

a) Enter a **Name** for the rule.
b) From the **Action** list, choose **Active Authentication**.
c) Click **Realm & Settings**.
d) From the **Realms** list, choose a realm or realm sequence to use for user authentication
e) (Optional.) Check **Identify as Guest if authentication cannot identify user**. For more information, see Captive portal fields, on page 1903.
f) Choose an **Authentication Protocol** from the list.

   You *cannot* authenticate users with a realm sequence if you choose **NTLM**, **Kerberos**, or **HTTP Negotiate** authentication protocols. Choose **HTTP Basic** or **HTTP Response Page** instead.

g) (Optional.) To exempt specific application traffic from captive portal, see Exclude applications from captive portal, on page 1905.
h) Add conditions to the rule (port, network, and so on) as discussed in Identity rule conditions, on page 1945.
i) Click **Add**.

Step 7 At the top of the page, click **Save**.

What to do next

Continue with Create a TCP port access control rule, on page 1896.

Update a custom authentication form

Allow users to see a list of domains when they authenticate with captive portal by adding a custom realm selection to your authentication form.

After you upgrade to version 7.4.1 (or later) from an earlier release, you must update custom authentication forms for users to see available domains during authentication. This task is always required if you use the HTTP Response Page authentication type; if users authenticate with a realm using another authentication type, this task is optional.

Procedure

Step 1 On the **Active Authentication** tab page of your identity rule, click **Edit** ( ).

Step 2 Enter the following code in the part of the form that requires the user to log in:

Example:

```
<select name="realm" id="realm"></select>
```

Users can now view and select from available domains during captive portal authentication.

Create a TCP port access control rule

Create an access control rule that allows the captive portal to communicate with clients using TCP port 885, enabling secure user authentication.

This part of the procedure shows how to create an access control rule that allows the captive portal to communicate with clients using TCP port 885, which is the captive portal's default port. You can choose another port if you wish, but the port must match the one you chose in Create an identity policy and active authentication rule, on page 1894.

Before you begin

For an overview of the entire captive portal configuration, see Configure the captive portal for user control, on page 1891.

Follow these steps to create a TCP port access control rule:

Procedure

Step 1 Log in to the Firewall Management Center if you have not already done so.

If you haven't done so already, create a certificate for the captive portal as discussed in PKI objects, on page 2389.

Step 2 Click **Policies** > **Access Control heading** > **Access Control** and create or edit an access control policy.

Step 3 Click **Add Rule**.

Step 4 Enter a **Name** for the rule.

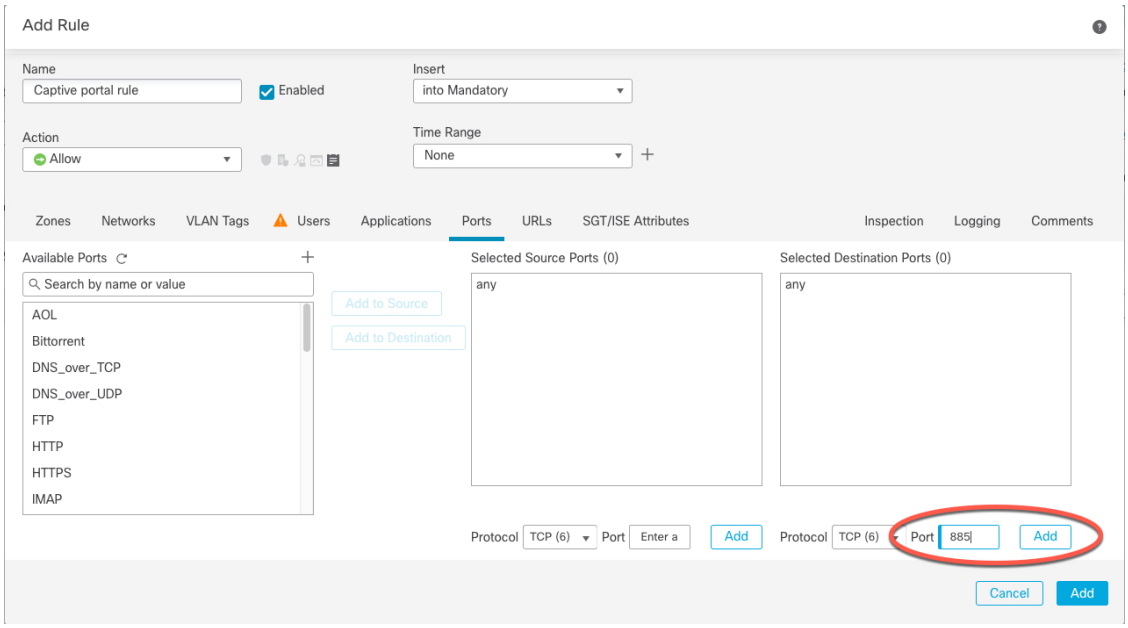
Step 5 Choose **Allow** from the **Action** list.

Step 6 Click **Ports**.

Step 7 From the **Protocol** list under the **Selected Destination Ports** field, choose **TCP**.

Step 8 In the **Port** field, enter **885** and click **Add** next to the **Port** field.

The following figure shows an example.



Step 9 Click **Add** at the bottom of the page.

What to do next

Continue with Create a user access control rule, on page 1898.

Create a user access control rule

Configure an access control rule to allow users in a specified realm to authenticate using captive portal, then adjust rule order in the policy editor to optimize traffic handling and resource use.

This part of the procedure discusses how to add an access control rule that enables users in a realm to authenticate using captive portal.

Before you begin

For an overview of the entire captive portal configuration, see Configure the captive portal for user control, on page 1891.

Procedure

Step 1 In the rule editor, click **Add Rule**.

Step 2 Enter a **Name** for the rule.

Step 3 Choose **Allow** from the **Action** list.

Step 4 Click **Users**.

Step 5 In the **Available Realms** list, click the realms to allow.

If no realms display, click **Refresh** ( ).

Step 6 In the **Available Users** list, choose the users to add to the rule and click **Add to Rule**.

Step 7 (Optional.) Add conditions to the access control policy as discussed in Identity rule conditions, on page 1945.

Step 8 Click **Add**.

Step 9 On the access control rule page, click **Save**.

In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption

What to do next

Create a decryption policy with an outbound rule, on page 1899

Create a decryption policy with an outbound rule

Create a decryption policy to decrypt and resign outbound traffic before captive portal authentication in the Secure Firewall Management Center.

This part of the procedure discusses how to create a decryption policy to decrypt and resign traffic before the traffic reaches the captive portal. The captive portal can authenticate traffic only after it has been decrypted.

Before you begin

You must have an internal certificate authority (CA) for your outbound server; in other words, the managed device that decrypts the traffic for captive portal users to authenticate. This certificate must be different from the *internal certificate* you use to authenticate the captive portal with the managed device.

Procedure

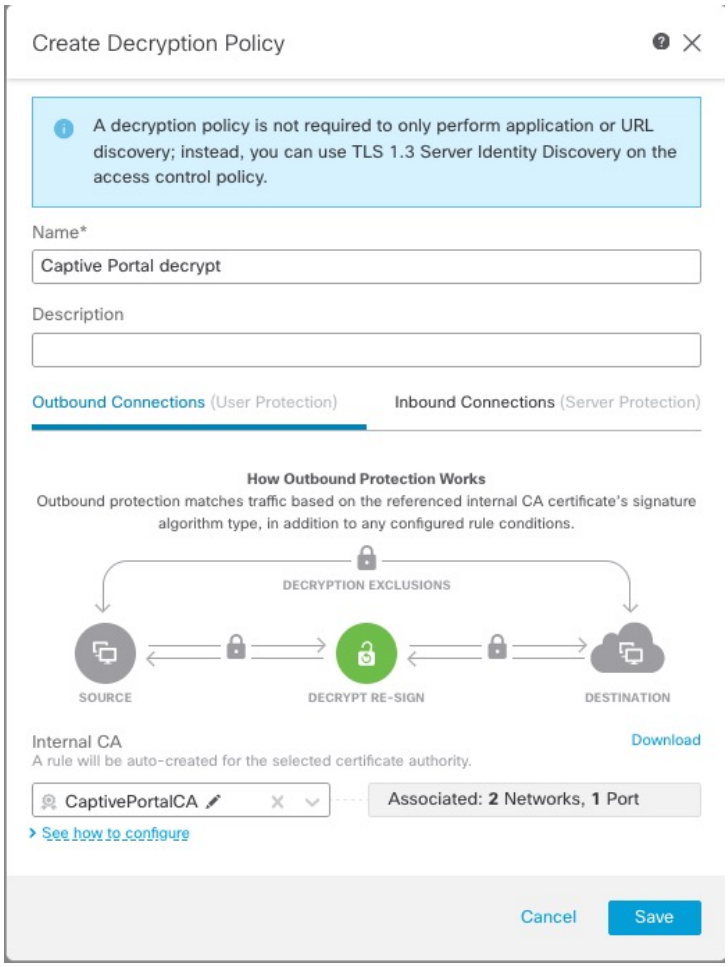
Step 1 Log in to the Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

Step 3 Click **New Policy**.

Step 4 Give the policy a unique **Name** and, optionally, a **Description**.

Step 5 Click the **Outbound Connections** tab.



Step 6 Upload or choose certificates for the rules.

The system creates one rule per combination of CA and networks/ports.

Step 7 (Optional.) Choose networks and ports.

For more information:

- Decryption Rule conditions, on page 1758
- Network rule conditions, on page 1321
- Best practice: use application-based rules over port-based rules, on page 1323

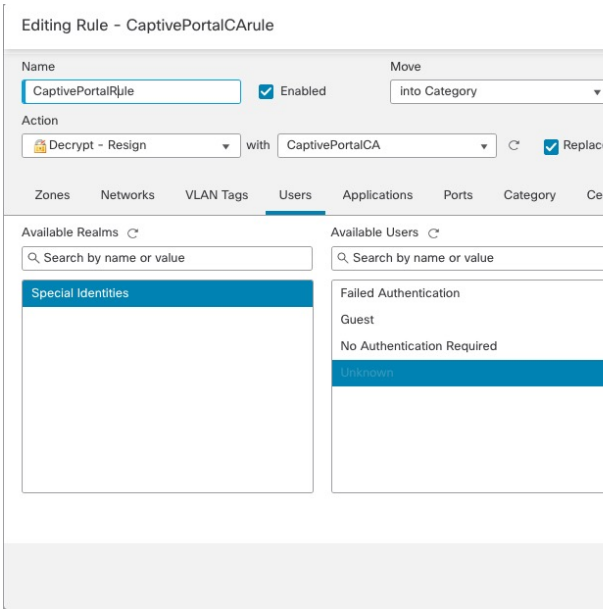
Step 8 Click **Save**.

What to do next

Configure the decryption rule.

Configure a decryption rule

Procedure

	Command or Action	Purpose
Step 1	Click **Edit** ( ) next to the decryption policy you just created.	
Step 2	Click **Edit** ( ) next to the decryption rule for captive portal.	
Step 3	Click **Users**.	
Step 4	Above the **Available Realms** list, click **Refresh** ( ).	
Step 5	In the **Available Realms** list, click **Special Identities**.	
Step 6	In the **Available Users** list, click **Unknown**.	
Step 7	Click **Add to Rule**.	The following figure shows an example. 
Step 8	(Optional.) Set other options as discussed in Decryption Rule conditions, on page 1758.	
Step 9	Click **Add**.	

Create A decryption policy with a Decrypt-Resign rule

Create a decryption policy to decrypt and resign traffic before the traffic reaches the captive portal.

This part of the procedure discusses how to create a decryption policy to decrypt and resign traffic before the traffic reaches the captive portal. The captive portal can authenticate traffic only after it has been decrypted.

Before you begin

For an overview of the entire captive portal configuration, see Configure the captive portal for user control, on page 1891.

Follow these steps to create A decryption policy with a Decrypt-Resign rule:

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center and create a certificate object to decrypt TLS/SSL traffic as discussed in PKI objects, on page 2389.

Step 2 Click **Policies** > **Access Control heading** > **Decryption**.

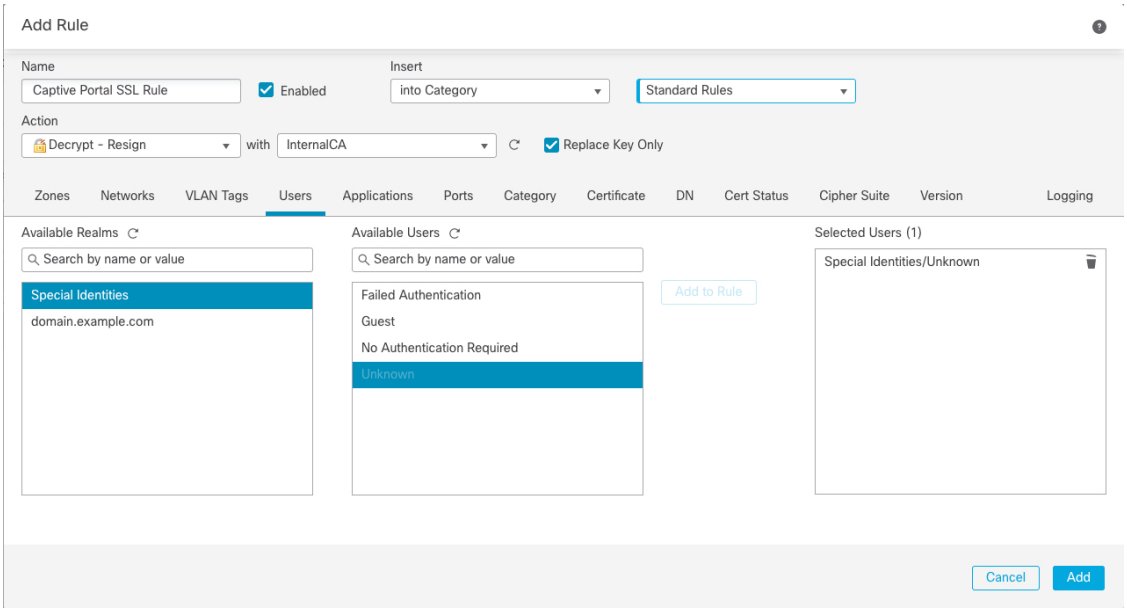
Step 3 Click **New Policy**.

Step 4 Enter a **Name** and choose a **Default Action** for the policy. Default actions are discussed in Decryption policy default actions, on page 1739.

Step 5 Click **Save**.

Step 6 Click **Add Rule**.

a) Enter a **Name** for the rule.
b) From the **Action** list, choose **Decrypt - Resign**.
c) From the **with** list, choose your PKI object.
d) Under the **Users** tab, refresh the **Available Realms**list by clicking **Refresh** ( ).
e) In the **Available Realms** list, click **Special Identities**.
f) In the **Available Users** list, click **Unknown**.
g) Click **Add to Rule**.
The following figure shows an example.



Step 7 (Optional.) Set other options as discussed in Decryption Rule conditions, on page 1758.

Step 8 Click **Add**.

Step 9 At the top of the page, click **Save**.

What to do next

Associate the identity and decryption policies with the access control policy from step 3.

This final step enables the system to authenticate users with the captive portal.

For more information, see Associate Identity and decryption policies with the access control policy, on page 1903.

Associate Identity and decryption policies with the access control policy

Associate the identity policy and TLS/SSL **Decrypt - Resign** rule with your access control policy to enable captive portal authentication.

This part of the procedure discusses how to associate the identity policy and TLS/SSL **Decrypt - Resign** rule with the access control policy you created earlier. After this, users can authenticate using the captive portal.

For an overview of the entire captive portal configuration, see Configure the captive portal for user control, on page 1891.

Procedure

Step 1 Click **Policies** > **Access Control heading** > **Access Control** and edit the access control policy you created as discussed in Create a TCP port access control rule, on page 1896. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 2 Either create a new access control policy or edit an existing policy.

Step 3 At the top of the page, click the word **Identity**.

Step 4 From the list, choose the name of your identity policy and, at the top of the page, click **Save**.

Step 5 Repeat the preceding steps to associate your captive portal decryption policy with the access control policy.

Step 6 If you haven't done so already, target the policy at managed devices as discussed in Assign access control policy to devices, on page 1583.

What to do next

- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes, on page 135.
- Monitor user activity as discussed in *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide*.

Captive portal fields

Use these fields to configure captive portal on the **Active Authentication** tab page of your identity policy. See also Identity rule fields, on page 1953 and Exclude applications from captive portal, on page 1905.

Server Certificate

An internal certificate presented by the captive portal daemon.

Note Captive portal does *not* support the use of Digital Signature Algorithm (DSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates.

Port

The port number to use for the captive portal connection. You must set up your access control rule with a TCP port to use for the captive portal, then associate the identity policy with that access control policy. For more information, see Create a TCP port access control rule, on page 1896.

Maximum login attempts

The maximum allowed number of failed login attempts before the system denies a user's login request.

Share active authentication sessions across firewalls

Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option.

- (Default, which continues previous behavior.) Check the box to allow users to authenticate with any managed device associated with the active authentication identity rule.
- Uncheck the box to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. Use this option if your organization requires authentication per location or site and a managed device is deployed per site.

Managed devices are either clustered or are in a high availability pair act as if they are the same device; in particular,

- Managed devices in the same cluster or high availability pair: Saves the user session to maintain consistency across the pair. On failover, the secondary has the current user session data.
- Managed devices in a different cluster or high availability pair: User session data is not shared with and therefore not stored on these devices.

Active Authentication Response Page

The system-provided or custom HTTP response page you want to display to captive portal users. After you select an **Active Authentication Response Page** in your identity policy active authentication settings, you also must configure one or more identity rules with **`HTTP Response Page`** as the **Authentication Protocol**.

The system-provided HTTP response page includes **Username** and **Password** fields, a list of realms if you chose to authenticate with a realm sequence, as well as a **Login as guest** button to allow users to access the network as guests. To display a single login method, configure a custom HTTP response page.

An example of what users see when logging in with a response page is shown in Create a sample identity policy with an active authentication rule, on page 1956.

Choose these options:

- To use a generic response, click **System-provided**. You can click **View** ( ) to view the HTML code for this page.
- To create a custom response, click **Custom**. A window with system-provided code is displayed that you can replace or modify. When you are done, save your changes. You can edit a custom page by clicking **Edit** ( ).

Exclude applications from captive portal

This task allows you to exempt specific applications from captive portal active authentication, enabling their traffic to pass through the identity policy without requiring authentication.

You can select applications (identified by their HTTP `User-Agent` strings) and exempt them from captive portal active authentication. This allows traffic from the selected applications to pass through the identity policy without authenticating.

Note Only applications with the **`User-Agent Exclusion` Tag** are displayed in this list.

Before you begin

Follow these steps to exclude applications from captive portal authentication:

Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Edit the identity policy that contains the captive portal rule.

Step 4 On **Realm & Settings** tab page, expand **HTTP User Agent Exclusions**.

- In the first column, select the check box next to each item to filter applications, then one or more applications, and click **Add to Rule**.

  Check boxes are ANDed together.
- To narrow the filters that are displayed, type a search string in the **Search by name** field; this is especially useful for categories and tags. To clear the search, click **Clear** ( ).
- To refresh the filters list and clear any selected filters, click **Reload** ( ).

Note The list displays 100 applications at a time.

Step 5 Choose the applications that you want to add to the filter from the **Available Applications** list:

- To narrow the individual applications that appear, enter a search string in the **Search by name** field. To clear the search, click **Clear** ( ).

- Use paging at the bottom of the list to browse the list of individual available applications.
- To refresh the applications list and clear any selected applications, click **Reload** ( ).

Step 6 Add the selected applications to exclude from external authentication. You can click and drag, or you can click **Add to Rule**. The result is the combination of the application filters you selected.

What to do next

- Continue configuring the identity rule as described in Create an identity rule, on page 1952.

Troubleshoot the captive portal identity source

For other related troubleshooting information, see Troubleshoot realms and user downloads, on page 1877 and Troubleshoot user control, on page 1962.

If you experience issues with captive portal, check these items:

- The time on your captive portal managed device must be synchronized with the time on the Firewall Management Center.
- If you have DNS resolution configured and you create an identity rule to perform **`Kerberos`** (or **`HTTP Negotiate`**, if you want Kerberos as an option) captive portal, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the hostname you provided when configuring DNS.

  For more information, see Hostname redirect, on page 1888.
- If you're using Kerberos authentication, the managed device's host name must be less than 15 characters (it's a NetBIOS limitation set by Windows); otherwise, captive portal authentication fails. You set the managed device host name when you set up the device. For more information, see an article like this one on the Microsoft documentation site: Naming conventions in Active Directory for computers, domains, sites, and OUs.

  DNS must return a response of 64KB or less to the hostname; otherwise, the AD connection test fails. This limit applies in both directions and is discussed in RFC 6891 section-6.2.5.
- If the device you want to use for captive portal contains both inline and routed interfaces, you must configure a zone condition in your captive portal identity rules to target only the routed interfaces on the captive portal device.
- If the captive portal is configured correctly but the redirect to an IP address or fully-qualified domain name (FQDN) fails, disable endpoint security software. This type of software can interfere with the redirection.
- The ERR_CONNECTION_TIMED_OUT error during active authentication occurs when the redirect URL fails to resolve to the managed device's IP address. This error could prevent the client from receiving a user authentication prompt after redirection, cause client traffic on port 885 to be missing from managed device packet captures, or lead to other connection issues. To mitigate connection issues, ensure that the redirect URL resolves to the managed device's IP address on the client's ingress path, where active portal

authentication is configured. Verify the configuration by using the `system support captive-portal-debug` command.

- To securely log a user out of captive portal and prevent the user from logging in again, an administrator can close their session: **Analysis** > **Users heading** > **Active Sessions**. If the user closes their browser, the browser does not reauthenticate automatically.
- If you select **`Kerberos`** (or **`HTTP Negotiate`**, if you want Kerberos as an option) as the **Authentication Type** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.

  If you select **`HTTP Basic`** as the **Authentication Type** in an identity rule, users on your network might not notice their sessions time out. Most web browsers cache the credentials from **`HTTP Basic`** logins and use the credentials to seamlessly begin a new session after an old session times out.
- If the connection between your Firewall Management Center and a managed device fails, no captive portal logins reported by the device can be identified during the downtime, unless the users were previously seen and downloaded to the Firewall Management Center. The unidentified users are logged as Unknown users on the Firewall Management Center. After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.
- Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, see RFC 959.

  When the captive portal authenticates users that match an identity rule, any user in a Microsoft Active Directory or LDAP group that has not been downloaded is identified as Unknown. To avoid users being identified as Unknown, configure the realm or realm sequence to download users in all groups you expect to authenticate with captive portal. Unknown users are handled according to the associated access control policy; if the access control policy is configured to block Unknown users, these users are blocked.

  To make sure the system downloads all users in a realm or realm sequence, make sure the groups are in the Available Groups list in the realm's configuration.

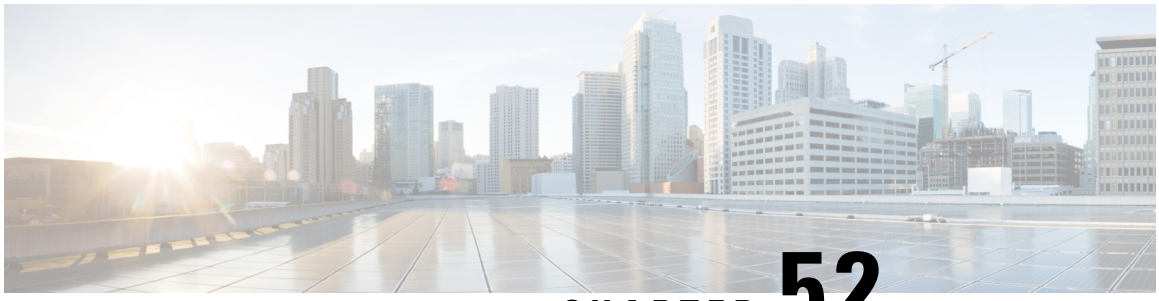
  For more information, see Synchronize users and groups, on page 1865.

History for captive portal

This reference provides the development history and version information for the captive portal feature across different software releases.

Feature	Minimum Firewall Management CenterFirewall Management Center	Minimum Firewall Threat Defense	Details
Authentication using a realm or realm sequence.	7.4.1	7.4.1	You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules. In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously. Microsoft Azure Active Directory cannot be used with captive portal. New/modified screens: • **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** • **Identity policy** > **(edit)** > **Add Rule** > **Passive Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** • **Identity policy** > **(edit)** > **Add Rule** > **Active Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established**
Share active authentication sessions across firewalls.	7.4.1	7.4.1	Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option. • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls**
Hostname redirect.	7.1.0	7.1.0 with Snort 3	You can use a network object that contains the fully-qualified host name (FQDN) of the interface that captive portal can use for active authentication requests.
Guest login.	6.1.0	6.1.0	Users can log in as guest using captive portal.

Feature	Minimum Firewall Management CenterFirewall Management Center	Minimum Firewall Threat Defense	Details
Captive portal.	6.0.0	6.0.0	Feature introduced. You can use the captive portal to require users to enter their credentials when prompted in a browser window. The mapping also allows policies to be based on a user or group of users.



CHAPTER 52

Identity Source: ISE/ISE-PIC

The following topics discuss how to perform user awareness and user control with ISE/ISE-PIC:

- The ISE/ISE-PIC identity source, on page 1911
- License requirements for ISE/ISE-PIC, on page 1913
- Requirements and prerequisites for ISE/ISE-PIC, on page 1913
- Best practices for ISE/ISE-PIC integration, on page 1914
- ISE/ISE-PIC configurations for user control , on page 1916
- ISE/ISE-PIC configuration, on page 1919
- Configure ISE for user control, on page 1924
- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues, on page 1927
- History for ISE/ISE-PIC, on page 1929

The ISE/ISE-PIC identity source

The ISE/ISE-PIC identity source is an authoritative identity source that

- provides user awareness data for users who authenticate using Active Directory (AD), LDAP, RADIUS, or RSA
- enables passive authentication and user control on Active Directory users
- integrates with the system to manage network access and classify traffic in a Cisco TrustSec environment, and
- supports security group tags (SGT) for access control.

ISE/ISE-PIC integration capabilities

You can integrate your Cisco Identity Services Engine (ISE) or ISE Passive Identity Connector (ISE-PIC) deployment with the system to use ISE/ISE-PIC for passive authentication.

In addition to user awareness and control, if you use ISE Cisco ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as both source and destination matching criteria. This enables you to block or allow access based on security group membership rather than IP addresses or network objects. Also see Best practices for ISE/ISE-PIC integration, on page 1914.

ISE/ISE-PIC does not report failed login attempts or the activity of ISE Guest Services users.

Note The system does not parse IEEE 802.1x machine authentication but it *does* parse 802.1x user authentication. If you are using 802.1x with ISE, you must include user authentication. 802.1x machine authentication will not provide a user identity to the Firewall Management Center that can be used in policy.

For more information on Cisco ISE/ISE-PIC, see the Identity Services Engine Passive Identity Connector administrator guides or the Identity Services Engine administrator guides.

Note We strongly recommend you use the latest version of ISE/ISE-PIC to get the latest feature set and the most number of issue fixes.

Source and destination security group tag (SGT) matching

If you use Cisco ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as both source and destination matching criteria. This enables you to block or allow access based on security group membership rather than IP addresses or network objects.

Benefits and implementation details

Matching on SGT tags provides these benefits:

- The Firewall Management Center can subscribe to Security Group Tag eXchange Protocol (SXP) mappings from ISE.

  ISE uses SXP to propagate the IP-to-SGT mapping database to managed devices. When you configure Firewall Management Center to use an ISE server, you enable the option to listen to the SXP topic from ISE. This causes the Firewall Management Center to learn about the security group tags and mappings directly from ISE. The Firewall Management Center then publishes SGTs and mappings to managed devices.

  The SXP Topic receives security group tags based on static and dynamic mappings learned through the SXP protocol between ISE and other SXP compliant devices (like switches).

  You can create security group tags in ISE and assign host or network IP addresses to each tag. You can also assign SGTs to user accounts, and the SGT is assigned to the user's traffic. If the switches and routers in the network are configured to do so, these tags then get assigned to packets as they enter the network controlled by ISE, the Cisco TrustSec cloud.

  SXP is *not* supported by ISE-PIC.

- The Firewall Management Center and managed devices can learn about SGT mappings without deploying additional policy. (In other words, you can view connection events for SGT mappings without deploying an access control policy.)
- Supports Cisco TrustSec, which enables you to segment your network to protect critical business assets.
- When a managed device evaluates SGT as a traffic matching criteria for a rule, it uses this priority:

  1. The source SGT tag defined in the packet, if any.

For the SGT tag to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.

For the SGT tag to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.

2. The SGT assigned to the user session, as downloaded from the ISE session directory. The SGT can be matched to source or destination.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is in the range for an SGT, then the traffic matches the rule that uses the SGT. The SGT can be matched to source or destination.

SGT matching examples

- In ISE, create an SGT tag named Guest Users and associate it with the 192.0.2.0/24 network.

  For example, you could use Guest Users as a source SGT condition in your access control rule and restrict access to certain URLs, web site categories, or networks from anyone who accesses your network.

- In ISE, create an SGT tag named Restricted Networks and associate it with the 198.51.100.0/8 network.

  For example, you could use Restricted Networks as a destination SGT rule condition and block access from Guest Users and other networks that have users who are not authorized to access the network.

License requirements for ISE/ISE-PIC

This reference provides license requirements for ISE and ISE-PIC systems.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for ISE/ISE-PIC

Supported domains

Any

User roles

- Admin
- Access Admin

- Network Admin

Best practices for ISE/ISE-PIC integration

ISE/ISE-PIC version and configuration compatibility

Ensure your ISE/ISE-PIC version and configuration supports proper integration with the Secure Firewall Management Center.

- Use the latest version of ISE/ISE-PIC to get the latest feature set.
- Synchronize the time on the ISE/ISE-PIC server and the Secure Firewall Management Center. Otherwise, the system might perform user timeouts at unexpected intervals.
- Configure and enable a realm for the ISE server assuming the pxGrid persona to implement user control using ISE or ISE-PIC data as described in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- Ensure each Secure Firewall Management Center host name that connects to an ISE server is unique; otherwise, the connection to one of the Secure Firewall Management Centers will be dropped.
- If you use ISE 3.4 Patch 4 or later as an identity source for Secure Firewall Management Center in a hybrid deployment, where authorization can use either Microsoft Entra ID (Azure) or on-prem Active Directory, ensure that your ISE authorization policy rule order evaluates on-premises Active Directory external identity source rules before any Entra ID-based authorization rules. This guideline applies to hybrid deployments in which remote access VPN users can authenticate with Microsoft Entra ID, and Secure Firewall Management Center uses the on-premises Microsoft Active Directory realm for user identity and user-based access control.

For the specific versions of ISE/ISE-PIC that are compatible with this version of the system, see the Cisco Firepower Compatibility Guide.

If you configure ISE/ISE-PIC to monitor a large number of user groups, the system might drop user mappings based on groups due to managed device memory limitations. As a result, rules with realm or user conditions might not perform as expected.

For any device running version 6.7 or later, you can optionally use the **configure identity-subnet-filter** command to limit the subnets that the managed device monitors. For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Alternatively, you can configure a network object and apply that object as an Identity Mapping Filter in the identity policy. See Create an identity policy, on page 1943.

IPv6 support

Verify IPv6 compatibility between ISE/ISE-PIC and your managed devices.

- Compatible versions of ISE/ISE-PIC version 2.x include support for IPv6-enabled endpoints.
- Version 3.0 (patch 2) and later of ISE/ISE-PIC enables IPv6 communication between ISE/ISE-PIC and the Firewall Management Center.

Client approval in ISE

Manually approve clients in ISE before the connection between the ISE server and the Firewall Management Center succeeds. Typically, there are two clients: one for the connection test and another for ISE agent.

You can also enable **Automatically approve new accounts** in ISE as discussed in the chapter on Managing users and external identity sources in the *Cisco Identity Services Engine Administrator Guide*.

Unreachable session management

If a user session in ISE/ISE-PIC is reported as unreachable, the system prunes that session so another user with the same IP cannot match the unreachable user's identity rules.

You can control this behavior in ISE/ISE-PIC by going to **Providers** > **Endpoint Probes** and clicking one of these options:

- **Enabled** to cause ISE/ISE-PIC to monitor endpoint connections and therefore to cause the Secure Firewall Management Center prune a session from an unreachable user.
- **Disabled** to cause ISE/ISE-PIC to ignore endpoint connections.

Security group tags (SGT) implementation

A Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network. Cisco ISE and Cisco TrustSec use a feature called Security Group Access (SGA) to apply SGT attributes to packets as they enter the network. These SGTs correspond to a user's assigned security group within ISE or TrustSec. If you configure ISE as an identity source, the Firepower System can use these SGTs to filter traffic.

Security Group Tags can be used both as source and destination matching criteria in access control rules.



Note

- To implement user control using only the ISE SGT attribute tag, you do not need to configure a realm for the ISE server. ISE SGT attribute conditions can be configured in policies with or without an associated identity policy.
- In some rules, custom SGT conditions can match traffic tagged with SGT attributes that were *not* assigned by ISE. This is not considered user control, and works only if you are not using ISE/ISE-PIC as an identity source.

To match destination SGT tags in addition to source SGT tags, verify these requirements:

Required ISE version: 2.6 patch 6 or later, 2.7 patch 2 or later

Router support: Any Cisco router that supports SGT inline tagging over Ethernet. For more information, consult a reference such as the Cisco Group Based Policy Platform and Capability Matrix Release

Limitations:

- Quality of Service (QoS) policy uses source SGT matching only; it does *not* use destination SGT matching
- RA-VPN does not receive SGT mappings directly through RADIUS

ISE and high availability

When the primary ISE/ISE-PIC server fails, understand the impact on operations.

As a result of the integration with pxGrid v2, the Secure Firewall Management Center round-robins between both configured ISE hosts until one accepts the connection.

If the connection is lost, the Secure Firewall Management Center resumes round-robin attempts to the connected hosts.

Endpoint location (or location IP)

An Endpoint Location attribute is the IP address of the network device that used ISE to authenticate the user, as identified by ISE.

You must configure and deploy an identity policy to control traffic based on **Endpoint Location (Location IP)**.

ISE attributes

Configuring an ISE connection populates the Secure Firewall Management Center database with ISE attribute data. You can use ISE attributes for user awareness and user control. This is not supported with ISE-PIC.

Endpoint profile (or device type)

An Endpoint Profile attribute is the user's endpoint device type, as identified by ISE.

You must configure and deploy an identity policy to control traffic based on **Endpoint Profile (Device Type)**.

ISE/ISE-PIC configurations for user control

An ISE/ISE-PIC configuration uses realms, identity policies, and access control policies to control user access to network resources.

Configuration options

You can use ISE/ISE-PIC in any of these configurations:

- With a realm, identity policy, and associated access control policy: Use a realm to control *user* access to network resources in policy. You can still use ISE/ISE-PIC Security Group Tags (SGT) metadata in your policies.
- With an access control policy only. No realm or identity policy are necessary: Use this method to control network access using SGT metadata alone.

Configure ISE/ISE-PIC without a realm

Configure ISE to allow or block access to the network using SGT tags for enhanced network security and access control.

This topic provides a high-level overview of tasks you must complete to configure ISE to be able to allow or block access to the network using SGT tags.

Procedure

Step 1 SGT matching: Enable SXP on ISE.

This enables the Secure Firewall Management Center to receive updates from ISE when SGT metadata changes.

Step 2 Export system certificates from ISE/ISE-PIC.

The certificates are required to connect securely between the ISE/ISE-PIC pxGrid, monitoring (MNT) servers and the Secure Firewall Management Center. See Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center, on page 1921

Step 3 Import the certificates in the Secure Firewall Management Center.

The certificates must be imported as follows:

- pxGrid client certificate: internal certificate with key (**Objects** > **Object Management** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **Object Management** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Step 4 Create the ISE/ISE-PIC identity source.

The ISE/ISE-PIC identity source enables you to control user activity using Security Group Tags (SGT) provided by ISE/ISE-PIC.

Step 5 Create an access control rule.

The access control rule specifies an action to take (for example, allow or block) if traffic matches the rule criteria. You can use source and destination SGT metadata as matching criteria in the access control rule. See Access control rules, on page 1609.

Step 6 Deploy the access control policy to managed devices.

Before your policy can take effect, it must be deployed to managed devices. See Deploy configuration changes, on page 135.

What to do next

Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center, on page 1921

Configure ISE/ISE-PIC for user control using a realm

This task enables you to configure ISE/ISE-PIC for user control and to allow or block user or group access to the network. Users and groups can be stored in any server listed in Supported servers for realms, on page 1841.

This topic provides a high-level overview of tasks you must complete to configure ISE/ISE-PIC for user control and to be able to allow or block user or group access to the network.

Procedure

Step 1 Enable SXP on ISE for destination SGT only.

This enables the Secure Firewall Management Center to receive updates from ISE when SGT metadata changes.

Step 2 Export system certificates from ISE/ISE-PIC.

The certificates are required to connect securely between the ISE/ISE-PIC pxGrid, monitoring (MNT) servers and the Secure Firewall Management Center. See the following:

- pxGrid server and MNT server certificate: Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center, on page 1921
- pxGrid client certificate: Generate a self-signed certificate, on page 1923

Step 3 Import the certificates in the Secure Firewall Management Center.

The certificates must be imported as follows:

- pxGrid client certificate: internal certificate with key (**Objects** > **Object Management** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **Object Management** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Step 4 Create a realm.

You must create a realm only to control access to the network by the users and groups you choose.

See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

a) Download users and groups, and enable the realm.

Downloading users and groups enables you to use them in access control rules. See Synchronize users and groups, on page 1865.

Step 5 Create the ISE/ISE-PIC identity source.

The ISE/ISE-PIC identity source enables you to control user activity using Security Group Tags (SGT) provided by ISE/ISE-PIC.

Step 6 Create an identity policy.

An identity policy is a container for one or more identity rules. See Create an identity policy, on page 1943.

a) Create an identity rule.

An identity rule specifies how a realm is used to control access to the network by users and groups. See Create an identity rule, on page 1952.

Step 7 Associate the identity policy with an access control policy.

This enables the access control policy to use users and groups in the realm.

a) Create an access control rule.

The access control rule specifies an action to take (for example, allow or block) if traffic matches the rule criteria. You can use source and destination SGT metadata as matching criteria in the access control rule. See Access control rules, on page 1609.

Step 8 Deploy the access control policy to managed devices.

Before your policy can take effect, it must be deployed to managed devices. See Deploy configuration changes, on page 135.

What to do next

Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center, on page 1921

ISE/ISE-PIC configuration

This section explains how to configure the ISE/ISE-PIC server for use with identity policies in the Firewall Management Center, including:

- export certificates from the ISE/ISE-PIC server to authenticate with the Firewall Management Center
- publish SXP topics so the Firewall Management Center can be updated with Security Group Tags (SGT) on the ISE server.

Configure security groups and SXP publishing in ISE

This task enables static SGT-to-IP address mappings for Secure Firewall Threat Defense devices, allowing TrustSec policies and access control based on source and destination security group tags (SGT).

There is a lot of configuration that you must do in Cisco Identity Services Engine (ISE) to create the TrustSec policy and security group tags (SGT). Please look at the ISE documentation for more complete information on implementing TrustSec.

The following procedure picks out the highlights of the core settings you must configure in ISE for the Firewall Threat Defense device to be able to download and apply static SGT-to-IP address mappings, which can then be used for source and destination SGT matching in access control rules. See the ISE documentation for detailed information.

The figures in this procedure are based on ISE 2.4. The exact paths to these features might change in subsequent releases, but the concepts and requirements will be the same. Although ISE 2.4 or later is recommended, and preferably 2.6 or later, the configuration should work starting with ISE 2.2 patch 1.

Before you begin

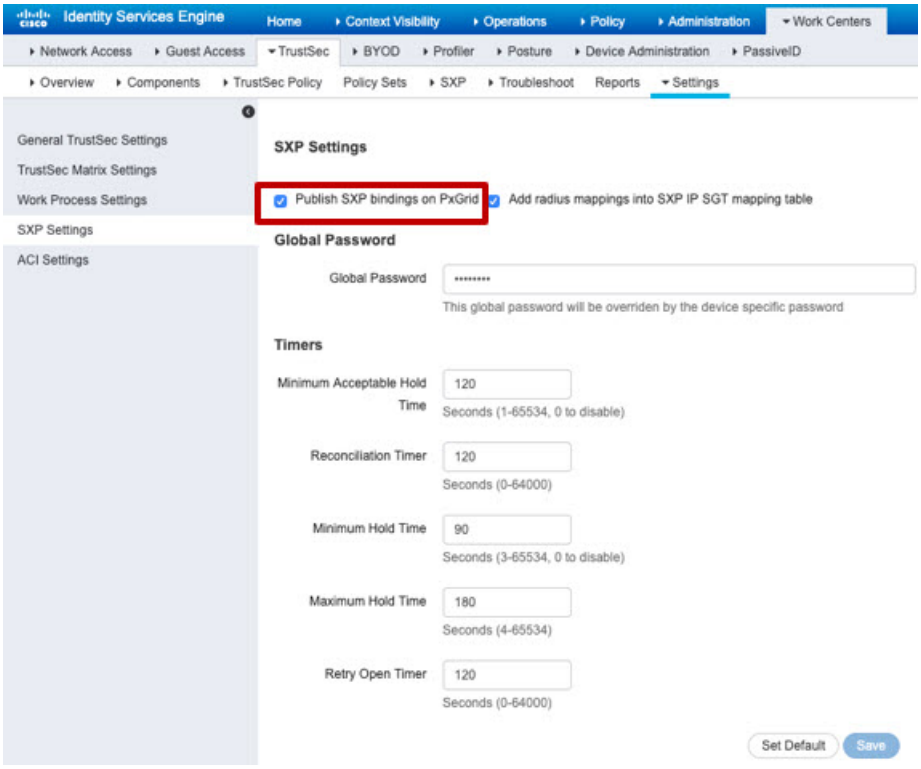
You must have the ISE Plus license to publish SGT-to-IP address static mappings and to get user session-to-SGT mappings so that the Firewall Threat Defense device can receive them.

Procedure

Step 1 Choose **Work Centers** > **TrustSec** > **Settings** > **SXP Settings**, and select the **Publish SXP Bindings on PxGrid** option.

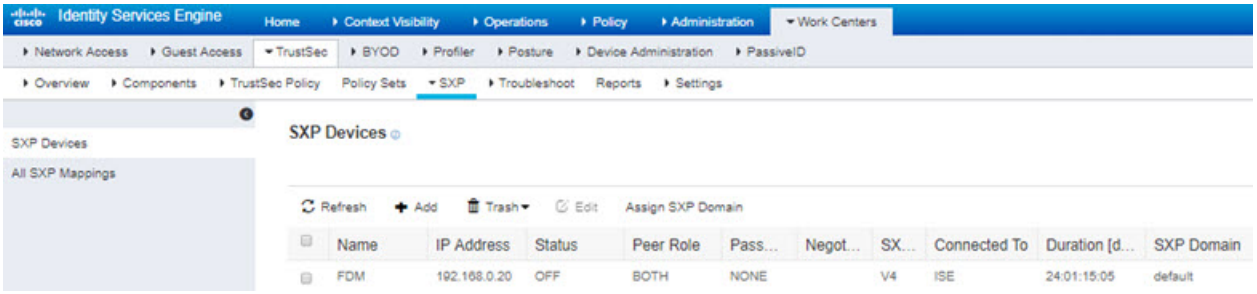
This option makes ISE send the SGT mappings out using SXP. You must select this option for the Firewall Threat Defense device to "hear" anything from listing to the SXP topic. This option must be selected for the

Firewall Threat Defense device to get static SGT-to-IP address mapping information. It is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.

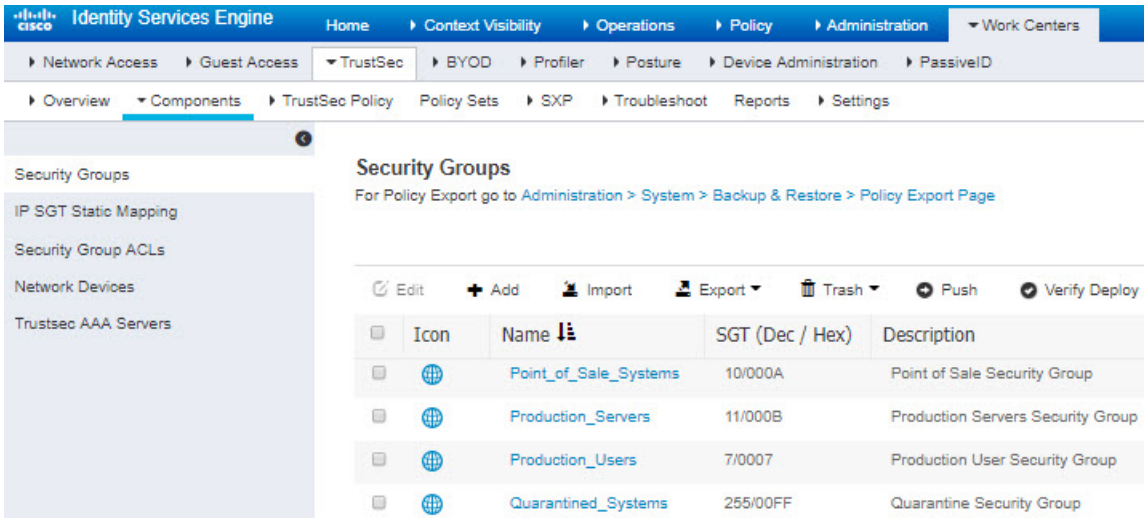


Step 2 Choose **Work Centers** > **TrustSec** > **SXP** > **SXP Devices**, and add a device.

This does not have to be a real device, you can even use the management IP address of the Firewall Threat Defense device. The table simply needs at least one device to induce ISE to publish the static SGT-to-IP address mappings. This step is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.

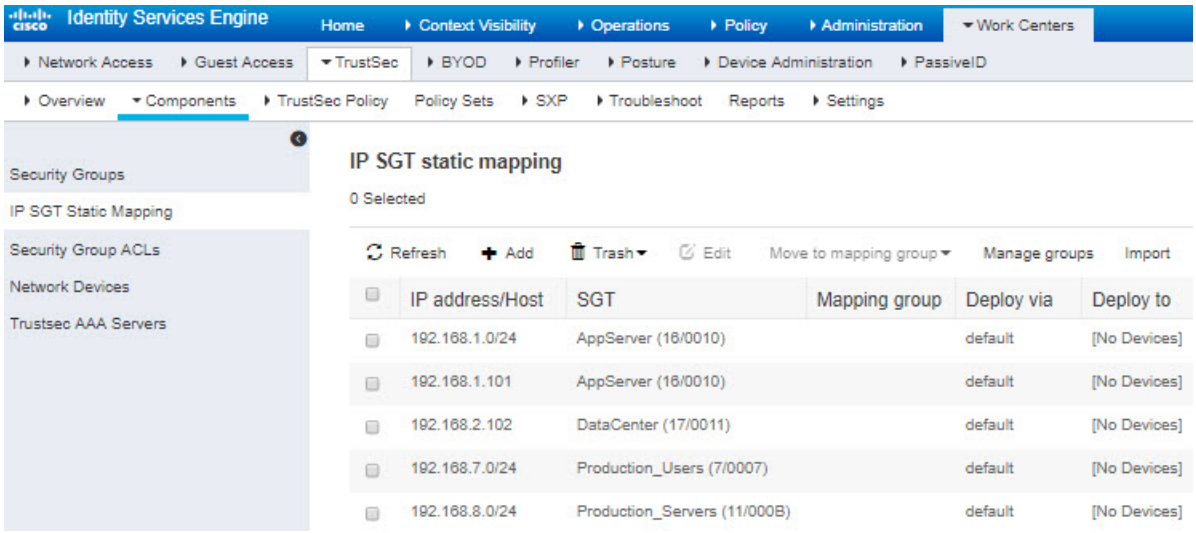


Step 3 Choose **Work Centers** > **TrustSec** > **Components** > **Security Groups** and verify there are security group tags defined. Create new ones as necessary.



Step 4 Choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** and map host and network IP addresses to the security group tags.

This step is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.



You have configured ISE with the necessary security groups, SXP publishing settings, and static SGT-to-IP mappings required for Secure Firewall Threat Defense devices to receive and apply TrustSec policies.

Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center

Certificate exported from Identity Services Engine (ISE) / Identity Services Engine - Passive Identity Connector (ISE-PIC) servers enables secure authentication between the Firewall Management Center and ISE systems.

You might need to export one, or as many as three, certificates, depending on how your ISE system is set up:

- One certificate for the pxGrid server
- One certificate for the monitoring (MNT) server
- One certificate, including the private key, for the pxGrid client (that is, the Firewall Management Center)

  Unlike the first two certificates, this is a self-signed certificate.

These certificates are then imported into the Firewall Management Center:

- pxGrid client certificate: internal certificate with key (**Objects** > **Object Management** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **Object Management** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Export a system certificate

Export a system certificate or a certificate with its associated private key for backup or transfer to another system.

You can export a system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Procedure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Check the check box next to the certificate that you want to export and click **Export**.

Step 3 Choose whether to export only the certificate, or the certificate and its associated private key.

Tip We do not recommend exporting the private key that is associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wildcard system certificate to be imported into the other Cisco ISE nodes for inter-node communication), specify an encryption password for the private key. You must specify this password while importing this certificate into another Cisco ISE node to decrypt the private key.

Step 4 Enter the password if you have chosen to export the private key. The password should be at least eight characters long.

Step 5 Click **Export** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the PEM format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the PEM format and the encrypted private key file.

Generate a self-signed certificate

Generate a self-signed certificate to add a new local certificate for internal testing and evaluation purposes in Cisco ISE.

Add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you plan to deploy Cisco ISE in a production environment, use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

Note If you use a self-signed certificate and you want to change the hostname of your Cisco ISE node, log in to the administration portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE continues to use the self-signed certificate with the old hostname.

Before you begin

To perform this task, you must be a Super Admin or System Admin.

Follow these steps to generate a self-signed certificate:

Procedure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

To generate a self-signed certificate from a secondary node, choose **Administration** > **System** > **Server Certificate**.

Step 2 In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**.

Step 3 Click **Generate Self Signed Certificate** and enter the details in the window displayed.

Step 4 Check the check boxes in the **Usage** area based on the service for which you want to use this certificate.

Step 5 Click **Submit** to generate the certificate.

To restart the secondary nodes, from the CLI, enter these commands in this order:

a) **application stop ISE**
b) **application start ISE**

Import ISE/ISE-PIC certificates

Import certificates and keys from your ISE or ISE-PIC server to the firewall to enable secure pxGrid and MNT integration for cloud-delivered firewall management.

This procedure is optional.

- pxGrid client certificate: internal certificate with key (**Objects** > **Object Management** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **Object Management** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Before you begin

Export certificates from the ISE/ISE-PIC server as discussed in Export a system certificate, on page 1922. The certificates and key must be present on the machine from which you log in to the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not already done so.

Step 2 Click **Objects** > **Object Management** > **PKI** > **Internal Certs**.

Step 3 Click **Add Internal Cert**.

Step 4 Follow the prompts on your screen to import the certificate and private key.

Step 5 Click **Trusted CAs**.

Step 6 Click **Add Trusted CA**.

Step 7 Follow the prompts on your screen to import the pxGrid server certificate.

Step 8 Repeat the preceding steps, if necessary, to import the MNT server's trusted CA.

Configure ISE for user control

Configure ISE/ISE-PIC identity source to enable user session retrieval from Microsoft Active Directory or LDAP servers for identity-based access control.

The following procedure discusses how to configure the ISE/ISE-PIC identity source. You must be in the global domain to perform this task.

Before you begin

- To get user sessions from a Microsoft Active Directory Server or supported LDAP server, configure and enable a realm for the Cisco ISE server, assuming the pxGrid persona, as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- To get all mappings that are defined in Cisco ISE, including SGT-to-IP address mappings published through SXP, use the procedure that follows. As an alternative, you have the following options:

- To use the SGT information in the packets only, and not use mappings downloaded from Cisco ISE, skip the steps discussed in Create and edit access control rules, on page 1631. Note that in this case, you can use SGT tags as a source condition only; these tags will never match destination criteria.
- To use SGT in packets and user-to-IP-address/SGT mappings only, do not subscribe to the SXP topic in the Cisco ISE identity source, and do not configure ISE to publish SXP mappings. You can use this information for both source and destination matching conditions.

- Export certificates from the ISE/ISE-PIC server and optionally import them into the Secure Firewall Management Center as discussed in Export certificates from the ISE/ISE-PIC server for use in the Secure Firewall Management Center, on page 1921.
- To publish SXP topics so the Secure Firewall Management Center can be updated with Security Group Tags (SGT) on the ISE server, see ISE/ISE-PIC configuration, on page 1919.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Integration** > **Other Integrations** > **Identity Sources**.

Step 3 Click **Identity Services Engine** for the **Service Type** to enable the ISE connection.

Note To disable the connection, click **None**.

Step 4 Enter a **Primary Host Name/IP Address** and, optionally, a **Secondary Host Name/IP Address**.

Step 5 Click the appropriate certificate authorities from the **pxGrid Server CA** and **MNT Server CA** lists, and the appropriate certificate from the **pxGrid Client Certificate** list. You can also click **Add** (+) to add a certificate.

Note The **pxGrid Client Certificate** must include the **clientAuth** extended key usage value, or it must not include any extended key usage values.

Step 6 (Optional.) Enter an **ISE Network Filter** using CIDR block notation.

Step 7 In the Subscribe To section, check the following:

- **Session Directory Topic** to receive ISE user session information from the ISE server.
- **SXP Topic** to receive updates to SGT-to-IP mappings when available from the ISE server. This option is required to use destination SGT tagging in access control rules.

Step 8 To test the connection, click **Test**.

If the test fails, click **Additional Logs** for more information about the connection failure.

Note If you set up load balancing with ISE, the node that responds to the test should be the currently active node. For more information, see Cisco pxGrid Node.

What to do next

- Specify users to control and other options using an identity policy as described in Create an identity policy, on page 1943.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Use Security Group Tags (SGT) from Cisco ISE as dynamic attributes in access control policies.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes, on page 135.
- Monitor user activity as discussed in *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide*.

ISE/ISE-PIC configuration fields

The fields in this reference are used to configure a connection to ISE/ISE-PIC.

Connection and certificate configuration fields for ISE/ISE-PIC integration:

- **Primary and Secondary Host Name/IP Address**: The hostname or IP address for the primary and, optionally, the secondary pxGrid ISE servers. The ports used by the host names you specify must be reachable by both ISE and the Secure Firewall Management Center.
- **pxGrid Server CA**: The trusted certificate authority for the pxGrid framework. If your deployment includes a primary and a secondary pxGrid node, the certificates for both nodes must be signed by the same certificate authority.
- **MNT Server CA**: The trusted certificate authority for the ISE certificate when performing bulk downloads. If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.
- pxGrid Client Certificate: The internal certificate and key that the Secure Firewall Management Center must provide to /ISE-PIC to connect to /ISE-PIC or to perform bulk downloads.

Note The **pxGrid Client Certificate** must include the clientAuth extended key usage value, or it must not include any extended key usage values.

Data filtering, subscription, and proxy configuration fields:

- **ISE Network Filter**: An optional filter you can set to restrict the data that ISE reports to the Secure Firewall Management Center. If you provide a network filter, ISE reports data from the networks within that filter. You can specify a filter in these ways:
  - Leave the field blank to specify **`any`**.
  - Enter a single IPv4 address block using CIDR notation.
  - Enter a list of IPv4 address blocks using CIDR notation, separated by commas.
- **Subscribe to**: **Session Directory Topic**: Check this box to subscribe to user session information from the ISE server. Includes SGT and endpoint metadata. **SXP Topic**: Check this box to subscribe to SXP mappings from the ISE server.

Note This version of the system does not support filtering using IPv6 addresses, regardless of your ISE version.

Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues

This reference helps you troubleshoot issues with Cisco TrustSec, ISE, or ISE-PIC integration to ensure Security Group Tag propagation, user mapping, and certificate requirements are correctly configured for Cloud-Delivered Firewall Management Center and Secure Firewall Management Center deployments.

Troubleshoot Cisco TrustSec issues

A device interface can be configured to propagate Security Group Tags (SGTs) either from ISE/ISE-PIC or from a Cisco device on the network (referred to as Cisco TrustSec.) On the device management page (**Devices** > **Device Management**), the **Propagate Security Group Tag** check box for an interface is disabled by default. If you want the interface to propagate TrustSec data, check the box.

Troubleshoot ISE/ISE-PIC issues

For other related troubleshooting information, see Troubleshoot realms and user downloads, on page 1877 and Troubleshoot user control, on page 1962.

If you experience issues with the ISE or ISE-PIC connection, check these items:

- The pxGrid Identity Mapping feature in ISE must be enabled before you can successfully integrate ISE with the system.
- When the primary server fails, you must manually promote the secondary to primary; there is no automatic failover.
- Before a connection between the ISE server and the Firewall Management Center succeeds, you must manually approve the clients in ISE. (Typically, there are two clients: one for the connection test and another for ISE agent.)

  You can also enable **Automatically approve new accounts** in ISE as discussed in the chapter on Managing users and external identity sources in the Identity Services Engine administrator guides.
- The **pxGrid Client Certificate** must include the **clientAuth** extended key usage value, or it must not include any extended key usage values.

- The time on your ISE server must be synchronized with the time on the Secure Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.
- If your deployment includes a primary and a secondary pxGrid node,
  - The certificates for both nodes must be signed by the same certificate authority.
  - The ports used by the host name must be reachable by both the ISE server and by the Secure Firewall Management Center.
- If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.

To exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE, use the **configure identity-subnet-filter** {**add** | **remove**} command. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

If you experience issues with user data reported by ISE or ISE-PIC, note these items:

- After the system detects activity from an ISE user whose data is not yet in the database, the system retrieves information about them from the server. Activity seen by the ISE user is *not* handled by access control rules, and is *not* displayed in the web interface until the system successfully retrieves information about them in a user download.
- You cannot perform user control on ISE users who were authenticated by an LDAP, RADIUS, or RSA domain controller.
- The Secure Firewall Management Center does not receive user data for ISE Guest Services users.
- If ISE monitors the same users as TS Agent, the Secure Firewall Management Center prioritizes the TS Agent data. If the TS Agent and ISE report identical activity from the same IP address, only the TS Agent data is logged to the Secure Firewall Management Center.
- Your ISE version and configuration impact how you can use ISE in the system. For more information, see The ISE/ISE-PIC identity source, on page 1911.
- If you have Secure Firewall Management Center high availability configured and the primary fails, see the section on ISE and high availability in Best practices for ISE/ISE-PIC integration, on page 1914.
- ISE-PIC does not provide ISE attribute data.
- ISE-PIC cannot perform ISE ANC remediations.
- Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, refer to RFC 959.

If you experience issues with supported functionality, see The ISE/ISE-PIC identity source, on page 1911 for more information about version compatibility.

ISE/ISE-PIC user timeout

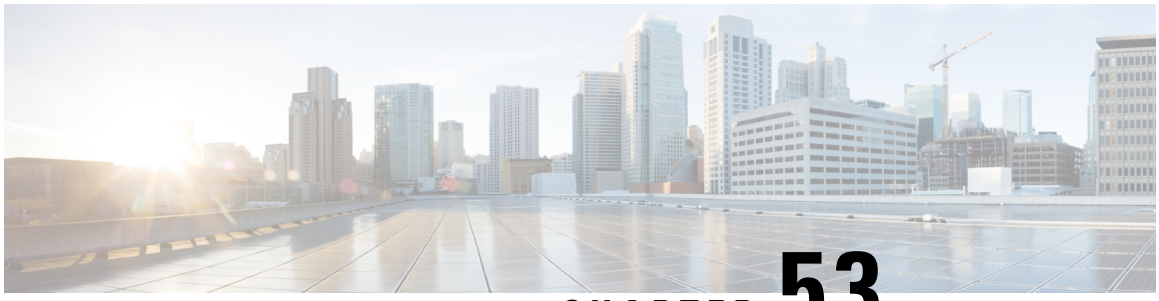
If you're setting up ISE/ISE-PIC without a realm, be aware there is a user session timeout that affects how users are seen by the Firewall Management Center.

History for ISE/ISE-PIC

This reference provides the historical development of ISE and ISE-PIC integration features across different software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
pxGrid 2.0 is the default for supported ISE/ISE-PIC versions	6.7.0	6.7.0	Note: • Supported ISE/ISE-PIC versions: 2.6 patch 6 or later, 2.7 patch 2 or later • Adaptive Network Control (ANC) policies replace Endpoint Protection Service (EPS) remediations. If you have EPS policies configured in the Firewall Management Center, you must migrate them to use ANC.
Optionally exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.	6.7.0	6.7.0	New command: **configure identity-subnet-filter** {**add** | **remove**}
Destination Security Group Tag matching (SGT)	6.5.0	6.5.0	Feature introduced. Enables you to use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE. New/modified screens: • New options to configure Destination SGT matching: **System** > **Integration** > **Identity Sources** > **ISE/ISE-PIC** • **Session Directory Topic**: Subscribe to ISE user session information. • **SXP Topic**: Subscribe to SGT tag updates on the ISE server. • New and renamed columns in **Analysis** > **Connections** > **Events** • Renamed: Security Groups Tags renamed to Source SGT • New: Destination SGT
Integration with ISE-PIC	6.2.1	6.2.1	You can now use data from ISE-PIC.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
SGT tags for user control.	6.2.1	6.2.0	You no longer need to create a realm or identity policy to perform user control based on ISE Security Group Tag (SGT) data.
Integration with ISE.	6.0	6.0	Feature introduced. By subscribing to Cisco's Platform Exchange Grid (PxGrid), the Firepower Management Center can download additional user data, device type data, device location data, and Security Group Tags (SGTs) —a method used by ISE to provide network access control).



CHAPTER 53

Identity Source: Remote Access VPN

The following topics discuss how to perform user awareness and user control with Remote Access VPN:

- Remote access VPN identity sources, on page 1931
- Configure Remote Access VPN for AD-authenticated users, on page 1932
- Hybrid Entra ID and on-premises AD deployments, on page 1933
- Troubleshooting guidelines for remote access VPN identity source, on page 1934
- History for RA VPN, on page 1935

Remote access VPN identity sources

A remote access VPN identity source authenticates a user before establishing secure remote connection to the network. It requires the user to provide credentials through a client to verify the identity.

Identity source configuration

Secure Client is the only client supported on endpoint devices for remote VPN connectivity to Firewall Threat Defense devices.

When you set up a secure VPN gateway as discussed in Configure a remote access VPN policy, you can set up an identity policy for those users and associate the identity policy with an access control policy, provided your users are in an Active Directory repository.

Note If you use remote access VPN with User Identity and RADIUS as the identity source, you must configure the realm (**Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group**).

The login information provided by a remote user is validated by an LDAP or AD realm or a RADIUS server group. These entities are integrated with the Secure Firewall Threat Defense secure gateway.

Note If users authenticate with remote access VPN using Active Directory as the authentication source, users must log in using their username; the format domain\username or username@domain fails. (Active Directory refers to this username as the logon name or sometimes as sAMAccountName.) For more information, see User Naming Attributes on MSDN.

If you use RADIUS to authenticate, users can log in with any of the preceding formats.

Once authenticated through a VPN connection, the remote user takes on a VPN identity. This VPN identity is used by identity policies on the Secure Firewall Threat Defense secure gateway to recognize and filter network traffic belonging to that remote user.

Identity policies are associated with access control policies, which determine who has access to network resources. It is in this way that a remote user blocked or allowed to access your network resources.

Related Topics

Secure Connections Overview, on page 1329
Remote access VPN
VPN basics, on page 1330
Configure a remote access VPN policy

Configure Remote Access VPN for AD-authenticated users

Configure remote access VPN for Active Directory-authenticated users. Manage VPN connections and apply identity-based policies to control user access and traffic filtering.

Remote access VPN user control allows you to implement identity-based policies that manage and monitor VPN user connections, providing enhanced security and access control for your network environment.

Before you begin

- Create a realm as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- To use authentication, authorization, and auditing (AAA), set up a RADIUS server group as discussed in Add a RADIUS server group, on page 2346.

Follow these steps to configure RA VPN for user control:

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Devices** > **VPN** > **Remote Access**.

Step 3 See Configure a remote access VPN policy.

Step 4 Specify users to control and other options using an identity policy as described in Create an identity policy, on page 1943.

Step 5 Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 6 Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes, on page 135.

What to do next

Monitor VPN user traffic as discussed in Monitor remote access VPNs.

Hybrid Entra ID and on-premises AD deployments

The hybrid Entra ID and on-premises AD deployment model enables secure, flexible authentication and authorization for remote access users, provided the correct policy order and rule configuration are maintained.

In a hybrid deployment, remote access VPN users can authenticate with Microsoft Entra ID (formerly Azure AD). Cisco ISE authorizes the session and Firewall Management Center uses an on-premises Microsoft Active Directory realm for user identity and user-based access control. In this deployment model:

- Remote access VPN (RA VPN) is configured on Firewall Threat Defense
- Microsoft Entra ID or Azure is used as the SAML identity provider for VPN authentication
- Cisco ISE is used for session authorization
- Cisco ISE authorization policies may include both Microsoft Entra ID/Azure and on-premises AD rules or conditions
- Firewall Management Center uses the on-premises AD domain as the realm for user identity and user enforcement

Best practice: ISE authorization policy order for hybrid deployments

Beginning with Cisco ISE Release 3.4 Patch 4, when ISE evaluates an Entra ID identity source during authorization, it associates Entra ID attributes with the session. If Firewall Management Center uses an on-premises AD realm, the presence of Entra ID attributes may prevent correct user-to-IP mapping for RA VPN sessions. Identity-based access control rules that depend on user or group identity might not match as expected.

To prevent this issue:

Place ISE authorization rules that use the on-premises AD external identity source before rules that evaluate Entra ID or Azure conditions for the same users. This ensures that the session attributes published to FMC through pxGrid align with the configured on-premises AD realm.

After configuring the authorization policy order, verify that new RA VPN sessions create user mappings in Firewall Management Center and that user-based or group-based access control rules match as expected.

Note This behavior applies to Cisco ISE Release 3.4 Patch 4 and later. If user mappings stopped appearing after an ISE upgrade, review the ISE authorization policy order as described in this section.

Troubleshooting guidelines for remote access VPN identity source

For other related troubleshooting information, see Troubleshoot realms and user downloads, on page 1877 and Troubleshoot user control, on page 1962.

If you experience issues with Remote Access VPN, check the connection between your Firewall Management Center and a managed device. If the connection fails, all Remote Access VPN logins reported by the device cannot be identified during the downtime, unless the users were previously seen and downloaded to the Firewall Management Center.

The unidentified users are logged as Unknown users on the Firewall Management Center. After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.

The host name of the managed device must be less than 15 characters for Kerberos authentication to succeed.

Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, see RFC 95

Not Observing Correct Settings for VPN Statistics

This task ensures that managed devices receive the correct health policy settings after modifying VPN statistics configurations.

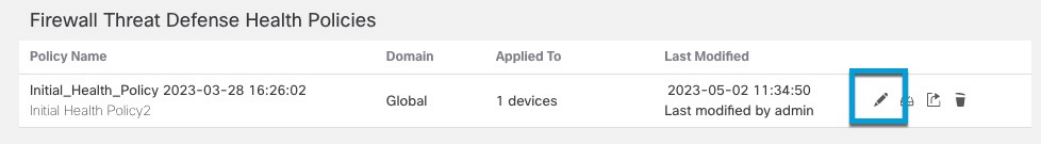
This task discusses steps you must take after either enabling or disabling the **VPN Statistics** setting in a health policy. Failure to perform this task means managed devices have a health policy with incorrect settings.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **System** (⚙) > **Health** > **Policy**.

Step 3 Under Firewall Threat Defense Health Policies, click **Edit** (✎) next to a policy to edit.



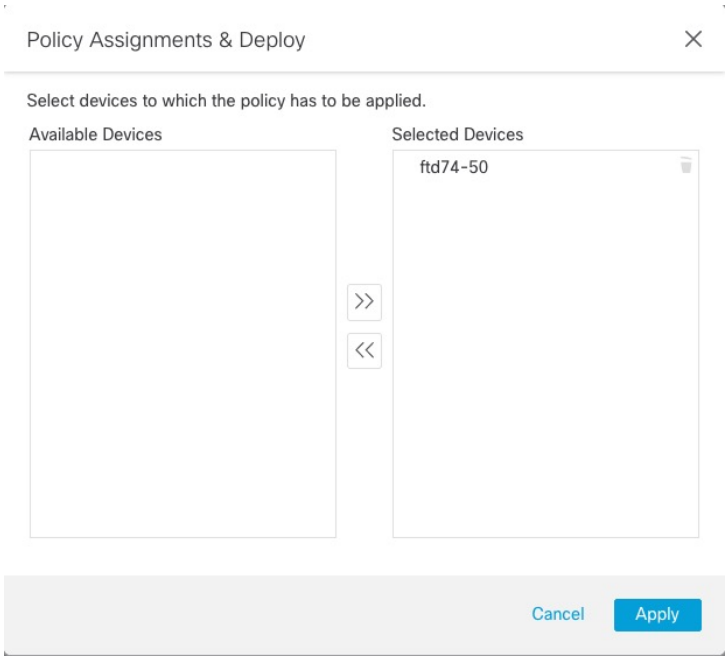
Step 4 On the **Health Modules** tab page, scroll down to locate **VPN Statistics**.

Step 5 Verify the VPN statistics setting is correct or change it if necessary.

Step 6 If you changed the setting, click **Save**, then click **Cancel** to return to the health policy.

Step 7 Under Firewall Threat Defense Health Policies, click **Deploy health policy** (🚀) to apply the policy.

Step 8 In the **Policy Assignments & Deploy** dialog box, move the devices to which to deploy the health policy to the **Selected Devices** field.



Step 9 Click **Apply**.
A message is displayed when the health policy is deployed.

Step 10 After the health policy has finished deploying, click **Policies** > **Access Control heading** > **Access Control** to edit an access control policy.

Step 11 Click **Edit** (✎) next to a policy to edit.

Step 12 Make a minor change to the policy, such as changing its name.

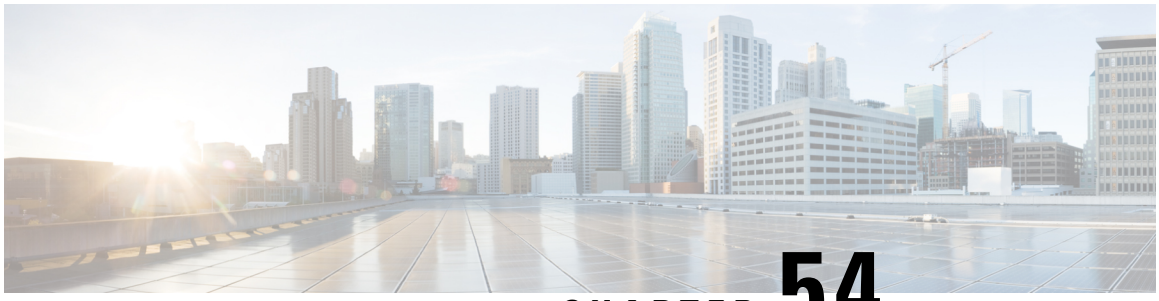
Step 13 Save the access control policy.

Step 14 Deploy configuration changes; see Deploy configuration changes, on page 135..

History for RA VPN

This reference provides the version history and introduction details for Remote Access VPN (RA VPN) feature support across Firewall Management Center and Firewall Threat Defense versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Remote Access VPN	6.2.1	Any	Feature introduced. RA VPN allows individual users to connect to a private business network from a remote location using a laptop or desktop computer connected to the internet, or an Android or Apple iOS mobile device. Remote users transfer data securely and confidentially using encryption techniques crucial for data being transferred over shared mediums and the Internet.



CHAPTER 54

Identity source: TS agent

To use the TS Agent as an identity source for user awareness and user control, install and configure the TS Agent software as discussed in the Terminal Services (TS) Agent guides.

What to do next:

- Specify users to control and other options using an identity policy as described in Create an identity policy, on page 1943.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes, on page 135.
- Monitor user activity as discussed in *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide* .

- Terminal services agent identity source, on page 1937
- Best practices for TS agent configuration, on page 1938
- Identity source: TS agent, on page 1938
- Troubleshoot the TS agent identity source, on page 1938
- History for TS agent, on page 1939

Terminal services agent identity source

The TS Agent is a passive authentication method and one of the authoritative identity sources supported by the system. A Windows Terminal Server performs the authentication, and the TS Agent reports it to a standalone or high availability .

TS agent functionality

When installed on Windows Terminal Servers, the TS Agent assigns a unique port range to individual users as they log in or log out of a monitored network. The Secure Firewall Management Center uses the unique port to identify individual users in the system. You can use one TS Agent to monitor user activity on one Windows Terminal Server and send encrypted data to a Secure Firewall Management Center.

The TS Agent does not report failed login attempts. The data gained from the TS Agent can be used for user awareness and user control.

Best practices for TS agent configuration

Configure the TS Agent on a Windows Terminal Server to monitor user activity and identity realms. The TS Agent enables user awareness in the Secure Firewall Management Center.

- Install and configure the TS Agent on a Windows Terminal Server.
- Configure one or more identity realms targeting the users your server is monitoring.

TS Agent data is visible in the Users, User Activity, and Connection Event tables and can be used for user awareness and user control. For detailed information about the multi-step TS Agent installation and configuration and a complete discussion of the server and system requirements, see the Terminal Services (TS) Agent guides.



Note If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Secure Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive identity source report activity by the same IP address, only the TS Agent data is logged to the Secure Firewall Management Center.

Identity source: TS agent

To use the TS Agent as an identity source for user awareness and user control, install and configure the TS Agent software as discussed in the Terminal Services (TS) Agent guides.

What to do next:

- Specify users to control and other options using an identity policy as described in Create an identity policy, on page 1943.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes, on page 135.
- Monitor user activity as discussed in *Using Workflows* in the *Cisco Secure Firewall Management Center Administration Guide* .

Troubleshoot the TS agent identity source

This reference provides troubleshooting guidance for TS Agent integration issues with the Secure Firewall Management Center. It addresses synchronization requirements, user data prioritization, and activity logging for overlapping passive identity sources.

For other related troubleshooting information, see Troubleshoot realms and user downloads, on page 1877 and Troubleshoot user control, on page 1962.

If you experience issues with the TS Agent integration, check:

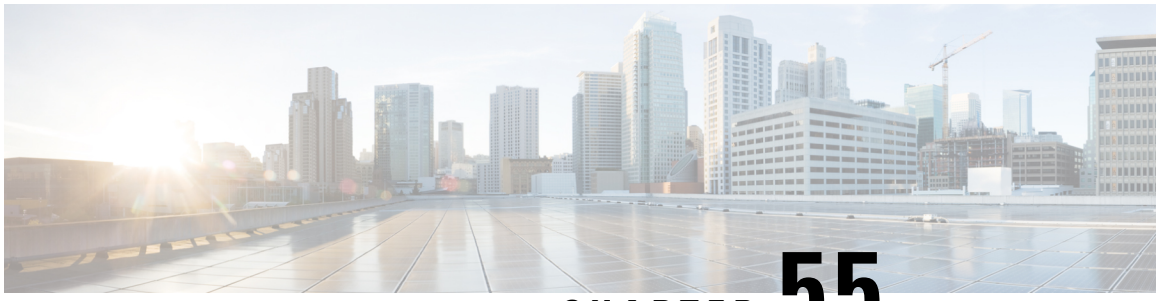
- You must synchronize the time on your TS Agent server with the time on the Secure Firewall Management Center.
- If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Secure Firewall Management Center prioritizes the TS Agent data. If the TS Agent and a passive identity source report activity by the same IP address, only the TS Agent data is logged to the Secure Firewall Management Center.
- Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, refer to RFC 959.

For more troubleshooting information, see the Terminal Services (TS) Agent guides.

History for TS agent

This reference provides the historical development timeline and version information for the TS Agent feature, including compatibility details and feature introductions across different Firepower Management Center and Threat Defense versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
TS Agent for user control.	7.2.0	6.2.0	Feature introduced. Firepower now provides the ability to better identify individual users in shared environments, such as Citrix's Virtual Desktop Infrastructure (VDI), to accurately enforce user-based policy rules on the firewall. Users are identified by ports used. The TS Agent software is updated independently of the Firepower Management Center. For more information, see: • *Cisco Terminal Services (TS) Agent Guide* available on cisco.com • Cisco Firepower Compatibility Guide



CHAPTER 55

Identity Policies

The following topics discuss how to create and manage identity rules and identity policies:

- Identity policies, on page 1941
- License requirements for identity policies, on page 1942
- Requirements and prerequisites for identity policies, on page 1942
- Create an identity policy, on page 1943
- Identity rule conditions, on page 1945
- Create an identity rule, on page 1952
- Sample identity policies and rules, on page 1954
- Manage an identity policy, on page 1961
- Manage an identity rule, on page 1961
- Troubleshoot user control, on page 1962

Identity policies

Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

Configuration requirements

With the exception noted below, you must configure realms and authentication methods you plan to use before you can invoke them in your identity rules:

- You configure realms outside of your identity policy, at **Integration** > **Other Integrations** > **Realms** > **Realms**. For more information, see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- You configure ISE/ISE-PIC, a passive authentication identity source, at **Integration** > **Other Integrations** > **Identity Sources**.
- You configure the TS Agent, a passive authentication identity source, outside the system. For more information, see the *Cisco Terminal Services (TS) Agent Guide*.
- You configure captive portal, an active authentication identity source, within the identity policy. For more information, see Configure the captive portal for user control, on page 1891.
- You configure Remote Access VPN, an active authentication identity source, in Remote Access VPN policies. For more information, see Configure AAA settings for a remote access VPN policy.

After you add multiple identity rules to a single identity policy, order the rules. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles the traffic.

You can also filter traffic by network object, which limits the network each device monitors in the event your devices are at or near their memory limits.

After you configure one or more identity policies, you must associate one identity policy with your access control policy. When traffic on your network matches the conditions in your identity rule, the system associates the traffic with the specified realm and authenticates the users in the traffic using the specified identity source.

If you do not configure an identity policy, the system does not perform user authentication.

Exception to creating an identity policy

An identity policy is not required if all these conditions are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies.

Related Topics

Set up an identity policy, on page 1825

License requirements for identity policies

This reference provides license requirements for identity policies.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for identity policies

This reference provides the requirements and prerequisites necessary for implementing identity policies.

Model support

Any.

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Create an identity policy

Create an identity policy to control user and group access in a realm for access control policies.

This task discusses how to create an identity policy.

Before you begin

An identity policy is required to use users and groups in a realm in access control policies. Create and enable one or more realms as described in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.

(Optional.) If a particular managed device monitors a large number of user groups, the system might drop user mappings based on groups due to managed device memory limitations. As a result, rules with realm or user conditions might not perform as expected. Provided the devices run version 6.7 or later, you can configure the identity rule to monitor traffic by one network or network group object only. To create a network object, see Create a network object, on page 2388.

An identity policy is not required if all these conditions are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity** and click **New Policy**.

Step 3 Enter a **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

Step 5 To add a rule to the policy, click **Add Rule** as described in Create an identity rule, on page 1952.

Step 6 To create a rule category, click **Add Category**.

Step 7 To configure captive portal active authentication, click **Active Authentication** and see Create an identity policy and active authentication rule, on page 1894.

Step 8 (Optional.) To filter traffic by network object, click the **Identity Source** tab. From the list, click the network object to use to filter traffic for this identity policy. Click **Add** (+) to create a new network object.

Step 9 Click **Save** to save the identity policy.

What to do next

- Add rules to your identity policy that specify which users to match and other options; see Create an identity rule, on page 1952.
- Associate the identity policy with an access control policy to allow or block selected users from accessing specified resources; see Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- (Not required for Microsoft Azure AD realms.) Deploy configuration changes to managed devices; see Deploy configuration changes, on page 135.

If you encounter issues, see Troubleshoot user control, on page 1962.

Related Topics

Create an identity policy and active authentication rule, on page 1894
Captive portal fields, on page 1903
Troubleshoot user control, on page 1962
Create an identity mapping filter, on page 1944

Create an identity mapping filter

An identity mapping filter can be used to limit the networks to which an identity rule applies. For example, if your Firewall Management Center manages FTDs that have a limited amount of memory, you can limit the networks they monitor.

You must create separate identity mapping filters for IPv4 and IPv6 addresses.

You can also optionally exclude subnets from the following:

- Receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE.

You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

Before you begin

Perform the following tasks:

1. Create a realm, which is required for an identity policy. See Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
2. Create an identity policy. See Create an identity policy, on page 1943.
3. Create a network object or network group object as discussed in Create a network object, on page 2388. The network object or group you create should define the network you want managed devices to monitor in identity policies.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Click **Edit** ( ).

Step 4 Click the **Identity Source** tab.

Step 5 From the **Identity Mapping Filter** list, choose the name of a network object to use as a filter .

To create a new network object, see Create a network object, on page 2388.

Note To restrict traffic to IPv6 addresses, you must add at least one address, network, or group to the filter.

Step 6 Click **Save**.

Step 7 (Not required for Microsoft Azure AD realms.) Deploy configuration changes to managed devices; see Deploy configuration changes, on page 135.

What to do next

(Not required for Microsoft Azure AD realms.) Associate the identity policy with an access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

To check or change ISE identity mapping filters (also referred to as *subnet filters*), use these commands:

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

Identity rule conditions

Identity rule conditions enable you to fine-tune your identity policy to target specific users and networks you want to control. See one of the following topics for more information.

Related Topics

Security zone rule conditions, on page 1759
Network rule conditions, on page 1321
VLAN tag rule conditions, on page 1635
Best practice: use application-based rules over port-based rules, on page 1323
Realm & settings rule conditions, on page 1949

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.



Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

Security zone conditions in multidomain environments

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

Network rule conditions

A network condition is a traffic matching criterion that

- controls or decrypts traffic based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.



Note You *cannot* use FDQN network objects in identity rules.

Redirect to host name network rule conditions

(Snort 3.0 only)—You can use a network object that contains the fully-qualified host name (FQDN) of the interface that captive portal can use for active authentication requests.

The FQDN must resolve to the IP address of one of the interfaces on a managed device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to a managed device's IP address.

Certificate and redirection behavior

The certificate can specify one FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate.

If an identity rule requires active authentication for a user, but you do not specify a redirect FQDN, the user is redirected to the captive portal port on the managed device interface to which they are connected.

If you do not supply a Redirect to Host Name FQDN, the HTTP Basic, HTTP Response Page, and NTLM authentication methods redirect the user to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name *firewall-hostname.directory-server-domain-name*. If you use HTTP Negotiate without a Redirect to Host Name FQDN, update your DNS server to map this name to the IP addresses of all inside interfaces that require active authentication. If you do not update the DNS server, the redirection does not complete and users cannot authenticate.

We recommend that you always provide a Redirect to Host Name FQDN to ensure consistent behavior regardless of authentication method.

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details

Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

Best practice: use application-based rules over port-based rules

Use application filtering criteria instead of port filtering to target traffic. Applications can be configured to use unique ports to bypass access control blocks.

Port conditions allow you to control traffic by its source and destination ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

The traditional method targets applications by using port specifications, but applications can manipulate unique ports to bypass these controls

Application filtering is recommended for applications to avoid blocking legitimate applications, like Firewall Threat Defense, that dynamically open separate channels for control and data flow. Port-based access control rules could block such applications, impacting desirable operations.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP).

- For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).
- If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

Port, protocol, and ICMP code rule conditions (concept)

A port, protocol, and ICMP code rule condition is a traffic matching criterion that

- matches traffic based on source and destination ports
- supports TCP, UDP, ICMP, and other protocols that do not use ports, and
- controls traffic flow in access control and other policy rules.

Port condition types

Port conditions match traffic based on the source and destination ports. Depending on the rule type, "port" can represent any of these types:

- TCP and UDP—Control TCP and UDP traffic based on the port. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP (6) /22.
- ICMP—Control ICMP and ICMPv6 (IPv6-ICMP) traffic based on its internet layer protocol plus an optional type and code. For example: ICMP(1):3:3.

- Protocol—Control traffic using other protocols that do not use ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Best practices for port-based rules

Specifying ports is the traditional method used to target applications. However, applications can be configured to use unique ports to bypass access control blocks. Use application filtering criteria when possible; however, note that application filtering is unavailable in prefilter rules.

Use application filtering for FTP and similar applications that open separate channels for control and data flow. Using port-based access control rules can prevent these kinds of applications from performing correctly and could result in blocking desirable connections.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as destination port conditions in a single access control rule.

Matching non-TCP traffic with port conditions

You can match non-port-based protocols. By default, if you do not specify a port condition, you are matching IP traffic. Although configuring port conditions can match non-TCP traffic, restrictions apply:

- Access control rules—For Classic devices, match GRE-encapsulated traffic with an access control rule by using the GRE (47) protocol as a destination port condition. To a GRE-constrained rule, add only network-based conditions: zone, IP address, port, and VLAN tag. The system uses outer headers to match **all** traffic in access control policies with GRE-constrained rules. For Firewall Threat Defense devices, use tunnel rules in the prefilter policy to control GRE-encapsulated traffic.
- Decryption rules—These rules support only TCP port conditions.
- IMCP echo—A destination ICMP port with the type set to 0 or a destination ICMPv6 port with the type set to 129 only matches unsolicited echo replies. ICMP echo replies, sent in response to ICMP echo requests, are ignored. To match any ICMP echo, use ICMP type 8 or ICMPv6 type 128.

Realm & settings rule conditions

The **Realm & Settings** tab page enables you to choose a realm or realm sequence to which to apply the identity rule. If you are using captive portal, you have additional options.

Authentication realm

From the **Realm** list, click a realm or realm sequence.

The realm or realm sequence containing the users you want to perform the specified **Action** on. You must fully configure a realm or realm sequence before selecting it as the realm in an identity rule.

Note If remote access VPN is enabled and your deployment is using a RADIUS server group for VPN authentication, make sure you specify the realm associated with this RADIUS server group.

Active authentication only: other options

If you either choose **Active Authentication** as the authentication type or if you check the box, **Use active authentication if passive or VPN identity cannot be established**, you have these options.

Use active authentication if passive or VPN identity cannot be established

(Passive authentication rule only.) Selecting this option authenticates users using captive portal active authentication if a passive or a VPN authentication fails to identify them. You must configure an Active Authentication rule in your identity policy in order to select this option. (That is, users must authenticate using the captive portal.)

If you disable this option, users that do not have a VPN identity or that passive authentication cannot identify are identified as Unknown.

Also see the discussion of the **Authentication Realm** list later in this topic,

Identify as Special Identities/Guest if authentication cannot identify user

Selecting this option allows users who fail captive portal active authentication the specified number of times to access your network as a guest. These users appear in the Firewall Management Center identified by their username (if their username exists on the AD or LDAP server) or by **Guest** (if their user name is unknown). Their realm is the realm specified in the identity rule. (By default, the number of failed logins is 3.)

This field is displayed only if you configure **Active Authentication** (that is, captive portal authentication) as the rule **Action**.

Authentication Protocol

The method to use to perform captive portal active authentication. An example of what users see when logging in with a response page is shown in Create a sample identity policy with an active authentication rule, on page 1956.

The selections vary depending on the type of realm, LDAP or AD:

- Choose **HTTP Basic** if you want to authenticate users using an unencrypted HTTP Basic Authentication (BA) connection. Users log in to the network using their browser's default authentication pop-up window.

  Most web browsers cache the credentials from **HTTP Basic** logins and use the credentials to seamlessly begin a new session after an old session times out.

- Choose **NTLM** to authenticate users using a NT LAN Manager (NTLM) connection. This selection is available only when you select an AD realm. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication pop-up window.

- Choose **Kerberos** to authenticate users using a Kerberos connection. This selection is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent

authentication is not configured, users log in to the network using their browser's default authentication pop-up window.

Note The **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform Kerberos captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the host name you provided when configuring DNS.

For Firewall Threat Defense devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.

- Choose **HTTP Negotiate** to allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection. This type is available only when you select an AD realm.

Note The **Realm** you choose must be configured with an **AD Join Username** and **AD Join Password** for **HTTP Negotiate** to choose Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform **HTTP Negotiate** captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN of the device you are using for captive portal must match the hostname you provided when configuring DNS.

- Choose **HTTP Response Page** to enable users to choose a realm to log in to.

  You can optionally customize the response page; for example, to conform to company style standards.

Active Authentication Realm

(Passive authentication rule only.) If you clicked **Use active authentication if passive or VPN identity cannot be established**, you must click the name of a realm or realm sequence. The availability of a realm or realm sequence is determined by your choice for Authentication Protocol as follows:

- **HTTP Basic** or **HTTP Response Page** authentication protocol: You can choose either a realm or a realm sequence.
- **NTLM**, **Kerberos**, or **HTTP Negotiate** authentication protocol: You can choose a realm only. You *cannot* choose a realm sequence.

Create an identity rule

Identity rules enable you to control user authentication and traffic handling by specifying which identity realm should authenticate users for specific network criteria.

For details about configuration options for identity rules, see Identity rule fields, on page 1953.

Before you begin

You must create and enable a realm or realm sequence.

- Create a Microsoft Active Directory realm and realm directory as discussed in Create an LDAP realm or an Active Directory realm and realm directory, on page 1860.
- (Microsoft AD realm only.) Download users and groups and enable the realm as discussed in Synchronize users and groups, on page 1865.
- (Optional.) Create a realm sequence as discussed in Create a realm sequence, on page 1867.
- Rules are evaluated top-down. For a connection that matches the specified network criteria of a given rule, the user is evaluated against the identity realm specified in the rule. If the user is not part of that realm, they will be marked as unknown, and no further rules in the identity policy will be evaluated. Thus, if you have more than one realm that needs to be evaluated, be sure to use realm sequences instead of a single realm.



Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include a decryption policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Click **Edit** ( ) next to the identity policy to which to add the identity rule.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Click **Add Rule**.

a) Enter a **Name**.

b) If the Specified rule is applicable, check the check box of **Enabled**.

c)

d) To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.
e) Choose a rule **Action** from the list.
f) If you're configuring captive portal, see Configure the captive portal for user control, on page 1891.
g) (Optional) To add conditions to the identity rule, see Identity rule conditions, on page 1945.
h) Click **Add**.

Step 5 In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Identity rule fields

Configure identity rules to specify authentication actions for users, including Passive Authentication, Active Authentication, or No Authentication. Learn how VPN identity preference affects authentication and rule processing in remote access scenarios.

Use these fields to configure identity rules.

Enabled

Enabling this option enables the identity rule in the identity policy. Unselecting this option disables the identity rule.

Action

Specify the type of authentication you want to perform on the users in the specified realm: **Passive Authentication** (default), **Active Authentication**, or **No Authentication**. You must fully configure the authentication method, or *identity source*, before selecting it as the action in an identity rule.

Additionally, if VPN is enabled (configured on at least one managed device), remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule action. This means that, if VPN is enabled, VPN identity determination is performed first for all sessions regardless of the selected action. If a VPN identity is found on the specified realm, this is the identity source used. No additional captive portal active authentication is done, even if selected.

If the VPN identity source is not found, the process continues according to the specified action. You cannot restrict the identity policy to VPN authentication only because if the VPN identity is not found, the rule is applied according to the selected action.

Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include an SSL policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

For information about which passive and active authentication methods are supported in your version of the system, see About user identity sources, on page 1820.

Sample identity policies and rules

These sections provide examples of configuring an identity policy with either a passive authentication rule or an active authentication rule. In addition, because you can authenticate users with active authentication using either realms or realm sequences, separate examples are provided.

Authentication types

Active authentication means the user authenticates using the captive portal; the user enters network credentials before being allowed to access allowed resources. (RA-VPN is another type of active authentication but it cannot be used together with captive portal authentication. For more information, see Remote access VPN identity sources, on page 1931.)

Passive authentication covers all other types. Passive authentication includes using Microsoft Active Directory realms, Microsoft Azure Active Directory realms, Cisco Identity Services Engine, and others.

These examples use these assumptions:

- Microsoft Active Directory (AD) realm named forest.example.com with two child domains configured in a trust relationship:
  - US-West
  - US-East
- A realm sequence named US that includes both realms
- Passive authentication rule that authenticates users with a realm sequence
- Two active authentication rules:
  - One rule that authenticates users with a realm and uses the NTLM authentication protocol
  - One rule that authenticates users with a realm sequence and uses the HTTP Response Page authentication protocol
- Each sample identity rule is associated with a different identity policy

When you configure a Passive Authentication identity rule, you can choose to authenticate users either with LDAP, a Microsoft Active Directory realm, or a Microsoft AD realm sequence. You can use a realm to authenticate with any authentication type; realm sequence restricts the authentication types you can use. For an example, see Create an identity policy with a passive authentication rule, on page 1955.

When you configure an Active Authentication identity rule, you can choose to authenticate users either with LDAP, a Microsoft Active Directory realm, or a Microsoft AD realm sequence. You can use a realm to authenticate with any authentication type; realm sequence restricts the authentication types you can use.

You can also authenticate users with a Microsoft Active Directory realm sequence except for these authentication types:

- NTLM
- Kerberos
- HTTP Negotiate

For an example, see Create a sample identity policy with an active authentication rule, on page 1956.

Create an identity policy with a passive authentication rule

Create an identity policy that authenticates users using passive authentication with realm sequences for user identification.

This task discusses how to create an identity policy with a passive authentication rule that authenticates users using the US realm sequence. If a user is not found in the first realm in the sequence, the system searches the other realms in the sequence in the order listed in the realm sequence. If a user is still not found in the realm or realm sequence, the user is identified as Unknown.

You can optionally authenticate a user with the captive portal (that is, active authentication) if the user is not found in any realm in the sequence. For more information, see Best practices for captive portal guidelines and limitations, on page 1889.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Click **New Policy**.

a) Enter a **Name** for the policy and an optional **Description**.
b) Click **Save**.

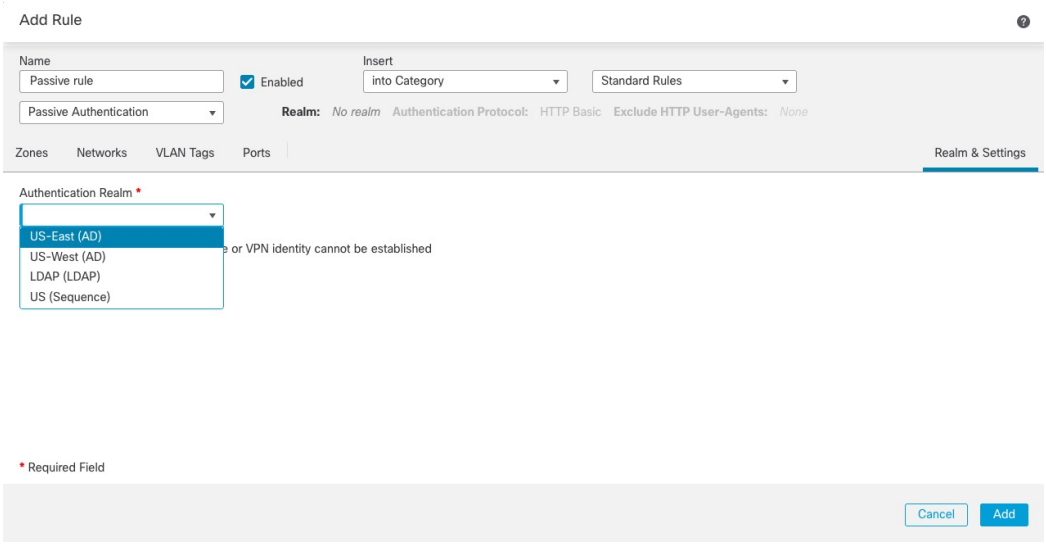
Step 4 Click **Add Rule**.

a) Enter a **Name** for the rule.
b) From the list, click **Passive Authentication**.

Step 5 Click the **Realms & Settings** tab page.

a) From the list, click the name of a realm or realm sequence.

The following figure shows an example.



- If you choose a realm (such as **US-East** in the example), the system searches that realm for users to match the rule. If a user is not found, the user is identified as Unknown.
- If you choose a realm sequence (**US (Sequence)** in the example), users are searched in every realm in the sequence in the order specified in the sequence. If the user is not found, the user is identified as Unknown.
- You can also choose an LDAP realm.
- For additional ways to authenticate the user, check **Use active authentication if passive or VPN identity cannot be established**. For more information, see Best practices for captive portal guidelines and limitations, on page 1889.

Step 6 (Optional.) To filter traffic by network object, click the **Identity Source** tab. From the list, click the network object to use to filter traffic for this identity policy. Click **Add** (+) to create a new network object.

Step 7 Set identity rule conditions as discussed in Identity rule conditions, on page 1945.

Step 8 Associate the identity rule with an access control rule as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 9 Deploy configuration changes to managed devices; see Deploy configuration changes, on page 135.

Create a sample identity policy with an active authentication rule

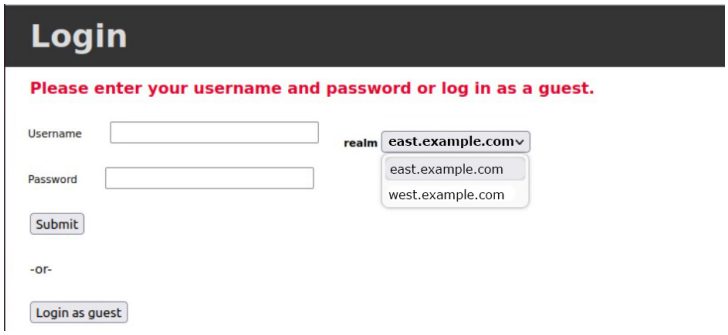
This task shows you how to configure an identity policy with an Active Authentication rule where authentication is performed using either a realm or a realm sequence. This enables secure network access management through customizable captive portal settings.

The associated tasks show an examples of configuring an identity policy with an **Active Authentication** rule where authentication is performed using either a realm or a realm sequence.

The differences follow:

- *Realm* enables you to use any supported authentication type (currently, **HTTP Basic**, **NTLM**, **Kerberos**, **HTTP Negotiate**, or **HTTP Response Page**).
- *Realm sequence* limits you to only the **HTTP Basic** or **HTTP Response Page** authentication types.

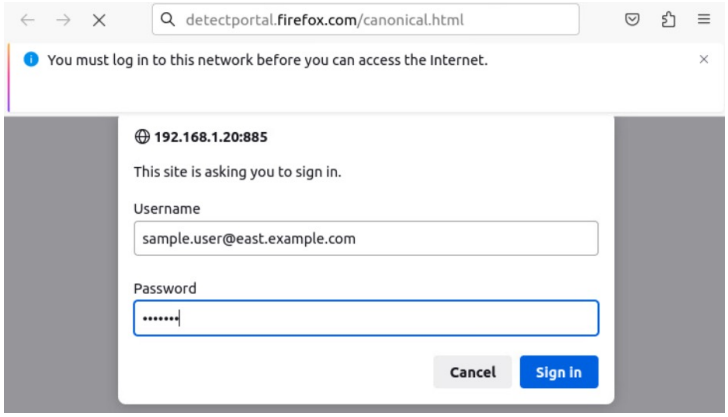
  Users who authenticate with a realm sequence and the HTTP Response Page authentication type see the following by default:



  The user can authenticate in any of the following ways:

  - If a list of realms in the realm sequence is displayed (as shown), the user must enter their user name and password in the provided fields and click the name of their realm from the list.
  - If realms are not displayed in a list, the user can enter their credentials in `username@domain` format.

  Users who authenticate with a realm and the HTTP Basic authentication page see the following:



  The user must enter their user name in `username@domain` format.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Click **New Policy**.

a) Enter a **Name** for the policy and an optional **Description**.

b) Click **Save**.

Step 4 Click the **Active Authentication** tab.

Enter the following information:

- **Server Certificate**: From the list, click an internal certificate object to use for secure connection to the Firewall Threat Defense device, or click **Add** (+) to add one.
- **Redirect to Host Name**: (Optional.) From the list, click a network object to which to redirect captive portal requests. If you omit this value, requests redirect to the IP address of the managed device. You can click **Add** (+) to create a new network object. For more information, see Redirect to host name network rule conditions, on page 1946.

  Managed devices must have Snort 3 enabled to use this option.
- **Port**: Enter a port for the captive portal to use. This port must be unique for the captive portal and must match an access control rule you set up as discussed in Create a TCP port access control rule, on page 1896. (Default is 885.)
- **Maximum login attempts**: Enter the maximum number of login attempts before login fails. (Default is 3.)
- **Share active authentication sessions across firewalls**: Uncheck to enable the Firewall Management Center to force users to reauthenticate every time they access your network using a different managed device than the last time.

  For more information about this option, see Captive portal fields, on page 1903.
- **Active Authentication Response Page**: Choose a system-provided or custom login page for captive portal users. For more information about your options, see Captive portal fields, on page 1903.

Step 5 Click **Save** to save your changes to the identity policy.

Step 6 Click the **Rules** tab.

Step 7 Click **Add Rule**.

a) Enter a **Name** for the rule.
b) From the list, click **Active Authentication**.

Step 8 Click the **Realms & Settings** tab page. Then configure an active authentication method for the users.

What to do next

Continue with one of the following sections:

- Active authentication using a realm, on page 1958
- Active authentication using a realm sequence, on page 1959

Active authentication using a realm

This task authenticates captive portal users with a realm and any available authentication protocol (currently, **HTTP Basic**, **NTLM**, **Kerberos**, **HTTP Negotiate**, or **HTTP Response Page**).

Active authentication using a realm provides secure user verification for captive portal access by integrating with your organization's authentication infrastructure.

Before you begin

Complete the task discussed in Create a sample identity policy with an active authentication rule, on page 1956.

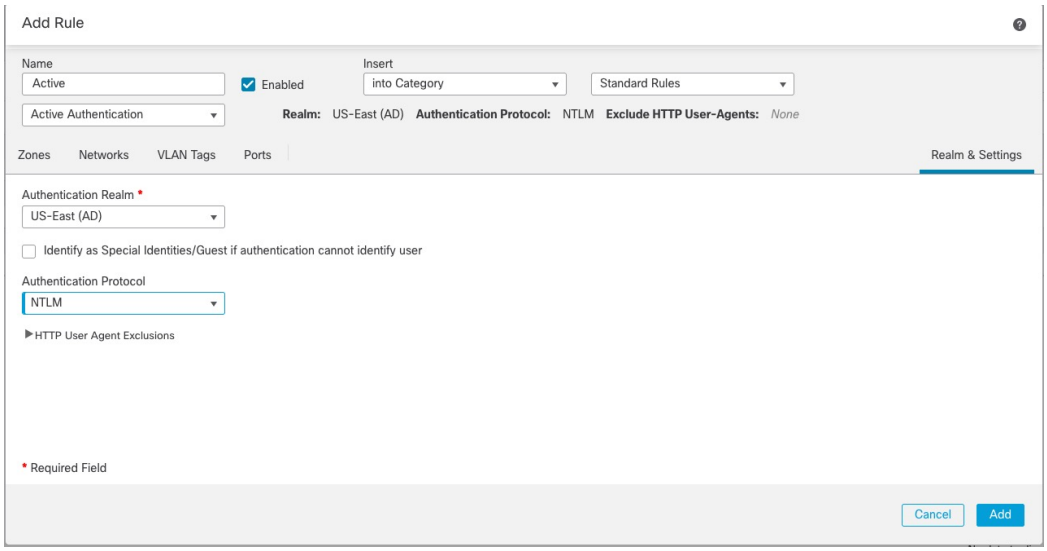
Procedure

Step 1 Continue from Create a sample identity policy with an active authentication rule, on page 1956.

Step 2 On the **Realms & Settings** tab page, click **US-East**.

Step 3 From the **Authentication Protocol** list, click **NTLM**.

The following figure shows an example.



If you choose a realm (such as in the example), the system searches that realm for users to match the rule. If a user is not found, the user is identified as Unknown.

Step 4 Click **Add**.

Step 5 (Optional.) To filter traffic by network object, click the **Identity Source** tab. From the list, click the network object to use to filter traffic for this identity policy. Click **Add** (+) to create a new network object.

Step 6 Set identity rule conditions as discussed in Identity rule conditions, on page 1945.

Step 7 Associate the identity rule with an access control rule as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 8 Deploy configuration changes to managed devices; see Deploy configuration changes, on page 135.

Active authentication using a realm sequence

This task enables authentication of captive portal users using a realm sequence, allowing you to control access through HTTP Basic or HTTP Response Page protocols. It helps you select realms, set identity rule conditions, and associate them with access control rules to filter network traffic and manage user identification.

This task discusses how to authenticate captive portal users with a realm sequence, which restricts you to the **HTTP Basic** or **HTTP Response Page** authentication protocols.

Before you begin

Complete the task discussed in Create a sample identity policy with an active authentication rule, on page 1956.

Procedure

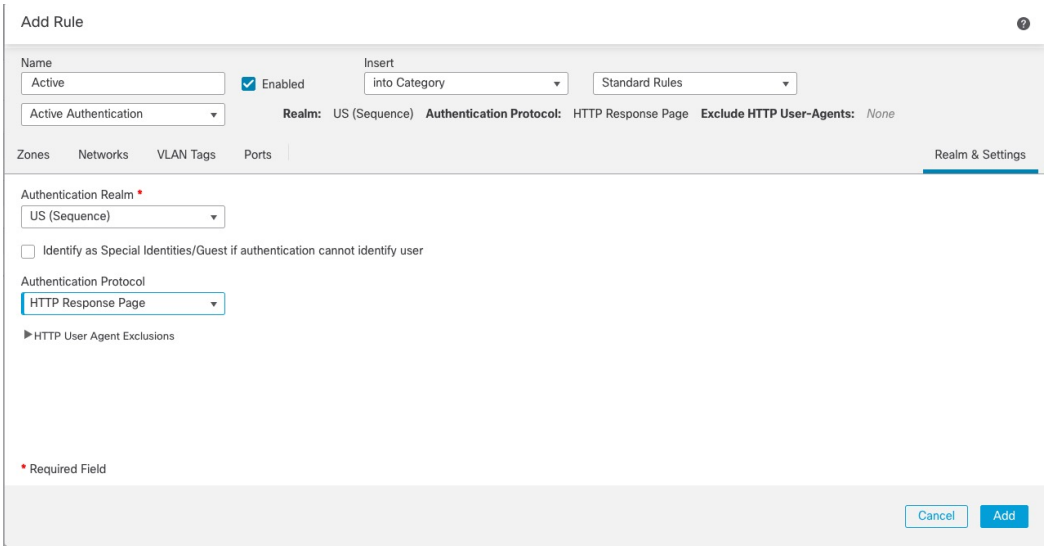
Step 1 Continue from Create a sample identity policy with an active authentication rule, on page 1956.

Step 2 On the **Realms & Settings** tab page, click the name of a realm from the list.

Step 3 From the list, click **US-East**.

Step 4 From the **Protocol** list, click **HTTP Response Page**.

The following figure shows an example.



If you choose a realm sequence (such as in the example), the system searches realms in the sequence in the order specified in the realm sequence. The first realm in the sequence can be referred to as the *default* realm; it's the realm that is used if the user does not change it. If a user is not found, the user is identified as Unknown.

(Only if you upgraded to version 7.4.1 from an earlier version.) Edit the HTTP response page so it shows the list of realms in the sequence as discussed in Update a custom authentication form, on page 1896.

Step 5 Click **Add**.

Step 6 (Optional.) To filter traffic by network object, click the **Identity Source** tab. From the list, click the network object to use to filter traffic for this identity policy. Click **Add** (+) to create a new network object.

Step 7 Set identity rule conditions as discussed in Identity rule conditions, on page 1945.

Step 8 Associate the identity rule with an access control rule as discussed in Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 9 Deploy configuration changes to managed devices; see Deploy configuration changes, on page 135.

Manage an identity policy

This task allows you to manage identity policies by performing various administrative actions including editing, deleting, copying, generating reports, and organizing policies into categories for optimized security policy administration.

Identity policies control access to network resources based on user identity. Managing these policies effectively ensures proper security enforcement and administrative organization within the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 To delete a policy, click **Delete** ( ). If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 To edit a policy, click **Edit** ( ) next to the policy and make changes as described in Create an identity policy, on page 1943. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 5 To copy a policy, click **Copy** ( ).

Step 6 To generate a report for the policy, click **Report** ( ) as described in Generate current policy reports, on page 153.

Step 7 To compare policies, see Compare policies, on page 152.

Step 8 To create a folder in which to organize policies, click **Add Category**.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

Manage an identity rule

This task allows you to edit, delete, or organize identity rules in access control policies to manage user access and security within the Secure Firewall Management Center.

Use this procedure to modify existing identity rules, remove unnecessary rules, or organize rules using categories to maintain effective security policies.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Identity**.

Step 3 Click **Edit** ( ) next to the policy you want to edit. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 To edit an identity rule, click **Edit** ( ) and make changes as described in Create an identity policy, on page 1943.

Step 5 To delete an identity rule, click **Delete** ( ).

Step 6 To create a rule category, click **Add Category** and choose the position and the rule.

Step 7 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Troubleshoot user control

If you notice unexpected user rule behavior, consider tuning your rule, identity source, or realm configurations. For other related troubleshooting information, see:

- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues, on page 1927
- Troubleshoot the TS agent identity source, on page 1938
- Troubleshoot the captive portal identity source, on page 1906
- Troubleshoot realms and user downloads, on page 1877

Rules targeting realms, users, or user groups are not matching traffic

If you configure a TS Agent or ISE/ISE-PIC device to monitor a large number of user groups, or if you have a very large number of users mapped to hosts on your network, the system may drop user records due to your Firewall Management Center user limit. As a result, rules with user conditions may not match traffic as expected.

Rules targeting user groups or users within user groups are not matching traffic as expected

If you configure a rule with a user group condition, your LDAP or Active Directory server must have user groups configured. The system cannot perform user group control if the server organizes the users in basic object hierarchy.

Rules targeting users in secondary groups are not matching traffic as expected

If you configure a rule with a user group condition that includes or excludes users who are members of a secondary group on your Active Directory server, your server may be limiting the number of users it reports.

By default, Active Directory servers limit the number of users they report from secondary groups. You must customize this limit so that all of the users in your secondary groups are reported to the Firewall Management Center and eligible for use in rules with user conditions.

Rules are not matching users when seen for the first time

After the system detects activity from a previously-unseen user, the system retrieves information about them from the server. Until the system successfully retrieves this information, activity seen by this user is *not* handled by matching rules. Instead, the user session is handled by the next rule it matches (or the policy's default action, if applicable).

For example, this might explain when:

- Users who are members of user groups are not matching rules with user group conditions.
- Users who were reported by a TS Agent or ISE device are not matching rules, when the server used for user data retrieval is an Active Directory server.

Note that this might also cause the system to delay the display of user data in event views and analysis tools.

Rules are not matching all ISE/ISE-PIC users

This is expected behavior. You can perform user control on ISE/ISE-PIC users who were authenticated by an Active Directory domain controller. You cannot perform user control on ISE/ISE-PIC users who were authenticated by an LDAP, RADIUS, or RSA domain controller.

Users and groups using too much memory

If processing users and groups is using too much memory, health alerts are displayed. Remember that all user sessions are propagated to all devices managed by the Firewall Management Center. If your Firewall Management Center manages devices with different amounts of memory, the device with the least amount of memory determines the number of user sessions the system can handle without errors.

It's not possible to tune memory allocated to identity processes; even if a device has available memory, it can report out-of-memory issues. If issues persist, you have these options:

- Segregate lower capacity managed devices on subnets and configure ISE/ISE-PIC to not report passive authentication data to those subnets.

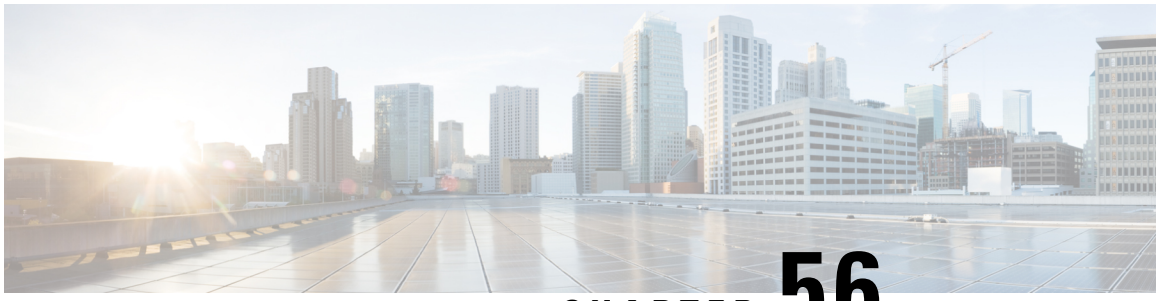
  See the chapter on managing network devices in the *Cisco Identity Services Engine Administrator Guide*.
- Unsubscribe from Security Group Tags (SGTs).
- Upgrade your managed device to a model with more memory.



PART XI

Advanced Policies and Settings for Access Control

- Prefilter Policies , on page 1967
- DNS Policies for Security Intelligence, on page 1993
- File Policies for Network Malware Protection, on page 2015
- Dynamic Attributes Connector, on page 2061
- Threat Intelligence Director, on page 2121
- Advanced Settings for Access Control, on page 2169
- Service Policies, on page 2191
- Threat Detection, on page 2211
- Elephant Flow Detection, on page 2221



CHAPTER 56

Prefilter Policies

The prefilter policy is the first security policy applied to incoming connections. Prefilter rules evaluate traffic on layer 3/4 criteria only, that is, protocol and source/destination IP address and port. They give you a chance to make early decisions on connections so you can avoid further processing and improve device performance.

- Prefilter policies, on page 1967
- Requirements and prerequisites for prefilter policies, on page 1976
- Guidelines and limitations for the prefilter policy, on page 1976
- Guidelines and limitations for encapsulated traffic handling, on page 1977
- Best practices for fastpath prefiltering, on page 1978
- Configure prefilter policies, on page 1979
- Examples of prefilter policy, on page 1988
- History for the prefilter policy, on page 1992

Prefilter policies

A prefilter policy is a security policy that

- serves as the first security policy applied to incoming connections
- evaluates traffic on layer 3/4 criteria only, including protocol and source/destination IP address and port
- enables early decisions on connections to avoid further processing and improve device performance, and
- can fast path connections and make them eligible for flow offload.

Prefilter policy actions

Use prefilter policies to implement these main actions:

- Improve performance—The sooner you exclude traffic that does not require inspection, the better. Specifically, you can perform these actions.
  - Offload trusted flows—If your device supports flow offload, use the prefilter Fastpath action to identify flows you trust to be eligible for offloading to NIC processing. No further processing, including inspection, is needed for these connections. Refer to Best practices for fastpath prefiltering, on page 1978 and Large flow offloads, on page 1971.
  - Block unwanted connections—For example, if you want to block entire subnets, protocols, or TCP/UDP ports, configure this in the prefilter policy.

- Rezone plain text encapsulated tunnels so you can handle them as a unit in the access control policy. Some protocols, such as GRE, create plain-text tunnels that include many connections. By rezoning a tunnel, you assign it a tag, which you can select in access control rules as a source or destination zone. This allows you to apply customized intrusion or other rules to the tunneled traffic and provides granular insight and control.

Note VPN or other encrypted tunnels are not plain-text tunnels and cannot be rezoned.

You must assign each access control policy a prefilter policy. However, the system comes with a pre-defined prefilter policy that might work for you.

Default prefilter policy

A default prefilter policy only analyzes plain-text encapsulated tunnels. It is automatically assigned when you create a new access control policy. It cannot be deleted from the system.

Default prefilter policy characteristics

Every access control policy must have an assigned prefilter policy. For convenience, the system includes a default prefilter policy that is automatically assigned when you create a new access control policy.

You can instead change the default policy to block all plain-text tunnels. See Configuring the default action, on page 1981.

If you want to do any other customization, including adding prefilter or tunnel rules, you must create your own prefilter policy and assign it to the appropriate access control policies, as explained in Assign access control policy to devices, on page 1583.

Prefilter policy rule order

Prefilter policy rule order is a traffic processing mechanism that determines which tunnel rules and prefilter rules handle network traffic first and applies the default action for unmatched tunnels.

Rule processing sequence

In a prefilter policy, tunnel rules, prefilter rules, and a default action handle network traffic:

- Tunnel and prefilter rules—First, rules in a prefilter policy handle traffic in the order you specify. Tunnel rules match specific tunnels only. Prefilter rules have a wider range of constraints.

  Rules are match in top-down order, first match wins. Thus, rule order is critical. For example, you might want to block an entire subnet except for two specific IP addresses on the subnet. In that case:

  - The first rule should specify the two allowable IP addresses as the source network, and the rule action would be Analyze. Connections from these two IP addresses would match this rule, and the next rule would not be processed.
  - The next rule should specify the entire subnet as the source network, with Block for the rule action.

  For more information, see Tunnel vs prefilter rules, on page 1969.

- Default action (tunnels only)—If a tunnel does not match any rules, the default action handles it. The default action can block these tunnels or continue access control on their individual encapsulated connections (Analyze action).

  There is no default action for nonencapsulated traffic. If a nonencapsulated connection does not match any prefilter rules, the system continues with access control. These connections might subsequently be blocked by other policies, or ultimately allowed.

If you need to change rule order, you can:

- Drag and drop the rule to the right location.
- Right click the rule and **Cut**, then find the right location, right click, and select **Paste Above** or **Paste Below**.
- Edit the rule and use the **Insert** control to change its location.

Tunnel vs prefilter rules

Choose to configure a tunnel rule or a prefilter rule based on the type of traffic you want to match and the actions or analysis you intend to perform.

Characteristic	Tunnel Rules	Prefilter Rules
Primary function	Quickly fastpath, block, or rezone plaintext, passthrough tunnels.	Quickly fastpath or block any other connection that benefits from early handling.
Encapsulation and port/protocol criteria	Encapsulation conditions match only plaintext tunnels over selected protocols: GRE, IP-in-IP, IPv6-in-IP, Teredo.	Port conditions can use a wider range of port and protocol constraints than tunnel rules; see Port, protocol, and ICMP code rule conditions (concept), on page 1323.
Network criteria	Tunnel endpoint conditions constrain the endpoints of the tunnels you want to handle.	Network conditions constrain the source and destination hosts in each connection.
Direction	Bidirectional or unidirectional (configurable). Tunnel rules are bidirectional by default, so they can handle all traffic between tunnel endpoints.	Unidirectional only (nonconfigurable). Prefilter rules match source-to-destination traffic only. Return traffic for allowed connections is also permitted.
Rezone sessions for further analysis	Supported, using tunnel zones; see Using tunnel zones to apply access control at the tunnel level, on page 1970.	Not applicable.

How the system processes plain-text tunnels

Some protocols, such as GRE, create plain-text (not encrypted) tunnels that contain (or encapsulate) multiple inner connections. These connections might flow between discontinuous networks. These tunnels are especially useful for routing custom protocols over IP networks, IPv6 traffic over IPv4 networks, and so on.

Summary

A plain-text tunnel has two sets of IP headers:

- Outer headers: Specify tunnel endpoint addresses for prefilter policy handling
- Inner headers: Contain actual connection endpoint addresses for granular inspection

Workflow

The system processes plain-text tunnels through these stages:

1. The system receives a plain-text tunnel with dual IP header structure.
   - Outer header—An outer encapsulation header specifies the source and destination IP addresses of the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.
   - Inner headers—Inner payload headers specify the source and destination IP addresses of the encapsulated connections' actual endpoints. There are separate headers for each connection contained within the tunnel.

   For regular, non-tunneled connections, there is only the "outer" header, as the connection does not contain any subordinate connections.
2. The prefilter policy processes the outer tunnel headers to determine handling approach.

   The prefilter policy uses outer headers to handle traffic. You can block or fast path entire plaintext, passthrough tunnels at this stage.

   If you do not want to allow plain-text tunnels at all, you can set the default action in the prefilter policy to block all plain-text tunnels. This block does not apply to encrypted tunnels such as VPN.
3. The system exposes inner headers for tunnels that pass prefilter analysis.

   Any tunnels that you analyze (that is, not block or fast path) have these inner headers exposed for use by the rest of the security policies and other features such as QoS. These features use the innermost detectable level of headers to ensure the most granular level of inspection and handling possible. This ensures that bad actors cannot hide illegitimate traffic within a plain-text tunnel.

   Alternatively, you can use tunnel zones to re-tag tunneled traffic so that you can write access control rules specifically for select tunnels. This lets you customize intrusion inspection or other layer 7 filtering to connections contained with a tunnel. See Using tunnel zones to apply access control at the tunnel level, on page 1970.

Using tunnel zones to apply access control at the tunnel level

A tunnel zone represents certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis. Although a tunnel zone is not an interface object, you can use it as an interface constraint in some configurations.

Tunnel zone implementation

As explained in How the system processes plain-text tunnels, on page 1969, once a plain-text tunneled connection passes through the prefilter policy, the access control policy applies its rules to each connection contained within the tunnel.

However, you might want to apply the same policy to all the connections within a tunnel. For example, you might have a special intrusion policy you want to use for tunneled connections.

To make it possible to apply access control rules to all connections within a tunnel, you must use the prefilter policy to re-zone the tunnel. Rezoning applies a tunnel zone tag to the plain-text tunnel. You can then use that tunnel zone instead of a security zone when you define the source interface criterion of an access control rule.

Because a tunnel zone does not contain interfaces, the source interface through which the tunnel enters the device is not relevant. You can apply a tunnel zone tag to multiple tunnels that enter the device through different interfaces and access control treats them all in the same way.

Note Connections in rezoned tunnels do not match security zone constraints in an access control rule. After you rezone a tunnel, access control rules match encapsulated connections with their newly assigned tunnel zone, not the original security zone.

See Rezone tunnels for customized inspection, on page 1988 for a walkthrough of a tunnel zone implementation, and a discussion of the implications of rezoning without explicitly handling rezoned traffic.

Large flow offloads

A large flow offload is a hardware-based traffic processing feature that

- handles certain fastpathed traffic in the NIC hardware rather than in the Firewall Threat Defense software
- results in higher throughput and lower latency for data-intensive applications such as large file transfers, and
- includes both static flow offload (based on prefilter policy configuration) and dynamic flow offload (based on trust and other criteria).

Supported models and offload types

For the following models, certain traffic that you configure to be fastpathed by a prefilter policy is handled by the hardware (specifically, in the NIC), not by the Firewall Threat Defense software:

- Firepower 4100/9300
- Secure Firewall 3100 (static only)
- Secure Firewall 4200 (static only)

Offloaded flows continue to receive limited stateful inspection, such as basic TCP flag and option checking. The system can selectively escalate packets to the firewall system for further processing if necessary.

Two types of flow offload are available:

- *Static flow offload*: Offloads flows based on prefilter policy configuration that applies the Fastpath action.
- *Dynamic flow offload*: By default, devices offload flows based on other criteria, including trust.

Applications that can benefit from offloading large flows include:

- High Performance Computing (HPC) Research sites, where the firewall is deployed between storage and high compute stations. When one research site backs up using FTP file transfer or file sync over NFS,

the large amount of data traffic affects all connections. Offloading FTP file transfer and file sync over NFS reduces the impact on other traffic.

- High Frequency Trading (HFT), where the firewall is deployed between workstations and the Exchange, mainly for compliance purposes. Security is usually not a concern, but latency is a major concern.

Flows that can be offloaded include:

- (Static flow offload only.) Connections that are fastpathed by the prefilter policy.
- Standard or 802.1Q tagged Ethernet frames only.
- (Dynamic flow offload only):
  - Inspected flows that the inspection engine decides no longer need inspection. These flows include:
    - Flows handled by access control rules that apply the Trust action and are based on security zone, source and destination network and port matching only.
    - TLS/SSL flows that are not selected for decryption using a decryption policy.
    - Flows that are trusted by the Intelligent Application Bypass (IAB) policy either explicitly or due to exceeding flow bypass thresholds.
    - Flows that match file or intrusion policies that result in trusting the flow.
    - Any allowed flow that no longer needs to be inspected.
  - IPS preprocessor inspected flows:
    - SSH and SMTP.
    - FTP preprocessor secondary connections.
    - Session Initiation Protocol (SIP) preprocessor secondary connections.
  - Intrusion rules that use keywords (also referred to as *options*)



Important For details, exceptions, and limitations to the above, see Restrictions for flow offload implementation, on page 1973.

Static flow offload configuration

To offload eligible traffic to hardware, create a prefilter policy rule that applies the **Fastpath** action. Use prefilter rules for TCP/UDP, and tunnel rules for GRE.

(Not recommended.) To disable flow offload, use FlexConfig:

- Disable static (and thereby dynamic) flow offload: **no flow-offload enable**
- Re-enable flow offload: **flow-offload enable**

For more information, see *Cisco Secure Firewall ASA Series Command Reference*.

Dynamic flow offload configuration

Dynamic flow offload is enabled by default. However, dynamic offload occurs only if static flow offload is enabled, regardless of whether prefiltering is configured.

To disable dynamic flow offload, use the device CLI:

- Disable dynamic offload: **configure flow-offload dynamic whitelist disable**
- Re-enable dynamic offload: **configure flow-offload dynamic whitelist enable**

Restrictions for flow offload implementation

Device limitations

The feature is supported on the following devices:

- Secure Firewall 3100 (static only)
- Secure Firewall 4200 (static only)
- Firepower 4100/9300

Flows that cannot be offloaded

Do not attempt to offload these flow types:

- Any flows that do not use IPv4 addressing, such as IPv6 addressing.
- Flows for any protocol other than TCP, UDP, and GRE.



Note PPTP GRE connections cannot be offloaded.

- Flows on interfaces configured in passive, inline, or inline tap mode. Routed and switched interfaces are the only types supported.
- (3100/4200.) Offload based on inner header for tunnelled flows.
- (3100/4200.) Multi-instance offload.
- Flows that require inspection by Snort or other inspection engines. In some cases, such as FTP, the secondary data channel can be offloaded although the control channel cannot be offloaded.
- IPsec and TLS/DTLS VPN connections that terminate on the device.



Note The Secure Firewall 3100 and Secure Firewall 4200 platforms are exceptions to this restriction. These platforms support flow-offload for IPsec and DTLS VPN connections terminating to the device. For detailed information on this feature and its implementation, please refer to the release notes specific to the Secure Firewall 3100 and Secure Firewall 4200 platforms.

- Flows that require encryption or decryption. For example, connections decrypted due to a decryption policy.
- Multicast flows in routed mode. They are supported in transparent mode if there are only two member interfaces in a bridge group.
- TCP Intercept flows.
- TCP state bypass flows. You cannot configure flow offload and TCP state bypass on the same traffic.
- Flows tagged with security groups.
- Reverse flows that are forwarded from a different cluster node, in the case of asymmetric flows in a cluster.
- Centralized flows in a cluster, if the flow owner is not the control unit.
- Flows that include IP options cannot be dynamically offloaded.

Additional limitations

Consider these operational restrictions when implementing flow offload:

- Flow offload and Dead Connection Detection (DCD) are not compatible. Do not configure DCD on connections that can be offloaded.
- If more than one flow that matches flow offload conditions are queued to be offloaded at the same time to the same location on the hardware, only the first flow is offloaded. The other flows are processed normally. This is called a *collision*. Use the **show flow-offload flow** command in the CLI to display statistics for this situation.
- Dynamic flow offload disables all TCP normalizer checks.
- Although offloaded flows pass through FXOS interfaces, statistics for these flows do not appear on the logical device interface. Thus, logical device interface counters and packet rates do not reflect offloaded flows.

Conditions for reversing offload

After a flow is offloaded, packets within the flow are returned to the firewall operating system for further processing if they meet these conditions:

- They include TCP options other than Timestamp.
- They are fragmented.
- They are subject to Equal-Cost Multi-Path (ECMP) routing, and ingress packets move from one interface to another.
- A change to the routing table applies to the flow. A packet is returned to the device to determine the new route.

Prefilter vs access control policy

Prefilter and access control policies both allow you to block and trust traffic. In a prefilter policy, the "trust" functionality is called "fastpathing" because it skips more inspection. If you do not configure a custom prefilter

policy, you can only approximate, but not replicate, prefilter functionality using Block and Trust rules placed early in the access control policy.

Characteristic	Prefilter Policy	Access Control Policy
Primary function	Quickly fastpath or block certain types of plaintext or passthrough tunnels, or tailor subsequent inspection to encapsulated traffic. Fastpath or block any other connections that benefit from early handling.	Inspect and control all network traffic, using simple or complex criteria, including contextual information and deep inspection results.
Sequence within access control	First The system matches traffic to prefilter criteria before all other access control configurations. Thus, fast-pathing in a prefilter policy skips many other policies and inspections.	Last Other policies that might inspect a connection, including Security Intelligence and decryption, are applied before access control rules are evaluated.
Rule actions	Fewer You can stop further inspection (Fastpath and Block) or allow further analysis with the rest of access control (Analyze).	More Access control rules have a larger variety of actions, including monitoring, deep inspection, block with reset, and interactive blocking. See Access control rule actions, on page 1614.
Bypass capability	Fastpath rule action Fastpathing traffic in the prefilter stage bypasses all further inspection and handling. This includes: • Security Intelligence • User identity discovery (identity policy) • Decryption • Access control rules • Deep inspection of packet payloads • Discovery • Rate limiting	Trust rule action Traffic trusted by access control rules is only exempt from intrusion inspection and discovery. If another policy that requires inspection is applied to a connection that is eventually trusted, the connection is inspected anyway. Trust means that intrusion and file policies are not applied to the connection.
Rule criteria	Limited Rules in the prefilter policy use simple network criteria: IP address, VLAN tag, port, and protocol. For tunnels, tunnel endpoint conditions specify the IP address of the routed interfaces of the network devices on either side of the tunnel.	Robust Access control rules use network criteria, but also user, application, requested URL, and other contextual information available in packet payloads. Network conditions specify the IP address of source and destination hosts.

Characteristic	Prefilter Policy	Access Control Policy
IP headers used (tunnel handling)	Outermost Using outer headers allows you to handle entire plaintext, passthrough tunnels. For nonencapsulated traffic, prefiltering still uses "outer" headers—which in this case are the only headers.	Innermost possible For a nonencrypted tunnel, access control acts on its individual encapsulated connections, not the tunnel as a whole. See How the system processes plain-text tunnels, on page 1969.
Rezone encapsulated connections for further analysis	Rezones tunneled traffic Tunnel zones allow you to tailor subsequent inspection to prefiltered, encapsulated traffic.	Uses tunnel zones Access control uses the tunnel zones you assign during prefiltering. See Using tunnel zones to apply access control at the tunnel level, on page 1970.
Connection logging	Fastpathed and blocked traffic only. Allowed connections may still be logged by other configurations.	Any connection

Requirements and prerequisites for prefilter policies

This reference provides the requirements and prerequisites necessary for configuring prefilter policies, including supported models, domain requirements, and required user roles.

Model support

Firewall Threat Defense

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Guidelines and limitations for the prefilter policy

You can log connections fast pathed and blocked by the prefilter policy. Prefilter connection events contain information on whether and how logged connections—including entire tunnels—were prefiltered. However, because fast pathed and blocked connections are not subject to deep inspection, associated connection events contain limited information.

Access control uses a hierarchical implementation that complements multitenancy. Along with other advanced settings, you can lock a prefilter policy association, enforcing that association in all descendant access control policies. For more information, see Access control policy inheritance, on page 1572.

When you deploy a prefilter policy, its rules are not applied on the existing connections. Hence, traffic on an existing connection is not bound by the new policy that is deployed. In addition, the policy hit count is incremented only for the first packet of a connection that matches a policy. Thus, the traffic on an existing connection that could match a policy is omitted from the hit count. To have the rules effectively applied, clear the existing connections, and then deploy the policy.

For a prefilter rule with action as Fastpath and logging options disabled, you might observe that the end-of-flow events are still generated in the system. However, the events are not visible on the management center event pages.

Guidelines and limitations for encapsulated traffic handling

Supported encapsulated traffic types

This topic discusses guidelines for the following types of encapsulated traffic:

- Generic Routing Encapsulation (GRE)
- Point-to-Point Protocol (PPTP). (This protocol is not handled by tunnel rules in the prefilter policy.)
- IPinIP
- IPv6inIP
- Teredo

GRE tunnel limitations

GRE tunnel processing is limited to IPv4 and IPv6 passenger flows. Other protocols, such as PPTP and WCCP, are not supported within the GRE tunnel.

GRE v1 and PPTP bypass restrictions

GRE v1 (sometimes referred to as *stateful GRE*) and PPTP traffic bypass outer flow processing.

- Sessions are over a single tunnel that is not load-balanced.
- There is no HA or clustering replication.
- Primary and secondary flow relationships are not maintained.
- Prefilter policy white and black lists are not supported.

Passenger flow processing is supported for IPv6inIP and Teredo but the following limitations apply:

GRE v0 sequence number field requirement

All endpoints sending traffic on the network must send GREv0 traffic with the sequence number field as optional; otherwise, the sequence number field is removed. RFC 1701 and RFC 2784 both specify the sequence field as optional.

Tunnel interface compatibility

Prefilter and access control policy rules are applied to all tunnel types on routed, transparent, inline-set, inline-tap, and passive interfaces.

Protocol references

For more information about the GRE and PPTP protocols, see the following:

- RFC 1701, RFC 2784, and RFC 2890 (GRE protocol v0)
- RFC 2637 (PPTP and GRE protocol v1)

Best practices for fastpath prefiltering

When you use the fastpath action in a prefilter rule, the matching traffic bypasses inspection and is simply transmitted through the device. Use this action for traffic that you can trust and that would not benefit from any of the security features available. Some examples of traffic that you can set fastpath prefiltering for are given below.

- VPN traffic that is going through the device. That is, the device is not an endpoint in the VPN topology.
- SQL traffic between trusted endpoints on the internal network.
- Scanner traffic. Scanner probes can create a lot of false-positive responses from intrusion policies.
- Voice/video.
- Backups.
- Management traffic (sftunnel) that traverses Firewall Threat Defense devices. Performing deep inspection on management traffic (using access control policies) can cause issues. You can prefilter based on port TCP/8305 between the management center and managed devices.

The Threat Defense Snort engine maintains state for each traffic flow and is designed to inspect each flow exactly once. Duplicate or double inspection is unsupported when repeated traffic maps to the same Snort flow key, because the subsequent instance is associated with the existing per-flow state and may be identified as an anomaly.

This can occur when a flow re-enters the device through a different interface or VLAN, is rerouted by an ACI fabric with different VLAN tags, or traverses VRF cross-VLAN paths. The resulting drop may appear in packet-tracer or capture output as:

```
Drop-reason: (stream) Blocked or blacklisted by the stream preprocessor.
```

If a flow-identifying attribute differs such that the traffic maps to a different Snort flow key, Snort can process the flows independently. However, differences in fields that are not part of the flow key do not create a separate flow.

From an optimal network architecture perspective, each traffic flow, in both directions, should traverse the Snort engine only once. If duplicate inspection cannot be avoided, use a prefilter or fastpath rule to bypass Snort inspection for the affected flows.

Configure prefilter policies

Configure prefilter policies to perform custom prefiltering and to control tunnel traffic analysis on managed devices.

To perform custom prefiltering, configure prefilter policies and assign them to access control policies. It is through the access control policy that prefilter policies get assigned to managed devices.

Only one person should edit a policy at a time, using a single browser window. If multiple users save the same policy, the last saved changes are retained. For your convenience, the system displays information on who (if anyone) is currently editing each policy. To protect the privacy of your session, a warning appears after 30 minutes of inactivity on the policy editor. After 60 minutes, the system discards your changes.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Prefilter**.

At the top of the page, there are convenient links to some related features: object management and access control.

You cannot tell from the prefilter page, or when editing a prefilter policy, whether it is used by an access control policy or which policies use it.

Step 2 Do any of the following:

- Create—Click **New Policy** to create a custom prefilter policy. You are prompted for a name and an optional description. The new policy is opened for edit after you click **Save**. A new prefilter policy has no rules and a default action of Analyze all tunnel traffic.
- Edit—Click **Edit** ( ) to open a policy so that you can add rules or otherwise modify it.
- Copy—Click **Copy** ( ). You are prompted for a name. The copy is added to the list when you click **OK**, but it is not opened for edit.
- Delete—Click **Delete** ( ) to remove a policy. You cannot delete a policy that is currently being used by an access control policy.

Step 3 When editing a prefilter policy, you can do the following:

- Set the default action—Set the default action for tunnels at the bottom of the policy. See Configuring the default action, on page 1981.
- Add prefilter rules—Click **Add Prefilter Rule**. The rule is added to the bottom of the policy. See Configure prefilter rules, on page 1981.
- Add tunnel rules—Click **Add Tunnel Rule**. The rule is added to the bottom of the policy. See Configure tunnel rules, on page 1984.
- Insert rules—Right click the rule before where you want to add the new rule, and select either **Insert New Prefilter Rule** or **Insert New Tunnel Rule**, as appropriate.

- Copy/cut and paste rules—To copy a rule, right-click the rule and select **Copy**. You can also cut the rule (remove it) by selecting **Cut**. Then, select where you want to insert the rule, right click, and select either **Paste Above** or **Paste Below**. When copying, a number in parentheses is added to the rule name; you should edit the rule and change the name and other criteria as needed. Cut rules retain the original name.
- Edit a rule—Click **Edit** ( ) to open the rule editor. You can also click on any element for the rule in the table. See Configure prefilter rules, on page 1981 and Configure tunnel rules, on page 1984.
- Delete rules—Click **Delete** ( ) to remove a rule.
- Move a rule—Click a rule and drag and drop it to the right location. Alternatively, cut the rule and then paste it in the right location. You can also change the rule location while editing it.

  Properly creating and ordering rules is a complex task, but one that is essential to building an effective deployment. If you do not plan carefully, rules can preempt other rules or contain invalid configurations. For more information, see Prefilter policy rule order, on page 1968.
- Move a prefilter rule to an associated access control policy—To move a prefilter rule from the prefilter policy to an associated access control policy, right-click the rule and select **Move to another policy**. You cannot move tunnel rules to an access control policy. See Move prefilter rules to an access control policy, on page 1987.
- View hit counts—To view statistics on how many connections matched each rule, click **Analyze Hit Counts**. See View rule hit counts, on page 1586.
- Search for rules—Use the **Search Rules** box to do a plain text search. Type the string and press enter. The search box shows the number of hits and up/down buttons to move through them.

  Matches are highlighted in the table. Matches include partial hits, but only to explicitly set items. For example, entering "any" does not match the default network, but "any-ipv4" will match because it is a network object and not a passive default. Action and rule type do not match the search string.
- View object details—To see the contents of an object used in a rule, right click the object and select **Object Details**.
- Change the policy description—To modify the description of a policy, click in the description text below the policy name at the top of the page. Click away from the description to save changes.

Be sure to click **Save** to save any changes you make.

Step 4 Use the prefilter policy in the appropriate access control policies.

For each access control policy that should use a custom prefilter policy:

- Edit the access control policy and select the prefilter policy in the **Prefilter Policy** link or in the advanced settings. See Associate prefilter, decryption, and identity policies with an access control, on page 1585.
- If you applied tunnel zone tags in any tunnel rules, create access control rules that use those tunnel zones as source interface criteria.

What to do next

Deploy the changes.

If you deploy time-based rules, specify the time zone of the device to which the policy is assigned. See Configure a time zone for a device, on page 911.

Configuring the default action

Use the default action to determine how plain-text encapsulated tunnels that do not match any tunnel rules should be handled.

The default action does not apply to non-tunnel traffic. Any other connections that do not match prefilter rules are passed on for processing by subsequent policies.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Prefilter** and create or edit a prefilter policy.

Step 2 Choose a **Default Action: Tunneled Traffic** option:

a. **Analyze all tunnel traffic**—These tunnels are allowed and their encapsulated connections are evaluated by the access control and other policies

Block all tunnel traffic—Tunnels are dropped and no longer evaluated.

Step 3 If you select **Block all tunnel traffic**, click **Logging** ( ) next to the default action.

See *Logging Connections with a Policy Default Action* in the *Cisco Secure Firewall Management Center Administration Guide* You can configure default action logging for blocked tunnels only.

Configure prefilter rules

Configure prefilter rules to provide early blocking for unwanted traffic and to fast path traffic that does not benefit from access control inspection.

Use prefilter rules in a non-default prefilter policy to provide early blocking for unwanted traffic, and to fast path traffic that does not benefit from access control inspection.

If your device supports flow offload, fast path traffic is eligible for flow offload if it meets all other criteria. See Large flow offloads, on page 1971.

Before you begin

You cannot create rules in the default prefilter policy. If you have not created a custom prefilter policy, do so now.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Prefilter** and create or edit a prefilter policy.

Click **Add Prefilter Rule**.

You can also right-click a rule and select **Insert New Prefilter Rule**.

Select whether the rule should be **Enabled**. A rule must be enabled to affect traffic through the device.

Step 2 Select the **Action** to be taken on matching traffic.

- Fastpath—Exempts matching traffic from all further inspection AND control, including access control, identity requirements, AND rate limiting. These connections are eligible for flow offload if the device supports it.
- Block—Blocks matching traffic without further inspection of any kind.
- Analyze—Allows traffic to continue to be analyzed by the rest of access control. If passed by access control AND any related deep inspection, this traffic may also be rate limited.

Step 3 Select where to **Insert** the rule.

The default is to insert the rule at the end of the policy, but you can select an existing rule and insert the new rule before or after that rule. The action of the first rule that matches a connection is applied to that connection, so order matters.

Step 4 (Optional.) Select the object that defines the **Time Range** for the rule.

You can limit what times of day, or which days, a rule is operational. For example, the rule could apply during business hours only. Select an existing time range object OR create a new one. For more information, see Create a time range object, on page 2435.

Step 5 Configure the traffic matching conditions for the rule.

The rule is applied to connections that match all of the conditions. Within a condition type, separate elements are OR'ed, so that matching any of the selected items counts as a match. For the rule as a whole, all condition types are AND'ed: a connection must match at least one item on each tab to match the rule. You can use these types of conditions:

- **Interface Objects**—Select the security zones OR interface groups that contain the interfaces to which the rule should apply. The default, no objects selected, applies the rule to all interfaces on the device.
- **Networks**—Select the network objects that define the source (**Add to Source**) OR destination (**Add to Destination**) IP addresses, OR both. The default (no objects selected) matches all source AND destination IP addresses.
- **VLAN tags**—Select the objects that define the VLANs to which the rule should apply. For more information, see VLAN tags rule conditions, on page 1983.
- **Ports**—Select the TCP/UDP ports, OR other protocol, for the connections AND add them to the source OR destination criteria. Source criteria is TCP/UDP only, but you can select other protocols for the destination. For more information, see Port rule conditions for prefilter rules, on page 1983.

Step 6 (Fastpath AND Block rules only.) Click **Logging** and configure how matching connections should be logged.

For more information, see *Logging Connections with Tunnel AND Prefilter Rules* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 7 (Optional.) Click **Comment** and add comments to the rule. Use comments to help you understand the purpose of the rule and its change history.

Step 8 Click **Add**. If you need to move the rule, do so now.

Step 9 Click **Save** to save the policy.

VLAN tags rule conditions

VLAN tags rule conditions are filtering mechanisms to control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic.

VLAN tag filtering behavior

Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

Port rule conditions for prefilter rules

Port conditions match traffic based on the source and destination ports.

Port condition types

Depending on the rule type, "port" can represent any of these types:

- TCP and UDP—You can control TCP and UDP traffic based on the port. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP(6)/22. TCP and UDP are the only source ports supported. You can also specify them as destination ports.
- ICMP—You can control ICMP and ICMPv6 (IPv6-ICMP) traffic based on its internet layer protocol plus an optional type and code. For example: ICMP(1):3:3. When you select ICMP as a destination port, you are prompted to specify the type and code.
- Protocol—You can control traffic using other protocols that do not use ports. Not all protocols are supported. You must select the protocol as a destination port.

Source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as destination port conditions in a single access control rule.

Matching Non-TCP Traffic with Port Conditions

You can match non-port-based protocols. By default, if you do not specify a port condition, you are matching IP traffic. However, when matching GRE, IP in IP, IPv6 in IP, or Teredo Port 3544, configure tunnel rules instead of port conditions in prefilter rules.

Configure tunnel rules

Configure tunnel rules to control how encapsulated tunnel traffic is processed by the firewall system.

- Provide early blocking for unwanted encapsulated tunnel traffic.
- Fast path tunnels that do not benefit from access control inspection.
- Place encapsulated tunnels into a tunnel zone, called rezoning, so that you can write access control rules to apply inspection to the connections within the tunnel as a whole.

The prefilter policy's default action applies to encapsulated tunnels. Thus, create rules for tunnel traffic only to apply different actions to specific tunnels.

For example, if the default action is to analyze tunnels, this means that all tunnels are passed on to the access control policies AND other policies that inspect, allow, AND potentially block connections, AND these policies will evaluate the inner connections. If that default action is what you want for all tunnels, then you do not need to create any tunnel rules.

If instead:

- The default action is to block encapsulated tunnels, use rules to exempt specific tunnels from blocking AND either pass them to other access control policies (analyze action) OR bypass any additional processing (fastpath).
- There are tunnels where you want to apply access control rules to all encapsulated connections, create rules to rezone the tunnels to the appropriate tunnel zone tag AND also write rules in the access control policy for those tunnel zone tags.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Prefilter**. Create or edit a prefilter policy.

Step 2 Click **Add Tunnel Rule**.

You can also right-click a rule AND select **Insert New Tunnel Rule**.

a) Enter a **Name** for the rule.
b) Select whether the rule should be **Enabled**.

A rule must be enabled to affect traffic through the device.

c) Select where to **Insert** the rule.

The default is to insert the rule at the end of the policy, but you can select an existing rule AND insert the new rule before OR after that rule. The action of the first rule that matches a connection is applied to that connection, so order matters.

d) (Optional.) Select the object that defines the **Time Range** for the rule.

You can limit what times of day, OR which days, a rule is operational. For example, the rule could apply during business hours only. Select an existing time range object OR create a new one. For more information, see Create a time range object, on page 2435.

Step 3 Select the **Action** to be taken on matching traffic.

- Fastpath—Exempts matching traffic from all further inspection AND control, including access control, identity requirements, AND rate limiting. Fastpathing a tunnel fastpaths all encapsulated connections. These connections are eligible for flow offload if the device supports it.
- Block—Blocks matching traffic without further inspection of any kind. Blocking a tunnel blocks all encapsulated connections.
- Analyze—Allows traffic to continue to be analyzed by the rest of access control using inner headers.. If passed by access control AND any related deep inspection, this traffic may also be rate limited.

a) (Analyze rules only; when rezoning only.) Select a tunnel zone tag in **Assign Tunnel Zone** if your intention is to rezone the tunnel.

Leave this option blank if you want access control to apply to the encapsulated connections within the tunnel without special processing. For more information about rezoning AND tunnel group tags, see:

- Using tunnel zones to apply access control at the tunnel level, on page 1970
- Creating tunnel zones, on page 1986
- Rezone tunnels for customized inspection, on page 1988



Caution Exercise caution when assigning tunnel zones. Connections in rezoned tunnels may not match security zone constraints in later evaluation. See Rezone tunnels for customized inspection, on page 1988 for a brief walkthrough of a tunnel zone implementation, AND a discussion of the implications of rezoning without explicitly handling rezoned traffic.

Step 4 Select one of these options to set the direction for the rule:

- **Match tunnels only from source** (unidirectional)—Match source-to-destination traffic only. Matching traffic must originate from one of the specified source interfaces OR tunnel endpoints, AND leave through one of the destination interfaces OR tunnel endpoints. Return traffic for allowed connections is also permitted. (Note that prefilter rules are always unidirectional.)

- **Match tunnels from source AND destination** (bidirectional)—Match both source-to-destination traffic AND destination-to-source traffic. The effect is identical to writing two unidirectional rules, one the mirror of the other. This is the default.

Step 5 Click the **Encapsulation & Ports** tab and select the protocols for this rule.

You must select at least one of these options in a tunnel rule to specify the encapsulation protocol used. The list includes the IP protocol number for the option.

- **GRE** (47)
- **IP-in-IP** (4)
- **IPv6-in-IP** (41)
- **Teredo** (UDP (17)/3455)

Step 6 Configure the traffic matching conditions for the rule.

The rule is applied to connections that match all of the conditions. Within a condition type, separate elements are OR'ed, so that matching any of the selected items counts as a match. For the rule as a whole, all condition types are AND'ed: a connection must match at least one item on each tab to match the rule. You can use these types of conditions:

- **Interface Objects**—Select the security zones OR interface groups that contain the interfaces to which the rule should apply. The default, no objects selected, applies the rule to all interfaces on the device.
- **Tunnel Endpoints**—The network objects that define the source (**Add to Source**) AND destination (**Add to Destination**) IP addresses of the tunnel. The default (no objects selected) matches all source AND destination IP addresses.
- **VLAN tags**—Select the objects that define the VLANs to which the rule should apply. For more information, see VLAN tags rule conditions, on page 1983.

Step 7 (Fastpath AND Block rules only.) Click **Logging** AND configure how matching connections should be logged.

For more information, see *Logging Connections with Tunnel AND Prefilter Rules* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 8 (Optional.) Click **Comment** AND add comments to the rule.

Use comments to help you understand the purpose of the rule AND its change history.

Step 9 Click **Add**.

If you need to move the rule, do so now.

Click **Save** to save the policy.

Creating tunnel zones

Create a tunnel zone tag to represent certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis.

A *tunnel zone* represents certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis. A tunnel zone is not an interface object, even though you can use it as an interface constraint in access control rules, as explained in Using tunnel zones to apply access control at the tunnel level, on page 1970.

You can create zones in the object manager or when editing a tunnel rule.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **Tunnel Zone** from the list of object types.

Step 3 Click **Add Tunnel Zone**.

You can also edit an existing tunnel or delete a tunnel zone that is not being used in a tunnel rule.

Step 4 Enter a **Name** and, optionally, a **Description**.

Step 5 Click **Save**.

What to do next

- Assign the tunnel zone to plaintext, passthrough tunnels as part of a tunnel rule. See Configure tunnel rules, on page 1984.
- Use the tunnel zone as source interface criteria in an access control rule.

Move prefilter rules to an access control policy

Moving prefilter rules to an access control policy allows you to reposition rules for better policy organization and effectiveness when the rules would function more appropriately within the access control policy structure.

You can move prefilter rules from a prefilter policy to the associated access control policy.

Before you begin

Note the following conditions before you proceed:

- Only prefilter rules can be moved to an access control policy. Tunnel rules cannot be moved.
- The prefilter rules can be moved only to an access control policy that uses the prefilter policy. Because you can use the same prefilter policy in multiple access control policies, you need to select the policies to which the rule should be moved.
- The prefilter rules that use interface groups to define interface criteria cannot be moved. You can move only those rules that use security zones, or that include no interface criteria.
- The **Action** parameter in the prefilter rule is changed to a suitable action in the access control rule when moved.
  - **Analyze** becomes allow.
  - **Block** becomes block.

- **Fastpath** becomes trust.

- The logging configuration in the rule is retained.
- The comments in the prefilter rule configuration are lost after moving the rule. However, a new comment is added in the moved rule mentioning the source prefilter policy.
- While moving rules from the source policy, if another user modifies those rules, you are warned. You can continue with the process after refreshing the page.

Procedure

Step 1 In the prefilter policy editor, select the rules that you want to move with a left-click on your mouse.



Tip To select multiple rules, use Shift+click.

Step 2 Right-click the selected rules and choose **Move to another policy**.

Step 3 Select the destination access control policies and click **Add** to add them to the list of selected policies.

Step 4 From the **Place Rules** drop-down list, choose where you want to position the moved rules:

- To position as the last set of rules in the **Default** section, choose **At the bottom (within the Default section)**.
- To position as the first set of rules in the **Mandatory** section, choose **At the top (within the Mandatory section)**.

Step 5 Click **Move**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Examples of prefilter policy

These topics provide examples of using the prefilter policy.

Rezone tunnels for customized inspection

Rezone GRE tunnels to enable customized inspection policies for encapsulated traffic while maintaining different inspection policies for other traffic in the same security zone.

This example procedure summarizes how you might rezone GRE tunnels for further analysis, using tunnel zones. You can adapt the concepts described here to other scenarios requiring tailored traffic inspection of connections encapsulated in plaintext or passthrough tunnels.

Consider a situation where your organization's internal traffic flows through the Trusted security zone. The Trusted security zone represents a set of interfaces across multiple managed devices deployed in various locations. Your organization's security policy requires that you allow internal traffic after deep inspection for exploits and malware.

Internal traffic sometimes includes plaintext, passthrough, GRE tunnels between particular endpoints. Because the traffic profile of this encapsulated traffic is different from your "normal" interoffice activity—perhaps it is known and benign—you can limit inspection of certain encapsulated connections while still complying with your security policy.

In this example, after you deploy configuration changes:

- Plaintext, passthrough, GRE-encapsulated tunnels detected in the Trusted zone have their individual encapsulated connections evaluated by one set of intrusion and file policies.
- All other traffic in the Trusted zone is evaluated with a different set of intrusion and file policies.

You accomplish this task by *rezoning* GRE tunnels. Rezoning ensures that access control associates GRE-encapsulated connections with a custom *tunnel* zone, rather than their original Trusted *security* zone. Rezoning is required due to the way access control handles encapsulated traffic; see How the system processes plain-text tunnels, on page 1969 and Using tunnel zones to apply access control at the tunnel level, on page 1970.

Procedure

Step 1 Configure custom intrusion and file policies that tailor deep inspection to encapsulated traffic, and another set of intrusion and file policies tailored to nonencapsulated traffic.

Step 2 Configure custom prefiltering to rezone GRE tunnels flowing through the Trusted security zone.

Create a custom prefilter policy and associate it with access control. In that custom prefilter policy, create a tunnel rule (in this example, **`GRE_tunnel_rezone`**) and a corresponding tunnel zone (**`GRE_tunnel`**). For more information, see Configure tunnel rules, on page 1984.

Table 110: GRE_tunnel_rezone tunnel rule

Rule Component	Description
Interface object condition	Match internal-only tunnels by using the Trusted security zone as both a Source Interface Object and Destination Interface Object constraint.
Tunnel endpoint condition	Specify the source and destination endpoints for the GRE tunnels used in your organization. Tunnel rules are bidirectional by default. If you do not change the **Match tunnels from...** option, it does not matter which endpoints you specify as source and which as destination.
Encapsulation condition	Match GRE traffic.
Assign Tunnel Zone	Create the **`GRE_tunnel`** tunnel zone, and assign it to tunnels that match the rule.
Action	Analyze (with the rest of access control).

Step 3 Configure access control to handle connections in rezoned tunnels.

In the access control policy deployed to your managed devices, ensure that the prefilter policy is used. Then, configure a rule (in this example, **`GRE_inspection`**) that handles the traffic you rezoned. For more information, see Create and edit access control rules, on page 1631.

Table 111: GRE_inspection access control rule

Rule Component	Description
Security zone condition	Match rezoned tunnels by using the GRE_tunnel tunnel zone as a Source Zone constraint.
Action	Allow, with deep inspection enabled. Choose the file and intrusion policies tailored to inspect encapsulated internal traffic.

Caution If you skip this step, the rezoned connections may match **any** access control rule not constrained by security zone. If the rezoned connections do not match any access control rules, they are handled by the access control policy default action. Make sure this is your intent.

Step 4 Configure access control to handle nonencapsulated connections flowing through the Trusted security zone.

In the same access control policy, configure a rule (in this example, **`internal_default_inspection`**) that handles non-rezoned traffic in the Trusted security zone.

Table 112: Internal_default_inspection access control rule

Rule Component	Description
Security zone condition	Match non-rezoned internal-only traffic by using the Trusted security zone as both a Source Zone and Destination Zone constraint.
Action	Allow, with deep inspection enabled. Choose the file and intrusion policies tailored to inspect nonencapsulated internal traffic.

Step 5 Evaluate the position of the new access control rules relative to preexisting rules. Change rule order if necessary.

If you place the two new access control rules next to each other, it does not matter which you place first. Because you rezoned GRE tunnels, the two rules cannot preempt each other.

Step 6 Save all changes.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Offload large flows

This task helps improve performance quickly for large connections that you know you can trust by proactively identifying connections as being offload eligible through matching them to a prefilter fastpath rule.

You can use the prefilter policy to configure static flow offload. If your hardware model supports it, flow offload moves eligible fast path connections to NIC processing, avoiding performance intensive inspection.

Some hardware models will dynamically identify off-loadable connections automatically, but you can proactively identify connections as being offload eligible by matching them to a prefilter fastpath rule. This static configuration helps you improve performance quickly for large connections that you know you can trust.

In the following example, it is assumed that two servers are behind sufficient protection so that you can trust the connections between them. Perhaps one server is using the other for backups. Thus, you can write a fastpath rule for any traffic going from the main server, 10.100.1.20/24, to the backup server, 10.100.2.2/24. The example assumes the servers are accessible through regular, physical routed interfaces.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Prefilter** and create or edit a custom prefilter policy.

Step 2 Click **Add Prefilter Rule**.

You can also right-click a rule and select **Insert New Prefilter Rule**.

Step 3 Enter a **Name** for the rule. For example, Offload_Server_A.

Step 4 In **Action**, select **Fastpath**.

Step 5 In **Insert**, select the rule above or below which the rule should be inserted.

You can also move the rule after you create it.

Step 6 Click the **Networks** tab and specify the source and destination servers.

- In the edit box below **Source Networks**, type 10.100.1.20 and click **Add**.
- In the edit box below **Destination Networks**, type 10.100.2.2 and click **Add**.

Step 7 (Optional.) Configure the other traffic matching characteristics for the flow.

Click these tabs to fill in the criteria. Only the Networks tab needs to be configured for this example, so configure these settings only if they make sense for your situation.

- **Interface objects**—The security zones or interface objects that define the source or destination interfaces, or both. This specification is not needed for this example.
- **VLANs**—Because this example uses routed physical interfaces instead of switch interfaces, this setting is not relevant. Even in those circumstances, you do not need to limit the rule based on VLAN.
- **Ports**—If you want to limit the offload to specific TCP/UDP ports, you can specify them. This limits the scope of the rule to these ports only.

Step 8 (Optional.) Click **Logging** and decide whether you want to see syslog events for matching traffic.

Step 9 Click **Add** to add the rule.

Take the time to move the rule to the right location in the policy if it is not already there.

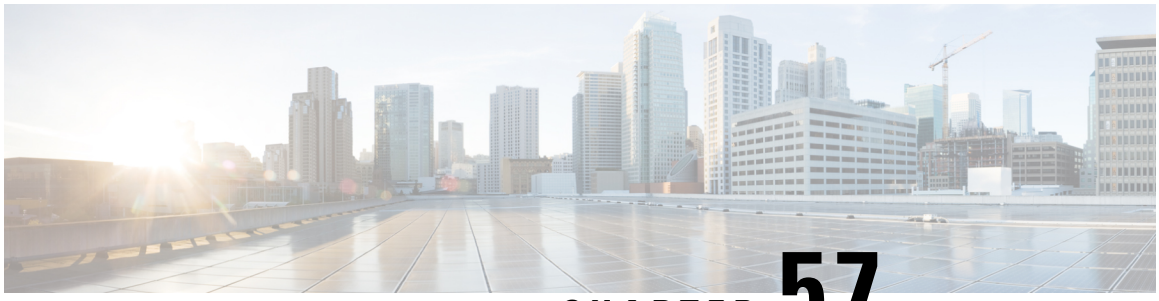
Click **Save** to save the policy.

The next time you deploy the configuration, the rule will be applied to the target devices.

History for the prefilter policy

This reference tracks the evolution of prefilter policy features across software releases, helping administrators understand when specific capabilities were introduced or modified.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Moving prefilter rules to an access control policy	6.7	Any	You can move prefilter rules from a prefilter policy to the associated access control policy. New/modified pages: In the prefilter policy page, the right-click menu for the selected rules provides a new **Move to another policy** option. Supported platforms: Firewall Management Center
Time-based rules	6.6	Any	Ability to apply prefilter and tunnel rules depending on the date and time, as determined by the time zone of the device.
View Object Details from prefilter rule page	6.6	Any	Feature introduced: Option to view details for an object or object group when viewing prefilter rules. New options: Right-clicking a value in any of these columns in the prefilter rule list offers an option to view object details: Source Networks, Destination Networks, Source Port, Destination Port, and VLAN Tag.



CHAPTER 57

DNS Policies for Security Intelligence

The following topics explain DNS policies, DNS rules, and how to deploy DNS policies to managed devices.

- DNS policies, on page 1993
- Cisco umbrella DNS policies, on page 1994
- DNS policy components, on page 1995
- License requirements for DNS policies, on page 1996
- Requirements and prerequisites for DNS policies, on page 1996
- Managing DNS and Umbrella DNS Policies, on page 1996
- DNS rules, on page 1998
- DNS rules, on page 2005
- Requirement: deploy DNS policy configuration changes, on page 2008
- Cisco umbrella DNS policies, on page 2008

DNS policies

A DNS policy is a security configuration that

- blocks traffic based on the domain name requested by a client, using a Security Intelligence Block list
- uses Cisco-provided domain name intelligence to filter traffic
- supports custom lists and feeds of domain names tailored to your deployment, and
- requires association with an access control policy for deployment to managed devices.

DNS policy behavior

Traffic on a DNS policy Block list is immediately blocked and therefore is not subject to any further inspection—not for intrusions, exploits, malware, and so on, but also not for network discovery. You can use a Security Intelligence Do Not Block list to override a Block list and force access control rule evaluation, and, recommended in passive deployments, you can use a "monitor-only" setting for Security Intelligence filtering. This allows the system to analyze connections that would have been blocked by a Block list, but also logs the match to the Block list and generates an end-of-connection Security Intelligence event.

Note DNS-based Security Intelligence may not work as intended for a domain name unless the DNS server deletes a domain cache entry due to expiration, or a client's DNS cache or the local DNS server's cache is cleared or expires.

You configure DNS-based Security Intelligence using a DNS policy and associated DNS rules. To deploy it to your devices, you must associate your DNS policy with an access control policy, then deploy your configuration to managed devices.

Cisco umbrella DNS policies

A Cisco Umbrella DNS policy is a security mechanism that

- redirects DNS queries to Cisco Umbrella for domain validation and policy enforcement,
- allows or blocks requests based on domain names and applies DNS-based security policies, and
- provides two lines of protection through local DNS inspection and cloud-based Cisco Umbrella policies.

DNS query redirection process

Cisco Umbrella DNS Connection in the management center helps to redirect DNS queries to Cisco Umbrella. This allows Cisco Umbrella to validate requests, allow or block them based on the domain names, and apply DNS-based security policy on the request. If you use Cisco Umbrella, you must configure the Cisco Umbrella Connection (**Integration** > **Other Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**) to redirect DNS queries to Cisco Umbrella.

The Umbrella Connector is part of the system's DNS inspection. If your existing DNS inspection policy map decides to block or drop a request based on your DNS inspection settings, the request is not forwarded to Cisco Umbrella. Thus, you have two lines of protection:

- Your local DNS inspection policy
- Your Cisco Umbrella cloud-based policy

When redirecting DNS lookup requests to Cisco Umbrella, the Umbrella Connector adds an EDNS (Extension mechanisms for DNS) record. An EDNS record includes the device identifier information, organization ID, and client IP address. Your cloud-based policy can use those criteria to control access in addition to the reputation of the FQDN. You can also elect to encrypt the DNS request using DNSCrypt to ensure the privacy of usernames and internal IP addresses.

To redirect DNS requests from the management center to Cisco Umbrella:

1. Configure the Cisco Umbrella connection settings.
2. Create and configure an Umbrella DNS policy.
3. Associate the Umbrella DNS policy with an access control policy.
4. Deploy the changes.

For detailed information about how to set up the Umbrella DNS Connector in the management center, see Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center.

DNS policy components

DNS policy components are configuration elements that

- enable blocking of connections based on domain name using a Block list
- exempt connections from blocking using a Do Not Block list, and
- provide granular network traffic handling through configurable rules and settings.

DNS policy configuration options

These configurations can be changed after creating a DNS policy:

- **Name and Description**: Each DNS policy must have a unique name. A description is optional.
- **Rules**: Rules provide a granular method of handling network traffic based on the domain name. Rules in a DNS policy are numbered, starting at 1. The system matches traffic to DNS rules in top-down order by ascending rule number.

When you create a DNS policy, the system populates it with a default Global Do-Not-Block List for DNS rule and a default Global Block List for DNS rule. Both rules are fixed to the first position in their respective categories. You cannot modify these rules, but you can disable them.



Note If multitenancy is enabled for your Firewall Management Center, the system is organized into a hierarchy of domains, including ancestor and descendant domains. These domains are distinct and separate from the domain names used in DNS management.

A descendant list contains the domains on the Block or Do Not Block lists of system subdomain users. From an ancestor domain, you cannot view the contents of descendant lists. If you do not want subdomain users to add domains to a Block or Do Not Block list:

- disable the descendant list rules, and
- enforce Security Intelligence using the access control policy inheritance settings

The system evaluates rules in this order:

1. Global Do-Not-Block List for DNS rule (if enabled)
2. Descendant DNS Do-Not-Block Lists rule (if enabled)
3. Rules with a Do Not Block action
4. Global Block List for DNS rule (if enabled)
5. Descendant DNS Block Lists rule (if enabled)
6. Rules with an action other than Do Not Block

Usually, the system handles DN-based network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic. If no DNS rules match the traffic, the system continues evaluating the traffic based on the associated access control policy's rules. DNS rule conditions can be simple or complex.

License requirements for DNS policies

This reference provides the license requirements necessary for implementing DNS policies across different Firepower system configurations.

Threat Defense License

IPS

Classic License

Protection

Requirements and prerequisites for DNS policies

This reference provides the requirements and prerequisites needed to configure and implement DNS policies, including model support, domain compatibility, and required user roles.

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin



Important You must apply the Network Discovery policy on the device for a successful DNS validation on the traffic.

Managing DNS and Umbrella DNS Policies

Use the DNS Policy page to create, edit, delete, copy, and compare custom DNS and Umbrella DNS policies for comprehensive network security management.

Use the DNS Policy page (**Policies** > **Access Control heading** > **DNS**) to manage custom DNS and Umbrella DNS policies.

In addition to custom policies that you create, the system provides the Default DNS Policy and Default Umbrella DNS Policy. The default DNS policy uses the default Block list and Do Not Block list. You can edit and use this system-provided custom policies.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **DNS**.

Step 2 Manage your DNS policy:

- Compare—To compare DNS policies, click **Compare Policies** and proceed as described in Compare policies, on page 152.
- Copy—To copy a DNS policy, click **Copy** ( ) and proceed as described in Edit DNS policies, on page 1998.
- Create—To create a new Umbrella DNS policy, click **New Policy** > **Umbrella DNS Policy** and proceed as described in Create an umbrella DNS policy, on page 2012.
- Delete—To delete a DNS or Umbrella DNS policy, click **Delete** ( ), then confirm you want to delete the policy.
- Edit—To modify an existing DNS policy, click **Edit** ( )) and proceed as described in Edit DNS policies, on page 1998. To modify an existing Umbrella DNS policy, click **Edit** ( )) and proceed as described in Edit Umbrella DNS policies and rules, on page 2012.

You have successfully managed your DNS policies. The policies are now available for deployment to your network devices for DNS-based security filtering.

Create basic DNS policies

Creating a basic DNS policy establishes a foundation for DNS traffic filtering and management that you can customize to meet your organization's security requirements.

When you create a new DNS policy, it contains default settings. You must then edit it to customize the behavior.

Follow these steps to create a basic DNS policy:

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **DNS**.

Step 2 Click **Add DNS Policy** > **DNS Policy**.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

The DNS policy is created with default settings and appears in the DNS policies list.

What to do next

Configure the policy. See Edit DNS policies, on page 1998.

Edit DNS policies

Edit DNS policies to update policy configurations, modify rule settings, and maintain network security requirements.

Only one person should edit a DNS policy at a time, using a single browser window. If multiple users attempt to save the same policy, only the first set of saved changes are retained.

To protect the privacy of your session, after thirty minutes of inactivity on the policy editor, a warning appears. After sixty minutes, the system discards your changes.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **DNS**.

Step 2 Click **Edit** ( ) next to the DNS policy you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Edit your DNS policy:

- Name and Description—To change the name or description, click the field and type the new information.
- Rules—To add, categorize, enable, disable, or otherwise manage DNS rules, click **Rules** and proceed as described in Create and edit DNS rules, on page 1999.

Step 4 Click **Save**.

The DNS policy is updated with your changes and ready for deployment.

What to do next

- Optionally, further configure the new policy as described in *Logging Connections with Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

DNS rules

A DNS rule is a Security Intelligence component that

- handles traffic based on the domain name requested by a host,
- operates after any traffic decryption and before access control evaluation, and
- matches traffic in the order specified, with the system handling network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic.

DNS rule components

In addition to its unique name, each DNS rule has these basic components:

- **State**: By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.
- **Position**: Rules in a DNS policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.
- **Conditions**: Conditions specify the specific traffic the rule handles. A DNS rule must contain a DNS feed or list condition, and can also match traffic by security zone, network, or VLAN.
- **Action**: A rule's action determines how the system handles matching traffic.

A rule's action determines how the system handles matching traffic:

- Traffic with a **Do Not Block** action is allowed, subject to further access control inspection.
- Monitored traffic is subject to further evaluation by remaining rules on the DNS Block list. If the traffic does not match a DNS Block list rule, it is inspected with access control rules. The system logs a Security Intelligence event for the traffic.
- Traffic on a Block list is dropped without further inspection. You can also return a Domain Not Found response, or redirect the DNS query to a sinkhole server.

Related Topics

Security intelligence, on page 1595

Create and edit DNS rules

Create and edit DNS rules to define how the system handles DNS queries by specifying actions and conditions for domain name resolution.

In a DNS policy, you can add up to a total of 32767 DNS lists to the Block list and Do Not Block list rules; that is, the number of lists in the DNS policy cannot exceed 32767.

Follow these steps to create and edit DNS rules:

Procedure

Step 1 In the DNS policy editor, you have the following options:

- To add a new rule, click **Add DNS Rule**.
- To edit an existing rule, click **Edit** ( ).

Step 2 Enter a **Name**.

Step 3 Configure the rule components, or accept the defaults:

- Action—Choose a rule **Action**; see DNS rule actions, on page 2001.
- Conditions—Configure the rule's conditions; see DNS rule conditions, on page 2002.
- Enabled—Specify whether the rule is **Enabled**.

Step 4 Click **Save**.

The DNS rule is created or updated with the specified configuration and is ready for deployment.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

DNS rule management

DNS rule management is a policy administration feature that enables you to add, edit, move, enable, disable, delete, and otherwise manage DNS rules within your policy.

DNS rule management interface

The **Rules** tab of the DNS policy editor provides the interface for DNS rule management operations.

For each rule, the policy editor displays this information:

- Rule name
- Summary of rule conditions
- Rule action

Additional icons represent **Warning** ( ), **Error** ( ), and other important **Information** ( ). Disabled rules are dimmed and marked `(disabled)` beneath the rule name.

Enable and disable DNS rules

Enable or disable DNS rules to control whether the system uses them to evaluate network traffic and generate warnings and errors.

When you create a DNS rule, it is enabled by default. If you disable a rule, the system does not use it to evaluate network traffic and stops generating warnings and errors for that rule. When viewing the list of rules in a DNS policy, disabled rules are dimmed, although you can still modify them. Note that you can also enable or disable a DNS rule using the DNS rule editor.

Follow these steps to enable or disable DNS rules:

Procedure

Step 1 In the DNS policy editor, right-click the rule and choose a rule state.

Step 2 Click **Save**.

The DNS rule state is updated. Disabled rules appear dimmed in the policy rule list but can still be modified.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

DNS rule order evaluation

DNS rule order evaluation is a traffic processing mechanism that

- matches traffic to DNS rules in top-down order by ascending rule number,
- handles network traffic according to the *first* DNS rule where *all* the rule's conditions match the traffic, and
- applies different continuation behavior based on rule type.

Rule evaluation behavior

Rules in a DNS policy are numbered, starting at 1. The system behavior differs based on rule type:

- For Monitor rules, the system logs the traffic, then continues evaluating traffic against lower-priority DNS Block list rules.
- For non-Monitor rules, the system does **not** continue to evaluate traffic against additional, lower-priority DNS rules after that traffic matches a rule.

Rule order precedence follows this hierarchy:

- The Global Do-Not-Block List for DNS is always first, and takes precedence over all other rules.
- The Do-Not-Block List section precedes the Block List section; Do-Not-Block List rules always take precedence over other rules.
- The Global Block List for DNS is always first in the Block List section, and takes precedence over all other Monitor and Block list rules.
- The Block List section contains Monitor and Block list rules.
- When you first create a DNS rule, the system positions it last in the Do-Not-Block List section if you assign a **Do Not Block** action, or last in the Block List section if you assign any other action.

You can drag and drop rules to reorder them.

DNS rule actions

A DNS rule action is a configuration setting that

- determines handling for matching traffic, governing whether the system will block, not block, or monitor traffic based on rule conditions,
- controls logging behavior, determining when and how details about matching traffic are recorded, and
- impacts action prioritization when configured with TID.

DNS rule action types

If configured, TID also impacts action prioritization. For more information, see Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

DNS rules support these action types:

- **Do Not Block**: Allows traffic to pass to the next phase of inspection, which is access control rules. The system does not log *Do Not Block list* matches. Logging of these connections depends on their eventual disposition.
- **Monitor**: Forces connection logging; matching traffic is neither immediately allowed nor blocked. Traffic is matched against additional rules to determine whether to permit or deny it. The first non-Monitor DNS rule matched determines whether the system blocks the traffic. If there are no additional matching rules, the traffic is subject to access control evaluation. For connections monitored by a DNS policy, the system logs end-of-connection Security Intelligence and connection events to the Firewall Management Center database.
- **Drop**: Drops the traffic without further inspection.
- **Domain Not Found**: Returns a non-existent internet domain response to the DNS query, which prevents the client from resolving the DNS request.
- **Sinkhole**: Returns a sinkhole object's IPv4 or IPv6 address in response to the DNS query (A and AAAA records only). The sinkhole server can log, or log and block, follow-on connections to the IP address. If you configure a **Sinkhole** action, you must also configure a sinkhole object.

Logging behavior varies based on the action type:

- For a connection blocked based on the **Drop** or **Domain Not Found** actions, the system logs beginning-of-connection Security Intelligence and connection events. Because blocked traffic is immediately denied without further inspection, there is no unique end of connection to log.
- For a connection blocked based on the **Sinkhole** action, logging depends on the sinkhole object configuration. If you configure your sinkhole object to only log sinkhole connections, the system logs end-of-connection connection events for the follow-on connection. If you configure your sinkhole object to log and block sinkhole connections, the system logs beginning-of-connection connection events for the follow-on connection, then blocks that connection.

DNS rule conditions

A DNS rule condition is a traffic identification criterion that

- identifies the type of traffic that rule handles,
- can be simple or complex, and
- must include a DNS feed or list condition within a DNS rule.

DNS rule condition requirements

You can also optionally control traffic by security zone, network, or VLAN.

When adding conditions to a DNS rule:

- If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion.
- You can configure multiple conditions per rule. Traffic must match **all** the conditions in the rule for the rule to apply to traffic. For example, a rule with a DNS feed or list condition and network condition but no VLAN tag condition evaluates traffic based on the domain name and source or destination, regardless of any VLAN tagging in the session.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches **any** of a condition's criteria satisfies the condition. For example, you can use a single rule to block traffic based on up to 50 DNS lists and feeds.

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

Security zone conditions in multidomain environments

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

Network rule conditions

A network condition is a traffic matching criterion that

- controls or decrypts traffic based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.



Note You *cannot* use FDQN network objects in identity rules.

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details



Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

DNS policy rule conditions

A DNS policy rule condition is a DNS rule component that

- allows you to control traffic if a DNS list, feed, or category contains the domain name requested by the client,

- must be defined in a DNS rule, and
- applies the configured rule action to traffic regardless of whether you add a global or custom Block or Do Not Block list.

DNS condition behavior

The system applies the configured rule action to the traffic regardless of the list type. For example, if you add the Global Do Not Block List to a rule, and configure a **Drop** action, the system blocks all traffic that should have been allowed to pass to the next phase of inspection.

DNS rules

A DNS rule is a network security mechanism that controls and filters DNS queries and responses within network traffic

Control traffic based on DNS and security zone

Control traffic flow by implementing DNS rules with security zone conditions to manage network access and security policies.

Zone conditions in DNS rules allow you to control traffic by its source security zone. A *security zone* is a grouping of one or more interfaces, which may be located across multiple devices.

Procedure

Step 1 In the DNS rule editor, click **Zones**.

Step 2 Find and select the zones you want to add from the **Available Zones**. To search for zones to add, click the **Search by name** prompt above the **Available Zones** list, then type a zone name. The list updates as you type to display matching zones.

Step 3 Click to select a zone, or right-click and then select **Select All**.

Step 4 Click **Add to Source**, or drag and drop.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 2007.

Step 6 Save or continue editing the rule.

The DNS rule is configured with security zone conditions to control traffic based on source security zones and DNS names.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Control traffic based on DNS and network

Control traffic by explicitly specifying the source IP addresses for the traffic you want to manage through DNS rules.

Network conditions in DNS rules allow you to control traffic by its source IP address. You can explicitly specify the source IP addresses for the traffic you want to control.

Procedure

Step 1 In the DNS rule editor, click **Networks**.

Step 2 Find and select the networks you want to add from the **Available Networks**, as follows:

- To add a network object on the fly, which you can then add to the condition, click **Add** (+) above the **Available Networks** list and proceed as described in Create a network object, on page 2388.
- To search for network objects to add, click the **Search by name or value** prompt above the **Available Networks** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.

Step 3 Click **Add to Source**, or drag and drop.

Step 4 Add any source IP addresses or address blocks that you want to specify manually. Click the **Enter an IP address** prompt below the **Source Networks** list; then type an IP address or address block and click **Add**.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 2007.

Step 6 Save or continue editing the rule.

The DNS rule is configured with network conditions to control traffic based on the specified source IP addresses and DNS names.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Control traffic based on DNS and VLAN

This task allows you to control VLAN-tagged traffic by configuring VLAN conditions in DNS rules, enabling precise traffic management based on DNS names and VLAN identifiers.

VLAN conditions in DNS rules allow you to control VLAN-tagged traffic. The system uses the innermost VLAN tag to identify a packet by VLAN.

When you build a VLAN-based DNS rule condition, you can manually specify VLAN tags. Alternately, you can configure VLAN conditions with VLAN tag *objects*, which are reusable and associate a name with one or more VLAN tags.

Procedure

Step 1 In the DNS rule editor, select **VLAN Tags**.

Step 2 Find and select the VLANs you want to add from the **Available VLAN Tags**, as follows:

- To add a VLAN tag object on the fly, which you can then add to the condition, click **Add** (+) above the Available VLAN Tags list and proceed as described in Create a VLAN tag object, on page 2456.
- To search for VLAN tag objects and groups to add, click the **Search by name or value** prompt above the **Available VLAN Tags** list, then type either the name of the object, or the value of a VLAN tag in the object. The list updates as you type to display matching objects.

Step 3 Click **Add to Rule**, or drag and drop.

Step 4 Add any VLAN tags that you want to specify manually. Click the **Enter a VLAN Tag** prompt below the **Selected VLAN Tags** list; then type a VLAN tag or range and click **Add**. You can specify any VLAN tag from 1 to 4094; use a hyphen to specify a range of VLAN tags.

Step 5 Click the **DNS** tab and add the lists or feeds that include the DNS names you are controlling. For more information, see Control traffic based on DNS list or feed, on page 2007.

Step 6 Save or continue editing the rule.

The DNS rule is configured with VLAN conditions, allowing the system to control traffic based on both DNS names and VLAN tags.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Control traffic based on DNS list or feed

Control network traffic by applying DNS-based filtering rules using predefined or custom DNS lists and threat intelligence feeds.

Use DNS lists and feeds in security policies to block or allow traffic based on domain reputation and threat intelligence data.

Procedure

Step 1 In the DNS rule editor, click **DNS**.

Step 2 Find and select the DNS lists and feeds you want to add from the **DNS Lists and Feeds**, as follows:

- To add a DNS list or feed on the fly, which you can then add to the condition, click **Add** (+) above the **DNS Lists and Feeds** list and proceed as described in Create custom security intelligence feeds, on page 2428.

- To search for DNS lists, feeds, or categories to add, click the **Search by name or value** prompt above the **DNS Lists and Feeds** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.
- For descriptions of the system-provided threat categories, see Security intelligence categories, on page 1602.

Step 3 Click **Add to Rule**, or drag and drop.

Step 4 Save or continue editing the rule.

The DNS lists and feeds are now configured in your rule and will filter traffic based on the selected criteria.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Requirement: deploy DNS policy configuration changes

After you finish updating your DNS policy configuration, you must deploy it as part of access control configuration.

- Associate your DNS policy with an access control policy, as described in Configure security intelligence, on page 1599.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Cisco umbrella DNS policies

A Cisco Umbrella DNS policy is a security mechanism that

- redirects DNS queries to Cisco Umbrella for domain validation and policy enforcement,
- allows or blocks requests based on domain names and applies DNS-based security policies, and
- provides two lines of protection through local DNS inspection and cloud-based Cisco Umbrella policies.

DNS query redirection process

Cisco Umbrella DNS Connection in the management center helps to redirect DNS queries to Cisco Umbrella. This allows Cisco Umbrella to validate requests, allow or block them based on the domain names, and apply DNS-based security policy on the request. If you use Cisco Umbrella, you must configure the Cisco Umbrella Connection (**Integration** > **Other Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**) to redirect DNS queries to Cisco Umbrella.

The Umbrella Connector is part of the system's DNS inspection. If your existing DNS inspection policy map decides to block or drop a request based on your DNS inspection settings, the request is not forwarded to Cisco Umbrella. Thus, you have two lines of protection:

- Your local DNS inspection policy

- Your Cisco Umbrella cloud-based policy

When redirecting DNS lookup requests to Cisco Umbrella, the Umbrella Connector adds an EDNS (Extension mechanisms for DNS) record. An EDNS record includes the device identifier information, organization ID, and client IP address. Your cloud-based policy can use those criteria to control access in addition to the reputation of the FQDN. You can also elect to encrypt the DNS request using DNSCrypt to ensure the privacy of usernames and internal IP addresses.

To redirect DNS requests from the management center to Cisco Umbrella:

1. Configure the Cisco Umbrella connection settings.
2. Create and configure an Umbrella DNS policy.
3. Associate the Umbrella DNS policy with an access control policy.
4. Deploy the changes.

For detailed information about how to set up the Umbrella DNS Connector in the management center, see Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center.

Redirect DNS requests to Cisco umbrella

Redirect DNS requests from the device to Cisco Umbrella for enhanced security and DNS filtering capabilities.

Use this procedure when you need to configure DNS redirection to Cisco Umbrella using the Firewall Management Center.

Procedure

Step 1 Ensure that you meet the prerequisites.

Prerequisites for configure the umbrella DNS connector, on page 2010

Step 2 Configure the Cisco Umbrella connection settings.

Configure Cisco umbrella connection settings, on page 2011

Step 3 Create an Umbrella DNS policy.

Create an umbrella DNS policy, on page 2012

Step 4 Configure the Umbrella DNS policy.

Edit Umbrella DNS policies and rules, on page 2012

Step 5 Associate the Umbrella DNS policy with an access control policy.

Associate the umbrella DNS policy with an access control policy, on page 2013

DNS requests from the device are now redirected to Cisco Umbrella for processing and security filtering.

Prerequisites for configure the umbrella DNS connector

This reference provides the prerequisites that must be met before configuring the Umbrella DNS Connector, including minimum platform requirements, account setup, certificate management, and network connectivity requirements.

Table 113: Minimum supported platforms

Product	Version
Secure Firewall Threat Defense	6.6 and above
Secure Firewall Management Center	7.2 and above

- Establish an account with Cisco Umbrella at https://umbrella.cisco.com, and log into Umbrella at http://login.umbrella.com.
- Import the CA certificate from the Cisco Umbrella server to the Firewall Management Center. In Cisco Umbrella, choose **Deployments** > **Configuration** > **Root Certificate** and download the certificate.

  You must import the root certificate to establish the HTTPS connection with the Cisco Umbrella registration server. The certificate needs to be trusted for SSL server validation, which is a non-default option in the Firewall Management Center. Copy and paste this certificate for the device in the Firewall Management Center(**Devices** > **Certificates**).

  ```
  MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
  EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
  HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
  MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
  Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
  CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
  EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
  V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
  muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
  Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
  FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
  A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
  BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
  LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
  YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
  RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
  RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
  BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
  3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
  u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
  50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
  YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
  SaZMkE4f97Q=
  ```

  When you add the certificate in the management center, ensure that you check the **CA Only** check box.
- Install the certificate on the device.
- Obtain this data from Umbrella:
  - Organization ID
  - Network Device Key
  - Network Device Secret

- Legacy Network Device Token

- Ensure that the Firewall Management Center is connected to the internet.
- Ensure that the base license with the export-controlled feature option is enabled in the Firewall Management Center.
- Ensure that the DNS server is configured to resolve api.opendns.com.
- Ensure that the Firewall Management Center can resolve management.api.umbrella.com for policy configuration.
- Configure the Firewall Threat Defense route to api.opendns.com.

Configure Cisco umbrella connection settings

Configure the token and settings required to register the device with Cisco Umbrella and enable DNS security services.

The Cisco Umbrella Connection settings define the token that is needed to register the device with Cisco Umbrella.

Before you begin

Establish an account with Cisco Umbrella https://umbrella.cisco.com, and then log into Umbrella at https://dashboard.umbrella.com and obtain the required information to establish connection to Cisco Umbrella.

Follow these steps to configure Cisco Umbrella connection settings:

Procedure

Step 1 Choose **Integration** > **Other Integrations** > **Cloud Services** and choose the **Cisco Umbrella Connection**.

Step 2 Obtain the following details and add them to the **General** settings:

- **Organization ID**—A unique number that identifies your organization on Cisco Umbrella. Every Umbrella organization is a separate instance of Umbrella and has its own dashboard. Organizations are identified by their name and their organization ID (Org ID).
- **Network Device Key**—The key to fetch umbrella policy from Cisco Umbrella.
- **Network Device Secret**—The secret to fetch umbrella policy from Cisco Umbrella.
- **Legacy Network Device Token**—An Umbrella Legacy Network Devices API token is issued through the Cisco Umbrella dashboard. Umbrella requires the API token to register a network device.

Step 3 Under **Advanced**, configure the following optional settings:

- **DNSCrypt Public Key**—DNSCrypt authenticates and encrypts the DNS queries between the endpoint and the DNS server. To enable DNScrypt, you can configure the DNScrypt public key for certificate verification. The key is a 32-byte hexadecimal value and is preconfigured to B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79, which is the public key of the Umbrella Anycast servers.
- **Management Key**—A key to fetch datacenter details from Umbrella cloud for VPN policy.

- **Management Secret**—A secret used to fetch datacenters from Umbrella cloud for VPN.

Step 4 Click **Test Connection**—Test if the Cisco Umbrella Cloud is reachable from the Firewall Management Center. When you provide the required organization ID and network device details, the umbrella connection is created.

Step 5 Click **Save**.

The Cisco Umbrella connection is configured and the device is ready to register with Cisco Umbrella using the specified credentials and settings.

Create an umbrella DNS policy

Create an Umbrella DNS policy to implement DNS-based security controls and filtering for network protection.

Umbrella DNS policies provide DNS security by blocking malicious domains and controlling access to web content through DNS filtering.

Before you begin

Follow these steps to create an Umbrella DNS policy:

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **DNS**.

Step 2 Click **Add DNS Policy** > **Umbrella DNS Policy**.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

The Umbrella DNS policy is created and ready for configuration with DNS security rules.

What to do next

Configure the policy. See Edit Umbrella DNS policies and rules, on page 2012.

Edit Umbrella DNS policies and rules

Edit Umbrella DNS policies and rules to modify protection policies, configure bypass domains, enable DNSCrypt encryption, and adjust connection timeout settings to meet your organization's specific DNS security requirements.

Use this procedure when you need to modify existing Umbrella DNS policies and their associated rules. You can update protection policy settings, configure local domain bypasses, enable encryption options, and adjust timeout parameters to optimize DNS security for your network environment.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **DNS**.

Step 2 In the DNS Policy page, select the Umbrella DNS policy that you want to edit and click **Edit** ( ).

Refresh the Umbrella Protection Policy

If you want to get the latest Umbrella Protection Policy from Cisco Umbrella, click the **Refresh** icon next to **Umbrella Protection Policy Last Updated**.

To configure or modify Umbrella Connection settings for the Management Center, go to **Integration** > **Other Integrations** > **Cloud Services** Choose the **Cisco Umbrella Connection**.

Step 3 In the Umbrella DNS policy editor, select the Umbrella DNS rule and click **Edit** ( ).

Step 4 Configure the rule components, or accept the defaults:

- **Umbrella Protection Policy**—Specify the name of the Cisco Umbrella policy to apply to the device.
- **Bypass Domain**—Specify the name of the local domains for which DNS requests should bypass Cisco Umbrella and instead go directly to the configured DNS servers.

  For example, you can have your internal DNS server resolve all names for the organization's domain name on the assumption that all internal connections are allowed.
- **DNSCrypt**— Enable DNSCrypt to encrypt connections between the device and Cisco Umbrella.

  Enabling DNScrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key. As DNScrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.
- **Idle Timeout**—Configure the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.

Step 5 Click **Save**.

Your Umbrella DNS policy and rule modifications are saved and ready to be deployed. The updated settings will take effect when the policy is applied to devices.

What to do next

Associate the Umbrella DNS policy with an access control policy. For more information, see Associate the umbrella DNS policy with an access control policy, on page 2013.

Associate the umbrella DNS policy with an access control policy

This task associates an Umbrella DNS policy with an access control policy to enable DNS-based security intelligence filtering before deploying the policy on the device.

Before you deploy the Umbrella DNS policy on the device, you must associate it with an access control policy.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control** and select the access policy to edit.

Step 2 Select **Security Intelligence**.

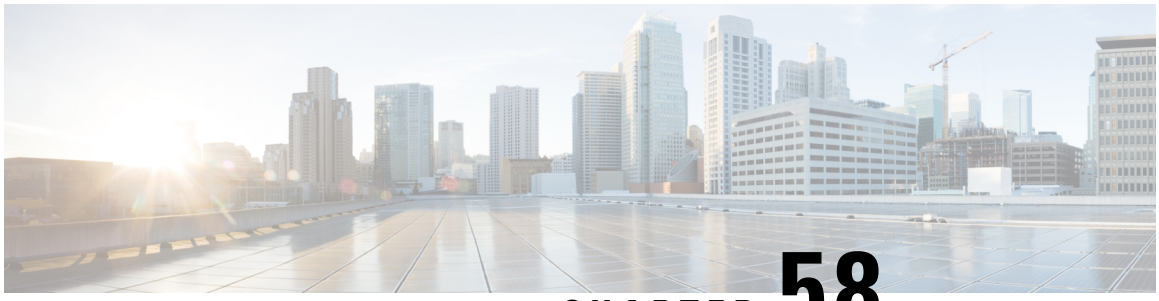
Step 3 From the **Umbrella DNS Policy** drop-down list, select the Umbrella DNS policy.

Step 4 Click **Save**.

The Umbrella DNS policy is now associated with the access control policy and will provide DNS-based security intelligence filtering when deployed.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.



CHAPTER 58

File Policies for Network Malware Protection

The following topics provide an overview of file control, file policies, file rules, Advanced Malware Protection (AMP), cloud connections, and dynamic analysis connections.

- Network malware protection and file policies, on page 2015
- Prerequisites for file policies, on page 2016
- License requirements for file and malware policies, on page 2017
- Best practices for file policies and malware detection, on page 2017
- Configure malware protection, on page 2021
- Cloud connections for malware protection, on page 2026
- File policies and file rules, on page 2035
- Retrospective disposition changes, on page 2051
- File and malware inspection performance and storage options, on page 2052
- Tune file and malware inspection performance and storage, on page 2053
- (Optional) Malware protection with Secure Endpoint, on page 2054
- History for network malware protection and file policies, on page 2058

Network malware protection and file policies

Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Secure Firewall Management Center web interface, this feature is called malware defense, formerly called AMP for Firepower. Advanced Malware Protection identifies malware using managed devices deployed inline and threat data from the Cisco cloud.

You associate file policies with access control rules that handle network traffic as part of your overall access control configuration.

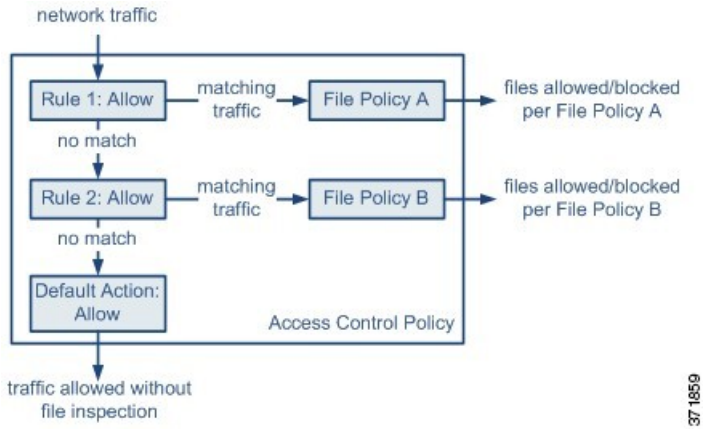
When the system detects malware on your network, it generates file and malware events. To analyze file and malware event data, see the *File/Malware Events and Network File Trajectory* chapter in the *Cisco Secure Firewall Management Center Administration Guide* .

File policies

A file policy is a set of configurations that the system uses to perform malware protection and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches an access control rule's conditions, it first inspects the file. Consider the following diagram of a simple access control policy in an inline deployment.

File policy traffic flow

Consider this diagram of a simple access control policy in an inline deployment.



The policy has two access control rules, both of which use the Allow action and are associated with file policies. The policy's default action is also to allow traffic, but without file policy inspection. In this scenario, traffic is handled as follows:

- Traffic that matches `Rule 1` is inspected by `File Policy A`.
- Traffic that does not match `Rule 1` is evaluated against `Rule 2`. Traffic that matches `Rule 2` is inspected by `File Policy B`.
- Traffic that does not match either rule is allowed; you cannot associate a file policy with the default action.

By associating different file policies with different access control rules, you have granular control over how you identify and block files transmitted on your network.

Prerequisites for file policies

This reference lists the prerequisites necessary for implementing file policies in your network security deployment.

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin

License requirements for file and malware policies

This reference provides the specific license requirements needed to implement various file rule actions and malware detection capabilities in file and malware policies.

To Do This	License Required	File Rule Action
Block or allow all files of a particular type (for example, block all .exe files)	IPS (for Firewall Threat Defense devices) Protection (for Classic devices)	Allow, Block, Block with Reset
Selectively allow or block files based on a judgment that it contains or is likely to contain malware	IPS (for Firewall Threat Defense devices) Protection (for Classic devices) Malware Defense	Malware Cloud Lookup, Block Malware
Store files	IPS (for Firewall Threat Defense devices) Protection (for Classic devices) Malware Defense	Any file rule action with **Store Files** selected

For details about Malware Defense licenses, refer to:

- *Malware Defense Licenses* in the *Cisco Secure Firewall Management Center Administration Guide*

Best practices for file policies and malware detection

In addition to the items described below, follow the steps in Configure malware protection, on page 2021 and referenced topics.

File rule best practices

Consider these guidelines and limitations when configuring file rules:

Prerequisites

- You cannot perform malware analysis on all file types detected by the system. After you select values from the **Application Protocol**, **Direction of Transfer**, and **Action** drop-down lists, the system constrains the list of file types.

- If a file rule is configured with a **Malware Cloud Lookup** or **Block Malware** action and the Firewall Management Center cannot establish connectivity with the AMP cloud, the system cannot perform any configured rule action options until connectivity is restored.

General file rule best practices

- A rule configured to block files in a passive deployment does not block matching files. Because the connection continues to transmit the file, if you configure the rule to log the beginning of the connection, you may see multiple events logged for this connection.
- A policy can include multiple rules. When you create the rules, ensure that no rule is "shadowed" by a previous rule.
- Cisco recommends that you enable **Reset Connection** for the **Block Files** and **Block Malware** actions to prevent blocked application sessions from remaining open until the TCP connection resets. If you do not reset connections, the client session will remain open until the TCP connection resets itself.

Dynamic Analysis

- The file types supported for dynamic analysis are a subset of the file types supported for other types of analysis. To view the file types supported for each type of analysis, navigate to the file rule configuration page, select the **Block Malware** action, and select the checkboxes of interest.

  To ensure that the system examines all file types, create separate rules (within the same policy) for dynamic analysis and for other types of analysis.
- If you are monitoring high volumes of traffic, do **not** store all captured files, or submit all captured files for dynamic analysis. Doing so can negatively impact system performance.

File detection best practices

Consider these notes and limitations when implementing file detection:

Prerequisite

If adaptive profiling is not enabled, access control rules cannot perform file control, including AMP.

General file detection best practices

- If a file matches a rule with an application protocol condition, file event generation occurs after the system successfully identifies a file's application protocol. Unidentified files do not generate file events.
- To detect ISO files, set the "Limit the number of bytes inspected when doing file type detection" option to a value greater than 36870, as described in File and malware inspection performance and storage options, on page 2052.
- .Exe files inside some .rar archives cannot be detected, including possibly rar5.
- If the file disposition is Neutral, it is an unknown disposition.

FTP-Specific considerations

- FTP transfers commands and data over different channels. In a passive or inline tap mode deployment, the traffic from an FTP data session and its control session may not be load-balanced to the same internal resource.

Email protocols considerations

- If the total number of bytes for all file names for files in a POP3, POP, SMTP, or IMAP session exceeds 1024, file events from the session may not reflect the correct file names for files that were detected after the file name buffer filled.
- When transmitting text-based files over SMTP, some mail clients convert newlines to the CRLF newline character standard. Since Mac-based hosts use the carriage return (CR) character and Unix/Linux-based hosts use the line feed (LF) character, newline conversion by the mail client can modify the size of the file. Note that some mail clients default to newline conversion when processing an unrecognizable file type.

File blocking best practices

Consider these notes and limitations for file blocking:

HTTP transfers

- File rules with **Block Files** and **Block Malware** actions block automatic resumption of file download via HTTP by blocking new sessions with the same file, URL, server, and client application detected for 24 hours after the initial file transfer attempt occurs.
- In rare cases, if traffic from an HTTP upload session is out of order, the system cannot reassemble the traffic correctly and therefore will not block it or generate a file event.

End-of-File detection

- If an end-of-file marker is not detected for a file, regardless of transfer protocol, the file will not be blocked by a **Block Malware** rule or the custom detection list. The system waits to block the file until the entire file has been received, as indicated by the end-of-file marker, and blocks the file after the marker is detected.
- If the end-of-file marker for an FTP file transfer is transmitted separately from the final data segment, the marker will be blocked and the FTP client will indicate that the file transfer failed, but the file will actually completely transfer to disk.

SMB or NetBIOS-ssn transfers

- If you transfer a file over NetBIOS-ssn (such as an SMB file transfer) that is blocked with a **Block Files** rule, you may see a file on the destination host. However, the file is unusable because it is blocked after the download starts, resulting in an incomplete file transfer.
- If you create file rules to detect or block files transferred over NetBIOS-ssn (such as an SMB file transfer), the system does not inspect the ongoing file transfers. However, the system inspects the new files that are transferred after you deploy an access control policy invoking the file policy.

- SMB has a functionality called multi-channel which creates multiple parallel sessions with the same IP address and different ports. For a given transaction over multi-channel, the file download is multiplexed across these sessions which is not inspected by the system as a single file.
- Files transferred concurrently in a single TCP or SMB session are not inspected.
- In a cluster environment, if an existing SMB session is moved to a new device due to a cluster role change or a device failure, then the files in any ongoing file transfers may not be inspected.
- Some SMB file transfers between Microsoft Windows systems use very high TCP window size for quick file transfers. To detect or block such file transfers, it is recommended that you increase the value of **Maximum Queued Bytes** and **Maximum Queued Segments** under **Network Analysis Policy** > **TCP Stream Configuration** > **Troubleshooting Options**.

High availability

If you configure Firewall Threat Defense high availability, and failover occurs while the original active device is identifying the file, the file type is not synced. Even if your file policy blocks that file type, the new active device downloads the file.

File policy best practices

Follow these best practices for file policy configuration to ensure proper functionality and optimal performance.

Prerequisites

- For file blocking to work, the NAP policy you apply to the access control policy must be operating in Protection mode, also known as Inline mode.
- You can associate a single file policy with an access control rule whose action is **Allow**, **Interactive Block**, or **Interactive Block with reset**.
- You **cannot** use a file policy to inspect traffic handled by the access control default action.

Encrypted traffic

By default, file inspection of encrypted payloads is disabled. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has file inspection configured.



Attention The File Inpsect preprocessor with the following generator IDs (GIDs) are enabled by default for file/malware policy: GID: 146 and GID: 147.

General file policy best practices

- For a new policy, the web interface indicates that the policy is not in use. If you are editing an in-use file policy, the web interface tells you how many access control policies use the file policy. In either case, you can click the text to jump to the Access Control Policies page.
- Based on your configuration, you can either inspect a file the first time the system detects it, and wait for a cloud lookup result, or pass the file on this first detection without waiting for the cloud lookup result.

- If you enable an access control policy with a file policy that uses either a Malware action or a Store Files option, the computing power and system performance of the device is reduced.
- NEW_OFFICE file type in file policy configuration identifies Microsoft files: DOCX, XLSX, and PPTX. When you apply a policy action to NEW_OFFICE, the action applies uniformly to all three file types—DOCX, XLSX, and PPTX.

  If your security requirements need differentiated handling of Office file formats, such as blocking DOCX documents while permitting XLSX spreadsheets, do not use the NEW_OFFICE aggregate file type. Instead, perform these steps:

  1. Select individual file types (DOCX, XLSX, PPTX) separately in your file policy rule.
  2. Create separate rules with distinct actions for each format you need to control granularly.
  3. Test your policy to ensure each Office format is handled according to your security intent.

  This approach ensures that your file policy aligns with your organization's security posture and prevents unintended blocking of legitimate business traffic.

Configure malware protection

You need to set up your system to protect your network from malicious software by following a series of configuration steps.

Procedure

Step 1 Plan and prepare for malware protection, on page 2022

Step 2 Configure file policies, on page 2023

Step 3 Add file policies to your access control configuration, on page 2023

Step 4 Configure network discovery policies to associate file and malware events with hosts on your network.

(Do not simply turn on network discovery; you must configure it to discover hosts on your network to build a network map of your organization.)

See Network Discovery Policies, on page 2305 and subtopics.

Step 5 Deploy policies to managed devices.

See Deploy configuration changes, on page 135.

Step 6 Test your system to be sure it is processing malicious files as you expect it to.

Step 7 Verify and monitor malware protection, on page 2025

What to do next

- (Optional) To further enhance detection of malware in your network, deploy and integrate Cisco's Secure Endpoint product. Refer to (Optional) Malware protection with Secure Endpoint, on page 2054 and subtopics.
- Understand how to investigate file and malware events.

Refer to *File/Malware Events and Network File Trajectory* in the *Cisco Secure Firewall Management Center Administration Guide*.

Plan and prepare for malware protection

This procedure is the first set of steps in the complete process for configuring your system to provide malware protection.

Procedure

Step 1 Purchase and install licenses.

Refer to License requirements for file and malware policies, on page 2017 and *Licenses* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 2 Understand how file policies and malware protection fit into your access control plan.

Refer to the chapter Access Control Policies, on page 1569.

Step 3 Understand the file analysis and malware protection tools.

Refer to File rule actions, on page 2042 and subtopics.

Consider also Advanced and archive file inspection options, on page 2036.

Step 4 Determine whether you will use public clouds or private (on-premises) clouds for malware protection (file analysis and dynamic analysis.)

Refer to Cloud connections for malware protection, on page 2026 and subtopics.

Step 5 If you will use private (on-premises) clouds for malware protection: Purchase, deploy, and test those products.

For information, contact your Cisco sales representative or authorized reseller.

Step 6 Configure your firewall to allow communications with your chosen clouds.

Refer to *Security, Internet Access, and Communication Ports* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 7 Configure connections between Firepower and the malware protection clouds (public or private, as applicable).

- For the AMP cloud, refer to Change AMP options, on page 2031.
- If you have deployed an on-premises Secure Malware Analytics Appliance, see Connect to an on-premises dynamic analysis appliance, on page 2032. (Access to the public Secure Malware Analytics Cloud does not require configuration.)

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 2021.

Configure file policies

File policies are a critical component of the malware protection workflow that allow you to define specific rules and advanced options for file inspection and handling.

Before you begin

Complete the tasks up to this point in the malware protection workflow:

Refer to Configure malware protection, on page 2021.

Procedure

Step 1 Review file policy and file rule restrictions.

Refer to Best practices for file policies and malware detection, on page 2017 and subtopics.

Step 2 Create a file policy.

Refer to Create or edit a file policy, on page 2035.

Step 3 Create rules within your file policy.

Refer to File rules, on page 2040 and subtopics.

Step 4 Configure advanced options.

Refer to Advanced and archive file inspection options, on page 2036.

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 2021.

Add file policies to your access control configuration

An access control policy can have multiple access control rules associated with file policies. You can configure file inspection for any Allow or Interactive Block access control rule, which permits you to match different file and malware inspection profiles against different types of traffic on your network before it reaches its final destination.

Before you begin

Complete the tasks up to this point in the malware protection workflow:

See Configure malware protection, on page 2021.

Procedure

Step 1 Review guidelines for file policies in access control policies. (These are different from the file rule and file policy guidelines.)

Review File and intrusion inspection order, on page 1618.

Step 2 Associate the file policy with an access control policy.

Refer to Configure an access control rule to perform malware protection, on page 2024

Step 3 Assign the access control policy to managed devices.

See Assign access control policy to devices, on page 1583.

What to do next

Continue with the next step in the malware protection workflow:

Refer to Configure malware protection, on page 2021.

Configure an access control rule to perform malware protection

Access control rules with file policies provide comprehensive malware protection by inspecting traffic flows and applying security analysis to files traversing your network.

Caution Enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis or MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware, Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Note Inline normalization is enabled automatically when a file policy is included in an access control rule. For more information, refer to The Inline Normalization Preprocessor.

Before you begin

- Adaptive profiling **must** be enabled (its default state) for access control rules to perform file control, including AMP.
- You must be an Admin, Access Admin, or Network Admin user to perform this task.

Procedure

Step 1 In the access control rule editor (from **Policies > Access Control)**, choose an **Action** of **Allow**, **Interactive Block**, or **Interactive Block with reset**.

Step 2 (Legacy UI only.) Click **Inspection**.

Step 3 Choose a **File Policy** to inspect traffic that matches the access control rule, or choose **None** to disable file inspection for matching traffic.

Step 4 (Optional) Disable logging of file or malware events for matching connections by clicking **Logging** and unchecking **Log Files**.

Note Cisco recommends that you leave file and malware event logging enabled.

Step 5 Save the rule.

Step 6 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Verify and monitor malware protection

Ongoing maintenance is essential for protecting your network.

Before you begin

Configure your system to protect your network from malware.

Refer to Configure malware protection, on page 2021 and referenced procedures.

Procedure

Step 1 Ensure that your system always has the most current and effective protection.

Refer to Maintain your system: file types eligible for dynamic analysis, on page 2034.

Step 2 Configure alerts for malware-related events and health monitoring.

See the *Cisco Secure Firewall Management Center Administration Guide* for information on *Configuring malware defense Alerting* and for information about the following modules:

- Local Malware Analysis
- Security Intelligence
- Threat Data Updates on Devices

- Intrusion and File Event Rate
- AMP for Firepower Status
- Secure Endpoint Status

What to do next

Review "What to do next items" in the malware protection workflow:

Refer to Configure malware protection, on page 2021.

Cloud connections for malware protection

Connections to public or private clouds are required in order to protect your network from malware.

AMP clouds

The Advanced Malware Protection (AMP) cloud is a Cisco-hosted server that uses big data analytics and continuous analysis to provide intelligence that the system uses to detect and block malware on your network.

The AMP cloud provides dispositions FOR possible malware detected IN network traffic by managed devices, as well as data updates FOR local malware analysis and file pre-classification.

If your organization has deployed Secure Endpoint and configured Firepower to import its data, the system imports this data from the AMP cloud, including scan records, malware detections, quarantines, and indications of compromise (IOC).

Cisco offers these options for obtaining data from the Cisco cloud about known malware threats:

- **AMP public cloud**: Your Secure Firewall Management Center communicates directly with the public Cisco cloud. There are three public AMP clouds, in the United States, Europe, and Asia.
- **An AMP private cloud**: An AMP private cloud is deployed on your network and acts as a compressed, on-premises AMP cloud, as well as an anonymized proxy to connect to the public AMP cloud. FOR details, see Cisco AMP private cloud, on page 2028.

  If you integrate with Secure Endpoint, the AMP private cloud has some limitations. See Secure Endpoint and AMP private cloud, on page 2056.

Dynamic analysis cloud

Dynamic analysis cloud options include:

- Secure Malware Analytics Cloud: Public cloud that processes eligible files that you send for dynamic analysis, and provides threat scores and dynamic analysis reports. Firepower supports 200 samples/day FOR Secure Malware Analytics analysis.
- On-premises Secure Malware Analytics Appliance: If your organization's security policy does not allow the system to send files outside of your network, you can deploy an on-premises appliance. This appliance does not contact the public Secure Malware Analytics Cloud.

For more information, refer to Dynamic analysis on-premises appliance (Cisco Secure Malware Analytics), on page 2032.

Configure connections to AMP and Secure Malware Analytics

- AMP cloud connection configurations, on page 2027
- Dynamic analysis connections, on page 2031

AMP cloud connection configurations

These topics describe AMP cloud connection configurations for different scenarios:

- Choose an AMP cloud, on page 2028
- Connect to an AMP private cloud, on page 2029
- Integrate Firepower and Secure Endpoint, on page 2056

Refer these topics:

- Cisco AMP private cloud, on page 2028
- Prerequisites and best practices for AMP cloud connections, on page 2027
- Manage connections to the AMP cloud (public or private), on page 2030

Prerequisites and best practices for AMP cloud connections

This topic lists the prerequisites and best practices for AMP cloud connections.

Prerequisites for AMP cloud connections

- You must be an Admin user to set up the AMP cloud.
- To ensure the Firewall Management Center can communicate with the AMP cloud, see *Security, Internet Access, and Communication Ports* in the *Cisco Secure Firewall Management Center Administration Guide*.

AMP and high availability

Although they share file policies and related configurations, Firewall Management Centers in a high availability pair do not share AMP cloud connections, captured files, file events, and malware events.

Both active and standby Firewall Management Centers must have access to the cloud to ensure continuity of operations and consistent malware dispositions.

These requirements apply to both public and private AMP clouds.

AMP cloud connections and multitenancy

In a multidomain deployment, configure the malware defense connection at the global level. Each Firewall Management Center can have only one malware defense connection.

Choose an AMP cloud

By default, a connection to the United States (US) AMP public cloud is configured and enabled for your system. (This connection appears in the web interface as malware defense and sometimes AMP for Firepower.) You cannot delete or disable an malware defense cloud connection, but you can switch between different geographical AMP clouds, or configure an AMP private cloud connection.

Before you begin

- If you will use an AMP private cloud, refer to Connect to an AMP private cloud, on page 2029 instead of this topic.
- Unless Firepower is integrated with Secure Endpoint, you can configure only one AMP cloud connection. This connection is labeled **AMP for Networks** or **AMP for Firepower**.
- If you have deployed Secure Endpoint and you want to add one or more AMP clouds to integrate that application with Firepower, refer to Integrate Firepower and Secure Endpoint, on page 2056.
- Refer to Prerequisites and best practices for AMP cloud connections, on page 2027.

Procedure

Step 1 Choose **Integration** > **AMP** > **AMP Management**.

Step 2 Click the edit icon to edit the existing cloud connection.

Step 3 From the **Cloud Name** drop-down list, choose the regional cloud nearest to your Secure Firewall Management Center.

APJC is Asia/Pacific/Japan/China.

Step 4 Click **Save**.

What to do next

- If your deployment is a high-availability configuration, refer to Prerequisites and best practices for AMP cloud connections, on page 2027.
- (Optional) Change AMP options, on page 2031.

Cisco AMP private cloud

The Firewall Management Center must connect to the AMP cloud for disposition queries for files detected in network traffic and receipt of retrospective malware events. This cloud can be public or private.

AMP private cloud connection details

Your organization may have privacy or security concerns that make frequent or direct connections between your monitored network and the AMP cloud difficult or impossible. In these situations, you can set up a Cisco AMP Private Cloud. Connecting a Firewall Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.

All connections to the AMP cloud funnel through the AMP private cloud, which acts as an anonymized proxy to ensure the security and privacy of your monitored network. This includes disposition queries FOR files detected IN network traffic, receiving of retrospective malware events, and so on. The AMP private cloud does not share any of your endpoint data over an external connection.



Note The AMP private cloud does not perform dynamic analysis, nor does it support anonymized retrieval of threat intelligence FOR other features that rely on Cisco Collective Security Intelligence (CSI), such as URL and Security Intelligence filtering.

For information about AMP private cloud (sometimes referred to as "AMPv"), refer to https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html.

Connect to an AMP private cloud

Use this connection when you have a dedicated AMP private cloud infrastructure that provides enhanced security and control over your malware analysis environment. The private cloud connection enables malware detection and analysis while keeping sensitive data within your controlled environment.

Before you begin

- Configure your Cisco AMP private cloud or clouds according to the directions in the documentation for that product. During configuration, note the private cloud host name. You will need this host name in order to configure the connection on the Firewall Management Center.
- Make sure the Firewall Management Center can communicate with the AMP private cloud, and confirm that the private cloud has internet access so it can communicate with the public AMP cloud. See the topics under *Security, Internet Access, and Communication Ports* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Unless your deployment is integrated with Secure Endpoint, each Firewall Management Center can have only one AMP cloud connection. This connection is labeled **AMP for Networks** or **AMP for Firepower**.

  If you integrate with Secure Endpoint, you can configure multiple Secure Endpoint cloud connections.

Procedure

Step 1 Choose **Integration** > **AMP** > **AMP Management**.

Step 2 Click **Add AMP Cloud Connection**.

Step 3 From the **Cloud Name** drop-down list, choose **Private Cloud**.

Step 4 Enter a **Name**.

This information appears in malware events that are generated or transmitted by AMP private cloud.

Step 5 In the **Host** field, enter the private cloud host name that you configured when you set up the private cloud.

Step 6 Click **Browse** next to the **Certificate Upload Path** field to browse to the location of a valid TLS or SSL encryption certificate for the private cloud. For more information, see the AMP private cloud documentation.

Step 7 If you want to use this private cloud for both malware defense and Secure Endpoint, check the **Use for AMP for Firepower** check box.

If you configured a different private cloud to handle malware defense communications, you can clear this check box; if this is your only AMP private cloud connection, you cannot.

In a multidomain deployment, this check box appears only in the Global domain. Each Firewall Management Center can have only one malware defense connection.

Step 8 Click **Register**, confirm that you want to disable existing direct connections to the AMP cloud, and finally confirm that you want to continue to the AMP private cloud management console to complete registration.

Log into the management console and complete the registration process. For further instructions, see the AMP private cloud documentation.

What to do next

In high availability deployments, configure AMP cloud connections on both management centers. These configurations are not synchronized.

Manage connections to the AMP cloud (public or private)

Use the Firewall Management Center to manage connections to public and private AMP clouds used for malware defense or Secure Endpoint or both.

You can delete a connection to a public or private AMP cloud if you no longer want to receive malware-related information from the cloud. Note that deregistering a connection using the Secure Endpoint or AMP private cloud management console does not remove the connection from the system. Deregistered connections display a failed state on the Secure Firewall Management Center web interface.

You can also temporarily disable a connection. When you reenable a cloud connection, the cloud resumes sending data to the system, including queued data from the disabled period.



Caution For disabled connections, the public or private AMP cloud can store malware events, indications of compromise, and so on until you re-enable the connection. In rare cases—for example, with a very high event rate or a long-term disabled connection—the cloud may not be able to store all information generated while the connection is disabled.

In a multidomain deployment, the system displays connections created in the current domain, which you can manage. It also displays connections created in ancestor domains, which you cannot manage. To manage connections in a lower domain, switch to that domain. Each Firewall Management Center can have only one malware defense connection, which belongs to the Global domain.

Procedure

Step 1 Select **Integration** > **AMP** > **AMP Management**.

Step 2 Manage your AMP cloud connections:

- **Delete** — Click **Delete** ( ), then confirm your choice.

- **Enable** or **Disable** — Click the slider, then confirm your choice.

What to do next

In high availability deployments, configure AMP cloud connections on both management centers. These configurations are not synchronized.

Change AMP options

Use this procedure to modify AMP (Advanced Malware Protection) for Networks configuration settings that control automatic signature updates and data sharing with the Cisco cloud.

Procedure

Step 1 Choose **Integration** > **Other Integrations** > **Cloud Services**.

Step 2 Configure these parameters:

Table 114: AMP for networks options

Option	Description
Enable Automatic Local Malware Detection Updates	The local malware detection engine statically analyzes and preclassifies files using signatures provided by Cisco. If you enable this option, the Firewall Management Center checks for signature updates once every 30 minutes.
Share URI from Malware Events with Cisco	The system can send information about the files detected in network traffic to the AMP cloud. This information includes URI information associated with detected files and their SHA-256 hash values. Although sharing is opt-in, transmitting this information to Cisco helps future efforts to identify and track malware.

Step 3 Click **Save**.

Dynamic analysis connections

Dynamic analysis connections are network connections that enable real-time security analysis and threat detection capabilities.

Prerequisites for dynamic analysis

This topic lists the prerequisites to use dynamic analysis.

- You must be an Admin, Access Admin, or Network Admin user, and be in the global domain, to use dynamic analysis.
- With the appropriate license, the system automatically has access to the Secure Malware Analytics Cloud.

- Dynamic analysis requires that managed devices have direct or proxied access to the Secure Malware Analytics Cloud or an on-premises Secure Malware Analytics Appliance on port 443.
- See also Files eligible for dynamic analysis, on page 2047.
- If you will connect to an on-premises Secure Malware Analytics Appliance, see also the prerequisites in Connect to an on-premises dynamic analysis appliance, on page 2032.

View the default dynamic analysis connection

By default, the Secure Firewall Management Center can connect to the public Secure Malware Analytics Cloud for file submission and report retrieval. You can neither configure nor delete this connection.

Procedure

Step 1 Choose **Integration** > **AMP** > **Dynamic Analysis ConnectionsAMP** > **Dynamic Analysis Connections**.

Step 2 Click **Edit** ( ).

Note For information about **Associate** ( ) on the **Integration** > **AMP** > **Dynamic Analysis Connections** page, refer to Enable access to dynamic analysis results in the public cloud, on page 2034.

Dynamic analysis on-premises appliance (Cisco Secure Malware Analytics)

If your organization has privacy or security concerns around submitting files to the public Secure Malware Analytics Cloud, you can deploy an on-premises Secure Malware Analytics Appliance. Like the public cloud, the on-premises appliance runs eligible files in a sandbox environment, and returns a threat score and dynamic analysis report to the system. However, the on-premises appliance does not communicate with the public cloud, or any other system external to your network.

For more information about on-premises Secure Malware Analytics Appliances, see https://www.cisco.com/c/en/us/products/security/threat-grid/index.html.

Connect to an on-premises dynamic analysis appliance

If you install an on-premises Secure Malware Analytics Appliance on your network, you can configure a dynamic analysis connection to submit files and retrieve reports from the appliance. When configuring the on-premises appliance dynamic analysis connection, you register the Secure Firewall Management Center to the on-premises appliance.

Before you begin

- Set up your on-premises Secure Malware Analytics Appliance.

  Documentation for this appliance is available from https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html.

  For version requirements, refer to the *Cisco Firepower Compatibility Guide*.

- If your Secure Malware Analytics Appliance uses a self-signed public-key certificate, download the certificate from the Secure Malware Analytics Appliance; see the *Administrator's Guide* for your Secure Malware Analytics Appliance for information.

  If you use a certificate signed by a Certificate Authority (CA), the certificate must meet the following requirements:

  - The server key and signed certificate must be installed on the Secure Malware Analytics Appliance. Follow the upload instructions in the *Administrator's Guide* for your Secure Malware Analytics Appliance.
  - If there is a multi-level signing chain of CAs, all required intermediate certificates and the root certificate must be contained in a single file that will be uploaded to the Firewall Management Center.
  - All certificates must be PEM-encoded.
  - The file's newlines must be UNIX, not DOS.

- If you want to connect to the on-premises appliance using a proxy, configure the proxy; refer to *Modify Firewall Management Center Management Interfaces* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Managed devices must have direct or proxied access to the Secure Malware Analytics Appliance on port 443.

Procedure

Step 1 Choose **Integration** > **AMP** > **Dynamic Analysis ConnectionsAMP** > **Dynamic Analysis Connections**.

Step 2 Click **Add New Connection**.

Step 3 Enter a **Name** and enter a **Host**.

Step 4 Next to **Certificate Upload**, click **Browse** to upload the certificate for the on-premises appliance.

If the Secure Malware Analytics Appliance will present a self-signed certificate, upload the certificate you downloaded from that appliance.

If the Secure Malware Analytics Appliance will present a CA-signed certificate, upload the file containing the certificate signing chain.

Step 5 If you want to use a configured proxy to establish the connection, check the check box of **Use Proxy When Available**.

Step 6 Click **Register**.

Step 7 Click **Yes** to display the on-premises Secure Malware Analytics Appliance login page.

Step 8 Enter your username and password to the on-premises Secure Malware Analytics Appliance and click **Sign in**.

Step 9 You have these options:

- If you previously registered the Secure Firewall Management Center to the on-premises appliance, click **Return**.

- If you did not register the Secure Firewall Management Center, click **Activate**.

Enable access to dynamic analysis results in the public cloud

Secure Malware Analytics offers more detailed reporting on analyzed files than is available in the Firewall Management Center. If your organization has a Secure Malware Analytics Cloud account, you can access the Secure Malware Analytics portal directly to view additional details about files sent for analysis from your managed devices. However, for privacy reasons, file analysis details are available only to the organization that submitted the files. Therefore, before you can view this information, you must associate your Firewall Management Center with the files submitted by its managed devices.

Before you begin

You must have a Secure Malware Analytics Cloud account, and have your account credentials ready.

Procedure

Step 1 Select **Integration** > **AMP** > **Dynamic Analysis ConnectionsAMP** > **Dynamic Analysis Connections**.

Step 2 Click **Associate** ( ) in the table row corresponding to the Secure Malware Analytics Cloud.

A Secure Malware Analytics portal window opens.

Step 3 Sign in to the Secure Malware Analytics Cloud.

Step 4 Click **Submit Query**.

Note Do not change the default value in the **Devices** field.

If you have difficulties with this process, contact your Secure Malware Analytics representative at Cisco TAC.

It may take up to 24 hours for this change to take effect.

What to do next

After the association is activated, refer to *Viewing Dynamic Analysis Results in the Cisco Cloud* in the *Cisco Secure Firewall Management Center Administration Guide* .

Maintain your system: file types eligible for dynamic analysis

The list of file types eligible for Dynamic Analysis is determined by the vulnerability database (VDB), which is updated periodically (but no more than once per day.) If you are an Admin user, you can update file types eligible for dynamic analysis.

The supported file types for automatic submission can vary in every release. The currently supported files for automatic submission are:

- PE Executable (32-bit Only)

- EXE
- DLL
- PDF
- MSOLE2 (Microsoft Object Linking and Embedding Compound File)
- DOCX, PPTX, XLSX

Note GZ and ZIP file types are not supported for automatic submission.

Procedure

Step 1 Do one of the following:

- (Recommended) Refer to *Vulnerability Database Update Automation* as discussed in the *Cisco Secure Firewall Management Center Administration Guide*
- Regularly check for new VDB updates, and *Manually Update the VDB* as discussed in the *Cisco Secure Firewall Management Center Administration Guide* when needed.

  If you choose this option, we recommend that you schedule regular reminders to do this.

Step 2 If your file policies specify individual file types instead of the **Dynamic Analysis Capable** file type category, update your file policies to use the newly supported file types.

Step 3 If the list of eligible file types changes, deploy to managed devices.

File policies and file rules

File policies and file rules work together to control file handling and inspection in network traffic.

Create or edit a file policy

File policies allow you to control file transfers and provide malware protection by defining rules that specify which files can be transferred, blocked, or inspected for threats.

Before you begin

If you are configuring policies for malware protection, refer to all required procedures in Configure file policies, on page 2023.

Procedure

Step 1 Select **Policies** > **Access Control heading** > **Malware & File** .

Step 2 Create a new policy, or edit an existing policy.

If you are editing an existing policy: If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Tip To make a copy of an existing file policy, click **Copy** ( ), then type a unique name for the new policy in the dialog box that appears. You can then modify the copy.

Step 3 Add one or more rules to the file policy as described in Create file rules, on page 2050.

Step 4 Optionally, select Advanced and configure advanced options as described in Advanced and archive file inspection options, on page 2036.

Step 5 Save the file policy.

What to do next

- If you are configuring policies for malware protection, see other required procedures in Configure file policies, on page 2023.
- Otherwise:
  - Add the file policy to an access control rule as described in Add file policies to your access control configuration, on page 2023.
  - Deploy configuration changes; see Deploy configuration changes, on page 135.

Advanced and archive file inspection options

The Advanced Settings in the file policy editor provides general options for file analysis and archive file inspection to enhance security policy configuration.

The Advanced Settings in the file policy editor has these general options:

- **First Time File Analysis**—Select this option to analyze first-seen files while AMP cloud disposition is pending. The file must match a rule configured to perform a malware cloud lookup and Spero, local malware, or dynamic analysis. If you deselect this option, files detected for the first time are marked with an Unknown disposition
- **Enable Custom Detection List**—Block files on the custom detection list.
- **Enable Clean List**—If enabled, this policy will allow files that are on the clean list.
- **If AMP Cloud disposition is Unknown, override disposition based upon threat score**—Select an option:
  - If you select **Disabled,** the system will not override the disposition provided by the AMP Cloud.

- If you set a threshold threat score, files with an AMP cloud verdict of Unknown are considered malware if their Dynamic Analysis score is equal to or worse than the threshold.
- If you select a lower threshold value, you increase the number of files treated as malware. Depending on the action selected in your file policy, this can result in an increase of blocked files.
- For numeric threat score ranges, see *Threat Scores and Dynamic Analysis Summary Reports* in the *Cisco Secure Firewall Management Center Administration Guide*.

The Advanced Settings in the file policy editor has these archive file inspection options:

- **Inspect Archives**—Enables inspection of the contents of archive files, for archive files as large as the **Maximum file size to store** advanced access control setting.
- **Block Encrypted Archives**—Blocks password-protected archives.
- **Block Uninspectable Archives**—Blocks archive files with contents that the system is unable to inspect for reasons other than encryption. This usually applies to corrupted files, or those that exceed your specified maximum archive depth.
- **Max Archive Depth**—Blocks nested archive files that exceed the specified depth. The top-level archive file is not considered in this count; depth begins at 1 with the first nested file.

Archive files

Archive files are files that contain other files, such as `.zip` or `.rar` files.

If any individual file in an archive matches a file rule with a block action, the system blocks the entire archive, not just the individual file.

Archive file inspection capabilities

The system provides various options for inspecting archive files.

- **File types**: A complete list of inspectable archive file types appears in the Firewall Management Center web interface on the file rule configuration page. To view that page, see Create file rules, on page 2050. Contained files that can be inspected appears in the same page.
- **File size**: You can inspect archive files as large as the **Maximum file size to store** file policy advanced access control setting.
- **Nested archives**: Archive files can contain other archive files, which can in turn contain archive files. The level at which a file is nested is its *archive file depth*. Note that the top-level archive file is not included in the depth count; depth begins at 1 with the first nested file. The system can inspect up to three levels of nested files beneath the outermost archive file (level 0). You can configure your file policy to block archive files that exceed that depth (or a lower maximum depth that you specify). If you choose not to block files that exceed the maximum archive file depth of 3, when archive files that contain some extractable contents and some contents nested at a depth of 3 or greater appear in monitored traffic, the system examines and reports data only for the files it was able to inspect. All features applicable to uncompressed files (such as dynamic analysis and file storage) are available for nested files inside archive files.
- **Encrypted files**: You can configure the system to block archives whose contents are encrypted or otherwise cannot be inspected.

- **Archives that are not inspected**: If traffic that contains an archive file is on a Security Intelligence Block list or Do Not Block list, or if the top-level archive file's SHA-256 value is on the custom detection list, the system does not inspect the contents of the archive file. If a nested file is blocked, the entire archive is blocked; however, if a nested file is allowed, the archive is not automatically passed (depending on any other nested files and characteristics). .Exe files inside some .rar archives cannot be detected, including possibly rar5.

For details about options for archive file inspection, see Advanced and archive file inspection options, on page 2036.

Archive file dispositions

Archive file dispositions are based on the dispositions assigned to the files inside the archive. All archives that contain identified malware files receive a disposition of `Malware`. Archives without identified malware files receive a disposition of `Unknown` if they contain any unknown files, and a disposition of `Clean` if they contain only clean files.

Table 115: Archive file disposition by contents

Archive File Disposition	Number of Unknown Files	Number of Clean Files	Number of Malware Files
`Unknown`	1 or more	Any	0
`Clean`	0	1 or more	0
`Malware`	Any	Any	1 or more

Archive files, like other files, may have dispositions of `Custom Detection` or `Unavailable` if the conditions for those dispositions apply.

Archive contents and details

If your file policy is configured to inspect archive file contents, you can use the context menu in a table on pages under the Analysis > Files menu, and the network file trajectory viewer to view information about the files inside an archive when the archive file appears in a file event, malware event, or as a captured file.

All file contents of the archive are listed in table form, with a short summary of their relevant information: name, SHA-256 hash value, type, category, and archive depth. A network file trajectory icon appears by each file, which you can click to view further information about that specific file.

Override file disposition using custom lists

Override file disposition using custom lists is a security mechanism that

- allows administrators to correct incorrect file dispositions from the AMP cloud by adding SHA-256 values to specific file lists
- enables treating files as clean or malware regardless of the original cloud disposition, and
- provides per-file policy control without reevaluating the file's disposition on subsequent detection.

File list types and usage

If a file has a disposition in the AMP cloud that you know to be incorrect, you can add the file's SHA-256 value to a file list that overrides the disposition from the cloud:

- To treat a file as if the AMP cloud assigned a clean disposition, add the file to the *clean list*.
- To treat a file as if the AMP cloud assigned a malware disposition, add the file to the *custom detection list*.

On subsequent detection, the device either allows or blocks the file without reevaluating the file's disposition. You can use the clean list or custom detection list per file policy.



Note To calculate a file's SHA-256 value, you must configure a rule in the file policy to either perform a malware cloud lookup or block malware on matching files.

For complete information about using file lists in Firepower, refer to File lists, on page 2377.

Alternatively, if applicable, use Centralized file lists from Secure Endpoint, on page 2039.

Centralized file lists from Secure Endpoint

If your organization has deployed Secure Endpoint, Firepower can use Block and Allow lists created in Secure Endpoint when it queries the AMP cloud for file dispositions.

Requirements for centralized file lists

Your deployment must meet these requirements:

- Your organization must be using the AMP public cloud.
- Your organization has deployed Secure Endpoint.
- You have registered your system to Secure Endpoint using the procedure in Integrate Firepower and Secure Endpoint, on page 2056.

To create and deploy these lists, refer to the documentation or online help for Secure Endpoint.



Note File lists created in Firepower override file lists created in Secure Endpoint.

Manage file policies

The **File Policies** page displays a list of existing file policies along with their last-modified dates. You can use this page to manage your file policies.

Note The system checks for updates to the list of file types eligible for dynamic analysis (no more than once a day). If the list of eligible file types changes, this constitutes a change in the file policy; any access control policy using the file policy is marked out-of-date if deployed to any devices. You must deploy policies before the updated file policy can take effect on the device. See Maintain your system: file types eligible for dynamic analysis, on page 2034.

Procedure

Step 1 Select **Policies** > **Access Control heading** > **Malware & File** .

Step 2 Manage your file policies:

- Compare—Click **Compare Policies**; see Comparing policies.
- **Create**— To create a file policy, click **New File Policy** and proceed as described in Create or edit a file policy, on page 2035.
- **Copy**— To copy a file policy, click **Copy** ( ).

  If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- **Delete**— If you want to delete a file policy, click **Delete** ( ), then click **Yes** and **OK** as prompted.

  If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Deploy—Choose **Deploy** > **Deploy**; see Deploy configuration changes, on page 135.
- **Edit**— If you want to modify an existing file policy, click **Edit** ( ).
- **Report**—Click **Report**( ); Refer to Generate current policy reports, on page 153.

File rules

A file policy, like its parent access control policy, contains rules that determine how the system handles files that match the conditions of each rule. You can configure separate file rules to take different actions for different file types, application protocols, or directions of transfer.

File rule actions

When a file matches a rule, the rule can:

- allow or block files based on simple file type matching
- block files based on disposition (whether or not evaluation indicates that it is malicious)
- store files to the device (For information, see Captured files and file storage, on page 2048)

- submit stored (captured) files for local malware, Spero, or dynamic analysis

In addition, the file policy can:

- automatically treat a file as if it is clean or malware based on entries in the clean list or custom detection list
- treat a file as if it is malware if the file's threat score exceeds a configurable threshold
- inspect the contents of archive files (such as `.zip` or `.rar`)
- block archive files whose contents are encrypted, nested beyond a specified maximum archive depth, or otherwise uninspectable

File rule components

File rules consist of several components that determine how the system detects and handles files transmitted over various application protocols. Understanding these components helps configure effective file detection and inspection policies.

Table 116: File rule components

File Rule Component	Description
application protocol	The system can detect and inspect files transmitted via FTP, HTTP, SMTP, IMAP, POP3, and NetBIOS-ssn (SMB). **Any**, the default, detects files in HTTP, SMTP, IMAP, POP3, FTP, and NetBIOS-ssn (SMB) traffic. To improve performance, you can restrict file detection to only one of those application protocols on a per-file rule basis.
direction of transfer	You can inspect incoming FTP, HTTP, IMAP, POP3, and NetBIOS-ssn (SMB) traffic for downloaded files; you can inspect outgoing FTP, HTTP, SMTP, and NetBIOS-ssn (SMB) traffic for uploaded files. **Tip** Use **Any** to detect files over multiple application protocols, regardless of whether users are sending or receiving.

File Rule Component	Description
file categories and types	The system can detect various types of files. These file types are grouped into basic categories, including multimedia (swf, mp3), executables (exe, torrent), and PDFs. You can configure file rules that detect individual file types, or on entire categories of file types. For example, you could block all multimedia files, or just ShockWave Flash (swf) files. Or, you could configure the system to alert you when a user downloads a BitTorrent (torrent) file. Note that executables include file types that can run macros and scripts, since these can contain malware. For a list of file types the system can inspect, select **Policies** > **Access Control heading** > **Malware & File** , create a temporary new file policy, then click **Add Rule**. Select a file type category and the file types that the system can inspect appear in the **File Types** list. **Note** Frequently triggered file rules can affect system performance. For example, detecting multimedia files in HTTP traffic (YouTube, for example, transmits significant Flash content) could generate an overwhelming number of events.
file rule action	A file rule's action determines how the system handles traffic that matches the conditions of the rule. Depending on the selected action, you can configure whether the system stores the file or performs Spero, local malware, or dynamic analysis on a file. If you select a Block action, you can also configure whether the system also resets the blocked connection. For descriptions of these actions and options, see File rule actions, on page 2042. File rules are evaluated in rule-action, not numerical, order. For details, see File rule actions: evaluation order, on page 2050.

File rule actions

File rules give you granular control over which file types you want to log, block, or scan for malware. Each file rule has an associated action that determines how the system handles traffic that matches the conditions of the rule. To be effective, a file policy must contain one or more rules. You can use separate rules within a file policy to take different actions for different file types, application protocols, or directions of transfer.

File rule actions include these types:

- *Detect Files* rules allow you to log the detection of specific file types to the database, while still allowing their transmission.
- *Block Files* rules allow you to block specific file types. You can configure options to reset the connection when a file transfer is blocked, and store captured files to the managed device.
- *Malware Cloud Lookup* rules allow you to obtain and log the disposition of files traversing your network, while still allowing their transmission.

- *Block Malware* rules allow you to calculate the SHA-256 hash value of specific file types, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

File rule action options

Depending on the action you select, you have different options:

File Rule Action Option	Block Files capable?	Block Malware capable?	Detect Files capable?	Malware Cloud Lookup capable?
Spero Analysis* for MSEXE	no	yes, you can submit executable files	no	yes, you can submit executable files
Dynamic Analysis*	no	yes, you can submit executable files with Unknown file dispositions	no	yes, you can submit executable files with Unknown file dispositions
Capacity Handling	no	yes	no	yes
Local Malware Analysis*	no	yes	no	yes
Reset Connection	yes (recommended)	yes (recommended)	no	no
Store files	yes, you can store all matching file types	yes, you can store file types matching the file dispositions you select	yes, you can store all matching file types	yes, you can store file types matching the file dispositions you select

* For complete information about these options, refer to Malware protection options, on page 2043 and its subtopics.



Caution Enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis or MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware, Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Malware protection options

The system applies several methods of file inspection and analysis to determine whether a file contains malware.

File inspection sequence

Depending on the options you enable in a file rule, the system inspects files using these tools, in order:

1. Spero analysis, on page 2045 and AMP cloud lookup, on page 2046
2. Local malware analysis, on page 2046
3. Dynamic analysis, on page 2047

For a comparison of these tools, see Comparison of malware protection options, on page 2044.

(You can also, if you choose, block all files based on their file type. For more information, see Block all files by type, on page 2049.)

Refer to information about Cisco's Secure Endpoint product at (Optional) Malware protection with Secure Endpoint, on page 2054 and subtopics.

Comparison of malware protection options

This table details the benefits and drawbacks of each type of file analysis, as well as the way each malware protection method determines a file's disposition.

Analysis Type	Benefit	Limitations	Malware Identification
Spero analysis	Structural analysis of executable files, submits Spero signature to the AMP Cloud for analysis	Less thorough than local malware analysis or dynamic analysis, only for executable files	Disposition changes from Unknown to Malware only on positive identification of malware.
Local malware analysis	Consumes fewer resources than dynamic analysis, and returns results more quickly, especially if the detected malware is common	Less thorough results than dynamic analysis	Disposition changes from Unknown to Malware only on positive identification of malware.
Dynamic analysis	Thorough analysis of unknown files using Secure Malware Analytics	Eligible files are uploaded to the public cloud or an on-premises appliance. It takes some time to complete analysis	Threat score determines maliciousness of a file. Disposition can be based on the threat score threshold configured in the file policy.
Spero analysis and local malware analysis	Consumes fewer resources than configuring local malware analysis and dynamic analysis, while still using AMP cloud resources to identify malware	Less thorough than dynamic analysis, Spero analysis only for executable files	Disposition changes from Unknown to Malware only on positive identification of malware.

Analysis Type	Benefit	Limitations	Malware Identification
Spero analysis and dynamic analysis	Uses full capabilities of AMP cloud in submitting files and Spero signatures	Results obtained less quickly than if using local malware analysis	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes based on configured threat score threshold in the file policy, and from Unknown to Malware if the Spero analysis identifies malware.
Local malware analysis and dynamic analysis	Thorough results in using both types of file analysis	Consumes more resources than either alone	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes from Unknown to Malware if local malware analysis identifies malware, or based on configured threat score threshold in the file policy.
Spero analysis, local malware analysis and dynamic analysis	Most thorough results	Consumes most resources in running all three types of file analysis	Threat score changes based on dynamic analysis results for files preclassified as possible malware. Disposition changes from Unknown to Malware if Spero analysis or local malware analysis identifies malware, or based on configured threat score threshold in the file policy.
(Block transmission of all files of a specified file type)	Does not require a Malware Defense license (This option is not technically a malware protection option.)	Legitimate files will also be blocked	(No analysis is performed.)

Note Preclassification does not itself determine a file's disposition; it is merely one of the factors that determine whether a file is eligible for Dynamic Analysis.

Spero analysis

Spero analysis examines structural characteristics such as metadata and header information in executable files. After generating a Spero signature based on this information, if the file is an eligible executable file, the device submits it to the Spero heuristic engine in the AMP cloud. Based on the Spero signature, the Spero engine determines whether the file is malware. You can also configure rules to submit files for Spero analysis without also submitting them to the AMP cloud.

Note You cannot manually submit files for Spero analysis.

AMP cloud lookup

For files that are eligible for assessment using Advanced Malware Protection, the Firewall Management Center performs a malware cloud lookup, querying the AMP cloud for the file's disposition based on its SHA-256 hash value.

Performance optimization

To improve performance, the system caches dispositions returned by the cloud and uses the cached disposition for known files rather than querying the AMP cloud. For more information about this cache, see Cached disposition longevity, on page 2046.

Local malware analysis

Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, and other types of files for the most common types of malware, using a detection rule set provided by the Talos Intelligence Group. Because local analysis does not query the AMP cloud, and does not run the file, local malware analysis saves time and system resources.

Local malware analysis behavior

When the system identifies malware through local malware analysis, it updates the existing file disposition from Unknown to Malware and generates a new malware event. If the system does not identify malware, it does not update the file disposition from Unknown to Clean.

After the system runs local malware analysis, it caches file information such as SHA-256 hash value, timestamp, and disposition, so that if detected again within a certain period of time, the system can identify malware without additional analysis. For more information about the cache, see Cached disposition longevity, on page 2046.

Local malware analysis does not require establishing communications with the Secure Malware Analytics Cloud. However, you must configure communications with the cloud to submit files for dynamic analysis, and to download updates to the local malware analysis ruleset.

Cached disposition longevity

Dispositions returned from an AMP cloud query, associated threat scores, and dispositions assigned by local malware analysis, have a time-to-live (TTL) value. After a disposition has been held for the duration specified in the TTL value without update, the system purges the cached information. Dispositions and associated threat scores have the following TTL values:

TTL values for dispositions and threat scores

Dispositions and associated threat scores have these TTL values:

- Clean — 4 hours
- Unknown — 1 hour
- Malware — 1 hour

If a query against the cache identifies a cached disposition that timed out, the system re-queries the local malware analysis database and the AMP cloud for a new disposition.

Dynamic analysis

Dynamic analysis is a security analysis method that

- automatically submits files for behavioral analysis using Secure Malware Analytics (formerly Threat Grid), Cisco's file analysis and threat intelligence platform,
- runs files in a sandbox environment to analyze behavior and determine maliciousness, and
- returns a threat score indicating the likelihood that a file contains malware.

Dynamic analysis process and capabilities

You can configure your file policy to automatically submit files for dynamic analysis using Secure Malware Analytics (formerly Threat Grid), Cisco's file analysis and threat intelligence platform.

Devices submit eligible files to Secure Malware Analytics (either the public cloud or to an on-premises appliance, whichever you have specified) regardless of whether the device stores the file.

Secure Malware Analytics runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Secure Malware Analytics to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.

For more information about Cisco Secure Malware Analytics, refer to https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

To configure your system to perform dynamic analysis, see the topics under Dynamic analysis connections, on page 2031.

Files eligible for dynamic analysis

A file's eligibility for dynamic analysis depends on the file type, the file size, and the file rule's action.

Additional requirements:

- The system submits only files that match the file rules you configure.
- The file must have a malware cloud lookup disposition of Unknown or Unavailable at the time the file is sent for analysis.
- The system must preclassify the file as potential malware.

Dynamic analysis and capacity handling

Capacity handling is a system feature that temporarily stores files that are otherwise eligible for dynamic analysis if the system is temporarily unable to submit files to the cloud, either because the device cannot communicate with the cloud or because the maximum number of submissions has been reached. The system submits the stored files when the hindering condition has passed.

Storage options

Some devices can store files on the device hard drive or in a malware storage pack. Refer Malware storage packs, on page 2048.

Captured files and file storage

The file storage feature allows you to capture selected files detected in traffic, and automatically store a copy of the file temporarily to a device's hard drive, or, if installed, to the malware storage pack.

File capture and storage capabilities

After your device captures files, you can:

- Store captured files on the device's hard drive for later analysis.
- Download the stored file to a local computer for further manual analysis or archival purposes.
- Manually submit eligible captured files for AMP cloud lookup or dynamic analysis.

Note that once a device stores a file, it will not re-capture it if the file is detected in the future and the device still has that file stored.



Note When a file is detected for the first time on your network, you can generate a file event that represents the file's detection. However, if your file rule performs a malware cloud lookup, the system requires additional time to query the AMP cloud and return a disposition. Due to this delay, the system cannot store this file until the second time it is seen on your network, and the system can immediately determine the file's disposition.

Whether the system captures or stores a file, you can:

- Review information about the captured file from **Analysis** > **Unified Events**, including whether the file was stored or submitted for dynamic analysis, file disposition, and threat score, allowing you to quickly review possible malware threats detected on your network.

  Alternatively, you can also view information about the captured file from **Analysis** > **Files** > **Captured Files**.
- View the file's trajectory to determine how it traversed your network and which hosts have a copy.
- Add the file to the clean list or custom detection list to always treat the file as if it had a clean or malware disposition on future detection.

You configure file rules in a file policy to capture and store files of a specific type, or with a particular file disposition, if available. After you associate the file policy with an access control policy and deploy it to your devices, matching files in traffic are captured and stored. You can also limit the minimum and maximum file sizes to store.

Stored files are not included in system backups.

You can view captured file information under **Analysis** > **Files** > **Captured Files**, and download a copy for offline analysis.

Malware storage packs

A malware storage pack

- provides additional storage capacity for file data when installed in security devices
- allows the primary hard drive to store events and configuration files by dedicating the entire storage pack to captured files, and
- automatically receives stored files from the primary hard drive when installed on devices that already contain file data.

Storage allocation and file management

Based on your file policy configuration, your device may store a substantial amount of file data to the hard drive. You can install a malware storage pack in the device; the system stores files to the malware storage pack, allowing more room on the primary hard drive to store events and configuration files. The system periodically deletes older files. If the device's primary hard drive does not have enough available space, and does not have an installed malware storage pack, you cannot store files.



Caution Do not attempt to install a hard drive that was not supplied by Cisco in your device. Installing an unsupported hard drive may damage the device. Malware storage pack kits are available for purchase **only** from Cisco. Contact Support if you require assistance with the malware storage pack.

Without a malware storage pack installed, when you configure a device to store files, it allocates a set portion of the primary hard drive's space to captured file storage. If you configure capacity handling to temporarily store files for dynamic analysis, the system uses the same hard drive allocation to store these files until it can resubmit them to the cloud.

When you install a malware storage pack in a device and configure file storage or capacity handling, the device allocates the entire malware storage pack for storing these files. The device cannot store any other information on the malware storage pack.

When the allocated space for captured file storage fills to capacity, the system deletes the oldest stored files until the allocated space reaches a system-defined threshold. Based on the number of files stored, you may see a substantial drop in disk usage after the system deletes files.

If a device has already stored files when you install a malware storage pack, the next time you restart the device, any captured files or capacity handling files stored on the primary hard drive are moved to the malware storage pack. Any future files the device stores are stored to the malware storage pack.

For more information on using MSP on the Firepower devices, see the Firepower Hardware Installation Guide for your device.

Block all files by type

If your organization wants to block not only the transmission of malware files, but all files of a specific type, regardless of whether the files contain malware, you can do so.

File type categories and licensing

File control is supported for all file types where the system can detect malware, plus many additional file types. These file types are grouped into basic categories, such as multimedia (swf, mp3), executables (exe, torrent), and PDFs.

Blocking all files based on their type is not technically a malware protection feature; it does not require a Malware Defense license and does not query the AMP cloud.

File rule actions: evaluation order

A file policy will likely contain multiple rules with different actions for different situations. If more than one rule can apply to a particular situation, the evaluation order described in this topic applies. In general, simple blocking takes precedence over malware inspection and blocking, which takes precedence over simple detection and logging.

The order of precedence of file-rule actions is:

- *Block Files*
- *Block Malware*
- *Malware Cloud Lookup*
- *Detect Files*

If configured, TID also impacts action prioritization. For more information, see Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

Create file rules

Use this procedure when you need to add file rules to an existing file policy to control file handling and security actions.

Caution Enabling or disabling **Store files** in a **Detect Files** or **Block Files** rule, or adding the first or removing the last file rule that combines the **Malware Cloud Lookup** or **Block Malware** file rule action with an analysis option (**Spero Analysis or MSEXE**, **Dynamic Analysis**, or **Local Malware Analysis**) or a store files option (**Malware, Unknown**, **Clean**, or **Custom**), restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Before you begin

If you are configuring rules for malware protection, refer to Configure file policies, on page 2023.

Procedure

Step 1 Select **Policies** > **Access Control heading** > **Malware & File** .

Step 2 Click the edit icon to modify an existing file policy.

Step 3 In the file policy editor, click **Add Rule**.

Step 4 Select an **Application Protocol** and **Direction of Transfer** as described in File rule components, on page 2041.

Step 5 Select one or more **File Types**.

The file types you see depend on the selected application protocol, direction of transfer, and action.

You can filter the list of file types in these ways:

- Select one or more **File Type Categories**, then click **All types in selected Categories.**

- Search for a file type by its name or description. For example, type **`Windows`** in the **Search name and description** field to display a list of Microsoft Windows-specific files.



Tip Hover your pointer over a file type to view its description.

Step 6 Select a file rule **Action** as described in File rule actions, on page 2042, with consideration for File rule actions: evaluation order, on page 2050.

The actions available to you depend on the licenses you have installed. Refer to License requirements for file and malware policies, on page 2017.

Step 7 Depending on the action you selected, configure options:

- reset the connection after blocking the file
- store files that match the rule
- enable Spero analysis*
- enable local malware analysis*
- enable dynamic analysis* and capacity handling

* For information about these options, refer to File rule actions, on page 2042 and Malware protection options, on page 2043 and its subtopics.

Step 8 Click **Add.**

Step 9 Click **Save** to save the policy.

What to do next

- If you are configuring policies for malware protection, return to Configure file policies, on page 2023.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Access control rule logging for malware protection

When the system detects a prohibited file (including malware) according to the settings in the file policy, it automatically logs an event to the Secure Firewall Management Center database. If you do not want to log file or malware events, you can disable this logging on a per-access-control-rule basis.

The system also logs the end of the associated connection to the Secure Firewall Management Center database, regardless of the logging configuration of the invoking access control rule.

Retrospective disposition changes

File dispositions can change. For example, as new information is discovered, the AMP cloud can determine that a file that was previously thought to be clean is now identified as malware, or the reverse—that a

malware-identified file is actually clean. When the disposition changes for a file you queried in the past week, the AMP cloud notifies the system so it can automatically take action the next time it detects that file being transmitted. A changed disposition is called a retrospective disposition.

File and malware inspection performance and storage options

Increasing the file sizes can affect the performance of the system.

Table 117: Advanced access control file and malware defense options

Field	Description	Guidelines and Restrictions
Limit the number of bytes inspected when doing file type detection	Specifies the number of bytes inspected when performing file type detection.	0 - 4294967295 (4GB) 0 removes the restriction. The default value is the maximum segment size of a TCP packet (1460 bytes). In most cases, the system can identify common file types using the first packet. To detect ISO files, enter a value greater than 36870.
Allow file if cloud lookup for Block Malware takes longer than (seconds)	Specifies how long the system will hold the last byte of a file that matches a **Block Malware** rule and that does not have a cached disposition, while malware cloud lookup occurs. If the time elapses without the system obtaining a disposition, the file passes. Dispositions of Unavailable are not cached.	0 - 30 seconds Do *not* set this option to 0 without contacting Support. Cisco recommends that you use the default value to avoid blocking traffic because of connection failures.
Do not calculate SHA-256 hash values for files larger than (in bytes)	Prevents the system from storing files larger than a certain size, performing a malware cloud lookup on the files, or blocking the files if added to the custom detection list.	0 - 4294967295 (4GB) 0 removes the restriction. This value must be greater than or equal to **Maximum file size to store (bytes)** and **Maximum file size for dynamic analysis testing (bytes)**.

Maximum file size for advanced file inspection and storage (bytes)	These settings specify:
	• The file size that the system can inspect using these detectors:
	  • Spero analysis
	  • Sandboxing and preclassification
	  • Local malware analysis/ClamAV
	  • Archive inspection
	• The file size that the system can store using a file rule.
		0 - 10485760 (10MB)
		0 disables file storage.
		Must be less than or equal to **Maximum file size to store (bytes)** and **Do not calculate SHA-256 hash values for files larger than (in bytes)**.

Minimum file size for advanced file inspection and storage (bytes)		0 - 10485760 (10MB) 0 disables file storage. Must be greater than or equal to **Minimum file size to store (bytes)**, and less than or equal to **Do not calculate SHA-256 hash values for files larger than (in bytes)**.

Field	Description	Guidelines and Restrictions
Maximum file size for dynamic analysis testing (bytes)	Specifies the minimum file size the system can submit to the AMP cloud for dynamic analysis.	0 -10485760 (10MB) Must be less than or equal to **Maximum file size for dynamic analysis testing (bytes)** and **Do not calculate SHA-256 hash values for files larger than (in bytes)**. The file size for dynamic analysis must be within the limits defined by the minimum and maximum settings for file analysis. The system checks the AMP cloud for updates to the minimum file size you can submit (no more than once a day). If the new minimum size is larger than your current value, your current value is updated to the new minimum, and your policy is marked out-of-date.
Minimum file size for dynamic analysis testing (bytes)	Specifies the maximum file size the system can submit to the AMP cloud for dynamic analysis.	0 -10485760 (10MB) Must be greater than or equal to **Minimum file size for dynamic analysis testing (bytes)**, and less than or equal to **Do not calculate SHA-256 hash values for files larger than (in bytes)**. The file size for dynamic analysis must be within the limits defined by the minimum and maximum settings for file analysis. The system checks the AMP cloud for updates to the maximum file size you can submit (no more than once a day). If the new maximum size is smaller than your current value, your current value is updated to the new maximum, and your policy is marked out-of-date.

Tune file and malware inspection performance and storage

File and malware inspection can impact system performance and storage utilization. Tuning these settings helps ensure optimal security posture while maintaining acceptable system performance.

Before you begin

You must be an Admin, Access Admin, or Network Admin user to perform this task.

Procedure

Step 1 In the access control policy editor, click **Advanced Settings**.

Step 2 Click **Edit** ( ) next to **Files and Malware Settings**.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 3 Set any of the options described in File and malware inspection performance and storage options, on page 2052.

Step 4 Click **OK**.

Step 5 Click **Save** to save the policy.

(Optional) Malware protection with Secure Endpoint

Cisco's Secure Endpoint is a separate malware-protection product that can supplement malware protection provided by the system and be integrated with your Firepower deployment.

Secure Endpoint is Cisco’s enterprise-class Advanced Malware Protection solution that runs as a lightweight connector on individual users' endpoints (computers and mobile devices) to discover, understand, and block advanced malware outbreaks, advanced persistent threats, and targeted attacks.

Benefits of Secure Endpoint

- Configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files
- Perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes
- Configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non-quarantined executables from running, and exclusion lists
- Create custom protections, block execution of certain applications based on group policy, and create custom Allowed Applications lists
- Use the Secure Endpoint management console to help you mitigate the effect of malware. The management console provides a robust, flexible web interface where you control all aspects of your Secure Endpoint deployment and manage all phases of an outbreak.

For detailed information about Secure Endpoint, refer to:

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html.
- Online help in the Secure Endpoint management console.
- Secure Endpoint documentation available from: http://docs.amp.cisco.com.

Comparison of malware protection: Firepower vs. Secure Endpoint

This table compares the advanced malware protection differences between Firepower malware protection and Secure Endpoint across various features including detection methods, network traffic inspection, malware analysis, mitigation capabilities, and licensing requirements.

Table 118: Advanced malware protection differences by detecting product

Feature	Firepower Malware Protection (malware defense)	Secure Endpoint
File type detection and blocking method (file control)	In network traffic, using access control and file policies	Not supported
Malware detection and blocking method	In network traffic, using access control and file policies	On individual endpoints (end-user computers and mobile devices), using a connector that communicates with the AMP cloud
Network traffic inspected	Traffic passing through a managed device	None; connectors installed on endpoints directly inspect files
Malware intelligence data source	AMP cloud (public or private)	AMP cloud (public or private)
Malware detection robustness	Limited file types	All file types
Malware analysis choices	Firewall Management Center-based, plus analysis in the AMP cloud	Firewall Management Center-based, plus additional options on the Secure Endpoint management console
Malware mitigation	Malware blocking in network traffic, Firewall Management Center-initiated remediations	Secure Endpoint-based quarantine and outbreak control options, Firewall Management Center-initiated remediations
Events generated	File events, captured files, malware events, and retrospective malware events	Malware events
Information in malware events	Basic malware event information, plus connection data (IP address, port, and application protocol)	In-depth malware event information; no connection data
Network file trajectory	Firewall Management Center-based	Firewall Management Center and the Secure Endpoint management console each have a network file trajectory. Both are useful.
Required licenses or subscriptions	Licenses required to perform file control and malware defense	Secure Endpoint subscription. No license is required to bring Secure Endpoint data into Firewall Management Center.

Integrate Secure Firewall with Secure Endpoint

If your organization has deployed Secure Endpoint, you can optionally integrate that product with your Secure Firewall deployment.

Integration with Secure Endpoint does not require a dedicated Secure Firewall license.

Benefits of integrating Firepower and Secure Endpoint

Integrating your Secure Endpoint deployment with your system offers these benefits:

- Centralized Blocked Applications and Allowed Applications lists configured in Secure Endpoint can determine verdicts for file SHAs sent from Firepower to the AMP cloud for disposition.

  Refer to Centralized file lists from Secure Endpoint, on page 2039.

- The system can import malware events detected by Secure Endpoint into Secure Firewall Management Center so you can manage these events along with malware events generated by the system. Imported data for these events includes scans, malware detections, quarantines, blocked executions, and cloud recalls, as well as indications of compromise (IOCs) that Firewall Management Center displays for hosts that it monitors.

  For more information, refer to *Malware Event Analysis with Secure Endpoint* in the *Cisco Secure Firewall Management Center Administration Guide* .

- You can view file trajectory and other details in the Secure Endpoint console.

  For details, refer to *Work with Event Data in the Secure Endpoint Console* in the *Cisco Secure Firewall Management Center Administration Guide* .

Important If you use a Cisco AMP Private Cloud, refer to limitations at Secure Endpoint and AMP private cloud, on page 2056.

Secure Endpoint and AMP private cloud

If you configure a Cisco AMP private cloud to collect Secure Endpoint data on your network, all Secure Endpoint connectors send data to the private cloud, which forwards that data to the Secure Firewall Management Center. The private cloud does not share any of your endpoint data over an external connection.

Private cloud functionality and limitations

The private cloud acts as an anonymized proxy to ensure the security and privacy of your monitored network. This includes importing Secure Endpoint data. The private cloud does not share any of your endpoint data over an external connection.

The integration features that are not available with an AMP private cloud are:

- Use of Blocked Applications and Allowed Applications lists configured in Secure Endpoint. (These lists are used to block or allow files.)
- Visibility in Secure Endpoint of malware events generated from Firepower.

You can configure multiple private clouds to support the capacity you require.

Integrate Firepower and Secure Endpoint

If your organization has deployed Cisco's Secure Endpoint product, you can integrate that application with Firepower to achieve the benefits described in Benefits of integrating Firepower and Secure Endpoint, on page 2055.

When you integrate with Secure Endpoint, you must configure the Secure Endpoint connection even if you already have malware defense (AMP for Firepower) connections configured. You can configure multiple Secure Endpoint cloud connections.

Note Secure Endpoint connections that have not registered successfully do not affect malware defense.

Before you begin

- You must be an Admin user to perform this task.
- If your deployment uses Cisco AMP Private Cloud, refer to limitations at Secure Endpoint and AMP private cloud, on page 2056.
- Secure Endpoint must be set up and working properly on your network.
- The Firewall Management Center must have internet access.
- Make sure your Firewall Management Center and Secure Endpoint can communicate with each other. Refer to *Security, Internet Access, and Communication Ports* in the *Cisco Secure Firewall Management Center Administration Guide*.
- If you are connecting to the AMP cloud after either reimaging or restoring your Firewall Management Center from backup, use the Secure Endpoint management console to remove the previous connection.
- You will need your Secure Endpoint credentials to log in to the Secure Endpoint console during this procedure.

Procedure

Step 1 Choose **Integration** > **AMP** > **AMP Management**.

Step 2 Click **Add AMP Cloud Connection**.

Step 3 From the **Cloud Name** drop-down list, choose the cloud you want to use.

- The AMP cloud closest to the geographical location of your Firewall Management Center.

  APJC is Asia/Pacific/Japan/China.

- For AMP private cloud (AMPv), choose **Private Cloud** and proceed as described in Cisco AMP private cloud, on page 2028.

Step 4 If you want to use this cloud for both malware defense and Secure Endpoint, select the **Use for AMP for Firepower** check box.

If you configured a different cloud to handle malware defense (AMP for Firepower) communications, you can clear this check box; if this is your only AMP cloud connection, you cannot.

Step 5 Click **Register**.

A **Spinning state** () icon indicates that a connection is pending, for example, after you configure a connection on the Firewall Management Center, but before you authorize it using the Secure Endpoint management console. A **Denied** () icon indicates that the cloud denied the connection or the connection failed for another reason.

Step 6 Confirm that you want to continue to the Secure Endpoint management console, then log into the management console.

Step 7 Using the management console, authorize the AMP cloud to send Secure Endpoint data to Firewall Management Center.

Step 8 If you want to restrict the data that the Firewall Management Center receives, select specific groups within your organization for which you want to receive information.

By default, the AMP cloud sends data for all groups. To manage groups, choose **Management** > **Groups** on the Secure Endpoint management console. For detailed information, see the management console online help.

Step 9 Click **Allow** to enable the connection and start the transfer of data.

Clicking **Deny** returns you to the Firewall Management Center, where the connection is marked as denied. If you navigate away from the Applications page on the Secure Endpoint management console, and neither deny nor allow the connection, the connection is marked as pending on the Firewall Management Center's web interface. The health monitor does **not** alert you of a failed connection in either of these situations. If you want to connect to the AMP cloud later, delete the failed or pending connection, then recreate it.

Incomplete registration of the Secure Endpoint connection does not disable the malware defense connection.

What to do next

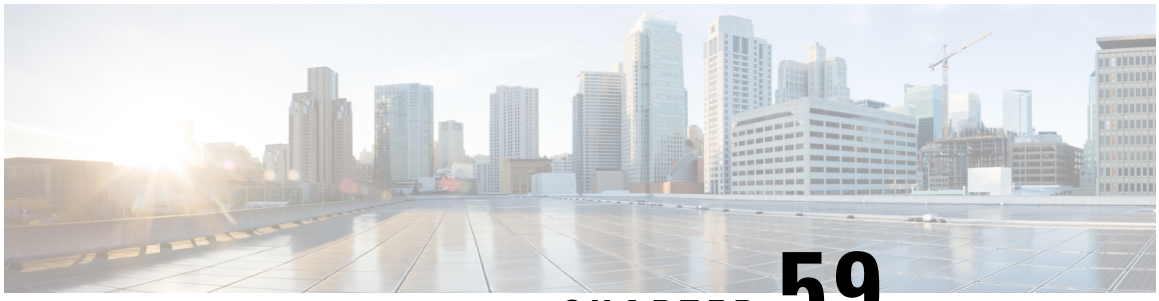
- In the Secure Endpoint console window, configure settings as needed. For example, define group membership for your management center and assign policies. For information, see the Secure Endpoint online help or other documentation.
- In high availability deployments, configure AMP cloud connections on both management centers. These configurations are not synchronized.
- The default health policy warns you if the Firewall Management Center cannot connect to the Secure Endpoint portal after an initial successful connection, or if the connection is deregistered using the AMP portal.

  Verify that the Secure Endpoint Status monitor is enabled under **System** (⚙) > **Health** > **Policy**.
- To verify that the connection is correctly configured:
  1. On the **Integration** > **AMP** > **AMP Management** page, click the Cloud Name that includes Secure Endpoint in the **Cisco AMP Solution Type** column.
  2. In the Secure Endpoint console window that displays, choose **Accounts > Applications**.
  3. Verify that your Firewall Management Center is on the list.
  4. In the Secure Endpoint console window, choose **Manage > Computers**.
  5. Verify that your Firewall Management Center is on the list.

History for network malware protection and file policies

This reference provides a comprehensive history of changes and updates to network malware protection and file policy features across different software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Communication with AMP cloud	7.0	Any	Legacy port 32137 is no longer supported for communicating with the AMP public or private cloud. New/Modified screens: On the **System** > **Integration** > **Cloud Services** page, the **Use Legacy Port 32137 for AMP for Networks** option is no longer available.
Chapter restructure	Changes were made in 6.4 timeframe, but will appear in any version that is republished	Any	Restructured this chapter's content to reduce confusion. Some content was moved to or from the chapter for *File/Malware Events and Network File Trajectory* in the *Cisco Secure Firewall Management Center Administration Guide* .
Moved URL Filtering information to the new URL Filtering chapter	6.3	Any	Moved information about configuring cloud communications for URL Filtering to the new URL Filtering chapter. Made related changes to the structure of the Cisco CSI topics in the chapter.



CHAPTER 59

Dynamic Attributes Connector

The following topics discuss how to configure and use the Dynamic Attributes Connector.

- About the dynamic attributes connector , on page 2061
- How Cisco secure dynamic attributes connector works, on page 2061
- System requirements for the dynamic attributes connector, on page 2063
- Enable the dynamic attributes connector, on page 2063
- Dashboard, on page 2065
- Connectors, on page 2072
- Create dynamic attributes filters, on page 2092
- Manually get a certificate authority (CA) chain, on page 2094
- Dynamic objects in access control rules, on page 2097
- Create dynamic attributes filters, on page 2098
- Dynamic attributes rule conditions, on page 2099
- Create access control rules using dynamic attributes filters, on page 2100
- Dynamic Firewall, on page 2101
- Disable the dynamic attributes connector, on page 2116
- Troubleshoot the Dynamic Attributes Connector, on page 2117
- Recommendation: security requirements for network deployment, on page 2117
- Internet access requirements, on page 2117
- History for the dynamic attributes connector, on page 2119

About the dynamic attributes connector

The dynamic attributes connector enables your access control policy to adapt in real time to the changes in public and private cloud workloads and business-critical software-as-a-service (SaaS) applications. It simplifies policy management by keeping rules up to date without tedious manual updates and policy deployment. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

How Cisco secure dynamic attributes connector works

This topic discusses the architecture of the dynamic attributes connector.

The system functions by querying cloud services and providing attribute information to the secure management center.

Summary

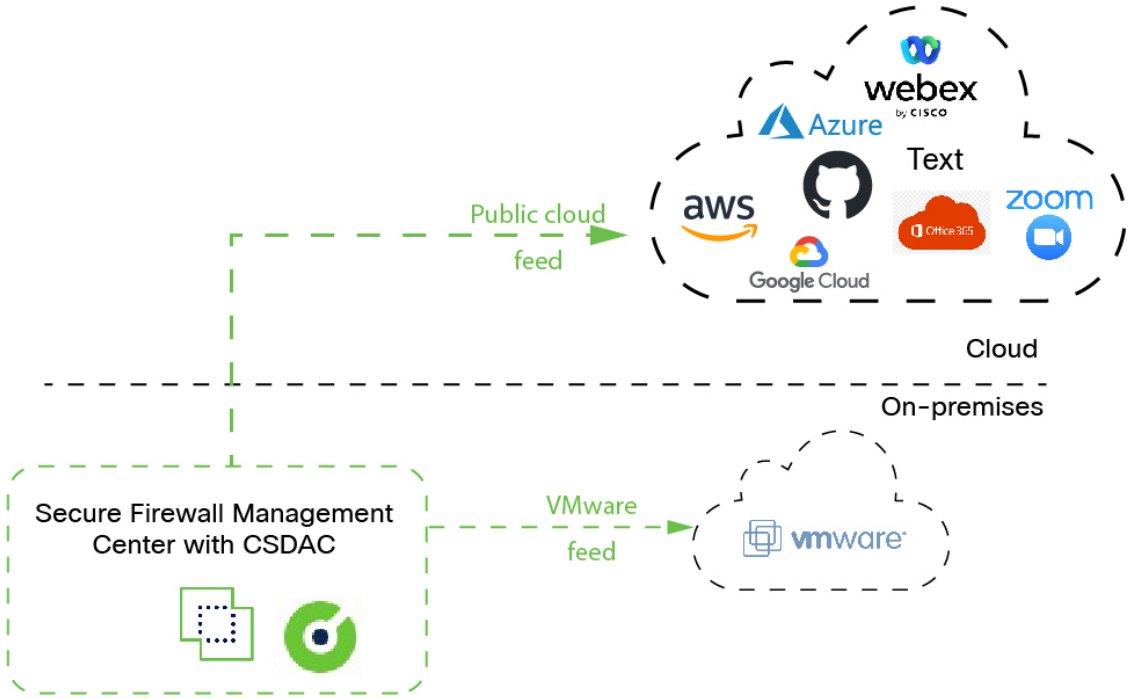
The key components involved in this process are:

- The system supports certain public cloud providers.

  This topic discusses supported *connectors* (which are the connections to those providers).

- The dynamic attributes connector is provided with Secure Firewall Management Center.

Workflow



These stages describe how the Cisco Secure Dynamic Attributes Connector processes cloud service information:

1. *Connectors* contain the tags and containers to query.

   For example, typically these tags define dynamically allocated network and IP addresses for which you cannot create access control rules. Persisted feeds from the connectors are stored on the dynamic attributes connector for fast access.

2. Tag information is persisted on the dynamic attributes connector where you create *dynamic attributes filters* that define which information is important to use in access control rules.

   For example, if AWS defines networks for the Accounting and Finance Departments virtual machines, you can create a dynamic attributes filter that specifies only the Finance network.

3. The Secure Firewall Management Center receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.

What's next

Related topics

- Enable the dynamic attributes connector, on page 2063
- Dashboard, on page 2065

System requirements for the dynamic attributes connector

The Dynamic Attributes Connector has specific memory requirements that must be met to ensure proper deployment and operation. These limits apply to both virtual machines and physical machines to avoid deployment issues.

FMCv: Amount of RAM	Secure Firewall Management Center hardware model	Maximum number of (connectors + Azure AD realms)
At least 32 GB	Firepower 1000, Firepower 1600, vFMC	10
At least 64 GB	Firepower 2500, Firepower 2600,vFMC 300	20
At least 128 GB	Firepower 4500, Firepower 4600	30

The preceding limits apply to both virtual machines and physical machines.

The system prevents you from exceeding these limits to avoid deployment issues.

Enable the dynamic attributes connector

Enable the dynamic attributes connector to allow objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Slide to **Enabled**.

Step 4 The system displays messages when the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

See Connectors, on page 2072.

Configure networks and subnets for Docker containers

The Dynamic Attributes Connector uses Docker containers to retrieve connector data in the Secure Firewall Management Center . You can change Docker IP addresses and ranges to avoid conflicts with the Secure Firewall Management Center management interface and other network IP addresses.

The Docker daemon used by the dynamic attributes connector requires the following networks:

- `docker0` : Used internally by the Docker daemon.
- IPv6 networks (`vethnumber`): Internal bridge networks used by the dynamic attributes connector .
- Docker bridge networks (`br-number`): Used by dynamic attributes connector connectors.

To change Docker networks and subnets, run the following command as a user with `root` privileges:
`/usr/local/sf/bin/change_docker_subnet.sh -b CIDR-network -s address-pool-size`

- `-b CIDR-network` : Sets a network base address pool in CIDR notation.
- `-s address-pool-size` : Sets a netmask for the network base address to limit the number of addresses and ensure compatibility with available system RAM.



Important The networks you assign to Docker must be in an internal network range and must *not* conflict with networks used by the Secure Firewall Management Center or by other devices in your internal network.

Table 119: Recommended Docker Network Settings

Secure Firewall Management Center model	Recommended -s value	Sample -b value	Dynamic Attributes Connector container addresses used
Firepower 1000, Firepower 1600, vFMC	27 (netmask 255.255.255.224)	172.19.0.0/16	30 IP addresses
Firepower 2500, Firepower 2600, vFMC 300	26 (netmask 255.255.255.192)	192.168.0.0/16	62 IP addresses
Firepower 4500, Firepower 4600	25 (netmask 255.255.255.128)	192.168.0.0/16	126 IP addresses

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
        sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
        sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

Troubleshooting

Table 120: Common Docker Network Errors

Error	Solution
Pull subnet value can not be greater than size	Change the value of `-s` so it is less than the CIDR network value. For example, INCORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8` CORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`
Docker networks are wrong	Restart the Docker daemon: `sudo pmtool restartbyid docker`
Cannot connect to the Docker daemon `Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?`	Restart Docker: `pmtool restartbyid docker`
Input can't be empty	The `-s` parameter is required.

Dashboard

Dashboard capabilities include:

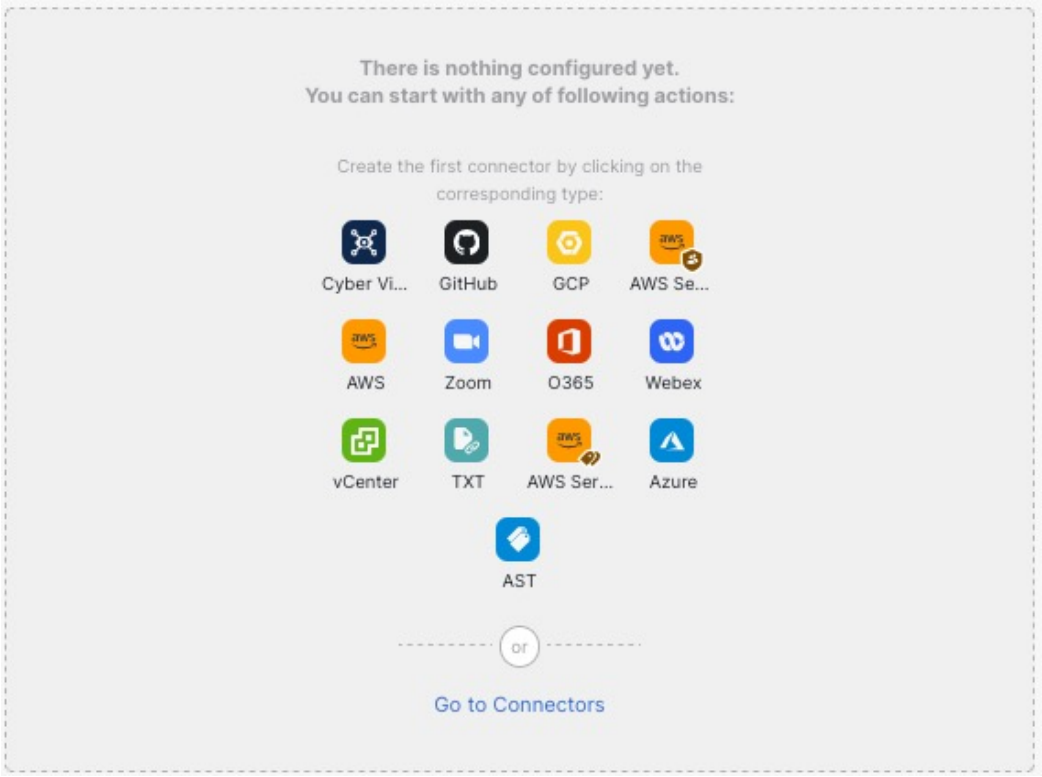
- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

Dashboard access and functionality

To access the dynamic attributes connector dashboard, log in to the Secure Firewall Manager and click **Integration** > **Dynamic Attributes Connector** at the top of the page.

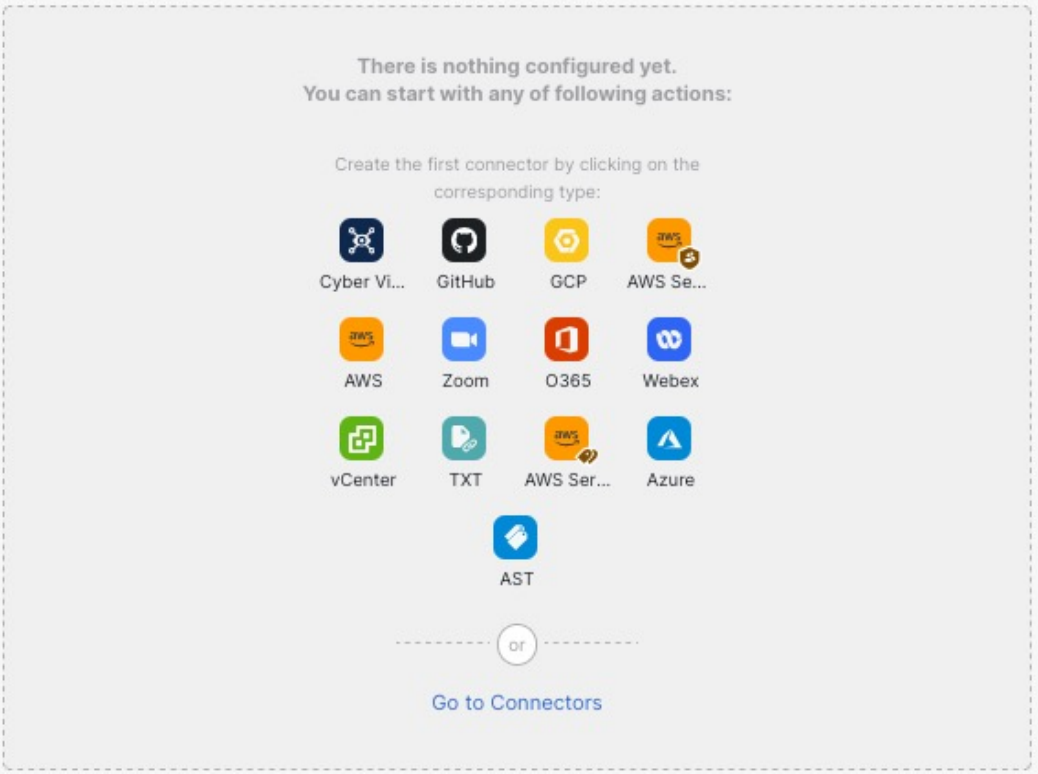
If the dynamic attributes connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

The dynamic attributes connector Dashboard page displays an example of an unconfigured system:

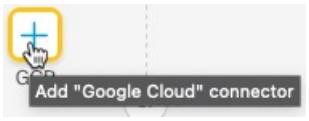


Dashboard of an unconfigured system

This sample dynamic attributes connector Dashboard page shows how an unconfigured system appears initially.



The Dashboard initially displays all the types of connectors you can configure for your system. You can do any interaction:

- Hover the mouse pointer over a connector and click 

to create a new one.
- Click **Go to Connectors** to add, edit, or delete connectors (good for creating, editing, or deleting multiple connectors at the same time).

  For more information, see Connectors, on page 2072.

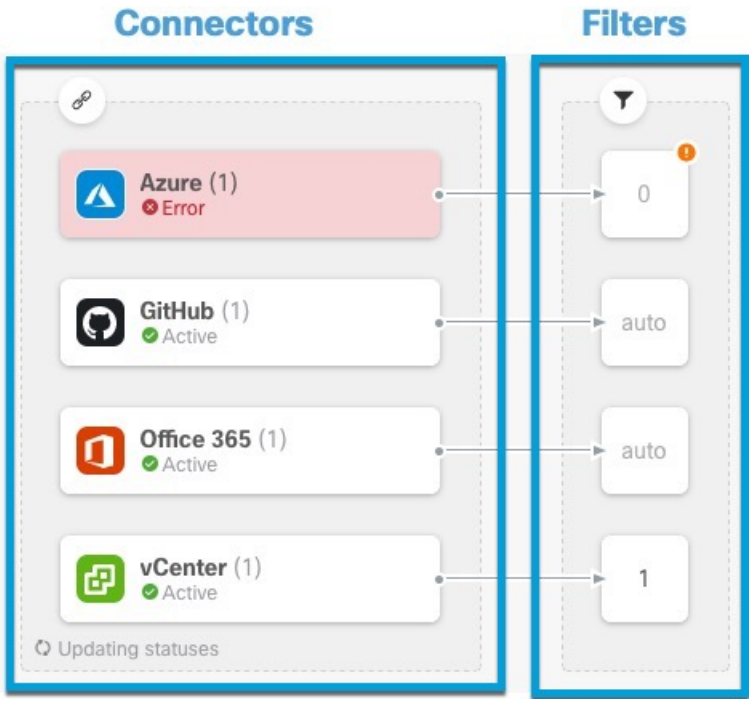
Related Topics:

- Dashboard of a configured system, on page 2067
- Add, edit, or delete connectors, on page 2069
- Add, edit, or delete dynamic attributes filters, on page 2070

Dashboard of a configured system

Sample dynamic attributes connector Dashboard page of a configured system displays at-a-glance information about configured connectors, filters, and adapters.

Click an area in the figure to learn more about it or click one of the links that follow the figure.



1 Connectors, on page 2072

2 Create dynamic attributes filters, on page 2092

The Dashboard shows the following (from left to right):

Connectors column	Filters column
List of connectors with a number indicating how many of each type are configured. Connectors collect dynamic attributes that could be sent to the Secure Firewall Manager. Dynamic attributes filters specify what data is sent. Click to view more information about all configured connectors. You can also click the name of a connector to add, edit, or delete connectors; or to view detailed information about them. For more information, see Add, edit, or delete connectors, on page 2069.	List of dynamic attributes filters associated with each connector with a number indicating how many of each filter are associated with a connector. Click to view more information about all configured filters. You can also click the name of a filter to add, edit, or delete filters; or to view detailed information about them. For more information, see Add, edit, or delete dynamic attributes filters, on page 2070.

Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

The Dashboard indicates whether or not an object is available. The Dashboard page is refreshed every 15 seconds but you can click **Refresh** ( ) at the top of the page at any time to refresh immediately. If issues persist, check your network connection.

Add, edit, or delete connectors

The Dashboard enables you to manage connectors by viewing, adding, editing, or deleting them. You can also view error information for connectors and troubleshoot issues.

Use the dynamic attributes connector dashboard when you need to manage connectors for your network security infrastructure. The dashboard provides comprehensive options for connector management and troubleshooting.

Procedure

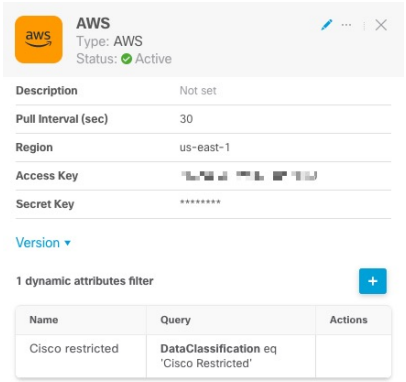
Step 1 Access the connector dashboard and select your desired action.

The Dashboard enables you to view or edit connectors. You can click the name of a connector to view all instances of that connector or you can click  for the following additional options:

- **Go to Connectors** to view all connectors at the same time; you can add, edit, and delete connectors from there.
- **Add Connector** > ***type*** to add a connector of the indicated type.

Step 2 Click any connector in the connectors column ( ) to display more information about it.

An example follows:

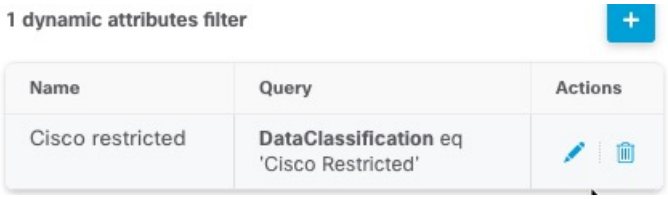


Step 3 Choose from the following management options.

- Click the Edit icon ( ) to edit this connector.
- Click the More icon ( ) for additional options.
- Click to close the panel.
- Click **Version** to display the version of the . You can optionally copy the version to the clipboard if necessary for Cisco TAC.

Step 4 Use the table at the bottom of the panel to add dynamic attributes filters or to edit or delete connectors.

A sample follows:



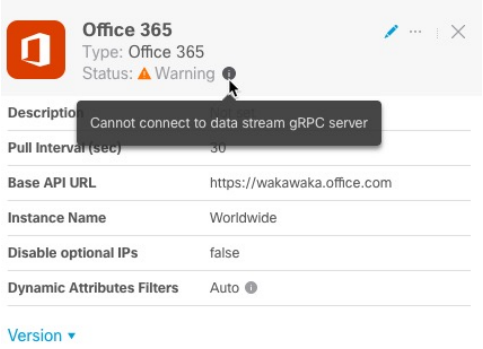
Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters, on page 2092.

Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

Step 5 To view error information for a connector, click the name of the connector that is displaying the error.

Step 6 In the right pane, click **Information** ( ).

An example follows.



Step 7 To resolve this issue, edit the connector settings as discussed in Create an office 365 connector, on page 2085.

Step 8 If you cannot resolve the issue, click **Version** and copy the version to a text file.

Add, edit, or delete dynamic attributes filters

The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click for additional options.

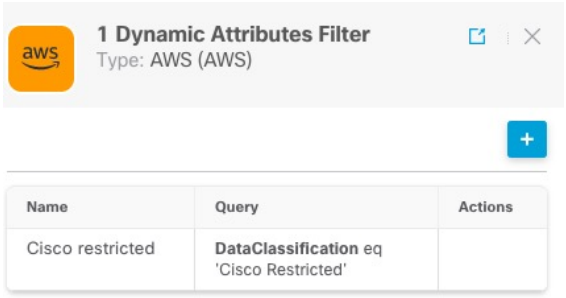
You can click the name of a filter to view all instances of that filter or you can click for the following additional options:

- **Go to Dynamic Attributes Filters** to view all configured dynamic attributes filters. You can add, edit, or delete dynamic attributes filters from there.

- **Add Dynamic Attributes Filters** to add a filter.

For more information about adding dynamic attributes filters, see Create dynamic attributes filters, on page 2092.

An example follows:



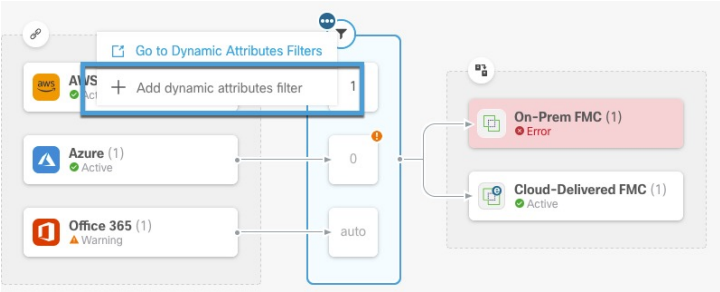
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have these options:

- Click a filter instance to view summary information about dynamic attributes filters associated with a connector.
- Click the Add icon ( ) to add a new dynamic attributes filter.

  For more information, see Create dynamic attributes filters, on page 2092.
- Click in the filters column ( ) indicates the indicated connector has no associated dynamic attributes filters. Without associated filters, the connector can send nothing to Firewall Management Center.

  One way to resolve the issue is to click in the filters column and click **Add Dynamic Attributes Filter**. A sample follows.



- Click to add, edit, or delete filters.
- Click to close the panel.

Connectors

A connector is an interface with a cloud service. It retrieves network information from the cloud service to enable the network information to be used in policies on the Secure Firewall Management Center. It supports both air gap mode and network download mode configurations.

Supported connectors

We support these connectors:

Table 121: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Amazon Web Services connector user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Amazon Web Services (AWS) to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

The connector imports these dynamic attributes from AWS:

- *Tags*, user-defined key-value pairs you can use to organize your AWS EC2 resources.

  For more information, see Tag your EC2 Resources in the AWS documentation

- *IP addresses* of virtual machines in AWS.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with a policy that permits `ec2:DescribeTags`, `ec2:DescribeVpcs`, and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS user with minimal permissions for the dynamic attributes connector

This task creates a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

For a list of the dynamic attributes that can be sent, refer to Amazon Web Services connector user permissions and imported data, on page 2072.

Before you begin

You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see this article in the AWS documentation.

Follow these steps to create an AWS user with minimal permissions for the dynamic attributes connector:

Procedure

Step 1 Log in to the AWS console as a user with the admin role.

Step 2 From the Dashboard, click **Security, Identity & Compliance** > **IAM**.

Step 3 Click **Access Management** > **Users**.

Step 4 Click **Add Users**.

a) In the **User Name** field, enter a name to identify the user.
b) Click **Access Key - Programmatic Access**.
c) At the Set permissions page, click **Next** without granting the user access to anything. You can grant user access later.
d) Add tags to the user if desired.
e) Click **Create User**.
f) Click **Download .csv** to download the user's key to your computer.

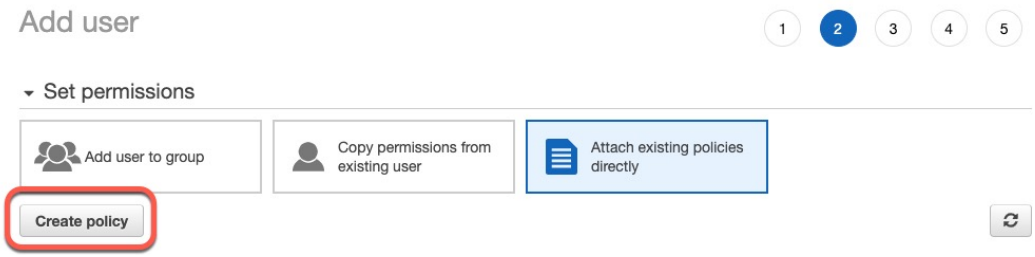
Note This is the only opportunity you have to retrieve the user's key.

g) Click **Close**.

Step 5 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 6 Click **Create Policy**.

a) On the Create Policy page, click **JSON**.



b) Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

c) Click **Next**.

Step 7 Click **Review**.

On the Review Policy page, enter the requested information and click **Create Policy**.

Step 8 Attach your policy

a) On the Policies page, enter all or part of the policy name in the search field and press Enter.
b) Click the policy you just created.
c) Click **Actions** > **Attach**.
d) If necessary, enter all or part of the user name in the search field and press Enter.
e) Click **Attach Policy**.

What to do next:

Create an AWS connector, on page 2074.

Create an AWS connector

Create a connector to send dynamic objects from AWS to the firewall for use in security policies.

This task discusses how to configure a connector that sends data from AWS to the Secure Firewall Management Center for use in policies.

Before you begin

Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector, on page 2073.

Follow these steps to create an AWS connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of these actions:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the required information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS.
Region	(Required.) Enter your AWS region code.
Access Key	(Required.) Enter your access key.
Secret Key	(Required.) Enter your secret key.

a) Click **Save**.

The Status column displays **Ok**.

What to do next:

Azure connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Azure to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

We import these dynamic attributes from Azure:

- *Tags*, key-value pairs associated with resources, resource groups, and subscriptions.

  For more information, see this page in the Microsoft documentation.

- *IP addresses* of virtual machines in Azure.

Minimum permissions required

The dynamic attributes connector requires a user at minimum with the **Reader** permission to be able to import dynamic attributes.

Create an Azure user with minimal permissions for the dynamic attributes connector

Create an Azure service account with minimal permissions to send dynamic attributes to Secure Firewall Management Center.

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center. For a list of these attributes, see Azure connector—About user permissions and imported data, on page 2075.

Before you begin

You must already have a Microsoft Azure account. To set one up, see this page on the Azure documentation site.

Follow these steps to create an Azure user with minimal permissions for the dynamic attributes connector:

Procedure

Step 1 Log in to the Azure Portal as the owner of the subscription.

Step 2 Click **Azure Active Directory**.

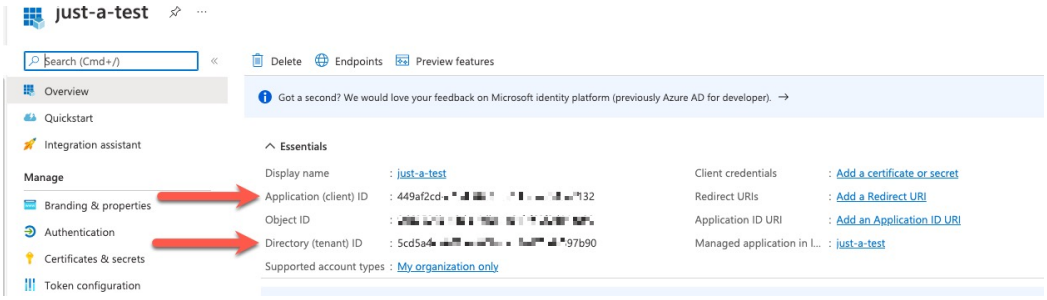
Find the instance of Azure Active Directory for the application you want to set up.

Step 3 Click **Add** > **App registration**.

a) In the **Name** field, enter a name to identify this application.
b) Enter other information on this page as required by your organization.
c) Click **Register**.

Step 4 On the next page, write down or copy the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

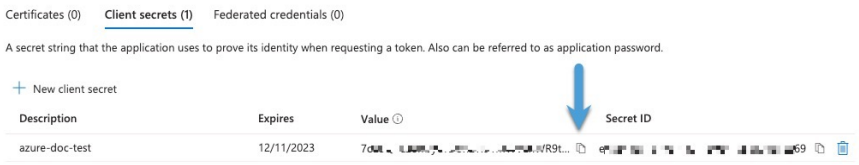
Here is a sample:



Step 5 Next to Client Credentials, click **Add a certificate or secret**.

Step 6 Click **New Client Secret**.

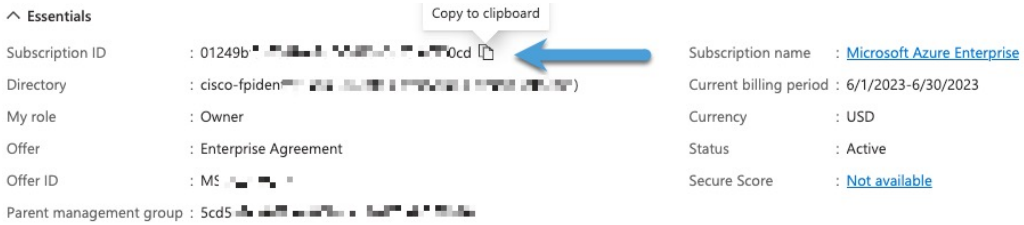
a) Enter the requested information and click **Add**.
b) Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



Step 7 Go back to the main Azure Portal page and click **Subscriptions**.

a) Click the name of your subscription.

b) Copy the subscription ID to the clipboard.



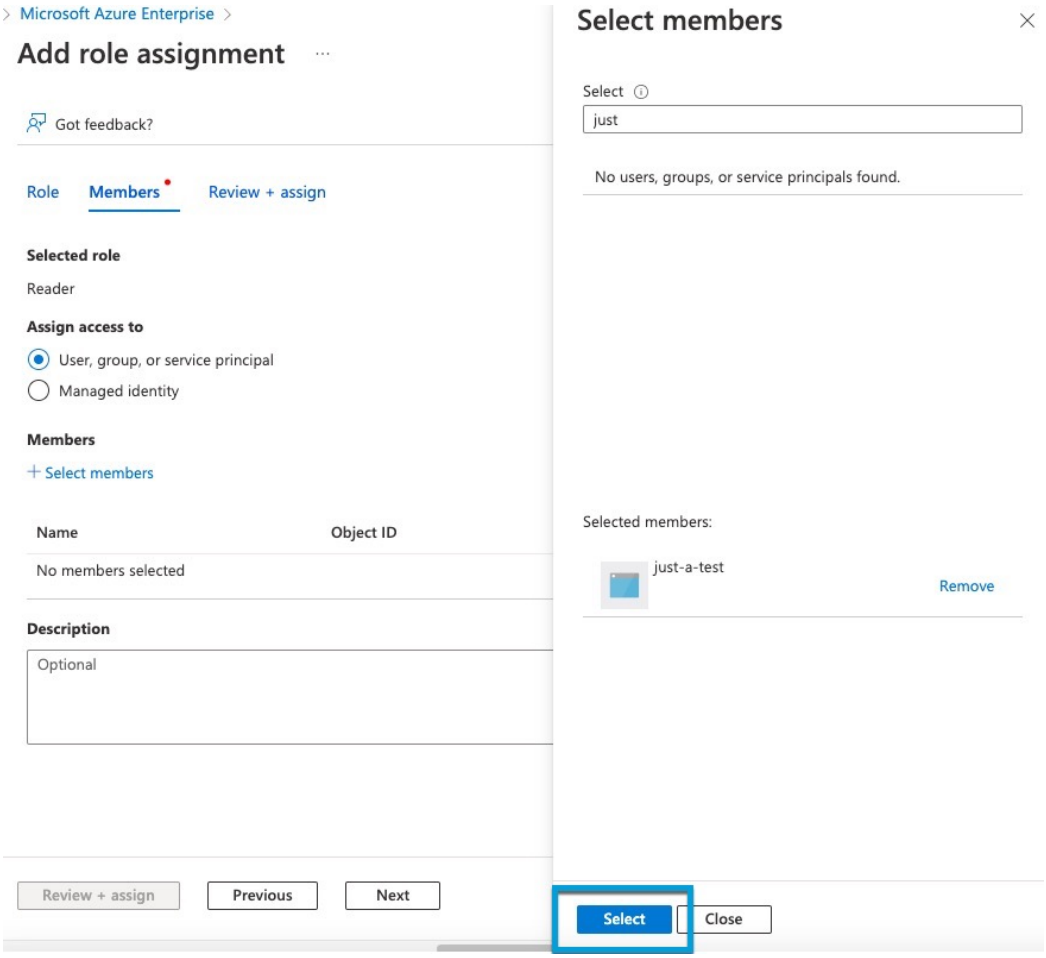
Step 8 Click **Access Control (IAM)**.

a) Click **Add** > **Add role assignment**.

b) Click **Reader** and click **Next**.

c) Click **Select Members**.

d) On the right side of the page, click the name of the app you registered and click **Select**.



e) Click **Review + Assign** and follow the prompts to complete the action.

Also see Create an Azure connector, on page 2078.

Create an Azure connector

Create a connector to send data from Azure to Secure Firewall Management Center for use in policies.

This connector enables integration between Azure and your security management platform to retrieve dynamic object information for policy implementation.

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure user with minimal permissions for the dynamic attributes connector, on page 2076.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription ID	(Required.) Enter your Azure subscription ID.
Tenant ID	(Required.) Enter your tenant ID.
Client ID	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

a) Click **Save**.

The Status column displays **Ok**.

Create an Azure service tags connector

Create a connector for Azure service tags to enable use in policies with automatically updated IP addresses from Microsoft.

This topic discusses how to create a connector for Azure service tags to the Secure Firewall Management Center for use in policies. The IP addresses associated with these tags are updated every week by Microsoft.

For more information, see Virtual network service tags on Microsoft TechNet.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the required information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Subscription ID	(Required.) Enter your Azure subscription ID.
Tenant ID	(Required.) Enter your tenant ID.
Client ID	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

a) Click **Save**.

The Status column displays **Ok**.

Create a generic text connector

Use this task to create a connector that retrieves IP addresses from text files and sends them to the firewall for use in access control rules.

This task discusses how to create an ad hoc list of IP addresses you maintain manually and retrieve at an interval you select (30 seconds by default). You can update the list of addresses anytime you want.

For example, you might have a list of IP addresses for an "allow list" in access control rules and another list of IP addresses for a "block list" in access control rules.

Before you begin

Create text files with IP addresses and put it on a web server that is accessible from the Secure Firewall Management Center . IP addresses can include CIDR notation. The text file must have only one IP address per line.

You can specify up to 10,000 IP addresses per text file.

Follow these steps to create a generic text connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information:

Item	Description
Name	Enter a name to identify the connector.
Description	(Optional.) Enter a description
Pull Interval	Change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from the text file. The default is 30 seconds. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
URLs	Enter a URL from which to retrieve IP addresses.
Add another URL	(Optional.) Click the link to add more URLs to an existing list.
Certificate	(Optional.) If a certificate chain is required for a secure connection to the web server, you have these options: • Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually get a certificate authority (CA) chain, on page 2094. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.
c) Status column displays **Ok**

Create a GitHub connector

Create a GitHub connector that sends data to the Secure Firewall Management Center for use in policies. The IP addresses associated with these tags are maintained by GitHub.

For more information, see About GitHub's IP addresses.

Note Do not change the URL because doing so will fail to retrieve any IP addresses.

Before you begin

You do not have to create a dynamic attributes filters.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter a **Name** and an optional description.

a) (Optional) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).

b) Click **Save**.

The Status column displays **Ok**.

Google cloud connector user permissions and imported data

A Google Cloud connector imports dynamic attributes from Google Cloud to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

The connector imports these dynamic attributes from Google Cloud:

- *Labels*: Key-value pairs assigned to virtual machine instances. Use the labels to organize your Google Cloud resources. For more information, see Creating and Managing Labels in the Google Cloud documentation.
- *Network tags*: Text values assigned to virtual machine instances that help identify groups of instances. For more information, see Creating and Managing Tags in the Google Cloud documentation.

- *IP addresses*: IP addresses associated with virtual machine instances in your Google Cloud project and region.

The dynamic attributes connector requires a user at minimum with the **Basic** > **Viewer** permission to be able to import dynamic attributes.

Create a Google Cloud user with minimal permissions for the dynamic attributes connector

Create a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

This task sets up a service account that provides the minimum permissions necessary for the dynamic attributes connector. For a list of these attributes, see Google cloud connector user permissions and imported data, on page 2082.

Before you begin

You must already have set up your Google Cloud account. For more information about doing that, see Setting Up Your Environment in the Google Cloud documentation.

Procedure

Step 1 Log in to your Google Cloud account as a user with the owner role.

Step 2 Click **IAM & Admin** > **Service Accounts** > **Create Service Account**.

Step 3 Enter the following information:

- **Service account name**: A name to identify this account; for example, `CSDAC`.
- **Service account ID**: Should be populated with a unique value after you enter the service account name.
- **Service account description**: Enter an optional description.

For more information about service accounts, see Understanding Service Accounts in the Google Cloud documentation.

Click **Create and Continue**.

Step 4 Follow the prompts on your screen until the Grant users access to this service account section is displayed.

Grant the user the **Basic** > **Viewer** role.

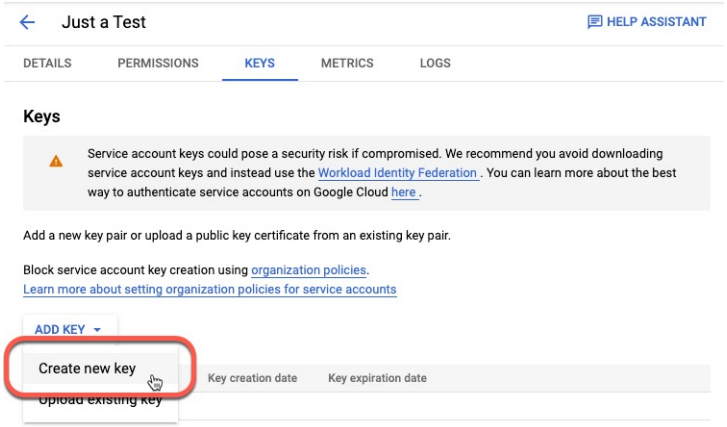
Click **Done**.

A list of service accounts is displayed.

Step 5 Click **More** (⋮) at the end of the row of the service account you created.

Step 6 Click **Manage Keys**.

Step 7 Click **Add Key** > **Create New Key**.



Step 8 Click **JSON**.

Step 9 Click **Create**.

The JSON key is downloaded to your computer.

Keep the key handy when you configure the GCP connector.

See Create a google cloud connector, on page 2084.

Create a google cloud connector

Create a Google Cloud connector to enable data transmission from your Google Cloud environment to the firewall for dynamic security attribute monitoring and management.

The Google Cloud connector allows the firewall to receive real-time data from your Google Cloud infrastructure, enabling dynamic security policies based on cloud resource attributes.

Before you begin

Have your Google Cloud JSON-formatted service account data ready; it's required to set up the connector.

Follow these steps to create a Google Cloud connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit or delete a connector: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
GCP region	(Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation.
Service account	Paste the JSON code for your Google Cloud service account.

a) Click **Save**.

The Status column displays **Ok**.

Create an office 365 connector

Create a connector for Office 365 tags to send data to the Secure Firewall Management Center for use in policies.

The IP addresses associated with these tags are updated every week by Microsoft. You do not have to create a dynamic attributes filter to use the data.

For more information, refer to Office 365 URLs and IP address ranges on docs.microsoft.com.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit or delete a connector: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.

Value	Description
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Base API URL	(Required.) Enter the URL from which to retrieve Office 365 information, if it's different from the default. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Instance name	(Required.) From the list, click an instance name. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Disable optional IPs	(Required.) Enter **true** or **false**.

Step 5 Click **Save**.

The Status column displays **Ok**.

vCenter connector—About user permissions and imported data

The Dynamic Attributes Connector imports dynamic attributes from vCenter to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

We import these dynamic attributes from vCenter:

- *Operating system*
- *MAC address*
- *IP addresses*
- *NSX tags*

Minimum permissions required

The Dynamic Attributes Connector requires a user at minimum with the **Read Only** permission to be able to import dynamic attributes.

Create a vCenter user with minimal permissions for the dynamic attributes connector

Create a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

This task provides the steps to set up a service account with minimum permissions required for the dynamic attributes connector. For a list of these attributes, see vCenter connector—About user permissions and imported data, on page 2086.

Before you begin

You must already have set up your vCenter Server account. For more information about doing that, see About vCenter Server Installation and Setup in the vCenter documentation.

Follow these steps to create a vCenter user with minimal permissions for the dynamic attributes connector:

Procedure

Step 1 Log into vCenter as an administrator.

Step 2 Click **Menu** > **Administration**.

Step 3 In the left pane, click **Single Sign On** > **Users and Groups**.

Step 4 From the **Domain** list, click the name of a domain to add the user.

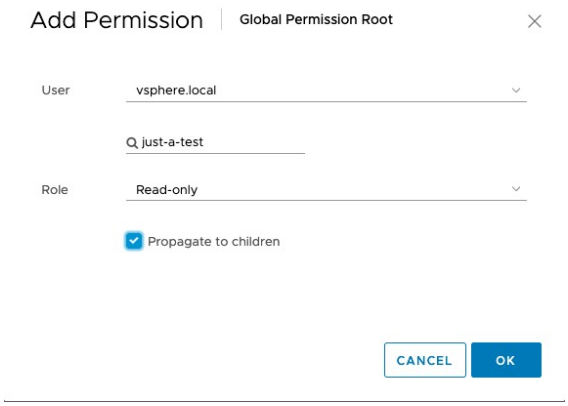
Step 5 Click **Add User**.

a) Enter the requested information and click **Add**.

Step 6 In the left pane, click **Access Control** > **Global Permissions**.

Step 7 Click **Add**(+).

a) From the **User** field, click the name of the vCenter domain in which you created the user.
b) In the search field, enter part of the user's name.
c) From the **Role** list, click **Read-only**.
d) Select the **Propagate to children** check box.



Step 8 Click **OK**.

What to do next

See Create a vCenter connector, on page 2088.

Create a vCenter connector

Create a connector for VMware vCenter to send data to the Secure Firewall Management Center for use in policies.

This connector enables the management center to receive dynamic attribute information from vCenter Server for use in security policies and monitoring.

Before you begin

If you use non-trusted certificates to communicate with vCenter, see Manually get a certificate authority (CA) chain, on page 2094.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

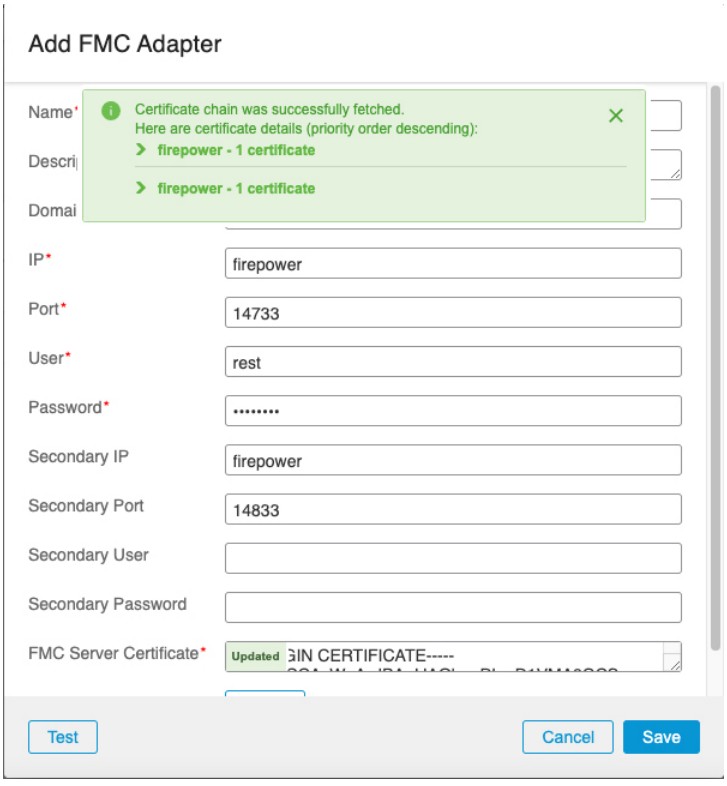
- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit or delete a connector: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Enter an optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from vCenter. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Host	(Required.) Enter any of the following: • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port *Do not* enter a scheme (such as **`https://`**) or trailing slash. For example, **`myvcenter.example.com`** or **`192.0.2.100:9090`**
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.

Value	Description
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.
NSX Password	Enter the NSX user's password.
vCenter Certificate	You have the following options: • Paste the certificate authority (CA) chain you got as discussed in Manually get a certificate authority (CA) chain, on page 2094. • Click **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually get a certificate authority (CA) chain, on page 2094. • Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually get a certificate authority (CA) chain, on page 2094. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:



Expanding the certificate CA chain at the top of the dialog box displays the certificates similar to the following.



If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually get a certificate authority (CA) chain, on page 2094.

Step 5 Click **Save**.

Create a Webex connector

This task creates a Webex connector that sends IP addresses to the management system for use in policies. The IP addresses associated with these tags are maintained by Webex.

This section discusses how to create a Webex connector that sends data to the Secure Firewall Management Center for use in policies. The IP addresses associated with these tags are maintained by Webex. You do not have to create a dynamic attributes filters.

For more information, see Port Reference for Webex Calling.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon ( ), then click the name of the connector.
- Edit or delete a connector: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Webex. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) (Required.) Slide to enabled to retrieve any reserved IP addresses.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.
c) The Status column displays **Ok**.

Create a Zoom connector

Create a Zoom connector that sends data to the Secure Firewall Management Center for use in policies.

The IP addresses associated with these tags are maintained by Zoom. You do not have to create a dynamic attributes filters.

For more information, see Zoom network firewall or proxy server settings.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter this information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Zoom. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) Slide to enabled to retrieve any reserved IP addresses.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

The Status column displays **Ok**.

Create dynamic attributes filters

Create dynamic attributes filters to expose them as dynamic objects in Secure Firewall Management Center for use in access control policies.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 2100.

Before you begin

Connectors, on page 2072

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Click **Integration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 2 Do any of the following:

- Add a new filter: click **Add** ( ).
- Edit or delete a filter: Click **More** ( ), then click **Edit** or **Delete** at the end of the row.

Step 3 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

Step 4 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 5 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 6 When you're finished, click **Save**.

Step 7 (Optional.) Verify the dynamic object in the Secure Firewall Management Center.

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

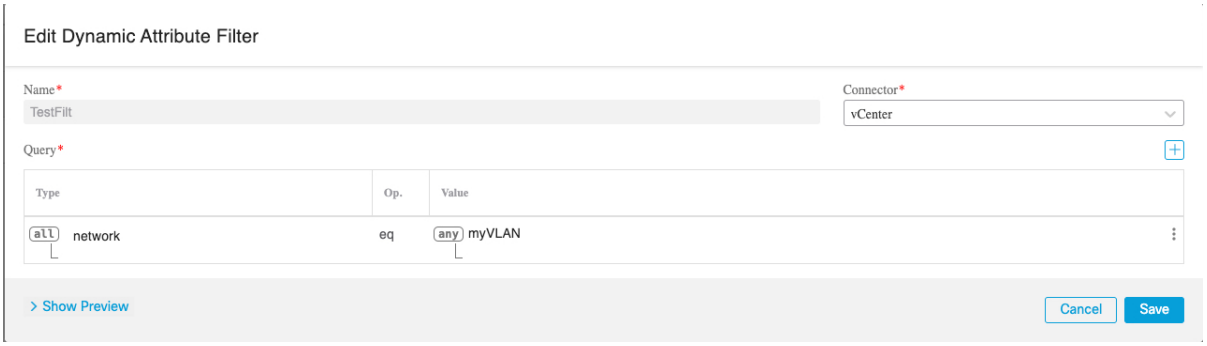
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

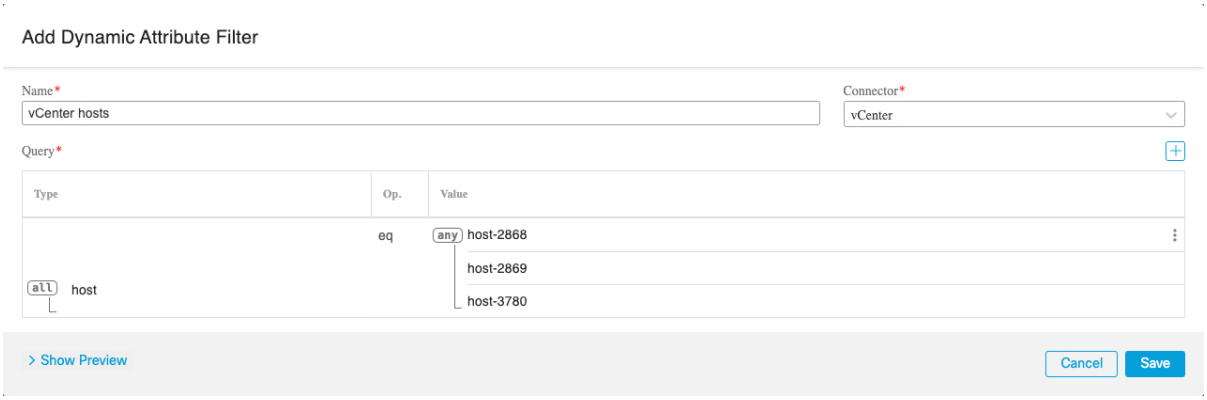
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

This example shows one criterion: a VLAN.

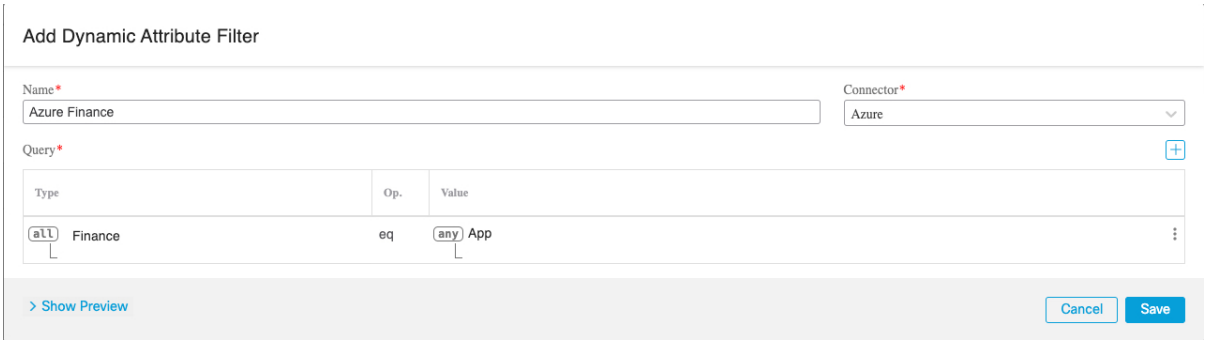


This example shows three criteria that are joined with OR: the query matches any of three hosts.



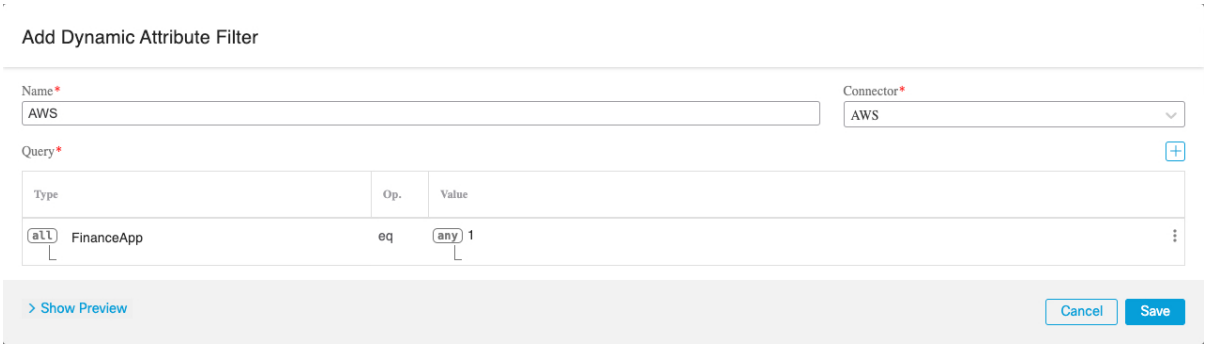
Example: azure

This example shows one criterion: a server tagged as a Finance app.



Example: AWS

This example shows one criterion: a FinanceApp with a value of 1.



Manually get a certificate authority (CA) chain

If the certificate authority chain is not fetched automatically, use one of these browser-specific procedures to get a certificate chain to securely connect to vCenter or Firewall Management Center .

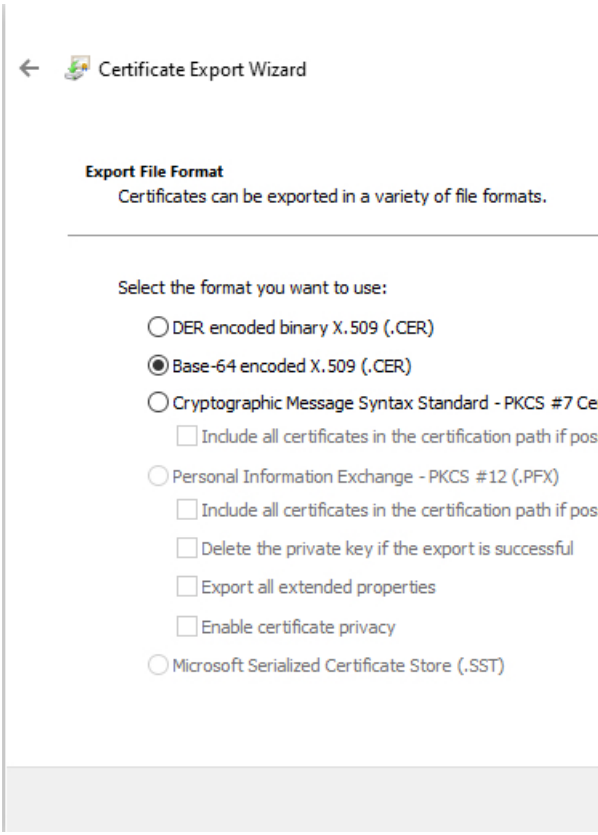
The *certificate chain* is the root certificate and all subordinate certificates.

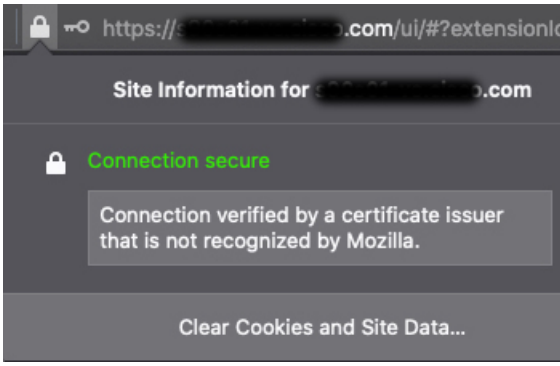
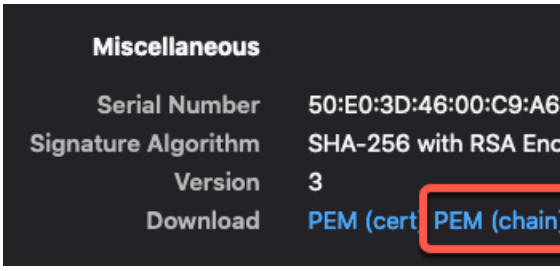
Procedure

	Command or Action	Purpose

Step 1	Get a Certificate Chain—Mac (Chrome and Firefox)	**a.** Open a Terminal window.
		b. Enter this command:
		`security verify-cert -P url[:port]`
		where *url* is the URL (including scheme) to vCenter or Firewall Management Center . For example:
		`security verify-cert -P https://myvcenter.example.com`
		If you access vCenter or Firewall Management Center using NAT or PAT, you can add a port as follows:
		`security verify-cert -P https://myvcenter.example.com:12345`
		c. Save the entire certificate chain to a plaintext file.
		• *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
		• *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.
		d. Repeat these tasks for vCenter Firewall Management Center .

Step 2	Get a Certificate Chain—Windows Chrome	**a.** Log in to vCenter or Firewall Management Center using Chrome. **b.** In the browser address bar, click the lock to the left of the host name. **c.** Click **Certificate**. **d.** Click the **Certification Path** tab. **e.** Click the top (that is, first) certificate in the chain. **f.** Click **View Certificate**. **g.** Click the **Details** tab.

	Command or Action	Purpose
		h. Click **Copy to File**. **i.** Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain. When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)**.  Follow the prompts to complete the export. Open the certificate in a text editor. Repeat the process for all certificates in the chain. You must paste each certificate in the text editor in order, first to last. Repeat these tasks for vCenter or Firewall Management Center .
Step 3	Get a Certificate Chain—Windows Firefox	**a.** Log in to vCenter or Firewall Management Center using Firefox.

	Command or Action	Purpose
		b. Click the lock to the left of the host name. **c.** Click the right arrow (**Show connection details**).  **d.** Click **More Information**. **e.** Click **View Certificate**. **f.** If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA. **g.** Scroll to the Miscellaneous section. **h.** Click **PEM (chain)** in the Download row.  **i.** Save the file. Repeat these tasks for vCenter or Firewall Management Center .

Dynamic objects in access control rules

A *dynamic object* is automatically pushed from the dynamic attributes connector to the Secure Firewall Manager after you create connectors and save a dynamic attributes filter on the connector.

You can use these dynamic objects on the access control rule's **Dynamic Attributes** tab page. You can add dynamic objects as source or destination attributes.

Dynamic object usage examples

In an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

Dynamic attributes filter limitations

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

Create dynamic attributes filters to expose them as dynamic objects in Secure Firewall Management Center for use in access control policies.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 2100.

Before you begin

Connectors, on page 2072

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Click **Integration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 2 Do any of the following:

- Add a new filter: click **Add** ().
- Edit or delete a filter: Click **More** (), then click **Edit** or **Delete** at the end of the row.

Step 3 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

Step 4 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 5 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 6 When you're finished, click **Save**.

Step 7 (Optional.) Verify the dynamic object in the Secure Firewall Management Center.

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attributes rule conditions

Dynamic attributes rule conditions allow you to specify access control rules based on real-time properties such as network objects, device types, locations, and security tags. These conditions determine how access control rules match traffic based on various attributes, optimizing policy flexibility and accuracy.

Types of dynamic attributes

Dynamic attributes include:

- (source or destination) Dynamic objects (such as from the dynamic attributes connector)

The dynamic attributes connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the Secure Firewall Management Center so they can be used in access control rules.

For more information about the dynamic attributes connector, see About the dynamic attributes connector , on page 2061.

- (source only) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and destination security group tag (SGT) matching, on page 1912 and Security group tags, on page 2376.
- (source only) Location IP objects, defined by Cisco ISE
- (source only) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Combining objects in rules

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use these guidelines:

- Objects of different types are ANDd together
- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1, the rule matches if device type 1 is detected on either SGT 1 or SGT 2.

If you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originating from, or destined to, one of those IP addresses.

Create access control rules using dynamic attributes filters

Create access control rules using dynamic objects that are based on dynamic attributes filters you have previously configured.

This topic discusses how to create access control rules using dynamic objects (these dynamic objects are named after the dynamic attributes filters you created previously).

To add dynamic attributes filters to DNS policies, see Create basic DNS policies, on page 1997.

Before you begin

Create dynamic attributes filters as discussed in Create dynamic attributes filters, on page 2092.

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Follow these steps to create access control rules using dynamic attributes filters:

Procedure

Step 1 Log in to the Secure Firewall Management Center

Click **Policies** > **Access Control heading** > **Access Control**.

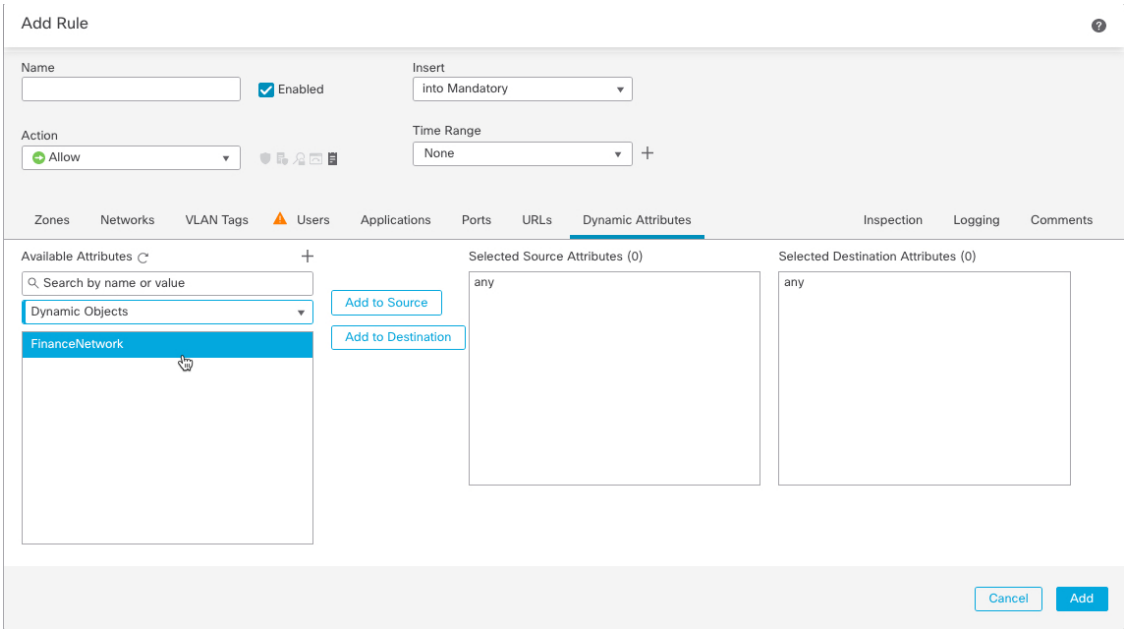
Step 2 Click **Edit** ( ) next to an access control policy.

Step 3 Click **Add Rule**.

Step 4 Click the **Dynamic Attributes** tab.

Step 5 In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.



This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.

Step 6 Add the desired object to source or destination attributes.

Step 7 Add other conditions to the rule if desired.

See Dynamic attributes rule conditions, on page 2099.

Dynamic Firewall

A dynamic firewall integrates user identity data with user trust data provided by Identity Intelligence to enhance your ability to detect identity-based exploits in your network.

Identity data integration

The dynamic firewall integrates user identity data from Microsoft AD and ISE with user trust data.

Dynamic Firewall

A dynamic firewall integrates identity sources with Identity Intelligence to provide user and device trust information.

Enhanced identity information

Previously, the collected information about users exclusively from the configured identity sources, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address.

The dynamic firewall enables you to pair user identity with intelligence and use that information in reporting and access control policies.

To use the dynamic firewall, you must:

- Have an Identity Intelligence tenant

  See Duo Identity Security with Cisco Identity Intelligence.

- Enable the Dynamic Attributes Connector
- Set up an identity source:
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid Cloud

    pxGrid Cloud combines identity and posture in the same feed

    More information: What is pxGrid?

  In addition to providing authentication information, Cisco ISE and pxGrid Cloud can provide the following:

  - SGT Exchange Protocol (SXP) over TCP binding and directory session information if desired. For more information, see the *Cisco Identity Services Engine Administrator Guide*
  - Posture and mobile device management compliance. For more information, see Compliance.

- Set up an identity realm:
  - Create an LDAP realm or an Active Directory realm and realm directory, on page 1860

The *identity source* provides authentication information (login, logout) as well as posture. The identity source can also provide SXP binding and session directory information if desired.

The *identity realm* provides user, group, and IP address information.

How to configure the dynamic firewall

This topic helps you understand the concepts and options to configure the dynamic firewall discussed in Dynamic Firewall, on page 2102.

Summary

The dynamic firewall integrates an identity source (such as Cisco ISE) with Cisco Identity Intelligence, which provides user trust information to the Secure Firewall Management Center.

1. Configure Cisco Identity Intelligence to collect user trust information.
2. Configure a supported Secure Firewall Management Center identity source.
3. Configure a supported identity realm.
4. Enable the dynamic attributes connector.
5. Configure the dynamic firewall.

Workflow

The following procedure provides a high-level overview of how to configure the dynamic firewall.

1. As a Duo user with the Owner role, provision a Cisco Identity Intelligence tenant.

   You can provision a tenant from Duo Advantage as discussed in *Provision Your Cisco Identity Intelligence Tenant*.

2. In Cisco Identity Intelligence, create an API integration and use the information to set up the dynamic firewall.

   We use Cisco Identity Intelligence to find user and device risk information in your network.

   For more information about Cisco Identity Intelligence, see How-to Guides.

   For more information about this task, see Get required information for Identity Intelligence, on page 2105.

3. (Microsoft Azure AD realm only.) In Identity Intelligence, create a Microsoft Entra ID integration.

   For more information, see Microsoft Entra ID (Azure AD) Data Integration.

4. Create an identity source. (If you already have an identity source, continue with the next step.)

   You can do this in any of the following ways:

   - The Configure Dynamic Firewall dialog box displays **Configure** links to start setting up your identity source.
   - Click **Integration** > **Other Integrations** > **Identity Sources**.

   For more information about creating identity sources, see:

   - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
   - Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
   - Configuring a pxGrid Cloud identity source

5. Create an identity realm.

   We support the following realms:

   - Create an LDAP realm or an Active Directory realm and realm directory, on page 1860

     Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

6. Enable the dynamic attributes connector.

   The dynamic attributes connector is required to use the dynamic firewall. It enables your identity source to integrate with Identity Intelligence to provide enhanced insights into user activity.

   See Enable the dynamic attributes connector, on page 2063.

7. Create the dynamic firewall instance. (If you already have a dynamic firewall instance, continue with the next step.)

   Click **Integration** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

   See Create a dynamic firewall instance, on page 2107.

8. Associate your identity source with Cisco Identity Intelligence.

   See Associate an identity source with Identity Intelligence, on page 2108.

9. View system-defined filters.

   We create dynamic attributes filters for the following:

   - Untrusted device
   - Trusted device
   - Untrusted user
   - Questionable user

   You can edit or replace these dynamic attributes filters as discussed in Create dynamic attributes filters, on page 2115.

10. View system-defined access control rules.

    We create an access control policy named Dynamic Firewall Policy (or similar) with the following rules:

    - Block an untrusted user from any source network to any destination network.
    - Monitor a questionable user from any source network to any destination network.
    - Block an untrusted device from any source network to any destination network.

    You can edit or delete the access control policy and rules as discussed in View and edit the system-created access control policy, on page 2114.

Enable the dynamic attributes connector

Enable the dynamic attributes connector to allow objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Slide to **Enabled**.

Step 4 The system displays messages when the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

See Connectors, on page 2072.

Get required information for Identity Intelligence

Get the necessary credentials and configuration values from Identity Intelligence to enable integration with the dynamic firewall.

This task discusses how to create an API client, which provides all the get required information to set up Identity Intelligence in the dynamic firewall.

If you already have an API client and you know the values of all these parameters, you can skip this procedure and continue with Create a dynamic firewall instance, on page 2107:

- **Client ID**
- **API URL**
- **Token URL**
- **Client Secret**

Before you begin

Integrating with the dynamic firewall requires you to create an *API client integration* in Identity Intelligence.

Among the values you must know about your API client integration is the client secret, which is displayed when you create the API client only. For that reason you might need to create the API integration first.

For more information about creating an API cilent integration, see Public API.

Follow these steps to get required information for Identity Intelligence:

Procedure

Step 1 Log in to your Identity Intelligence tenant.

Step 2 Click  (**Integrations**).

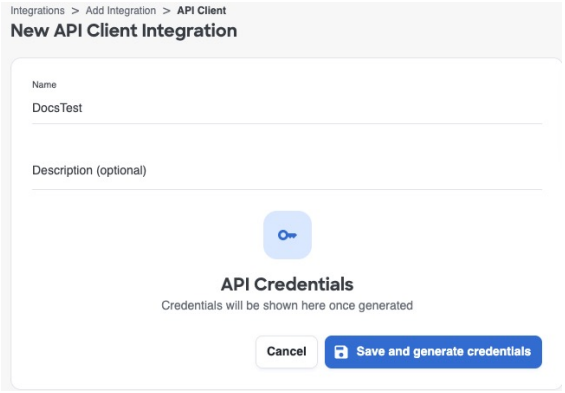
Step 3 Click **Add Integration**.

Step 4 On the next page, under API Clients, click **Add API Client**.

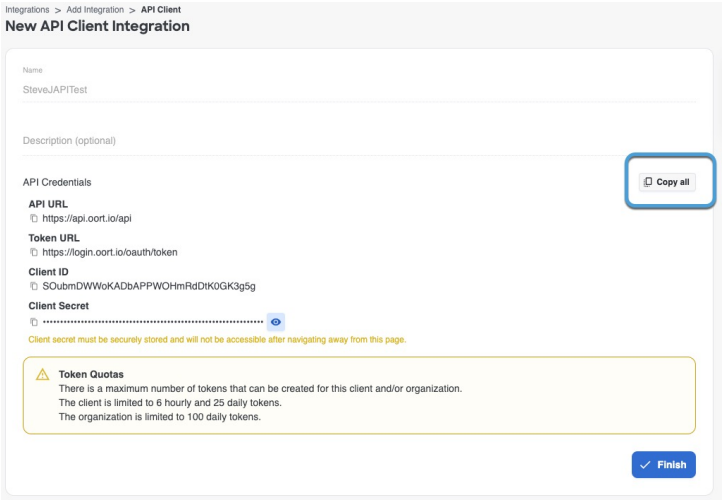
Step 5 Enter a **Name** and an optional **Description**.

Step 6 Click **Save and Generate Credentials**.

This figure shows an example.



Step 7 On the next page, click **Copy all** as this figure shows.



Step 8 Save the credentials for later use.

Step 9 Click **Finish**.

What to do next

See Create a dynamic firewall instance, on page 2107.

Create an identity source and realm for the dynamic firewall

Before you configure the dynamic firewall, you must configure a supported identity realm and identity source.

Configure an identity realm

These identity realms are supported:

- Create an LDAP realm or an Active Directory realm and realm directory, on page 1860

Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

Configure an identity source

These identity sources are supported:

- On-premises Cisco ISE: Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Single or multiple Cisco ISE clusters:
  - Configuring a pxGrid Cloud identity source
  - Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)

Create a dynamic firewall instance

Create a new instance of the dynamic firewall to establish an association between an identity source and Identity Intelligence.

This task discusses how to create a new instance of the dynamic firewall, which is an association between an identity source and Identity Intelligence.

Before you begin

Complete all these steps:

- Enable the dynamic attributes connector as discussed in Enable the dynamic attributes connector, on page 2063.
- Create an identity source:
  - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
  - Create a pxGrid Cloud identity source.

Follow these steps to create a dynamic firewall instance:

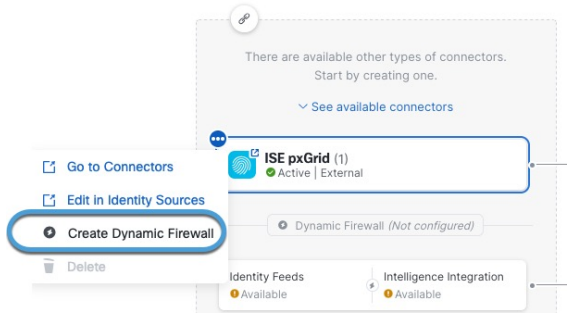
Procedure

Step 1 If you have not already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector**.

Step 3 Click next to the name of the identity source with which to add the dynamic firewall.

The following figure shows an example.



Note If you do not see an identity source, create one before continuing:

- Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
- Configuring a pxGrid Cloud identity source

Step 4 Click **Create Dynamic Firewall**.

Step 5 Continue with Associate an identity source with Identity Intelligence, on page 2108.

Associate an identity source with Identity Intelligence

Associate a supported identity source with Identity Intelligence to enable user and device trust ratings for dynamic firewall configuration.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device trust ratings to the .

For more information, see User Trust Level.

Before you begin

Before you begin, make sure you:

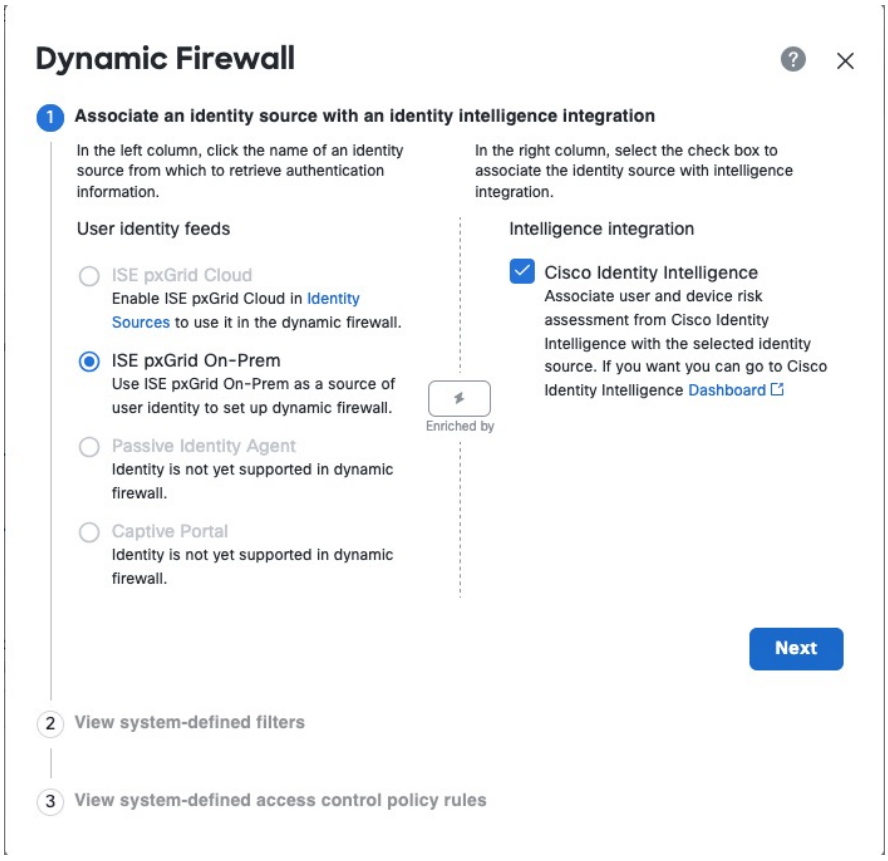
- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in Dynamic Firewall, on page 2102.
- Completed the tasks discussed in Create a dynamic firewall instance, on page 2107.

Procedure

Step 1 Start with Create a dynamic firewall instance, on page 2107.

Step 2 On the next page, from the left column, click your identity source. Then, in the right column, select the **Cisco Identity Intelligence** check box to add user intelligence, including user and device risk.

The following figure shows an example.



Step 3 Click **Next**.

Step 4 Continue with Configure Identity Intelligence, on page 2109.

Configure Identity Intelligence

This task enables integration between the dynamic firewall and Identity Intelligence.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

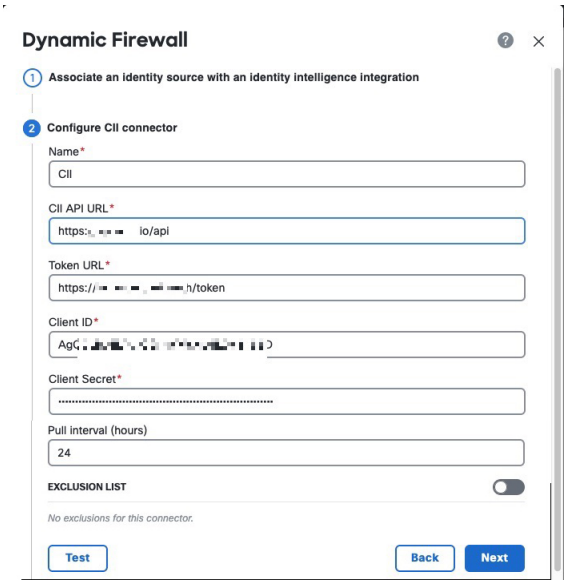
Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 2108.

Procedure

Step 1 Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 2108.

Step 2 If you selected the **Cisco Identity Intelligence** check box, enter the information you found for Identity Intelligence as described in Get required information for Identity Intelligence, on page 2105.

The following figure shows an example.



Step 3 (Optional.) For Identity Intelligence to consider a specific set of users as trusted, slide **Exclusion List** to **Slider enabled** ( ).

Enter one user name per line in **username@domain.com** format. Users in this list are considered trusted by Identity Intelligence.

Step 4 Click **Test**.

Only if the test succeeds, continue with the next step.

If any errors are displayed, check all of your Identity Intelligence values and try again.

Step 5 Click **Next**.

Step 6 Continue with View system-defined filters, on page 2110.

View system-defined filters

This task allows you to examine and understand the system-defined dynamic attributes filters that are automatically created during the configuration process.

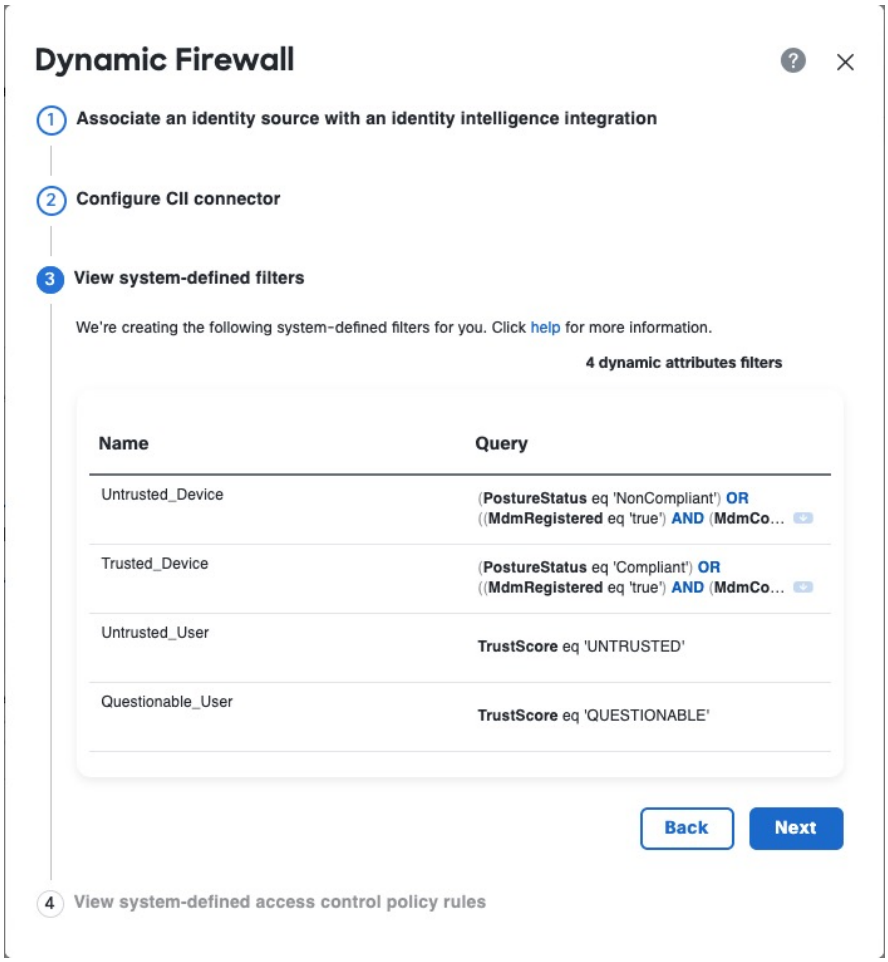
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

See Configure Identity Intelligence, on page 2109.

Procedure

Step 1 The system displays a set of system-defined dynamic attributes filters, as shown in the following figure.



Step 2 View the system-created filters. Click on any row to expand the filter so you can view the filter and see its details.

Step 3 Click **Next**.

Step 4 Continue with View system-defined access control rules, on page 2111.

View system-defined access control rules

This task allows you to review and decide whether to create system-defined access control rules for your dynamic firewall instance.

This task discusses access control rules created by the dynamic firewall.

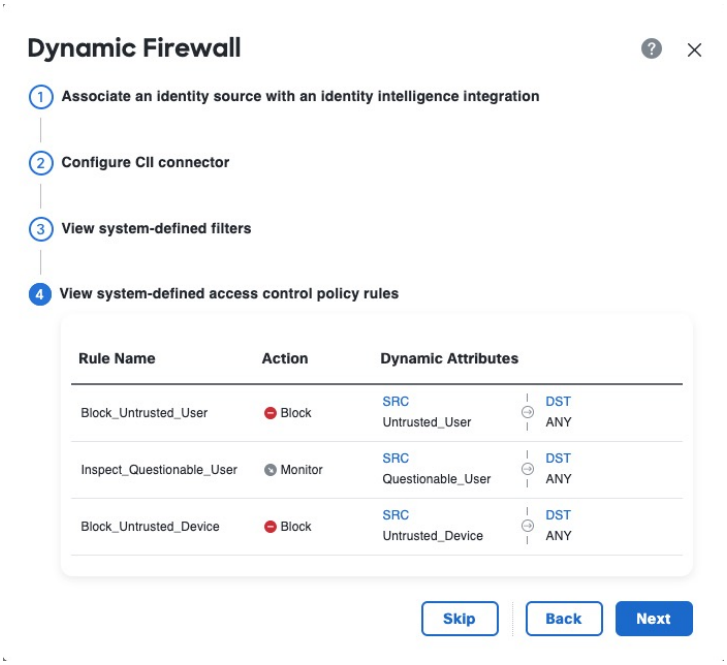
Before you begin

See View system-defined filters, on page 2110.

Procedure

Step 1 View the system-created access control rules.

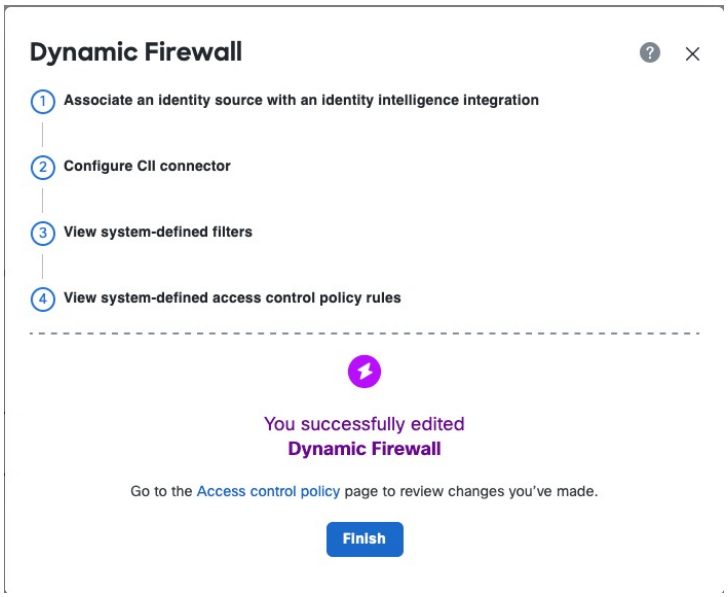
The following figure shows an example.



Step 2 Choose one of these options:

- Click **Skip** to skip creating these access control rules. You can create your own anytime.
- Click **Next** to create an access control policy named Dynamic Firewall Policy with the rules shown in the preceding figure.
- Click **Back** to return to system-created filters.

Step 3 After you click **Next**, if you created access control rules successfully, the following page is displayed:



Edit the user exclusion list

Specify users provided by Identity Intelligence as always being trusted.

You can instruct Identity Intelligence to treat specific users as trusted.

Before you begin

Configure the dynamic firewall as discussed in Create a dynamic firewall instance, on page 2107.

Procedure

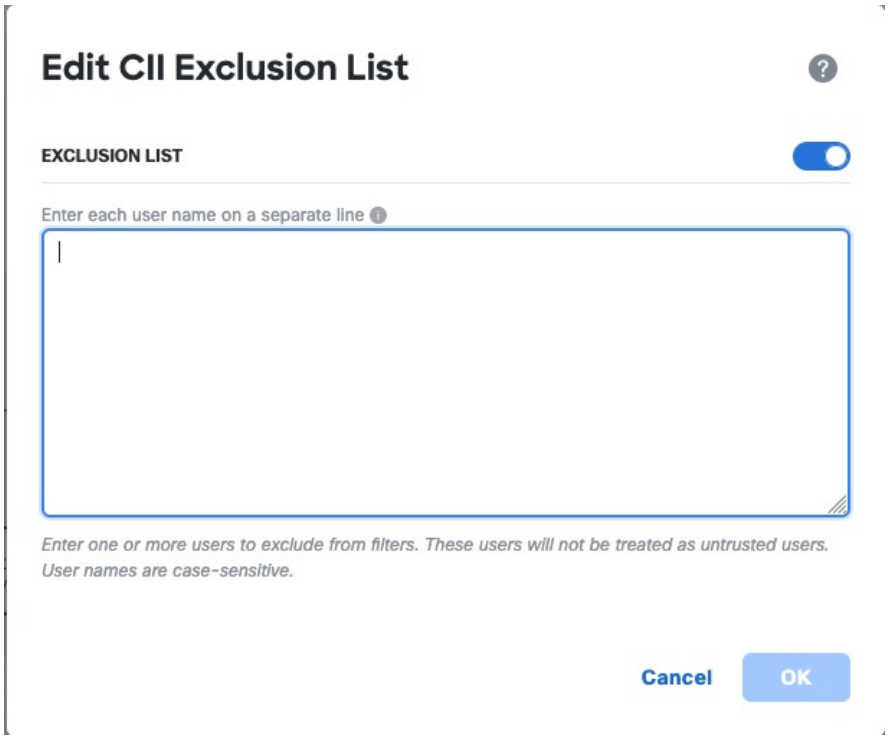
Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Click next to the name of the identity source.

Step 4 Click **Edit CII Exclusion List**.

The following dialog box is displayed.



Step 5 In the provided field, enter one user name in `username@domain.com` format on a line, press Enter, and enter another user name.

Each user name is considered as trusted by Identity Intelligence.

View and edit the system-created access control policy

Customize the system-created access control policy by adding devices, changing rules, reordering rules, or deleting rules to meet your specific network security requirements.

This topic discusses how you can edit the system-created access control rules and policy. Initially, the policy isn't associated with any devices but if you want to use it you can add devices, change rules, reorder rules, or delete rules.

Before you begin

Complete the tasks described in View system-defined access control rules, on page 2111.

Follow these steps to view and edit the system-created access control policy:

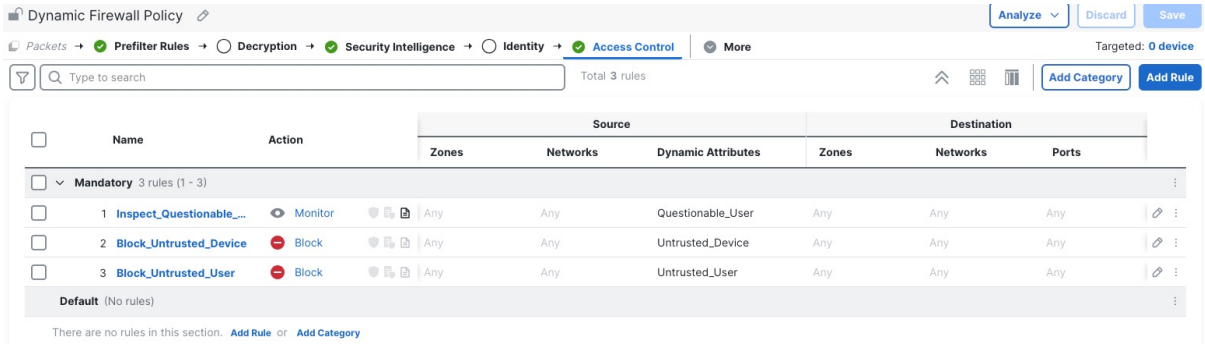
Procedure

Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Policies** > **Access Control heading** > **Access Control**.

Step 3 Click **Edit** ( ) next to the policy named Dynamic Firewall Policy (or similar).

The following figure shows a sample access control policy.



Note that in this access control policy, only the rule set to monitor questionable users logs anything. To adjust the logging settings, see Logging settings for access control policies, on page 1584.

Step 4 Do any of the following:

- Target the access control policy at devices: Assign access control policy to devices, on page 1583.
- Edit the policy, including adding logging: Manage access control policies, on page 1575.
- Edit access control rules: Access control rule management, on page 1630.
- Set advanced policy options: Configure advanced settings for the access control policy, on page 2170.
- Associate other policies with this access control policy: Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Create dynamic attributes filters

Create dynamic attributes filters that can be used as dynamic objects in access control policies to restrict access based on specific criteria such as group membership.

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, you could restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 2100.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new filter: click **Add** ( ).

- Edit or delete a filter: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

- **Name**: Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
- **Connector**: From the list, click the name of a connector to use.
- **Query**: Click Add .

Step 5 To add a query, enter the following information.

- **Key**: Click a key from the list. Keys are fetched from the connector.
- **Operation**: Click one of the following:
  - **Equals** to exactly match the key to the value.
  - **Contains** to match the key to the value if any part of the value matches.
- **Values**: Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

When you're finished, click **Save**.

What to do next

Verify the dynamic object in the Secure Firewall Management Center .

1. Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.
2. Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

Disable the dynamic attributes connector

Disable the Dynamic Attributes Connector when you no longer wish to collect dynamic objects from cloud sources.

If you no longer wish to collect dynamic objects from cloud sources, you can disable the Dynamic Attributes Connector in the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integration** > **Dynamic Attributes Connector**.

Step 3 Slide to **Disabled**.

Troubleshoot the Dynamic Attributes Connector

Troubleshoot using the Secure Firewall Management Center

Generate troubleshoot files to diagnose and resolve issues with the Secure Firewall Management Center.

This task discusses how to generate troubleshoot files for the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **System** (⚙) > **Health** > **Monitor**.

Step 3 In the left pane, click **Firewall Management Center**.

Step 4 At the top, click **System & Troubleshooting Details**.

Step 5 Click **Generate Troubleshooting Files**.

Step 6 Provide the files to Cisco TAC or to your Beta coordinator.

Recommendation: security requirements for network deployment

Install the dynamic attributes connector on a protected internal network. Although the dynamic attributes connector is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it.

If the dynamic attributes connector and the Secure Firewall Management Center reside on the same network, you can connect the Secure Firewall Management Center to the same protected internal network as the dynamic attributes connector.

Take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with. Regardless of how you deploy your appliances, inter-system communication is encrypted. However, you must still protect against distributed denial of service (DDoS) or adversary-in-the-middle attacks.

Internet access requirements

By default, the dynamic attributes connector is configured to communicate with the Firepower System over the internet using HTTPS on port 443/tcp (HTTPS). If you do not want the dynamic attributes connector to have direct access to the internet, you can configure a proxy server.

This information details the URLs the dynamic attributes connector use to communicate with the Secure Firewall Management Center and with external servers.

Table 122: Dynamic Attributes Connector access requirements

URL	Reason
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	Authentication
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET and POST dynamic objects
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	Add mappings
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id*** /object/dynamicobjects/***object-id***/mappings?action=remove**	Remove mappings

Table 123: Dynamic Attributes Connector vCenter access requirements

URL	Reason
https://*vcenter-ip***/rest/com/vmware/cis/session**	Authentication
https://*vcenter-ip***/rest/vcenter/VM**	GET VM information
https://*NSX-ip***/api/v1/fabric/virtual-machines/***VM-id***	GET NSX-T tag associated with the virtual machine

Migration from DockerHub to Amazon ECR

Docker images for the Dynamic Attributes Connector are being migrated from Docker Hub to Amazon Elastic Container Registry (Amazon ECR).

To use the new field packages, you must allow access through your firewall or proxy to all of the following URLs:

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

  For more information about Amazon Cloudfront URLs, see EKS Anywhere documentation.

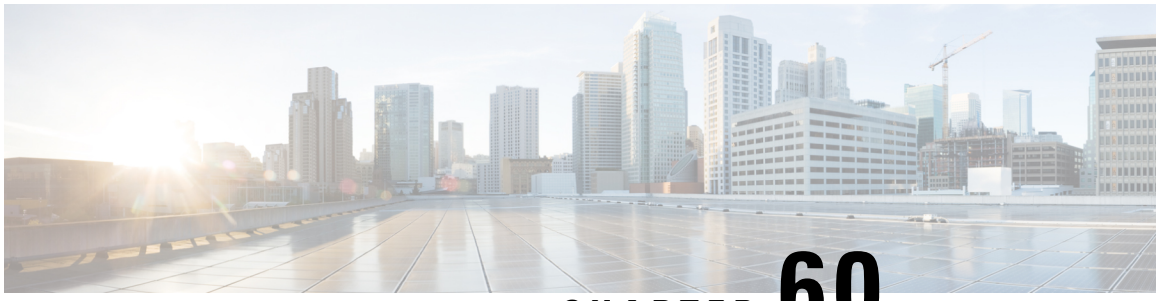
Dynamic Attributes Connector Azure access requirements

The dynamic attributes connector calls built-in SDK methods to GET instance information. These methods internally call https://login.microsoft.com (for authentication) and https://management.azure.com (to GET instance information).

History for the dynamic attributes connector

This document provides the history of features for the dynamic attributes connector, including feature introductions and modifications across different product versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dynamic Attributes Connector	7.4.0	7.4.0	This feature is introduced. The Dynamic Attributes Connector is now included in the Secure Firewall Management Center. You can use the dynamic attributes connector to get IP addresses from cloud-based platforms such as Microsoft Azure in access control rules without having to deploy to managed devices. More information: • The dynamic attributes connector included with this product: About the dynamic attributes connector , on page 2061 • The standalone dynamic attributes connector: *Cisco Secure Dynamic Attributes Connector Configuration Guide* New/modified screen: **Integration** > **Dynamic Attributes Connector**



CHAPTER 60

Threat Intelligence Director

The topics in this chapter describe how to configure and use Threat Intelligence Director.

- Secure Firewall Threat Intelligence Director, on page 2121
- Requirements and prerequisites for threat intelligence director, on page 2124
- Set up Threat Intelligence Director, on page 2126
- Analyze Threat Intelligence Director incident and observation data , on page 2136
- View and change Threat Intelligence Director configurations , on page 2148
- Troubleshoot Threat Intelligence Director, on page 2164
- History for Threat Intelligence Director, on page 2166

Secure Firewall Threat Intelligence Director

Secure Firewall Threat Intelligence Director is a threat defense feature that

- operationalizes threat intelligence data to help aggregate intelligence data and configure defensive actions,
- analyzes threats in your environment, and
- supplements other Secure Firewall functionality, offering an additional line of defense against threats.

Threat intelligence data flow and components

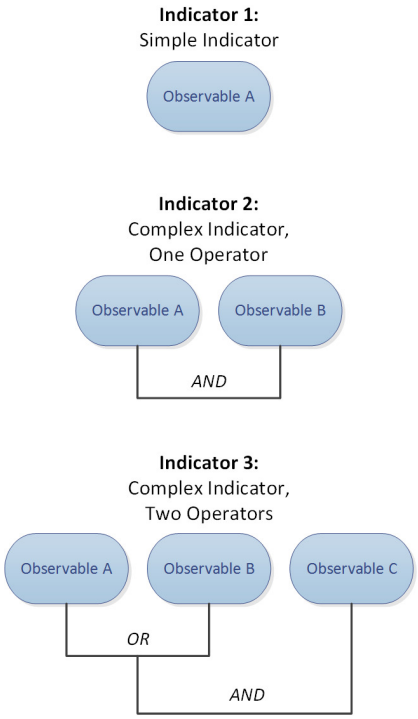
When configured on your hosting platform, Threat Intelligence Director ingests data from threat intelligence *sources* and publishes the data to all configured managed devices (*elements*.) For more information about the hosting platforms and elements supported in this release, refer to Platform, element, and license requirements, on page 2124.

Sources contain *indicators*, which contain *observables*. An indicator conveys all characteristics associated with a threat. Individual observables represent specific characteristics associated with the threat, such as an SHA-256 value.

- **Simple indicators**: Contain a single observable
- **Complex indicators**: Contain two or more observables

Observables and the AND/OR operators between them form an indicator's *pattern*, as illustrated in this example.

Figure 416: Example: indicator patterns



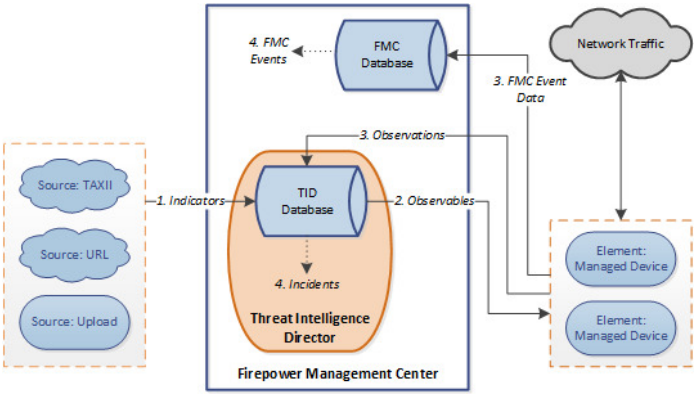
After the observables are published to the elements, the elements monitor traffic and report *observations* to the Firewall Management Center when the system identifies observables in traffic.

The Firewall Management Center collects observations from all elements, evaluates the observations against Threat Intelligence Director indicators, and generates or updates *incidents* associated with the observable's parent indicator(s).

An incident is *fully realized* when an indicator's pattern is fulfilled. An incident is *partially realized* if traffic matches one or more observables in the indicator but not the entire pattern. For more information, see Observation and incident generation, on page 2136.

This diagram shows data flow in a sample system configuration.

Figure 417: Firewall Management Center Data Flow



When a Threat Intelligence Director incident is fully or partially realized, the system takes the configured *action* (monitor, block, partially block, or no action). For details, refer to Factors that affect the action taken, on page 2144.

Threat Intelligence Director and Security Intelligence

Security Intelligence is a threat blocking feature that uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domains as part of your access control policy.

Security Intelligence uniquely provides access to industry-leading threat intelligence from Talos Intelligence Group. For more information on Security Intelligence, refer to Security intelligence, on page 1595.

Threat Intelligence Director enhances the system's ability to block connections based on security intelligence from third-party sources as follows:

- **Threat Intelligence Director supports additional traffic filtering criteria**—Security Intelligence allows you to filter traffic based on IP address, URL, and (if DNS policy is enabled) domain name. Threat Intelligence Director also supports filtering by these criteria and adds support for filtering on SHA-256 hash values.
- **Threat Intelligence Director supports additional intelligence ingestion methods**—With both Security Intelligence and Threat Intelligence Director, you can import threat intelligence into the system by either manually uploading flat files or configuring the system to retrieve flat files from a third-party host. Threat Intelligence Director provides increased flexibility in managing those flat files. In addition, Threat Intelligence Director can retrieve and ingest intelligence provided in Structured Threat Information eXpression (STIX™) format.
- **Threat Intelligence Director provides granular control of filtering actions**—With Security Intelligence, you can specify filtering criteria by network, URL, or DNS object. Security Intelligence objects, especially lists and feeds, can contain multiple IP addresses, URLs, or DNS domain names, but you can only block or not block based on entire objects, not on individual components of an object. With Threat Intelligence Director, you can configure filtering actions for individual criteria (that is, simple indicators or individual observables).
- **Threat Intelligence Director configuration changes do not require redeployment**—After you modify Security Intelligence settings in the access control policy, you must redeploy the changed configuration to managed devices. With Threat Intelligence Director, after initial deployment of the access control policy to the managed devices, you can configure sources, indicators, and observables without redeploying, and the system automatically publishes new Threat Intelligence Director data to the elements.

For information about what the system does when either Security Intelligence or Threat Intelligence Director could handle a particular incident, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

Performance impact of Threat Intelligence Director

This reference provides information about the performance impacts that may occur when using Threat Intelligence Director with your security infrastructure.

Secure Firewall Management Center

In some cases, you may notice the following:

- The system may experience minor performance issues while ingesting particularly large STIX sources, and ingestion may take longer than expected to finish.
- The system may take up to 15 minutes to publish new or modified Threat Intelligence Director data down to elements.

Managed device

There is no exceptional performance impact. Threat Intelligence Director impacts performance identically to the Secure Firewall Management Center Security Intelligence feature.

Requirements and prerequisites for threat intelligence director

Model support

Any

Supported domains

Any

User roles

Admin

Threat Intelligence Director User

Additional requirements

The following topics explain additional requirements for using Threat Intelligence Director.

Platform, element, and license requirements

This reference provides the specific requirements for hosting platforms, managed elements, and licensing necessary to deploy and operate Threat Intelligence Director in your environment.

Hosting platforms

You can host Threat Intelligence Director on physical and virtual Secure Firewall Management Centers

- running version 6.2.2 or later,
- configured with a minimum of 15 GB of memory, and
- configured with REST API access enabled. See *Enabling REST API Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

Elements

You can use any Secure Firewall Management Center-managed device as a Threat Intelligence Director element if the device is running version 6.2.2 or later.

Licensing

To configure the file policies for SHA-256 observable publishing, you need licensed devices with specific requirements:

- For smart licensed devices:
  - IPS License: For IPv4, IPv6, URL, and DNS detection and observables
  - Malware Defense License: For SHA-256 detection and observables
- For classic licensed devices:
  - Protect License: For IPv4, IPv6, URL, and DNS detection and observables
  - Malware License: For SHA-256 detection and observables

For more information, refer to Configure policies to support Threat Intelligence Director, on page 2127 and the *Licenses* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

Source requirements

This reference provides the specific requirements for different source types including STIX files and flat files that can be used for threat intelligence indicators.

STIX

Files must be STIX Version 1.0, 1.1, 1.1.1, or 1.2 and adhere to the guidelines in the STIX documentation: http://stixproject.github.io/documentation/suggested-practices/.

STIX files can include complex indicators.

The maximum size for a STIX file is 40 MB when configured via URL download or file upload. If you have STIX files larger than this, we recommend using a TAXII server.

Flat file

Files must be ASCII text files with one observable value on each line.

Flat files include only simple indicators, with one observable for each indicator.

Flat files can be up to 500 MB.

Threat Intelligence Director does **not** support:

- Delimiter characters separating observable values, for example, `observable,` are invalid.
- Enclosing characters around observable values, for example, `"observable"`, are invalid.

Each file should contain only one type of content:

- `SHA-256`—SHA-256 hash values.
- `Domain`—domain names as defined in RFC 1035.
- `URL`—URLs as defined in RFC 1738.

Note Threat Intelligence Director normalizes any URLs that contain port, protocol, or authentication information, and uses the normalized version when detecting indicators. For example, Threat Intelligence Director normalizes any of these URLs:

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

as:

```
example.com/index.htm
```

Or, for example, Threat Intelligence Director normalizes this URL:

```
http://abc@example.com:8080/index.htm
```

as

```
abc@example.com/index.htm/
```

- `IPv4`—IPv4 addresses as defined in RFC 791.

  Threat Intelligence Director does not accept CIDR blocks.

- `IPv6`—IPv6 addresses as defined in RFC 4291.

  Threat Intelligence Director does not accept prefix lengths.

Source content limitations

The system ingests and matches on only the first 1,000 characters of a URL observable.

Set up Threat Intelligence Director

This task establishes a fully functional Threat Intelligence Director deployment by ensuring proper installation requirements, policy configuration, and intelligence source integration.

Setting up Threat Intelligence Director involves configuring multiple components in a specific sequence to ensure optimal threat intelligence capabilities.

Note If you encounter an issue during Threat Intelligence Director configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 2164.

Procedure

Step 1 Ensure that your installation meets the requirements for running Threat Intelligence Director.

See Platform, element, and license requirements, on page 2124

Step 2 For each managed device, configure the policies required to support Threat Intelligence Director and deploy those policies to the devices.

See Configure policies to support Threat Intelligence Director, on page 2127.

You can configure elements before or after you ingest intelligence data sources.

Step 3 Configure the intelligence sources that you want Threat Intelligence Director to ingest.

See Source requirements, on page 2125 and the topics under Options for ingesting data sources, on page 2128.

Step 4 Publish data to the elements if you have not yet done so.

See Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

What to do next

- Include Threat Intelligence Director in your regularly scheduled backups. See About backing up and restoring Threat Intelligence Director data, on page 2135.

  If your Secure Firewall Management Center deployment is a high availability configuration, see also *Firewall Management Center High Availability Disaster Recovery* in the *Cisco Secure Firewall Management Center Administration Guide*.

- (Optional) Grant administrative access to Threat Intelligence Director functionality as desired. See User roles with Threat Intelligence Director access, on page 2135 and the *Users* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

- As needed during operation, fine-tune your configuration. For example, add observables that produce false positive incidents to the Do Not Block list. See View and change Threat Intelligence Director configurations , on page 2148.

Configure policies to support Threat Intelligence Director

This task configures access control policies to publish Threat Intelligence Director data from the Firewall Management Center to your managed devices and maximize observation and event generation.

You must configure access control policies to publish Threat Intelligence Director data from the Firewall Management Center to your managed devices (elements). In addition, we recommend that you configure your access control policies to maximize observation and Firewall Management Center event generation.

For each managed device that you want to support Threat Intelligence Director, perform these steps to configure the associated access control policy.

Elements that are configured to use Threat Intelligence Director after data has been published will automatically receive all currently-published observables.

Procedure

Step 1 Verify that the **Enable Threat Intelligence Director** check box is checked in **General Settings** of the access control policy. To navigate to **General Settings**, choose **Policies** > **Access Control heading** > **Access Control**, and click **Edit** > **More** > **Advanced Settings**. This option is enabled by default.

For more information, see General settings, on page 2172.

Step 2 Add rules that allow (rather than trust) connections to the access control policy if they are not already present. Threat Intelligence Director requires that the access control policy specify at least one rule.

Because Threat Intelligence Director depends on inspection, ensure that you allow traffic, rather than trust it, because the purpose of trusting traffic is to bypass inspection. For more information, see Creating a basic access control policy, on page 1575.

Step 3 If you choose **Intrusion Prevention** as the default action for the access control policy and you want to decrypt traffic for TID detection, associate a decryption policy with the access control policy; see Associate prefilter, decryption, and identity policies with an access control, on page 1585.

Step 4 If you want **SHA-256** observables to generate observations and Secure Firewall Management Center events:

a) Create a file policy containing one or more **Malware Cloud Lookup** or **Block Malware** file rules.

For more information, see Configure file policies, on page 2023.

b) Associate this file policy with one or more rules in the access control policy.

Step 5 If you want **IPv4**, **IPv6**, **URL**, or **Domain Name** observations to generate connection and security intelligence events, enable connection and security intelligence logging in the access control policy:

a) In access control rules where you invoked a file policy, enable **Log at End of Connection** and **File Events: Log Files**, if not already enabled.

For more information, see *Logging Connections with Access Control Rules* in the *Cisco Secure Firewall Management Center Administration Guide*.

b) Verify that default logging (**DNS Policy**, **Networks**, and **URLs**) is enabled in your Security Intelligence settings.

For more information, see *Logging Connections with Security Intelligence* in the *Cisco Secure Firewall Management Center Administration Guide*.

Step 6 Deploy configuration changes; see Deploy configuration changes, on page 135.

What to do next

Complete the remaining action items in Set up Threat Intelligence Director, on page 2126.

Options for ingesting data sources

Choose a configuration option based on the data type and delivery mechanism you want to use.

For more information about these data types, refer to Source requirements, on page 2125.

Table 124: Options for ingesting data sources

Data Type	Ingestion Options
STIX	• Ingest STIX feeds from a TAXII server. Refer to Fetch TAXII feeds to use as sources, on page 2129 • Download STIX data from a URL. Refer to Fetch sources from a URL, on page 2130 • Upload a STIX file. Refer to Upload a local file to use as a source, on page 2132
Flat file	• Download data from a URL. Refer to Fetch sources from a URL, on page 2130 • Upload a flat file. Refer to Upload a local file to use as a source, on page 2132

Fetch TAXII feeds to use as sources

This task establishes TAXII feeds as threat intelligence sources to automatically retrieve STIX data for threat detection and analysis.

TAXII feeds provide structured threat intelligence data that can enhance your security posture by automatically updating threat indicators. If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 2164.

Before you begin

Before configuring TAXII feeds, ensure your source meets the requirements in Source requirements, on page 2125.

Follow these steps to fetch TAXII feeds to use as sources:

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources**.

Step 2 Click **Add** (+).

Step 3 Choose `TAXII` as the **Delivery** method for the source.

Step 4 Enter information.

- If the host server requires an encrypted connection, configure the **SSL Settings** as described in Configure TLS/SSL settings for a Threat Intelligence Director source, on page 2133.
- You cannot change the **Action** selection for TAXII sources.

`Block` is not an **Action** option for TAXII sources, as STIX data can contain complex indicators, which the system cannot block. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.

However, after ingestion, you can block individual observables and simple indicators obtained from the source. For more information, see Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.

- It may take some time for the list of feeds to load.
- The **Update Every** interval specifies the frequency that Threat Intelligence Director retrieves updates from the TAXII source.

  Set an update frequency that makes sense for how often the data source is updated. For example, if the source is updated 3 times per day, set your update interval to 1440/3 or 480 minutes to regularly capture the latest data.
- After the number of days you specify for **TTL**, Threat Intelligence Director deletes:
  - all indicators for the source that are not included in subsequent source updates.
  - all observables not referenced by a surviving indicator.

Note If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

Step 5 If you want to immediately begin publishing to elements, confirm that the **PUBLISH Slider** ( ) is enabled.

When this option is enabled, the system automatically publishes the initial source data and any subsequent changes.

For details, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Step 6 Click **Save**.

What to do next

- TAXII feeds can contain a lot of data. It may take some time for the system to ingest all of the data. To view ingestion status, refresh the Sources page.
- If you see an error for this source, hover over status for details.
- If you are doing initial Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 2126.

Fetch sources from a URL

Configure a URL source if you want Threat Intelligence Director to fetch files from a host.

If you encounter an issue during TID configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 2164.

Before you begin

Follow these steps to fetch sources from a URL:

Procedure

Step 1 Make sure your source meets the requirements in Source requirements, on page 2125

Step 2 Choose **Integration** > **Intelligence** > **Sources**.

Step 3 Click **Add** (+).

Step 4 Choose **URL** as the **Delivery** method for the source.

Step 5 Complete the form.

- If you are ingesting a flat file, choose a **Type** that describes the data contained within the source.
- If the host server requires an encrypted connection, configure the **SSL Settings** as described in Configure TLS/SSL settings for a Threat Intelligence Director source, on page 2133.
- For Name: To simplify sorting and handling of incidents based on Threat Intelligence Director indicators, use a consistent naming scheme across sources. For example, <source>-<type>.

  Including the source name simplifies returning to the source for further information or feedback.

  Be sure to enter the name consistently. For example, for a source with IPv4 addresses, you might always use IPV4 (not IPv4 or ipv4 or IP_v4 or IP_V4 or IP-v4 or IP-v4, IP-V4, etc.)
- If you are ingesting a STIX file, **Block** is not an **Action** option, as STIX data can contain complex indicators, which the system cannot block. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.

  However, after ingestion, you can block individual observables and simple indicators obtained from the source. For more information, see Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.
- Set an update frequency that makes sense for how often the data source is updated. For example, if the source is updated three times per day, set your update interval to 1440/3 or 480 minutes to regularly capture the latest data.
- After the number of days you specify for the **TTL** interval, Threat Intelligence Director deletes:
  - all indicators from the source that are not included in subsequent source updates.
  - all observables not referenced by a surviving indicator.

Note If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

Step 6 If you want to immediately begin publishing to elements, confirm that the **Publish Slider** () is enabled.

When this option is enabled, the system automatically publishes the initial source data and any subsequent changes.

For details, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Step 7 Click **Save**.

What to do next

- To view ingestion status, refresh the Sources page. If you see an error, hover over status for details.
- If you are doing initial Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 2126.

Upload a local file to use as a source

This task allows you to manually upload a local STIX or flat file to create threat intelligence indicators in Threat Intelligence Director.

Use this procedure for a one-time manual upload of a local file.

When ingesting a STIX file, Threat Intelligence Director creates a simple or complex indicator from the contents of the STIX file.

When ingesting a flat file, Threat Intelligence Director creates a simple indicator for each observable value in the file.

If you encounter an issue during Threat Intelligence Director configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 2164

Procedure

Step 1 Make sure your file meets the requirements in Source requirements, on page 2125

Step 2 Choose **Integration** > **Intelligence** > **Sources**.

Step 3 Click **Add** ().

Step 4 Choose **Upload** as the **Delivery** method for the source.

Step 5 Complete the form.

- If you are uploading a flat file, choose a **Type** that describes the data contained within the source.
- For Name: To simplify sorting and handling of incidents based on Threat Intelligence Director indicators, use a consistent naming scheme across sources. For example, <source>-<type>.

  Including the source name simplifies returning to the source for further information or feedback.

  Be sure to enter the name consistently. For example, for a source with IPv4 addresses, you might always use IPV4 (not IPv4 or ipv4 or IP_v4 or IP_V4 or IP-v4 or IP-v4, IP-V4, etc.)

- If you are uploading a STIX file, **Block** is not an **Action** option, because STIX data can contain complex indicators. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.

  However, you can block a simple indicator at the indicator or observable level. For more information, see Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.

- After the number of days you specify for the **TTL** interval, Threat Intelligence Director deletes:
  - all of the source's indicators that are not included in a subsequent upload.
  - all observables not referenced by a surviving indicator.

Note If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

Step 6 If you want to immediately begin publishing to elements, confirm that the **Publish Slider** ( ) is enabled.

If you do not publish the source at ingestion, you cannot publish all source indicators at once later; instead, you must publish each observable individually. See Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Step 7 Click **Save**.

What to do next

- To view ingestion status, refresh the Sources page. If you see an error, hover over status for details.
- If you are doing initial Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 2126.

Handling of duplicate indicators

If a single indicator is included in multiple sources:

Each instance of the indicator generates an incident, so one encounter with a particular threat may generate multiple incidents.

To avoid future duplicate incidents, pause publishing of all but one of the duplicated indicators. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Configure TLS/SSL settings for a Threat Intelligence Director source

Configure TLS/SSL settings to establish secure encrypted connections with host servers that require certificate-based authentication.

Configure **SSL Settings** if the host server requires an encrypted connection.

Before you begin

- Configure a `TAXII` or `URL` source, as described in Fetch TAXII feeds to use as sources, on page 2129 or Fetch sources from a URL, on page 2130.

Follow these steps to configure TLS/SSL settings for a Threat Intelligence Director source:

Procedure

Step 1 In the **Edit Source** dialog box, expand the **SSL Settings** section.

Step 2 If your server certificate is self-signed:

a) Enable **Self-Signed CERTIFICATE**.

b) Choose a **SSL Hostname Verification** method.

- `Strict`—Threat Intelligence Director requires the source **URL** to match the hostname provided in the server certificate.

  If the hostname includes a wildcard, TID cannot match more than one subdomain.

- `Browser Compatible`—Threat Intelligence Director requires the source **URL** to match the hostname provided in the server certificate.

  If the hostname includes a wildcard, TID matches all subdomains.

- `Allow All`—Threat Intelligence Director does not require the source **URL** to match the hostname provided in the server certificate.

For example, if `subdomain1.subdomain2.cisco.com` is your source **URL** and `*.cisco.com` is the hostname provided in the server certificate:

- `Strict` hostname verification fails.
- `Browser Compatible` hostname verification succeeds.
- `Allow All` hostname verification ignores the hostname values completely.

c) For **Server CERTIFICATE**:

- If you have access to the PEM-encoded self-signed server certificate, open the certificate in a text editor and copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Enter this entire string into the field.
- If you do not have access to the self-signed server certificate, leave the field blank. After you save the source, Threat Intelligence Director retrieves the certificate from the server.

Step 3 If your server requires a user certificate:

a) Enter a **User certificate**:

Open the PEM-encoded certificate in a text editor and copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Enter this entire string into the field.

b) Enter a **User PRIVATE KEY**:

Open the PRIVATE KEY file in a text editor and copy the entire block of text, including the `BEGIN RSA PRIVATE KEY` and `END RSA PRIVATE KEY` lines. Enter this entire string into the field.

What to do next

- Take note of the certificate's expiration date. You may want to set a calendar reminder to enter a new server certificate after the current certificate expires.
- Continue configuring the source:
  - Fetch TAXII feeds to use as sources, on page 2129
  - Fetch sources from a URL, on page 2130

User roles with Threat Intelligence Director access

You can use Firewall Management Center user accounts to access the Threat Intelligence Director menus and pages.

The user roles that can access Threat Intelligence Director menus and pages are:

- Accounts with the **Admin** or **Threat Intelligence Director User** user role.
- Accounts with a custom user role containing the **Intelligence** permission.

In addition, you can use Firewall Management Center user accounts with the **Admin**, **Access Admin**, or **Network Admin** user role to enable or disable Threat Intelligence Director in your access control policies.

For more information about user accounts, refer to the *Users for the Firewall Management Center* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

About backing up and restoring Threat Intelligence Director data

You can use the Firewall Management Center to back up and restore all of the data needed for Threat Intelligence Director: Element data, security intelligence events, connection events, Threat Intelligence Director configurations, and Threat Intelligence Director data. For more information, refer to the *Backup/Restore* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

Note If you host Threat Intelligence Director on the active Firewall Management Center in a high availability configuration, the system does not synchronize Threat Intelligence Director configurations and Threat Intelligence Director data to the standby Firewall Management Center. We recommend performing regular backups of Threat Intelligence Director data on your active Firewall Management Center so that you can restore the data after failover.

Before you attempt to restore the Threat Intelligence Director data on the active Firewall Management Center, pause synchronization on the active peer. For more information, see *Pausing Communication Between Paired Firepower Management Centers* in the *Cisco Secure Firewall Management Center Administration Guide*.

Table 125: Threat Intelligence Director-Related Backup and Restore File Contents

Threat Intelligence Director-Related File Contents	Backup Selection	Restore Selection
Element data	**Back Up Configuration**	**Restore Configuration Data**
Secure Firewall Management Center event data	**Back Up Events**	**Restore Event Data**
Threat Intelligence Director configurations and Threat Intelligence Director data	**Back Up Threat Intelligence Director**	**Restore Threat Intelligence Director Data**

Analyze Threat Intelligence Director incident and observation data

To analyze incident and observation data generated by Threat Intelligence Director elements, use the Incidents table and Incident Details page.

Observation and incident generation

Observation and incident generation is a threat detection process that

- generates an incident when the first observable for an indicator is seen in traffic,
- fully realizes simple indicators after a single observation,
- partially realizes complex indicators until additional observations fulfill their pattern, and
- triggers new incidents for subsequent observations after an incident is fully realized.

How observation and incident generation works

Threat Intelligence Director generates an incident when the first observable for an indicator is seen in traffic. Simple indicators are fully realized after a single observation. Complex indicators are partially realized until one or more additional observations fulfill their pattern. Complex indicators need not necessarily be fulfilled during a single transaction; each observable can be fulfilled separately over time by different transactions.

Note When evaluating an indicator's pattern, Threat Intelligence Director ignores unsupported and invalid objects and observables on the Do Not Block list.

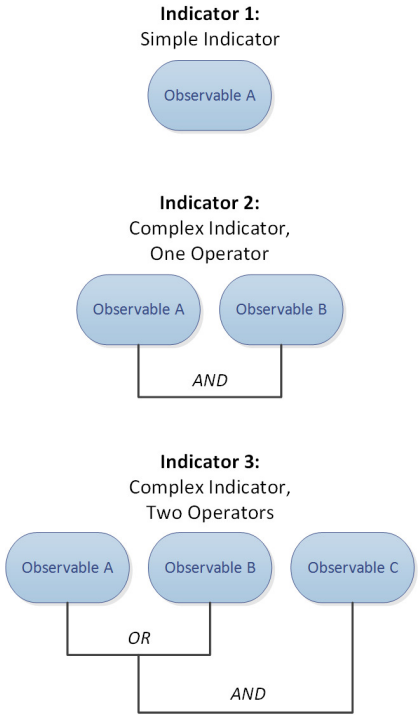
After an incident is fully realized, subsequent observations trigger new incidents.

If a particular indicator exists in multiple sources, you may see duplicate incidents. For more information, see Troubleshoot Threat Intelligence Director, on page 2164.

Incidents are generated only by actual traffic. If there is an observable for URL B, and a user visits URL A which displays a link to URL B, no incident occurs unless the user clicks the URL B link.

Indicator pattern processing example

Figure 418: Indicator patterns



If Threat Intelligence Director ingested the observables from the example above and the observables were seen in order, incident generation would proceed as follows:

1. When the system identifies Observable A in traffic, Threat Intelligence Director:
   - Generates a fully-realized incident for Indicator 1.
   - Generates partially-realized incidents for Indicator 2 and Indicator 3.
2. When the system identifies Observable B in traffic, Threat Intelligence Director:
   - Updates the incident to fully-realized for Indicator 2, since the pattern was fulfilled.
   - Updates the incident to partially-realized for Indicator 3.
3. When the system identifies Observable C in traffic, Threat Intelligence Director:
   - Updates the incident to fully-realized for Indicator 3, since the pattern was fulfilled.
4. When the system identifies Observable A for a second time, Threat Intelligence Director:
   - Generates a new fully-realized incident for Indicator 1.
   - Generates new partially-realized incidents for Indicator 2 and Indicator 3.

View and manage incidents

This task allows you to view and manage incidents to monitor security threats and track investigation progress.

The Incidents page displays summary information for up to 1.1 million of the most recent Threat Intelligence Director incidents. Refer to Incident summary information, on page 2139.

Before you begin

- Configure the feature as described in Set up Threat Intelligence Director, on page 2126.
- Understand observation and incident generation, as described in Observation and incident generation, on page 2136.

Follow these steps to view and manage incidents:

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Incidents**.

Step 2 View your incidents:

- Click **Filter** () to add one or more filters. The default filter duration is six hours. For more information, refer to Filter Threat Intelligence Director data in table views, on page 2156.
- To view the date and time an incident was last updated by Threat Intelligence Director, hover the cursor over the value in the **Last Updated** column.
- To view more information about the indicator associated with the incident, click the text in the **Indicator Name** column. Refer to View and manage indicators, on page 2152.

Step 3 View additional details by clicking a value in the **Incident ID** column.

For an explanation of the details you see, refer to Incident details, on page 2139.

- To view indicator details, click an indicator value (for example, an IP address or SHA-256 value) under the **Indicator** heading in the lower section of the window.
- To view observation details, click the arrow to the left of an observation immediately under the **Observations** heading.
- To view this incident on the Security Intelligence Events page, click the **Events** link in the observation details section.

Step 4 (Optional) Enter descriptive information on the incident details page:

To maximize consistency and usefulness of the options listed, plan ahead and document your naming conventions, category choices, and confidence level criteria.

- Enter any value you like in the following fields: **Name**, **Description**, and **Category**.
- Click a rating level for **Confidence**.

- Indicate the status of your investigation into the incident by choosing a value from the drop-down list in the **Status** field.

Incident summary information

The Incidents page displays summary information for all Threat Intelligence Director incidents.

Table 126: Incident summary information

Field	Description
Last Updated	The number of days since either the system or a user last updated the incident. To view the date and time of the update, hover the cursor over the value in this column.
Incident ID	The unique identifier for the incident. This ID has the format: `<type>-<date>-<number>` • `<type>`—The type of indicator or observable involved in the incident. For simple indicators, this value indicates the observable type: `IP` (IPv4 or IPv6), `URL` (URL), `DOM` (domain), or `SHA` (SHA-256). For complex indicators, this value is `COM`. • `<date>`—The date (*yyyymmdd*) on which the incident was created. • `<number>`—The daily incident number, that is, a number specifying where the incident occurs in the daily sequence of incidents. Note that this sequence starts at 0. For example, `DOM-20170828-10` is the 11th incident created on that day. Next to the identifier, the system displays an icon that indicates whether the incident is **Partially Realized** or **Fully Realized**. For more information, refer to Observation and incident generation, on page 2136.
Indicator Name	The name of the indicator involved in the incident. To view additional information about the indicator, click the value in this column. Refer to View and manage indicators, on page 2152.
Type	The type of indicator involved in the incident. • Indicators that contain a single observable display the data type (`URL`, `SHA-256`, etc.) • Indicators that contain two or more observables display as `Complex`.
Action Taken	The action taken by the system in relation to the incident. For more information, refer to Incident details, on page 2139.
Status	The status of your investigation into the incident. For more information, refer to Incident details, on page 2139.
Delete ( )	Clicking this icon permanently deletes the incident.

Incident details

The Incident Details window displays information about a single Threat Intelligence Director incident. This window is divided into two sections:

• Incident details: Basic information, on page 2140
• Incident details: Indicators and observations, on page 2141

Incident details: Basic information

The upper section of the Incident Details window provides the information described below.

Table 127: Basic incident information fields

Field	Description
Partially-Realized *IncidentID* or **Fully-Realized** *IncidentID*	An icon indicating the status of the incident (partially-realized or fully-realized), as well as the unique identifier for the incident. **Note** When determining the status of an incident, Threat Intelligence Director ignores unsupported and invalid observables and observables on the Do Not Block list.
Opened	The date and time the incident was last updated.
Name	A custom, optional incident name that you enter manually. Tip: If there is information from the source in the Description field (in the bottom part of the window), use information from that field to name the incident.
Description	A custom, optional incident description that you enter manually. Tip: If there is information from the source in the Description field (in the bottom part of the window), use information from that field to describe the incident.
Observations	The number of observations within the incident.
Confidence	An optional rating that you can manually select to indicate the relative importance of the incident.
Action Taken	The action taken by the system: `Monitored`, `Blocked`, or `Partially Blocked`. `Partially Blocked` indicates that the incident contained both `Monitored` and `Blocked` observations. **Note** The **Action Taken** indicates the action taken by the system, not necessarily the action selected in Threat Intelligence Director. For more information, see Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.
Category	A custom, optional tag or keyword that you manually add to the incident.

Field	Description
Status	A value indicating the current stage of your analysis of the incident. All incidents are `New` until you change the **Status** for the first time. This field is optional. Depending on the needs of your organization, consider using the status values as follows: • `New`—The incident requires investigation, but you have not started investigating. • `Open`—You are currently investigating the incident. • `Closed`—You investigated the incident and took action. • `Rejected`—You investigated the incident and determined there was no action to take.
Delete ( )	Clicking this icon permanently deletes this incident.

Incident details: Indicators and observations

The lower section of the Incident Details window provides an in-depth view of indicator and observation information. This information is organized as **Indicator** fields, the indicator pattern, and **Observations** fields.

Indicator section

When you first view indicator details, this section displays only the indicator name.

Click the indicator name to view the indicator on the Indicators page.

Click the down arrow next to the indicator name to view more indicator details without leaving the incident. Detail fields include:

Table 128: Indicator fields

Field	Description
Description	The indicator description provided by the source.
SOURCE	The source that contained the indicator. Click this link to access full source details.
Expires	The date and time the incident will expire, based on the source's **TTL** value.
Action	The action associated with the indicator. For more information, see Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.
Publish	The publish setting for the indicator. For more information, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.
Download STIX	If the source type is **STIX**, click this button to download the STIX file.

Indicator pattern

The indicator pattern is a graphical representation of the observables and operators that comprise the indicator. Operators link the observables within the indicator. AND relationships are indicated with the **AND** operator. OR relationships are indicated with the **OR** operator OR by a close grouping of several observables.

If an observable in the pattern has already been seen, the observable box is white. If an observable has not already been seen, the observable box is grey.

In the indicator pattern:

- Click the **Add to Do-Not-Block List** button to add the observable to the Do Not Block list. This icon is present in both white and grey observable boxes. For more information, see Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.
- If you hover the cursor over a white observable box, the system highlights the related observation in the **Observations** section.
- If you click a white observable box, the system highlights the related observation in the **Observations** section, scrolls that observation into view (if multiple observations are present), and expands that observation's detailed display.
- If you hover the cursor over or click a grey observable box in the indicator pattern, there is no change in the **Observations** section. Because the observable is unseen, there are no observation details to display yet.

Observations section

By default, the **Observations** section displays summary information, which includes:

- The type of observable that triggered the observation (for example, **Domain**)
- The data that comprises the observable
- Whether the observation is the first observation or a subsequent observation (for example, **1st** OR **3rd**)

Note If a single observable has been seen three or more times, Threat Intelligence Director displays the first and last observation details. The details for intermediary observations are not available.

- The date AND time of the observation
- The action configured for the observable

If you hover the cursor over an observation in the **Observations** section, the system highlights the related observable in the indicator pattern.

If you click an observation in the **Observations** section, the system highlights the related observable(s) in the indicator pattern and scrolls the first related observable into view (if multiple observables are present). Clicking an observation also expands the details of the observation in the **Observations** section.

Observation details include these fields:

Table 129: Observation detail fields

Field	Description
SOURCE	The source IP address and port for the traffic that triggered the observation.

Field	Description
DESTINATION	The destination IP address and port for the traffic that triggered the observation.
ADDITIONAL INFORMATION	DNS and authentication information related to the traffic that triggered the observation.
Events	This clickable link displays if the observation generated connection, security intelligence, file, or malware events. Click the link to view the events in the Secure Firewall Management Center event table; see *Cisco Secure Firewall Management Center Administration Guide*.

View events for a Threat Intelligence Director observation

View events associated with Threat Intelligence Director observations to analyze security incidents and understand system actions taken.

For more information about the Secure Firewall Management Center events that Threat Intelligence Director observations generate, refer to Threat Intelligence Director observations in Secure Firewall Management Center events, on page 2144.

The system action logged for Threat Intelligence Director-related events can vary, depending on the interaction of Threat Intelligence Director and other Secure Firewall Management Center features. For more information about action prioritization, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

Before you begin

- Configure the feature as described in Set up Threat Intelligence Director, on page 2126.
- Confirm that you enabled event logging required for Threat Intelligence Director in your access control policy, as described in Configure policies to support Threat Intelligence Director, on page 2127.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Incidents**.

Step 2 Click the **Incident ID** value for the incident.

Step 3 Click the observation in the **Indicator** section to display the observation box.

Step 4 Expand the observation box by clicking the arrow in the upper-left corner of the box.

Step 5 Click the **Events** link in the observation information. For more information on the Security Intelligence display, refer to the *Connection and Security Intelligence Events* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

Threat Intelligence Director observations in Secure Firewall Management Center events

If you fully configure your access control policy, Threat Intelligence Director observations generate specific Secure Firewall Management Center events.

Table 130: Secure Firewall Management Center Events Generated by Observations

Observation Content	Connection Events Table	Security Intelligence Events Table	File Events Table	Malware Events Table
SHA-256	Yes	No	Yes	Yes, if disposition is Malware or Custom Detection.
Domain Name, **URL**, or **IPv4/IPv6**	Yes Threat Intelligence Director-related connection events are identified with a Threat Intelligence Director-related **Security Intelligence Category** value.	Yes Threat Intelligence Director-related security intelligence events are identified with a Threat Intelligence Director-related **Security Intelligence Category** value.	No	No

Factors that affect the action taken

Factors that affect the action taken are system conditions that determine when the system takes action and what action the system takes when it detects traffic that matches a Threat Intelligence Director observable.

Action determination factors

The system considers these factors when determining actions:

- Features like Security Intelligence take action before Threat Intelligence Director does. For details, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.
- Generally, the action configured for an observable (which may differ from the action configured for its parent indicator or source) is the action that will be taken.
- Because Structured Threat Information eXpression (STIX) sources can contain complex indicators, the Action setting for the source can be set only to Monitor. However, individual simple indicators or observables contained in a STIX feed or file can be set to Block.
- Action settings for indicators and observables can be inherited or individually configured to override inheritance. Refer to Inheritance in Threat Intelligence Director configurations, on page 2157 and Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.
- Traffic that might otherwise be actionable might be on a Do Not Block list. For details, refer to Add Threat Intelligence Director observables to a Do Not Block list, on page 2164.
- The configured action is taken for both partially- and fully-realized incidents.
- An incident based on a complex indicator can be partially blocked. This can occur if the indicator includes both monitored and blocked observations.

- The actions the system takes are affected when publishing is paused. Refer to Pausing publishing, on page 2160 and Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.
- Pausing the Threat Intelligence Director feature prevents all actions. After you resume the feature, actionable data may be different from before. For details, refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 2161.

Threat Intelligence Director - Firewall Management Center action prioritization

If Threat Intelligence Director observable actions conflict with Firewall Management Center policy actions, the system prioritizes actions as follows:

- Security Intelligence Do Not Block
- TID Block
- Security Intelligence Block
- TID Monitor
- Security Intelligence Monitor

Specifically:

Table 131: Threat Intelligence Director URL Observable Action vs. Security Intelligence Action

Setting: Security Intelligence Action	Setting: Threat Intelligence Director Observable Action	Threat Intelligence Director Incidents Field: Action Taken	Security Intelligence Events Fields:		
			Action	Security Intelligence Category	Reason
`Do Not Block`	`Monitor` or `Block`	No TID incident	No Security Intelligence event		
`Block`	`Monitor`	`Blocked`	`Block`	as determined by system analysis; see Security intelligence categories, on page 1602	`URL Block`
	`Block`	`Blocked`	`Block`	`TID URL Block`	`URL Block`
`Monitor`	`Monitor`	`Monitored`	Determined by access control rules processed after Security Intelligence and TID.	`TID URL Monitor`	`URL Monitor`
	`Block`	`Blocked`	`Block`	`TID URL Block`	`URL Block`

Table 132: Threat Intelligence Director IPv4/IPv6 Observable Action vs. Security Intelligence Action

Setting: Security Intelligence Action	Setting: Threat Intelligence Director Observable Action	Threat Intelligence Director Incidents Field: Action Taken	Security Intelligence Events Fields:		
			Action	Security Intelligence Category	Reason
`Do Not Block`	`Monitor` or `Block`	No TID incident	No Security Intelligence event		
`Block`	`Monitor`	No TID incident	`Block`	as determined by system analysis; see Security intelligence categories, on page 1602	`IP Block`
	`Block`	`Blocked`	`Block`	`TID IPv4 Block` `TID IPv6 Block`	`IP Block`
`Monitor`	`Monitor`	`Monitored`	Determined by access control rules processed after Security Intelligence and TID.	`TID IPv4 Monitor` `TID IPv6 Monitor`	`IP Monitor`
	`Block`	`Blocked`	`Block`	`TID IPv4 Block` `TID IPv6 Block`	`IP Block`

Table 133: Threat Intelligence Director Domain Name Observable Action vs. DNS Policy Action

Setting: DNS Policy Action	Setting: Threat Intelligence Director Domain Name Observable Action	Threat Intelligence Director Incidents Field: Action Taken	Security Intelligence Events Fields:		
			Action	Security Intelligence Category	Reason
`Do Not Block`	`Monitor` or `Block`	No TID incident	No Security Intelligence event		

`Drop`, `Domain Not Found`
`Sinkhole—Log`
`Sinkhole—Block and Log`
	`Monitor`	`Blocked`	`Block`	as determined by system analysis; see Security intelligence categories, on page 1602	`DNS Block`

	`Block`	`Blocked`	`Block`	`TID Domain Name Block`	`DNS Block`

Setting: DNS Policy Action	Setting: Threat Intelligence Director Domain Name Observable Action	Threat Intelligence Director Incidents Field: Action Taken	Security Intelligence Events Fields:		
			Action	Security Intelligence Category	Reason
Monitor	Monitor	Monitored	Determined by access control rules processed after Security Intelligence and TID.	TID Domain Name Monitor	DNS Monitor
	Block	Blocked	Block	TID Domain Name Block	DNS Block

Table 134: TID SHA-256 Observable Action vs. Malware Cloud Lookup File Policy

File Disposition	Threat Intelligence Director SHA-256 Observable Action	Action Taken in Threat Intelligence Director Incidents	Action in File Events	Action in Malware Events
Clean	Monitor or Block	Monitored	Malware Cloud Lookup	n/a
Malware	Monitor or Block	Monitored	Malware Cloud Lookup	n/a
Custom	Monitor or Block	Monitored	• Malware Cloud Lookup , if SHA-256 is not in a custom detection list. • Custom Detection , if SHA-256 is in a custom detection list.	• Malware Cloud Lookup , if SHA-256 is not in a custom detection list. • Custom Detection , if SHA-256 is in a custom detection list.
Unknown	Monitor or Block	Monitored	Malware Cloud Lookup	n/a

Note Threat Intelligence Director matching occurs before the system sends a file for dynamic analysis.

Table 135: TID SHA-256 Observable Action vs. Block Malware File Policy

File Disposition	Threat Intelligence Director SHA-256 Observable Action	Action Taken in Threat Intelligence Director Incidents	Action in File Events	Action in Malware Events
Clean or Unknown	Monitor	Monitored	Malware Cloud Lookup	n/a
	Block	Blocked	• TID Block, if SHA-256 is not in a custom detection list. Modified file disposition is Custom. • Custom Detection Block, if SHA-256 is in a custom detection list.	TID Block Modified file disposition is Custom.
Malware or Custom	Monitor	Blocked	Block Malware	Block Malware
	Block	Blocked	• TID Block, if SHA-256 is not in a custom detection list. Modified file disposition is Custom. • Custom Detection Block, if SHA-256 is in a custom detection list.	TID Block Modified file disposition is Custom.

View and change Threat Intelligence Director configurations

Use the following information to review and fine-tune your configuration as needed.

View Threat Intelligence Director status of elements (managed devices)

This task allows you to monitor the status of managed devices and confirm that Threat Intelligence Director is properly enabled on elements.

All devices that are registered to the Firewall Management Center as managed devices appear automatically on the Elements page. All properly configured elements (as specified in Configure policies to support Threat Intelligence Director, on page 2127) will receive all currently published observables, including those ingested before the element was added.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Elements**.

Step 2 To see whether the element is connected and Threat Intelligence Director is enabled, hover over the icon beside the element name.

Note After deploying, it may take up to five minutes for information on this page to update, including the applied access control policy and whether TID is enabled.

View and manage sources

View summary information about all configured sources and manage their settings, including actions, publish status, updates, and deletion.

The Sources page displays summary information about all configured sources. Refer to Source summary information, on page 2150.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources**.

Step 2 View your sources.

- To filter the sources displayed on the page, click **Filter** ( ). For more information, refer to Filter Threat Intelligence Director data in table views, on page 2156.
- To view detailed ingestion status, hover the cursor over the text in the **Status** column. For more information, refer to Source status details, on page 2151.

Step 3 Manage your sources.

- To edit the **Action** setting, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159. If an action is fixed, it is the only supported action for the source **Type**.

- To edit the **Publish** setting, click **Slider** (). For more information, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.
- To pause or resume Threat Intelligence Director updating the source, click **Pause Updates** or **Resume Updates**. If you pause updates, updating is paused but existing indicators and observables remain in TID.
- To delete the source, click **Delete** (). The Delete option is unavailable if the source is still processing. Removing a source removes all indicators associated with that source. Associated observables may also be deleted; they are retained if they are associated with indicators remaining in the system.

Source summary information

The Sources page displays summary information for all configured sources. This reference provides brief descriptions of the fields in the summary display. For detailed information on these fields, see descriptions in the relevant configuration topic for the source. Refer to Options for ingesting data sources, on page 2128.

Table 136: Sources summary information

Field	Description
Name	The source name.
Type	The data format of the source, such as**STIX** or **Flat File**.
Delivery	The method Threat Intelligence Director uses to retrieve the source.
Action	The action (**Block** or **Monitor**) that the system is configured to perform on traffic matching the data contained within this source. For more information about Threat Intelligence Director actions, including availability, inheritance, and overriding inheritance, refer to Factors that affect the action taken, on page 2144.
Publish	**On** or **Off** toggle specifying whether Threat Intelligence Director publishes data from the source to registered elements (managed devices configured to support Threat Intelligence Director). Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Last Updated	The date and time Threat Intelligence Director last updated the source.

Field	Description
Status	The current status of the source: • **New**—The source is newly created. • **Scheduled**—The initial download or subsequent update is scheduled, but not yet in progress. • **Downloading**—Threat Intelligence Director is performing the initial download or update refresh. • **Parsing** or **Processing**—Threat Intelligence Director is ingesting the source. • **Completed**—Threat Intelligence Director finished ingesting the source. • **Completed with Errors**—Threat Intelligence Director finished ingesting the source, but some observables are unsupported or invalid. • **Error**—Threat Intelligence Director experienced a problem. If the source is a TAXII or URL source with an **Update Frequency** specified, and updates are not paused, Threat Intelligence Director retries on the next scheduled update. Refresh the page to update the status.
Edit ( )	Clicking this icon allows you to edit settings for the source.
Delete ( )	Clicking this icon permanently deletes the source.

Source status details

When you hover over the **Status** value of a source in the Sources summary page, Threat Intelligence Director provides additional details about the source status.

Data	Description
Status Message	Briefly describes the current status of the source.
Last Updated	Specifies the date and time Threat Intelligence Director last updated the source.
Next Update	For TAXII and URL sources, this value specifies when Threat Intelligence Director will update the source next.

Data	Description
Indicators	Specifies indicator counts. • **Consumed**—The number of indicators Threat Intelligence Director processed during the most recent source update. This number represents all indicators contained in the update, regardless of whether they were ingested or discarded. • **Discarded**—The number of malformed indicators that the system did not add to Threat Intelligence Director during the most recent update. **Note** For `TAXII` sources, Threat Intelligence Director provides separate **Last Update** and **Total** indicator counts, because TAXII updates add incremental data, rather than replacing existing data. For indicators from other source types, Threat Intelligence Director provides only the **Last Update** count, because updates from those sources replace the existing data set entirely. If all observables of an indicator are **Invalid**, Threat Intelligence Director discards the indicator.
Observables	Specifies observable counts. • **Consumed**—The number of observables Threat Intelligence Director processed during the most recent source update. This number represents all observables contained in the update, regardless of whether they were ingested or discarded. • **Unsupported**—The number of unsupported observables that the system did not add to Threat Intelligence Director during the most recent update. For more information about supported observable types, see information about content types in Source requirements, on page 2125. • **Invalid**—The number of invalid observables that the system did not add to Threat Intelligence Director during the most recent update. An observable is invalid if it is improperly constructed. For example, `10.10.10.10.123` is not a valid IPv4 address. **Note** For `TAXII` sources, Threat Intelligence Director provides separate **Last Update** and **Total** observable counts, because TAXII updates add incremental data, rather than replacing existing data. For observables from other source types, Threat Intelligence Director provides only the **Last Update** count, because updates from those sources replace the existing data set entirely.

View and manage indicators

This task enables you to view current indicators and manage their configuration settings including actions and publish status.

Indicators are generated automatically from ingested sources. For more information about the contents of this page, refer to Indicator summary information, on page 2153.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources**.

Step 2 Click **Indicators**.

Step 3 View your current indicators.

- To filter the indicators displayed on the page, click **Filter** (). For more information, refer to Filter Threat Intelligence Director data in table views, on page 2156.
- To view additional details about an indicator, including associated observables, click the indicator name. For more information, refer to Indicator details, on page 2154.
- In the **Incidents** column, click the number to view information about incidents associated with an indicator, or hover the cursor over Incidents to view whether the incidents are fully realized or partially realized.
- To determine whether Threat Intelligence Director finished ingesting an indicator from the source, view the **Status** column.

Step 4 Manage your current indicators.

- To edit the **Action**, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159. If an action is fixed, that is the only supported action for the source **Type**.
- To edit the **Publish** setting, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.
- To add one or more observables for an indicator to the Do Not Block list, click the indicator name to access the Indicator Details page. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.

Indicator summary information

The Indicators page displays summary information for all indicators associated with configured sources.

Table 137: Indicators summary information

Field	Description
Type	• Indicators that have a single observable list the data type of that observable (URL, SHA-256, etc.) • Indicators that have two or more observables are listed as **Complex**. Hover over the type to see the specific observable.
Name	The indicator name.
Source	The source that contained the indicator (the parent source).

Field	Description
Incidents	Information about any incidents associated with the indicator: • an icon specifying whether the incident is **Partially** or **Fully** realized • the number of incidents associated with the indicator
Action	The action associated with the indicator. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159. Indicators can inherit **Action** settings from a parent source, and observables can inherit **Action** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Publish	The publish setting for the indicator. For more information, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161. Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Last Updated	The date and time Threat Intelligence Director last updated the indicator.
Status	The current status of the indicator: • **Pending**—Threat Intelligence Director is ingesting the observables of the indicator. • **Completed**—Threat Intelligence Director successfully ingested all observables for the indicator. • **Completed With Errors**—Threat Intelligence Director finished ingesting the indicator, but some observables are unsupported or invalid.

Indicator details

The Indicator Details page displays indicator and observable data for an incident.

Table 138: Indicator details information

Field	Description
Name	The indicator name.
Description	The indicator description provided by the source.
Source	The source that contained the indicator.
Expires	The date and time the indicator will expire, based on the source's **TTL** value.
Action	The action associated with the indicator. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159. Indicators can inherit the **Action** setting from a parent source, and observables can inherit the **Action** setting from a parent indicator. For more information, see Inheritance in Threat Intelligence Director configurations, on page 2157.

Field	Description
Publish	The publish setting for the indicator. For more information, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161. Indicators can inherit the **Publish** setting from a parent source, and observables can inherit the **Publish** setting from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Indicator Pattern	The observables and operators that form the indicator's pattern. Operators link the observables within the indicator. AND relationships are indicated with the **AND** operator. OR relationships are indicated with the **OR** operator or by a close grouping of several observables. Optionally, click the **Add to Do-Not-Block List** button to add an observable to the Do Not Block list. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.

View and manage observables

This task allows you to view all successfully ingested observables and perform management operations such as editing actions, modifying publish settings, and adding observables to the Do Not Block list.

The Observables page displays all successfully ingested observables. Refer to Observable summary information, on page 2156.

Before you begin

- Configure one or more sources as described in Fetch TAXII feeds to use as sources, on page 2129, Fetch sources from a URL, on page 2130, or Upload a local file to use as a source, on page 2132.

Follow these steps to view and manage observables:

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources**.

Step 2 Click **Observables**.

Step 3 View your current observables.

- To filter the observables displayed on the page, click **Filter** (). For more information, refer to Filter Threat Intelligence Director data in table views, on page 2156.
- If the information in the **Value** column is cut off, hover over the value.
- To view indicators that contain the observable, click the number in the **Indicators** column. The Incidents page opens with the observable value as the filter. For more information, refer to View and manage indicators, on page 2152.

Step 4 Manage your current observables.

- To edit the **Action**, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159.

- To edit the **Publish** setting for an observable, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.
- To change the expiration date for an observable, modify the **TTL** for the parent source. For more information, refer to View and manage sources, on page 2149.
- To add an observable to the Do Not Block list, click the **Add to Do-Not-Block List** button. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.

Observable summary information

The Observables page displays summary information for all ingested observables.

Table 139: Observables summary information

Field	Description
Type	The type of observable data: `SHA-256`, `Domain`, `URL`, `IPv4`, or `IPv6`.
Value	The data that comprises the observable.
Indicators	The number of parent indicators containing the observable.
Action	The action configured for the observable. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159. Indicators can inherit **Action** settings from a parent source, and observables can inherit **Action** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Publish	The publish setting for the observable. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161. Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.
Updated At	The date and time Threat Intelligence Director last updated the observable.
Expires	The date that the observable will be automatically purged from Threat Intelligence Director based on **TTL** for the parent indicator.
Add to Do-Not-Block List button	Clicking this button adds the observable to the Do Not Block list. Refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.

Filter Threat Intelligence Director data in table views

Filter table views to narrow down and display only the Threat Intelligence Director data that matches your specific criteria.

Use this procedure when you need to focus on specific data within Threat Intelligence Director table views by applying attribute-based filters.

Procedure

Step 1 Choose one of these Threat Intelligence Director table views.

- **Integration** > **Intelligence** > **Incidents**
- **Integration** > **Intelligence** > **Sources**
- **Integration** > **Intelligence** > **Sources**, and click **Indicators**
- **Integration** > **Intelligence** > **Sources**, and click **Observables**

Step 2 Click **Filter** () and choose a filter attribute.

Step 3 Choose or enter a value for that filter attribute.

Filters are case-sensitive.

Step 4 (Optional) To filter by multiple attributes, click **Filter** () and repeat Step 2 and Step 3.

Step 5 To cancel the changes you have made since you last applied the filter, click **Cancel**.

Step 6 Click **Apply** to refresh the table with the filter applied.

Step 7 To remove a filter attribute individually, click **Remove** () next to the filter attribute and click **Apply** to refresh the table.

Inheritance in Threat Intelligence Director configurations

Inheritance in Threat Intelligence Director configurations is a hierarchical configuration mechanism that

- creates indicators and observables as child objects when Threat Intelligence Director ingests intelligence data from a source,
- ensures child objects automatically inherit **Action** and **Publish** settings from their parent configuration on creation, and
- maintains parent-child relationships where indicators inherit from source configurations and observables inherit from parent indicators.

Inheritance relationships

The inheritance hierarchy follows these parent-child relationships:

- An indicator inherits these settings from the parent source. An indicator can only have one parent source.
- An observable inherits these settings from the parent indicators. An observable can have multiple parent indicators.

For more information, refer to:

• Inheritance of TID settings from multiple parents, on page 2158
• Overriding inherited TID settings, on page 2158

Inheritance of TID settings from multiple parents

If an observable has multiple parent indicators, the system compares the inherited settings from all the parents and assigns the most secure option to the observable. Thus:

- **Action**: `Block` is more secure than `Monitor`
- **Publish**: `On` is more secure than `Off`

For example, SourceA might contribute IndicatorA and related ObservableA:

Setting	SourceA	IndicatorA	ObservableA
Action	`Block`	`Block`	`Block`
Publish	`Off`	`Off`	`Off`

If SourceB later contributes IndicatorB, which also includes ObservableA, the system modifies ObservableA in this way:

Setting	SourceB	IndicatorB	ObservableA
Action	`Monitor`	`Monitor`	`Block` (inherited from IndicatorA)
Publish	`On`	`On`	`On` (inherited from IndicatorB)

In this example, ObservableA has two parents: one parent for its **Action** setting and one parent for its **Publish** setting. If you manually edit the settings for the observable and then revert the settings, the system sets the **Action** setting to the IndicatorA value and the **Publish** setting to the IndicatorB value.

Overriding inherited TID settings

An overriding inherited TID setting is a configuration change that

- changes the inherited setting at the child level,
- retains the child object setting despite changes to parent objects, and
- breaks automatic cascading of setting changes from parent to child for that specific setting.

Override behavior and inheritance

To override an inherited setting, change the setting at the child level. Refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 2159 and Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161. After you override an inherited setting, the child object retains that setting despite changes to the parent object(s).

At the observable level, you can revert from an override setting to the inherited setting, and the system resumes cascading setting changes automatically from the parent indicator to that observable.

Override inheritance scenarios

For example, you might start with these original settings, with no overrides set:

Setting	SourceA	IndicatorA	ObservableA1	ObservableA2
Publish	Off	Off	Off	Off

If you override the setting for IndicatorA, the settings would be these:

Setting	SourceA	IndicatorA	ObservableA1	ObservableA2
Publish	Off	On	On	On

In this case, any changes to the **Publish** setting for SourceA no longer cascade automatically to IndicatorA. However, inheritance from IndicatorA to ObservableA1 and ObservableA2 continues, because the observable settings are not currently set to override values.

If you later override the setting for ObservableA1:

Setting	SourceA	IndicatorA	ObservableA1	ObservableA2
Publish	Off	On	Off	On

Any changes to the **Publish** setting for IndicatorA no longer cascade automatically to ObservableA1. However, those changes continue to cascade to ObservableA2, because it is not set to an override value.

Edit Threat Intelligence Director actions at the source, indicator, or observable Level

Configure action settings at the source, indicator, or observable level to control how threat intelligence data is handled within your security policies.

Editing the action for a parent sets the action for all children. If you edit the action at the source level, you set the action for all its indicators. If you edit the action at the indicator level, you set the action for all of its observables.

Editing the action for a child interrupts inheritance. If you edit the action at the indicator level, and subsequently edit it at the source level, the indicator's action is retained until you edit the action for the individual indicator. If you edit the action at the observable level, and subsequently edit it at the indicator level, the observable's action is retained until you edit the action for the individual observable. At the observable level, you can revert automatically to the parent indicator's action. For more information about inheritance, refer to Inheritance in Threat Intelligence Director configurations, on page 2157.

You may also want to review other Factors that affect the action taken, on page 2144.

Procedure

Step 1 Choose any of the following:

- **Integration** > **Intelligence** > **Sources**

Note Threat Intelligence Director does not support blocking TAXII sources at the source level. If the TAXII source contains a simple indicator, you can block at the indicator or observable level.

- **Integration** > **Intelligence** > **Sources**, and click **Indicators**

Note Threat Intelligence Director does not support blocking complex indicators. Instead, block individual observables within the complex indicator.

- **Integration** > **Intelligence** > **Sources**, and click **Observables**

Step 2 Use the **Action** dropdown to choose **Monitor** ( ) or **Block** ( ).

Step 3 (Observables only) If you want to resume inheriting the action setting from the parent indicator, click **Revert** next to the **Action** setting for the observable.

Pausing publishing

- If you pause publishing at the feature level, the system purges all Threat Intelligence Director observables stored on your elements. This means that Threat Intelligence Director cannot detect, monitor or block threats. Other security features on your system are not affected.
- If you pause publishing at the source, indicator, or observable level, the system removes the paused Threat Intelligence Director observables from your elements, preventing them from matching traffic.
- If you pause publication for a parent, the system pauses all children. For example, pausing publishing at the source level pauses publishing for all its indicators; pausing publishing at the indicator level pauses publishing for all of its observables.
- Pausing publication for a child interrupts inheritance. If you pause publishing at the indicator level, and subsequently publish at the source level, publishing for the indicator remains paused until you change the individual setting for the indicator. If you pause publishing at the observable level, and subsequently publish at the indicator level, publishing for the observable remains paused until you change the individual setting for the observable. At the observable level, you can revert automatically to the parent indicator's publishing status. For more information about inheritance, see Inheritance in Threat Intelligence Director configurations, on page 2157.
- Publishing for Uploaded sources can only be paused at the indicator level.
- For a comparison of pausing publishing for an observable vs adding the observable to the Do Not Block list, see Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.
- If you have specified a publish or pause setting for an individual observable or indicator, source updates do not change that setting if the update contains the same observable or indicator.
- Publishing can be disabled on the object management pages. See Modify the observable publication frequency, on page 2162.

- The option on the Sources page to pause updates is not related to publishing data to elements; it applies to updating sources on the Firewall Management Center from feeds.

Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements

This task allows you to pause Threat Intelligence Director operations across all elements and purge existing data when necessary.

Caution This setting pauses publishing to all elements, purges all Threat Intelligence Director observables stored on your elements, and stops inspecting traffic using the Threat Intelligence Director feature.

To disable observables at a more granular level, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Data on the management center (existing incidents and configured sources, indicators, and observables, and ingestion of sources) is not affected by this setting.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Settings**.

Step 2 Click **Pause**.

What to do next

When you are ready to resume synchronizing Threat Intelligence Director data on your elements and generating observations, manually **Resume** publishing from this page. Existing observables on the management center are published to all elements.

Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level

This task allows you to control the publishing of Threat Intelligence Director data by pausing or enabling publication at the source, indicator, or observable level.

If publishing is enabled at the Source level, the system automatically publishes the initial source data and any subsequent changes including:

- changes from periodic source refreshes
- changes resulting from system action (for example, **TTL** expiration)
- any user-initiated changes (for example, a change in the **Action** setting for an indicator or observable)

Note To purge all Threat Intelligence Director observables at once from your devices (elements), see Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 2161.

Before you begin

Before pausing publishing, review the ramifications described in Pausing publishing, on page 2160.

Procedure

Step 1 Choose any of these options.

- **Integration** > **Intelligence** > **Sources**
- **Integration** > **Intelligence** > **Sources**, and click **Indicators**
- **Integration** > **Intelligence** > **Sources**, and click **Observables**

Step 2 Locate the **Publish Slider** ( ) and use it to toggle publishing to elements.

Step 3 (Observables only) If you want to resume inheriting the publication setting from the parent indicator, click **Revert** next to the **Publish** setting for the observable.

What to do next

- Wait at least ten minutes for elements to receive changes. Changes involving large sources will take longer.
- (Optional) Change the publication frequency for TID data at the observable level. Refer to Modify the observable publication frequency, on page 2162.

Modify the observable publication frequency

This task allows you to set a custom publication interval for observables to TID elements, replacing the default 5-minute interval.

By default, the system publishes observables to TID elements every 5 minutes. Use this procedure to set this interval to a different value.

Before you begin

- Enable publication of TID data at the observable level. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 2161.

Follow these steps to modify the observable publication frequency:

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence** > **Network Lists and Feeds**.

Step 2 Click **Edit** ( ) next to the **Cisco-TID-Feed**.

Step 3 Choose a value from the **Update Frequency** drop-down list.

- Choose **Disable** to stop publication of observable data to elements.
- Choose any other value to set the interval for observable publication.

Step 4 Click **Save**.

Adding Threat Intelligence Director observables to the Do Not Block list

A Do Not Block list is a security feature that

- exempts observables in indicators from specified actions, allowing traffic to pass without monitoring or blocking,
- ignores listed observables when evaluating traffic in complex indicators while still evaluating other observables, and
- takes precedence over action settings regardless of whether they are inherited or override values.

Do not block list behavior

The Do Not Block list affects simple and complex indicators differently:

- Simple indicators: If you add an observable to the Do Not Block list, traffic passes without monitoring or blocking.
- Complex indicators: Threat Intelligence Director ignores observables on the Do Not Block list when evaluating traffic, but other observables in that indicator are still evaluated.

In a complex indicator that includes Observable 1 and Observable 2 linked by the AND operator:

- If you add Observable 1 to a Do Not Block list, Threat Intelligence Director generates a fully realized incident when Observable 2 is seen.
- If you disable publishing of Observable 1 instead of adding it to the Do Not Block list, Threat Intelligence Director generates a partially-realized incident when Observable 2 is seen.

Note If you add an observable to the Do Not Block list, this always takes precedence over the **Action** setting, whether the setting in the observable is an inherited or override value.

Source updates do not affect the Do Not Block list setting for individual observables if the update contains the same observable.

Add Threat Intelligence Director observables to a Do Not Block list

Adding observables to a Do Not Block list allows you to exempt specific items from being blocked, ensuring legitimate traffic is not inadvertently restricted.

For detailed information about using Do Not Block lists, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 2163.

Tip An "Add to Do Not Block List" button ( ) can appear in several places in the web interface. You can add an observable to a Do Not Block list in any of those locations by clicking this button.

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources**, and click **Observables**.

Step 2 Navigate to the observable that you want to allow.

Step 3 Click (**Add to Do-Not-Block List**) for that observable.

What to do next

(Optional) If you need to remove an observable from the Do Not Block list, click the button again.

View a STIX source file

Procedure

Step 1 Choose **Integration** > **Intelligence** > **Sources** , and click **Indicators** .

Step 2 Click the indicator name.

Step 3 Click **Download STIX** .

Step 4 Open the file in a text editor.

Troubleshoot Threat Intelligence Director

This reference describes possible solutions and mitigations for common Threat Intelligence Director issues.

Fetching or uploading flat file sources generates an error

If the system fails to fetch or upload a flat file source, check that the data in the flat file matches the **Type** column on the **Integration** > **Intelligence** > **Sources** page.

TAXII or URL source update generates an error

If a TAXII or URL source update generates a source status error, check that your Server Certificate is not expired. If the certificate has expired, enter a new **Server Certificate** or delete the existing **Server Certificate** so Threat Intelligence Director can retrieve a new certificate. For more information, refer to Configure TLS/SSL settings for a Threat Intelligence Director source, on page 2133.

"Block" action is not available for an indicator or source, only "monitor"

You can change the action for individual observables in the indicator or source.

Threat Intelligence Director table views return "No results"

Table views include the **Sources**, **Indicators**, **Observables**, and **Incidents** pages.

If you do not see data in one of the Threat Intelligence Director table views:

- Check your table filter and consider expanding the time window for the **Last Updated** filter attribute. Refer to Filter Threat Intelligence Director data in table views, on page 2156.
- Verify that you correctly configured your sources. Refer to Options for ingesting data sources, on page 2128.
- Verify that you configured your access control policy and related policies to support Threat Intelligence Director. Refer to Configure policies to support Threat Intelligence Director, on page 2127. For example, if your SHA-256 observables are not generating observations, verify that your deployed access control policy contains one or more access control rules that invoke a **Malware Cloud Lookup** or **Block Malware** file policy.
- Verify that you deployed the Threat Intelligence Director-supporting access control policy and related policies to your elements. Refer to Deploy configuration changes, on page 135.
- Verify that you did not pause Threat Intelligence Director data publication at the feature level. Refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 2161.

System is experiencing slowness or decreased performance

For more information about performance impact, refer to Performance impact of Threat Intelligence Director, on page 2123.

Secure Firewall Management Center table views do not show Threat Intelligence Director data

If you are publishing observables to your elements but no Threat Intelligence Director data appears in the connection, security intelligence, file, or malware events tables, check the access control and file policies deployed to your elements. For more information, refer to Configure policies to support Threat Intelligence Director, on page 2127.

One or more elements are overwhelmed by Threat Intelligence Director data

If Threat Intelligence Director data is overwhelming one or more of your devices, consider pausing Threat Intelligence Director publishing and purging the data stored on your elements. For more information, refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 2161.

System is performing a malware cloud lookup instead of a TID block

This is by design. For more information, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

System is performing a security intelligence or DNS policy action instead of a TID action

This is by design. For more information, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 2145.

TID is disabled

- Add memory to your appliance. Threat Intelligence Director can only be used on appliances with at least 15 GB of memory.
- Enable REST API access for the Secure Firewall Management Center. For more information, refer to *Enabling REST API Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

The system does not generate the Threat Intelligence Director incident or take the Threat Intelligence Director action that you expected

- Verify that all of your managed devices are properly enabled and configured for Threat Intelligence Director. Refer to View Threat Intelligence Director status of elements (managed devices), on page 2149 and Configure policies to support Threat Intelligence Director, on page 2127.
- It takes at least 5-10 minutes for changes to be published to elements, and significantly longer if publishing a large data feed.
- Check the action setting for the observable. Refer to View and manage observables, on page 2155.
- For a list of the other factors that influence the Threat Intelligence Director action that the system takes, refer to Factors that affect the action taken, on page 2144.
- Elements (managed devices) may not have the threat data you think they have. Refer to Pausing publishing, on page 2160.

One encounter with a particular threat generates multiple incidents

This can occur if a single indicator is included in multiple sources.

For details, refer to Handling of duplicate indicators, on page 2133.

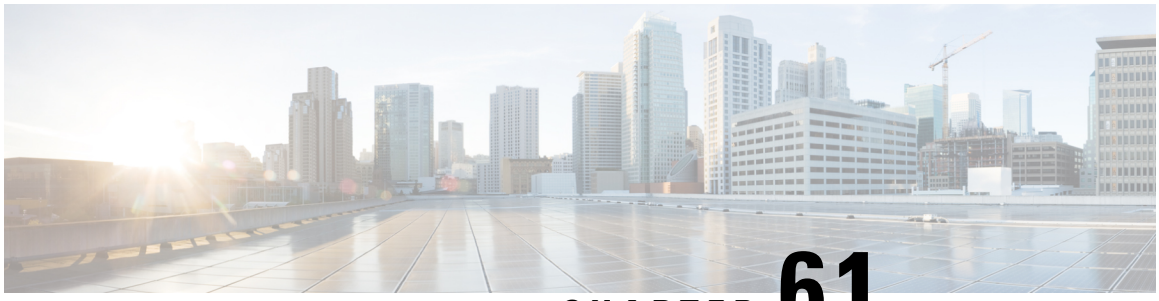
History for Threat Intelligence Director

This reference provides the complete version history for Threat Intelligence Director features, including implementation details, version requirements, and behavioral changes across different software releases.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Handling of an indicator that is included in multiple STIX feeds	7.1	Any	If STIX feeds contain identical indicators, an indicator is created for each feed, which may lead to multiple incidents being generated for the same indicator. Previously, only the feed that was downloaded last took effect.

Change in action prioritization	6.5	Any	These changes apply if more than one Firepower feature could apply to a particular observable.
			TID blocking/monitoring observable actions now have priority over blocking/monitoring by Security Intelligence.
			Important
			The system still effectively handles traffic as before. Traffic that was previously blocked is still blocked, and monitored traffic is still monitored. This simply changes the component reported in the event as responsible for the action. You may also see more TID incidents generated.
			• If you configure the Block TID observable action, even if the traffic also matches a Security Intelligence Block action:
			  • The Security Intelligence category in the connection event is a variant of TID Block.
			  • The system generates a TID incident with an action taken of Blocked.
			• If you configure the Monitor TID observable action, even if the traffic also matches a Security Intelligence Monitor rule:
			  • The Security Intelligence category in the connection event is a variant of TID Monitor
			  • The system generates a TID incident with an action taken of Monitored.
			Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident.

Secure Firewall Threat Intelligence Director	6.2.2	Any	Lets you use threat intelligence from external sources to identify and process threats. New screens: A new top-level **Intelligence** menu with multiple tabs. Supported platforms: Secure Firewall Management Center



CHAPTER 61

Advanced Settings for Access Control

Advanced access control policy settings typically require little or no modification. The default settings are appropriate for most deployments.

- Requirements and prerequisites for advanced settings, on page 2169
- Configure advanced settings for the access control policy, on page 2170
- History for advanced settings for the access control policy, on page 2187

Requirements and prerequisites for advanced settings

This reference provides the requirements and prerequisites needed to configure advanced settings for access control policy, including model support, domain compatibility, and user role permissions.

Model support

Any

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin
- You can define custom user roles to differentiate between the intrusion configuration in access control policy and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. The existing pre-defined user roles that included the Modify Access Control Policy permission support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions. The granular permissions are:
  - **Policies** > **Access Control heading** > **Access Control** and choose the **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** allows the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for network analysis and intrusion policies, the configuration of the Security Intelligence policy for the access

control policy, and intrusion actions in the policy default action. If a user has this option only, the user can modify no other part of the policy or rule.

- **Modify Remaining Access Control Policy Configuration** controls the ability to edit all other aspects of the policy.

Configure advanced settings for the access control policy

Configure advanced settings to customize access control policy behavior for specific security requirements and performance optimization.

Advanced access control policy settings typically require little or no modification. The default settings are appropriate for most deployments. Note that many of the advanced preprocessing and performance options in access control policies may be modified by rule updates as described in *Update Intrusion Rules* in the *Cisco Secure Firewall Management Center Administration Guide* .

Caution See Configurations that restart the snort process when deployed or activated, on page 131 for a list of advanced setting modifications that restart the Snort process, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Before you begin

Inheriting settings from a parent policy:

- If the access control policy has a base policy, you can elect to inherit settings from the base policy. Select **Inherit from (*base policy*)** for each setting group where you want to use the parent policy's settings. If you are allowed to configure unique settings for the policy, you must deselect the option to make your edits.
- If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. In this case, inheritance has been configured so that these settings are locked. The settings are read-only.

Follow these steps to configure advanced settings for the access control policy:

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Create or edit an access control policy.

Step 3 Select **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 For each settings group, click **Edit** ( ) and configure the settings as needed.

For each feature group, a separate dialog box is opened where you can make your changes. Click **OK** to save any changes.

- **General Settings**—These settings apply broadly to the policy, including URL filtering options. For more information, see General settings, on page 2172.
- **Identity Policy Settings**—Select the policy to be used to implement user identity discovery. You must implement an identity policy to get user or user group information in connection events, or to write access control rules based on users or groups. For more information, see Identity policies, on page 1941.
- **Decryption Policy Settings**—Select the policy to be used when decrypting connections. You must decrypt traffic to apply inspection to encrypted connections.
- **TLS Server Identity Discovery**—Whether to allow the firewall to extract certificate details such as Common Name (CN), Organization, or Subject Alternative Names (SANs) even when TLS 1.3 encryption would normally hide them. This improves policy accuracy without requiring a decryption rule; the original client connection remains encrypted. For more information, see TLS server identity discovery, on page 2173.
- **Prefilter Policy Settings**—Select the policy to be used for statically offloading large flows, implementing early connection blocks, or rezoning plain-text tunnel traffic.
- **Network Analysis and Intrusion Policies**—Advanced network analysis and intrusion policy settings allow you to:
  - Specify the intrusion policy and associated variable set that are used to inspect packets that must pass before the system can determine exactly how to inspect that traffic.
  - Change the access control policy's default network analysis policy, which governs many preprocessing options.
  - Use custom network analysis rules and network analysis policies to tailor preprocessing options to specific security zones, networks, and VLANs.
- **Threat Defense Service Policy**—Use the service policy to apply services to specific traffic classes. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications. The service policy rules are applied after the access control rules. For more information, see Service Policies, on page 2191.
- **Files and Malware Settings**—Tune file and malware inspection performance and storage, on page 2053 provides information on performance options for file control and malware defense.
- **Threat Detection**—Configure the portscan detector to detect and prevent portscan activity in all types of traffic to protect networks from eventual attacks. Portscan traffic can be detected efficiently in both allowed and denied traffic. For more information, see Threat Detection, on page 2211.
- **Elephant Flow Settings**—Elephant flows are large, long duration, and fast flows that can cause duress for Snort cores. There are two actions that you can apply on elephant flows to reduce system stress, CPU hogging, packet drops, and so on. These actions are:
  - Bypass any or all applications—This action bypasses flow from Snort inspection.
  - Throttle—This action applies dynamic rate limit policy (10% reduction) on elephant flows.

  For more information, see Configure elephant flow detection, on page 2222.
- **Intelligent Application Bypass Settings**—(Use **Elephant Flow Settings** instead of this option.) Intelligent application bypass (IAB) is an expert-level configuration that specifies applications to bypass or test for bypass if traffic exceeds a combination of inspection performance and flow thresholds.

IAB settings are applicable for Snort2 devices or pre 7.2.0 Snort3 devices. For more information, see Intelligent application bypass, on page 2175.

- **Transport/Network Layer Preprocessor Settings**—Advanced transport and network preprocessor settings apply globally to all networks, zones, and VLANs where you deploy your access control policy. For more information, see Transport/network layer preprocessor settings, on page 2181.
- **Detection Enhancement Settings**—Detection enhancement settings determine whether adaptive profiles are used for application detection and intrusion rules in the access control policy. Typically, the system uses the static settings in your network analysis policy to preprocess and analyze traffic. With adaptive profile updates, the system can adapt processing behavior using host information either detected by network discovery or imported from a third party. For more information, see Detection enhancement settings, on page 2182.
- **Performance Settings**—Settings for improving the performance of your system as it analyzes traffic for attempted intrusions. These settings are very advanced and should be left as defaults by most users. See Performance settings, on page 2184.
- **Latency-Based Performance Settings**—Settings specific to latency-based performance. These settings are very advanced and should be left as defaults by most users. See Latency-based performance settings, on page 2186.

Step 5 Click **Save** to save the changes to the access control policy.

- To get back to the rules list, click **Access Control** in the packet flow line.
- You must deploy the configuration to apply changes to the managed devices.

The advanced settings for the access control policy are configured and saved. The changes will take effect after deployment to the managed devices.

General settings

General settings are advanced configuration options that

- control URL logging and character limits for connection events,
- manage user bypass timeouts for interactive blocking,
- determine URL cache lookup behavior and traffic inspection settings, and
- enable threat intelligence and DNS reputation enforcement features.

General advanced settings configuration options

These are the general advanced settings that you can configure for an access control policy:

- **Maximum URL characters to store in connection events**—Sets the maximum character length of each URL requested by users in end-of-connection events. Disabling or limiting the number of stored URL characters might improve system performance. The default is 1024. The range is 0 to 4096.

  Set the length to 0 to disable URL logging. Storing zero characters does not affect URL filtering. The system filters traffic based on requested URLs even though the system does not record them.

- **Allow an Interactive Block to bypass blocking for (seconds)**—Sets the time allowed for browsing after the user bypasses a URL filtering block. After the timeout expires, the user must bypass the block again. The default is 600 seconds (10 minutes). The range is 0 to 31536000 (8760 hours).

  Setting this value to 0 means the interactive block response is displayed once and the user bypass never expires.

- **Retry URL cache miss lookup**—This setting determines what the system does when it needs to look up a URL's category and reputation in the cloud.

  The first time the system encounters a URL that does not have a locally stored category and reputation, it looks up that URL in the cloud and adds the result to the local data store. This allows faster processing of that URL in the future.

  By default, this setting is enabled. The system momentarily delays the traffic while it checks the cloud for the URL's reputation and category, and uses the cloud verdict to handle the traffic.

  If you disable this setting, when the system encounters a URL that is not in its local cache, the traffic is immediately passed and handled according to the rules configured for uncategorized and reputationless traffic.

  In passive deployments, the system does not retry the lookup, as it cannot hold packets.

- **Enable Threat Intelligence Director**—Whether to use Threat Intelligence Director. Disable this option to stop publishing TID data to your configured devices. The default is enabled. For more information, see Set up Threat Intelligence Director, on page 2126.

- **Enable reputation enforcement on DNS traffic**—Whether to have the system evaluate domain category and reputation early in URL transactions, when the browser looks up the domain name to get the IP address. Enable this option to improve URL filtering performance and efficacy. The default is enabled. For details and additional instructions, see DNS filtering, on page 1665 and subtopics.

- **Inspect traffic during policy apply**—Whether to inspect traffic when you deploy configuration changes unless specific configurations require restarting the Snort process. The default is enabled.

  When this option is enabled, resource demands could result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. The assigned device determines whether traffic drops during this interruption or passes without further inspection. See Snort restart scenarios, on page 127 for more information.

TLS server identity discovery

TLS server identity discovery is an access control policy advanced setting that enables early application detection and URL categorization for encrypted traffic.

TLS server identity discovery configuration

The latest version of the Transport Layer Security (TLS) protocol 1.3, defined by RFC 8446, is the preferred protocol for many web servers to provide secure communications. Because the TLS 1.3 protocol encrypts the server's certificate for additional security, and the certificate is needed to match application and URL filtering criteria in access control rules, the Firepower System provides a way to extract the server certificate *without* decrypting the entire packet.

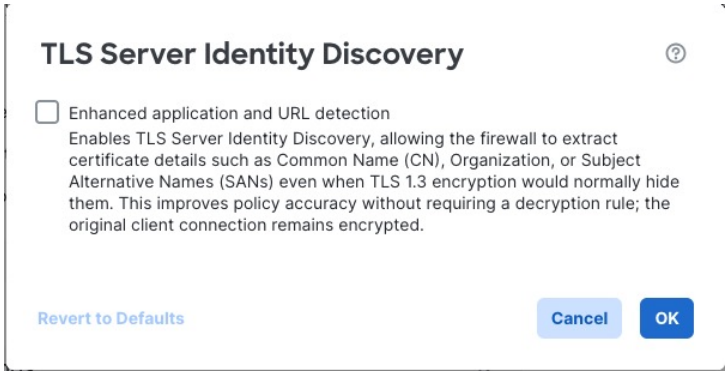
You can enable this feature, referred to as *TLS server identity discovery*, when you configure advanced settings for an access control policy. Certain features are not supported, such as STARTTLS traffic, the HTTP CONNECT method, and in a network where another device is already decrypting traffic.

If you enable this option, we recommend you also enable the decryption policy's advanced TLS adaptive server identity probe option as well. Together, these options enable more efficient decryption of TLS 1.3 traffic. For more information, see TLS 1.3 decryption best practices, on page 1743.

When a new connection starts that will be affected by TLS server identity discovery, the Firewall Threat Defense holds the original ClientHello packet to determine the identity of the server to which it connects before continuing. The Firewall Threat Defense device sends a specialized connection from the Firewall Threat Defense to the server. The server's response includes the server certificate, the specialized connection is terminated, and the original connection is evaluated as required by the access control policy.

TLS server identity discovery prioritizes the certificate's Common Name (CN) over the Server Name Indication (SNI).

To enable TLS server identity discovery, click the **Advanced** tab, click **Edit** (✎) for the setting, and select **Early application detection and URL categorization**.



We strongly recommend enabling it for any traffic you want to match on application or URL criteria, especially if you want to perform deep inspection of that traffic. An decryption policy is not required because *traffic is not decrypted* in the process of extracting the server certificate.

Note

- TLS server identity discovery *cannot* be used with any of the following:
  - STARTTLS traffic
  - The HTTP CONNECT method
  - Traffic that is already being decrypted by another device on the network
- Because the certificate is decrypted, TLS server identity discovery can reduce performance depending on the hardware platform.
- TLS server identity discovery is not supported in inline tap mode or passive mode deployments.
- Enabling TLS server identity discovery is supported on any Secure Firewall Threat Defense Virtual version deployed in AWS. TLS server identity is incompatible with certain deployment scenarios that involve Gateway Load Balancer (GWLB). Whether the device initiates a server certificate probe depends on its deployment method with GWLB and the traffic direction.
  - Geneve single-arm flow: The probe *is not initiated* for either east–west or north–south traffic. A connection event **PROBE_FLOW_DROP_BYPASS_PROXY** increments every time the device attempts to extract the server certificate.
  - Geneve dual-arm flow: The probe *is initiated only* for north–south traffic.
- TLS Server Identity Discovery also operates on TLS 1.2 sessions.

Intelligent application bypass

Intelligent application bypass (IAB) is a security feature that

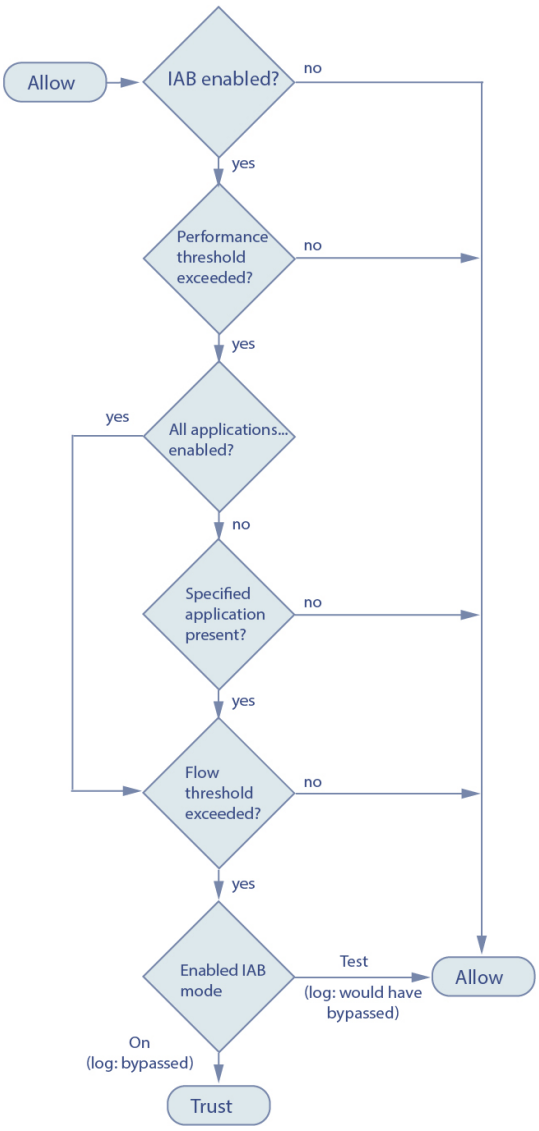
- identifies applications that you trust to traverse your network without further inspection if performance and flow thresholds are exceeded
- implements on traffic allowed by access control rules or the access control policy's default action, before the traffic is subject to deep inspection, and
- can be configured so that when an inspection performance threshold is exceeded, IAB trusts all traffic that exceeds any flow bypass threshold, regardless of the application type.

Additional information

For example, if a nightly backup significantly impacts system performance, you can configure thresholds that, if exceeded, trust traffic generated by your backup application.

A test mode allows you to determine whether thresholds are exceeded and, if so, to identify the application flows that would have been bypassed if you had actually enabled IAB (called *bypass mode*).

This graphic illustrates the IAB decision-making process:



Configure intelligent application bypass

This task enables intelligent application bypass (IAB) to improve system performance by bypassing inspection of specified traffic when performance thresholds are exceeded.

Not all deployments require IAB, and those that do might use it in a limited fashion. Do not enable IAB unless you have expert knowledge of your network traffic, especially application traffic, and system performance, including the causes of predictable performance issues. Before you run IAB in bypass mode, make sure that trusting the specified traffic does not expose you to risk.

Before you begin

IAB settings are applicable for Snort2 devices or pre 7.2.0 Snort3 devices. For Snort 3 devices, use elephant flow detection instead.

Follow these steps to configure intelligent application bypass:

Procedure

Step 1 In the access control policy editor, click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line. Then, click **Edit** ( ) next to **Intelligent Application Bypass Settings**.

Step 2 Set the enabled **State** for IAB.

Turn IAB **Off** or **On**, or enable IAB in **Test** mode.

In test mode, connection events and dashboards tell you what the system would have done if IAB had been on, but traffic is not impacted. Use test mode to check your configuration.

Step 3 Set the **Performance Sample Interval**.

The **Performance Sample Interval** specifies the time in seconds between IAB performance sampling scans, during which the system collects system performance metrics for comparison to IAB performance thresholds. The default is 5 seconds. The range is 1 to 1000 seconds.

Step 4 Select the **Bypassable Applications and Filters**.

Choose from:

- ***X* Applications/Filters**—Click the link and select the applications or application filters whose traffic you want to bypass. You can select by general attributes, specific applications, or both. For example, you could limit bypassable traffic to very low risk applications only.
- **All applications including unidentified applications**—Do not restrict bypass. When an inspection performance threshold is exceeded, IAB trusts all traffic that exceeds any flow bypass threshold, regardless of the application type. This is the default.

Step 5 Configure the performance and flow thresholds.

You must configure at least one **Inspection Performance Thresholds** and one **Flow Bypass Thresholds**. However, all have defaults and you do not need to change the settings if the defaults are appropriate for your network.

When a performance threshold is exceeded, the system examines flow thresholds and, if one threshold is exceeded, trusts the specified traffic. If you enable more than one of either, only one of each must be exceeded.

a) Click **Configure** under **Inspection Performance Thresholds** and configure the options.

Inspection performance thresholds provide intrusion inspection performance limits that, if exceeded, trigger the inspection of flow thresholds. Inspection performance thresholds set to 0 are ignored.

You can configure one or more of these thresholds:

- **Drop Percentage**—The average packets dropped as a percentage of total packets, when packets are dropped because of performance overloads caused by expensive intrusion rules, file policies, decompression, and so on. This does not refer to packets dropped by normal configurations such as intrusion rules.

  Note that specifying an integer greater than 1 activates IAB when the specified percentage of packets is dropped. When you specify 1, any percentage from 0 through 1 activates IAB. This allows a small number of packets to activate IAB.

  The default is 5%. The range is 0 to 100.

- **Processor Utilization Percentage**—Average percentage of processor resources used. The default is 95. The range is 0 to 100.
- **Packet Latency**—The average packet latency in microseconds. The default is 1000. The range is 0 to 1000000.
- **Flow Rate**—The rate at which the system processes flows, measured as the number of flows per second. Note that this option configures IAB to measure flow *rate*, not flow *count*. The default is 0. The range is 0 to 1000000.

b) Click **Configure** under **Flow Bypass Thresholds** and configure the options.

Flow bypass thresholds provide flow limits that, if exceeded, trigger IAB to trust bypassable application traffic in bypass mode or allow application traffic subject to further inspection in test mode. Flow bypass thresholds set to 0 are ignored.

You can configure one or more of these flow bypass thresholds:

- **Bytes per Flow**—The maximum number of kilobytes a flow can include. The default is 500000. The range is 0 to 2147483647.
- **Packets per Flow**—The maximum number of packets a flow can include. The default is 0. The range is 0 to 2147483647.
- **Flow Duration**—The maximum number of seconds a flow can remain open. The default is 0. The range is 0 to 2147483647.
- **Flow Velocity**—The maximum transfer rate in kilobytes per second. The default is 250000. The range is 0 to 2147483647.

Step 6 Click **OK** to save IAB settings.

Step 7 Click **Save** to save the policy.

Intelligent application bypass is configured for the access control policy with the specified performance and flow thresholds.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

IAB logging and analysis

IAB logging and analysis is a monitoring system that

- forces an end-of-connection event. This event logs both bypassed flows and flows that would have been bypassed, regardless of whether you have enabled connection logging
- provides connection events. These events indicate when flows are bypassed in bypass mode or would have been bypassed in test mode, and
- enables custom dashboard widgets and reports based on connection events. These widgets and reports display long-term statistics for bypassed and would-have-bypassed flows.

IAB connection events

IAB connection events provide specific information about bypassed and would-have-bypassed flows through these key fields:

- Action: When **Reason** includes `Intelligent App Bypass`:
  - **Allow**—indicates that the applied IAB configuration was in test mode and traffic for the application specified by **Application Protocol** remains available for inspection.
  - **Trust**—indicates that the applied IAB configuration was in bypass mode and traffic for the application specified by **Application Protocol** has been trusted to traverse the network without further inspection.
- Reason: `Intelligent App Bypass` indicates that IAB triggered the event in bypass or test mode.
- Application Protocol: This field displays the application protocol that triggered the event.

You can create custom analysis dashboard widgets to display long-term IAB statistics based on connection events. Specify these settings when creating the widget:

- **Preset**: None
- **Table**: Application Statistics
- **Field**: any
- **Aggregate**: either of:
  - IAB Bypassed Connections
  - IAB Would Bypass Connections
- **Filter**: any

You can create custom reports to display long-term IAB statistics based on connection events. Specify these settings when creating the report:

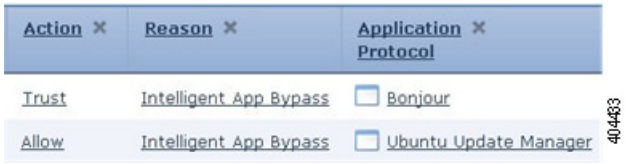
- **Table**: Application Statistics
- **Preset**: None
- **Filter**: any
- **X-Axis**: any
- **Y-Axis**: either of:
  - IAB Bypassed Connections
  - IAB Would Bypass Connections

Connection event examples

In the truncated graphic, some fields are omitted. The graphic shows the **Action**, **Reason**, and **Application Protocol** fields for two connection events resulting from different IAB settings in two separate access control policies.

For the first event, the `Trust` action indicates that IAB was enabled in bypass mode and Bonjour protocol traffic was trusted to pass without further inspection.

For the second event, the `Allow` action indicates that IAB was enabled in test mode, so Ubuntu Update Manager traffic was subject to further inspection but would have been bypassed if IAB had been in bypass mode.

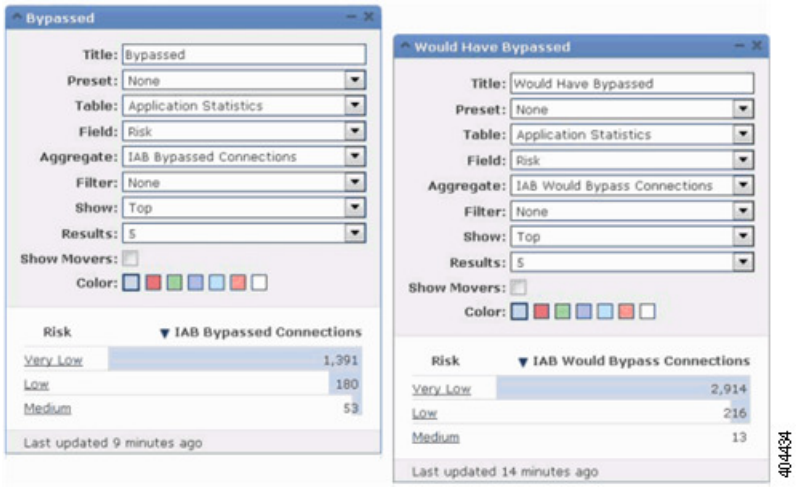


In the truncated graphic, some fields are omitted. The flow in the second event was both bypassed (**Action**: `Trust`; **Reason**: `Intelligent App Bypass`) and inspected by an intrusion rule (**Reason**: `Intrusion Monitor`). The `Intrusion Monitor` reason indicates that an intrusion rule set to **Generate Events** detected but did not block an exploit during the connection. In the example, this happened before the application was detected. After the application was detected, IAB recognized the application as bypassable and trusted the flow.



In the custom analysis dashboard widget examples:

- The *Bypassed* example shows statistics for application traffic bypassed because the applications were specified as bypassable and IAB was enabled in bypass mode in the deployed access control policy.
- The *Would Have Bypassed* example shows statistics for application traffic that would have been bypassed because the applications were specified as bypassable and IAB was enabled in test mode in the deployed access control policy.



The graphic shows two abbreviated report examples:

- The *Bypassed* example shows statistics for application traffic bypassed because the applications were specified as bypassable and IAB was enabled in bypass mode in the deployed access control policy.
- The *Would Have Bypassed* example shows statistics for application traffic that would have been bypassed because the applications were specified as bypassable and IAB was enabled in test mode in the deployed access control policy.



Transport/network layer preprocessor settings

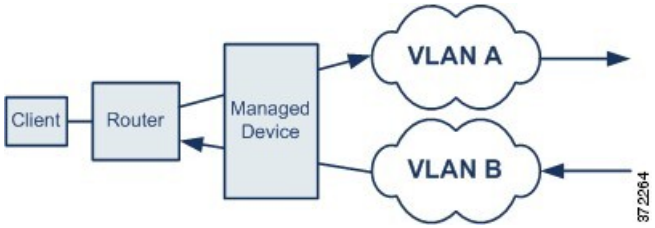
Transport/network layer preprocessor settings are access control policy configurations that

- apply globally to all networks, zones, and VLANs where you deploy your access control policy
- control how the system handles VLAN headers, active responses, and connection tracking, and
- affect traffic reassembly and rule processing for transport and network layer communications.

Configuration options

These settings control various aspects of transport and network layer processing:

- **Ignore the VLAN header when tracking connections**—Whether to ignore or include VLAN headers when identifying traffic. Different VLAN tags in traffic traveling in different directions for the same connection can affect traffic reassembly and rule processing. For example, traffic for the same connection could be transmitted over VLAN A and be received over VLAN B. Select this option if the device might see different VLANs for the same connection. This option is off by default.



- **Maximum Active Responses**—For a TCP connection that triggers a preprocessor/intrusion drop rule that is configured to provide an active response, the maximum number of active responses per TCP connection. When additional traffic occurs on a connection where an active response has been initiated, and the traffic occurs more than **Minimum Response Seconds** after a previous active response, the system sends another active response unless the specified maximum has been reached. A setting of 0 disables additional active responses triggered active response rules. The default is no limit. The range is 0 to 25.

Note You have to specifically configure drop rules to provide active responses. For TCP connections, the active response is a RESET packet. For UDP connections, the system sends an ICMP unreachable packet to the source of the connection.

- **Minimum Response Seconds**—Until **Maximum Active Responses** occur, specifies the number of seconds to wait before any additional traffic on a connection where the system has initiated an active response results in a subsequent active response. The default is no limit. The range is 1 to 300.
- **Session Termination Logging Threshold**—Do not modify this option unless instructed to do so by Cisco Technical Support.

  Support might ask you during a troubleshooting call to configure your system to log a message when an individual connection exceeds the specified threshold. Changing the setting for this option will affect performance and should be done only with Support guidance. This option specifies the number of bytes that result in a logged message when the session terminates and the specified number was exceeded. The upper limit is 1GB.

Detection enhancement settings

Detection enhancement settings are adaptive profile configurations that

- determine whether adaptive profiles are used for application detection and intrusion rules in the access control policy
- enable the system to adapt processing behavior using host information either detected by network discovery or imported from a third party, and
- provide control over profile update frequency and network scope for performance optimization.

Detection enhancement setting options

Typically, the system uses the static settings in your network analysis policy to preprocess and analyze traffic. With adaptive profile updates enabled, the system adapts processing behavior using host information detected by network discovery or imported from a third party.

Note To enable adaptive profiles in Snort 3, you must select both the **Enable** and **Enable Profile Updates** options.

The detection enhancement settings include these options:

- **Enable**—You must enable adaptive profiling (its default state) for access control rules to perform application and file control, including malware protection (AMP), and for intrusion rules to use service metadata.
- **Enable Profile Updates**—Profile updates, like the target-based profiles you can configure manually in a network analysis policy, help to defragment IP packets and reassemble streams in the same way as the operating system on the target host. The intrusion rules engine then analyzes the data in the same format as that used by the destination host. Profile updates also compare metadata in an intrusion rule to host information to determine whether a rule should apply for a particular host. For more information, see:

- Adaptive profile updates, on page 2183
- Adaptive profile updates and recommended rules, on page 2184

- **Adaptive Profiles – Attribute Update Interval**—When profile updates are enabled, you can control how frequently in minutes network map data is synced from the management center to its managed devices. The system uses the data to determine what profiles should be used when processing traffic. Increasing the value for this option can improve performance in a large network.
- **Adaptive Profiles – Networks**—Optionally, when profile updates are enabled, you can improve performance by constraining profile updates to a comma-separated list of IP addresses, address blocks, and network variables. If you use a network variable, the system uses the variable's value in the variable set linked to the default intrusion policy for your access control policy. For example, you could enter 192.168.1.101, 192.168.4.0/24, or $HOME_NET. IPv4 and IPv6 are supported.

  The default value (0.0.0.0/0) applies adaptive profile updates to all networks.

Adaptive profile updates

An adaptive profile update is a network analysis feature that

- adapts processing behavior using host information either detected by network discovery or imported from a third party
- switches to the appropriate operating system profile based on the operating system in the host profile for the target host, and
- helps to defragment IP packets and reassemble streams in the same way as the operating system on the target host.

Adaptive profile operation

Typically, the system uses the static settings in your network analysis policy to preprocess and analyze traffic. With adaptive profile updates, the system can adapt processing behavior using host information either detected by network discovery or imported from a third party.

Profile updates, like the target-based profiles you can configure manually in a network analysis policy, help to defragment IP packets and reassemble streams in the same way as the operating system on the target host. The intrusion rules engine then analyzes the data in the same format as that used by the destination host.

Manually configured target-based profiles apply either the default operating system profile you select, or profiles you bind to specific hosts. Profile updates, however, switch to the appropriate operating system profile based on the operating system in the host profile for the target host.

Adaptive profile update scenario

Consider a scenario where you configure profile updates for the 10.6.0.0/16 subnet and set the default IP Defragmentation target-based policy to Linux. The Firewall Management Center where you configure the settings has a network map that includes the 10.6.0.0/16 subnet.

- When the system detects traffic from Host A, which is not in the 10.6.0.0/16 subnet, it uses the Linux target-based policy to reassemble IP fragments.

- When the system detects traffic from Host B, which is in the 10.6.0.0/16 subnet, it retrieves Host B's operating system data from the network map. The system uses a profile based on that operating system to defragment the traffic destined for Host B.

Adaptive profile updates and recommended rules

Adaptive profile updates and recommended rules are security features that

- compare metadata in a rule to host information to determine whether a rule should apply for a particular host
- provide different approaches to rule optimization, with adaptive profiles applying rules dynamically on a packet-by-packet basis while recommended rules provide suggestions for rule state changes, and
- can be used in combination to ensure appropriate rule enablement and efficient rule application for specific traffic.

Feature characteristics and differences

The adaptive profile updates feature is an advanced setting in an access control policy that applies globally to all intrusion policies invoked by that access control policy. The Cisco recommended rules feature applies to the individual intrusion policy where you configure it.

Like recommended rules, profile updates compare metadata in a rule to host information to determine whether a rule should apply for a particular host. However, while recommended rules provide recommendations for enabling or disabling rules using that information, profile updates use the information to apply specific rules to specific traffic.

This table compares the key differences between adaptive profile updates and recommended rules:

Recommended rules require your interaction to implement suggested changes to rule states. Profile updates, on the other hand, do not modify intrusion policies. Treatment of rules based on profile updates happens on a packet-by-packet basis.

Additionally, recommended rules can result in enabling disabled rules. Profile updates, in contrast, only affect the application of rules that are already enabled in intrusion policies. Profile updates never change the rule state.

You can use profile updates and recommended rules in combination. Profile updates use the rule state for a rule when your intrusion policy is deployed to determine whether to include it as a candidate for applying, and your choices to accept or decline recommendations are reflected in that rule state. You can use both features to ensure that you have enabled or disabled the most appropriate rules for each network you monitor, and then to apply enabled rules most efficiently for specific traffic.

Performance settings

Performance settings are access control policy advanced settings that

- tune the performance of your system as it analyzes traffic for attempted intrusions
- apply to Snort and are relevant only if you apply intrusion policies in rules or as the default action, and
- should be changed only if you are a Snort intrusion rule expert, or at the direction of Cisco Technical Support.

Performance setting categories

These settings are organized into separate tabs for each group of settings:

- **Pattern Matching Limits**: The maximum number of events to queue and TCP payload detection options
- **Performance Statistics**: Time range and packet count settings for performance sampling
- **Regular Expression Limits**: PCRE matching and recursion limits
- **Intrusion Event Logging Limits**: Event queue and logging configuration

Pattern Matching Limits include these options:

- **Maximum Pattern States to Analyze Per Packet**: The maximum number of events to queue. The default is 5.
- **Disable Content Checks on Traffic Subject to Future Reassembly**: Whether to detect TCP payload before reassembly. It includes inspection of packets before and after stream reassembly. This process requires more processing overhead and may decrease performance. If the option is not selected, the TCP payload is detected after reassembly. The default is off.

Performance Statistics settings control when the system updates performance statistics. When the number of seconds specified elapses between performance statistics updates, the system verifies it has analyzed the specified number of packets. If it has, the system updates performance statistics. Otherwise, the system waits until it analyzes the specified number of packets.

- **Sample time (seconds)**: The time range for taking a performance sample. The default is 300 seconds.

  Configuring a very low value (for example, 1 second) for the sample time can cause a huge impact on the device; the performance statistics logged on the device can cause disk space issues and affect the operation of the device. Hence, we recommend you do not configure a very low value.

- **Minimum number of packets**: How many packets to consider the minimum for a valid performance statistic. The default is 0.
- **Troubleshooting Options**:
  - **Log Session/Protocol Distribution**: Support might ask you during a troubleshooting call to enable this option to configure the system to calculate the performance statistics only when the Snort process is shut down or restarted.
  - **Summary**: Enable this option only if instructed by Cisco Technical Support.

Regular Expression Limits ensure a minimum level of performance. The default Perl compatible regular expression (PCRE) limits ensure a minimum level of performance. Overriding these limits could increase security but could also significantly impact performance by permitting packet evaluation against inefficient regular expressions.

- **Match Limit State**: The limit for matching regular expressions. You can select **Default Value**, which is 3500, **Unlimited**, or **Custom**. If you select custom, specify the number of times to attempt to match a pattern defined in a PCRE regular expression in **Match Limit**. Specify 0 to completely disable PCRE match evaluations.
- **Match Recursion Limit State**: The limit for matching regular expression recursions. You can select **Default Value**, which is 3500, **Unlimited**, or **Custom**. If you select custom, specify the number of

recursions when evaluating a PCRE regular expression against the packet payload in **Match Recursion Limit**. Specify 0 to completely disable PCRE recursions.

Note For a custom match recursion limit to be meaningful, it must be smaller than the match limit.

Intrusion Event Logging Limits control event queuing and reporting. When the intrusion rules engine evaluates traffic against rules, it places the events generated for a given packet or packet stream in an event queue, then reports the top events in the queue to the user interface. When configuring the intrusion event logging limits, you can specify how many events can be placed in the queue and how many are logged, and select the criteria for determining event order within the queue.

- **Maximum Events Stored Per Packet**: The maximum number of events that can be stored for a given packet or packet stream. The default is 8.
- **Maximum Events Logged Per Packet**: The number of events logged for a given packet or packet stream. This cannot exceed the **Maximum Events Stored Per Packet** value. The default is 5.
- **Prioritize Events Logging By**: The value used to determine event ordering within the event queue. The highest ordered event is reported through the user interface. You can select:
  - **Content Length** (the default), which orders events by the longest identified content match. When events are ordered by content length, rule events always take precedence over decoder and preprocessor events.
  - **Priority**, which orders events in the queue by the event priority.

Latency-based performance settings

Latency-based performance settings are policy configurations that

- use thresholding to manage packet and rule processing performance,
- apply to Snort and are relevant only if you apply intrusion policies in rules or as the default action, and
- are automatically populated by the latest deployed intrusion rule update by default.

Performance setting behavior

By default, latency-based performance settings for both packet and rule handling are automatically populated by the latest deployed intrusion rule update, and we recommend that you do not change the default. Change these settings only if you are a Snort intrusion rule expert, or at the direction of Cisco Technical Support.

The latency settings that are applied depend on the security level of the network analysis policy (NAP) associated with the access control policy. Generally, this is the default NAP policy. However, if custom network analysis rules are configured, and if any of these specify a NAP policy that is more secure than the default NAP policy, then latency settings are based on the most secure NAP policy among the custom rules. If the default NAP policy or any custom rules invoke a custom NAP policy, then the security level used in the evaluation is the system-provided base policy on which each custom NAP policy is based.

The above is true regardless of whether the effective threshold and/or network analysis configurations are inherited or configured directly in the policy.

Use these settings to tune the latency-based performance of your system:

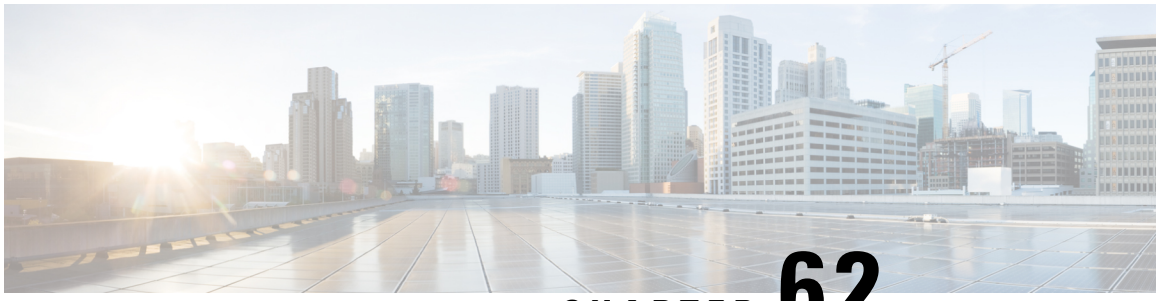
- **Apply Settings From**: Whether to apply latency-based performance settings from an **Installed Rule Update**, the default, or from your **Custom** settings.
- **Packet Handling**: Packet latency thresholding measures the total elapsed time taken to process a packet by applicable decoders, preprocessors, and rules, and ceases inspection of the packet if the processing time exceeds a configurable threshold. By default, the latency-based performance setting for packet handling is disabled. You may choose to enable it. However, Cisco recommends that you do not change the default value for the threshold setting. Select **Enabled** to turn it on. If you selected **Custom**, also enter the **Threshold** time in microseconds for when inspection of a packet should cease. The default is 256.
- **Rule Handling**: Rule latency thresholding measures the elapsed time each rule takes to process an individual packet, suspends the violating rule along with a group of related rules for a specified time if the processing time exceeds the rule latency threshold a configurable consecutive number of times, and restores the rules when the suspension expires. You can configure these options only if you select **Custom**.
  - **Enabled**: This option is selected automatically if you select custom. If you do not want use this feature, deselect the option. All other settings on this tab require the feature to be enabled.
  - **Threshold (microseconds)**: Specifies the time in microseconds that rules should not exceed when examining a packet. The default is 512.
  - **Consecutive Threshold Violations Before Suspending Rule**: Specifies the consecutive number of times rules can take longer than the time set for threshold to inspect packets before rules are suspended. The default is 3.
  - **Suspension Time**: How long a suspended rule should be suspended. The default is 10.

History for advanced settings for the access control policy

This reference provides a comprehensive history of feature changes by release for advanced settings for the access control policy, helping administrators track the evolution and capabilities of access control policy configurations across different software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Improved portscan detection.	7.2	7.2 running Snort 3	With an improved portscan detector, you can easily configure the system to detect or prevent portscans. You can refine the networks you want to protect, set the sensitivity, and so on. For devices running Snort 2 and for devices running Version 7.1 and earlier, continue to use the network analysis policy for portscan detection. New/modified screens: We added **Threat Detection** to the access control policy's Advanced tab. New/Modified commands: **clear threat-detection portscan**, **show threat-detection portscan**.
Bypass inspection or throttle elephant flows on Snort 3 devices.	7.2.0	7.2.0 with Snort 3	You can now detect and optionally bypass inspection or throttle elephant flows. By default, access control policies are set to generate an event when the system sees an unencrypted connection larger than 1 GB/10 sec; the rate limit is configurable. For the Firepower 2100 series, you can detect elephant flows but not bypass inspection or throttle. For devices running Snort 2 and for devices running Version 7.1 and earlier, continue to use Intelligent Application Bypass (IAB). New/modified screens: We added **Elephant Flow Settings** to the access control policy's Advanced tab. For more information, see Elephant Flow Detection.
DNS filtering	7.0.0 6.7.0 (experimental)	Any	If URL filtering is enabled and configured, a new option to enhance category and reputation filtering efficacy is enabled by default for each new access control policy. For more information, see DNS filtering, on page 1665 and subtopics. The Advanced tab of access control policy has a new option under General Settings: **Enable reputation enforcement on DNS traffic**.
TLS server identity discovery	6.7.0	Any	Enable access control policies to evaluate URL and application conditions when a client connects to a TLS 1.3-enabled server. TLS server identity discovery enables these conditions to be evaluated without decrypting traffic. Enabling this feature can impact device performance, depending on model. The Advanced tab page of access control policy has new options: • Warning is displayed on the Advanced tab; moving the slider to the right enables TLS server identity discovery. • New option on the Advanced tab page: **TLS Server Identity Discovery**.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Threat Defense Service Policy.	6.3	Any	You can now configure a Threat Defense Service Policy as part of your access control policy advanced options. You can use Threat Defense Service Policies to apply services to specific traffic classes. Features supported include TCP State Bypass, randomizing TCP sequence numbers, decrementing the time-to-live (TTL) value on packets, Dead Connection Detection, setting a limit on the maximum number of connections and embryonic connections per traffic class and per client, and timeouts for embryonic, half closed, and idle connections. New screen: **Policies** > **Access Control** > **Access Control**, **Advanced** tab, **Threat Defense Service Policy**. Supported platforms: Secure Firewall Threat Defense



CHAPTER 62

Service Policies

- Threat defense service policies, on page 2191
- Requirements and prerequisites for service policies, on page 2193
- Guidelines and limitations for service policies, on page 2193
- Configure threat defense service policies, on page 2194
- Monitor service policies, on page 2203
- Examples for service policy rules, on page 2204
- History for threat defense service policy, on page 2208

Threat defense service policies

Use Threat Defense service policies to apply services to specific traffic classes. Service policies let you apply different services to different connections entering the device or interface.

For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications. A service policy consists of multiple actions or rules applied to an interface or applied globally.

Traffic class types

A traffic class is a combination of the interface and an extended access control list (ACL). The ACL "allow" rules determine which connections are part of the class. Any "denied" traffic in the ACL simply does not have the service applied to it: these connections are not actually dropped. You can use IP addresses and TCP/UDP ports to identify matching connections as precisely as you require.

There are two types of traffic class:

- **Interface-based rules**—If you specify a security zone or interface group in a service policy rule, the rule applies to the ACL "allowed" traffic that goes through any interface that is part of the interface objects.

  Interface-based rules that are applied to the ingress interface always take precedence over global rules for any feature. If an ingress interface-based rule applies to a connection, the system ignores any matching global rule. If no ingress interface or global rule applies, then an interface service rule on the egress interface is applied.

- **Global rules**—These rules apply to all interfaces. If an interface-based rule does not apply to a connection, the global rules are checked and applied to any connections that the ACL "allows." If none apply, then the connections proceed without any services applied.

A given connection can match only one traffic class, either interface-based or global, for a given feature. There should be at most one rule for a given interface object/traffic flow combination.

Service policy rules are applied after access control rules. These services are configured only for connections you are allowing.

Service policy relationships with FlexConfig and other features

Connection-related service policy features are managed separately from other service-rule features, so overlapping traffic classes generally aren't an issue, but they should still be configured carefully.

Service policy feature interactions

Because connection-related service policy features are treated as a separate feature group from other service-rule implemented features, you should not run into problems with overlapping traffic classes. However, please be mindful when configuring these features:

- QoS policy rules: QoS policy rules are implemented using the service policy CLI. These rules are applied before connection-based service policy rules. However, both QoS and connection settings can be applied to the same or overlapping traffic classes.
- FlexConfig policies: You can use FlexConfig policies to implement custom application inspections and NetFlow. Use the **show running-config** command to examine the CLI that already configures service rules, including the **policy-map**, **class-map**, and **service-policy** commands. Netflow and application inspection are compatible with QoS and connection settings, but you need to understand the existing configuration before implementing FlexConfig. Connection settings are applied before application inspections and Netflow.



Note Traffic classes that are created from the Threat Defense service policy are named **class_map_***ACLname*, where *ACLname* is the name of the extended ACL object used in the service policy rule.

Connection settings

Connection settings refer to a variety of features that manage connections through a device.

Connection setting types

Connection settings include these types:

- **Global timeouts for various protocols**—All global timeouts have default values. Change them only if you experience premature connection loss. You configure global timeouts in the Threat Defense platform policy. Select **Devices** > **Platform Settings**.
- **Connection timeouts per traffic class**—You can override the global timeouts for specific types of traffic using service policies. All traffic class timeouts have default values, so you do not have to set them.
- **Connection limits and TCP Intercept**—By default, there are no limits on how many connections can go through (or to) the Firewall Threat Defense. Use service policy rules to set limits on particular traffic classes. This protects servers from denial of service attacks. Particularly, you can set limits on embryonic connections (those that have not finished the TCP handshake), which protects against SYN flooding

attacks. When embryonic limits are exceeded, the TCP Intercept component activates to proxy connections and throttle attacks.

- **Dead connection detection (DCD)**—Enable dead connection detection if you have persistent connections that are valid but often idle. These connections may get closed when they exceed idle timeout settings. Dead connection detection identifies idle but valid connections and keeps them alive by resetting their idle timers. Whenever idle times are exceeded, DCD probes both sides of the connection to see if both sides agree that the connection is valid. The **show service-policy** command output includes counters to show the amount of activity from DCD. You can use the **show conn detail** command to get information about the initiator and responder and how often each has sent probes.
- **TCP sequence randomization**—Each TCP connection has two initial sequence numbers (ISN): one generated by the client and one generated by the server. By default, the Firewall Threat Defense randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions. Randomization prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session. However, TCP sequence randomization effectively breaks TCP SACK (Selective Acknowledgement), as the sequence numbers the client sees are different from what the server sees. You can disable randomization per traffic class if desired.
- **TCP normalization**—The TCP Normalizer protects against abnormal packets. You can configure how some types of packet abnormalities are handled by traffic class. You can configure TCP Normalization using the FlexConfig policy.
- **TCP state bypass**—You can bypass TCP state checking if you use asymmetrical routing in your network.

Requirements and prerequisites for service policies

- You must have one of these user roles: **Admin**, **Access Admin**, or **Network Admin**.
- Assign an access control policy to each target device before you add or edit service-policy rules.
- Create an extended access control list (ACL) for each traffic class. Include **Allow** rules for the connections that should receive the service.
- For interface-based rules, configure the interfaces on the target devices and add them to security zones or interface groups.

Guidelines and limitations for service policies

Service policies apply to routed or switch interfaces only, in either routed or transparent mode. They do not apply to inline set or passive interfaces.

You can configure up to 25 traffic classes for an interface or the global policy.

- Global policy: You can configure up to 25 service policy rules for a given security zone or interface group.
- Interface-based rules: The limit applies to the interfaces themselves, not to each zone or interface group. Because an interface can belong to both a security zone and an interface group, the number of rules allowed for a zone or group might be lower than 25, depending on its member interfaces.

You can have at most one rule for a given interface object/traffic flow combination.

When you make service policy changes to the configuration, all new connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. If you want all connections to immediately use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. Use an SSH or Console CLI session to enter the **clear conn** or **clear local-host** commands.

QoS rules and service policy rules (in the access control policy) are translated to commands on the firewall. This includes creating policy maps. There can be only one policy map per interface. The system automatically combines QoS and service policy configurations in a single policy map per interface.

However, you can also create policy maps manually using FlexConfig. For lower-end firewalls, such as the Secure Firewall 3100, you can create up to 64 policy maps in the configuration. For more powerful firewalls, such as the Firepower 4100, you can create up to 128. Be careful not to exceed this limit, or deployment will fail. You can view the device configuration from the CLI or use the deployment transcript to see how rules are translated to commands.

Configure threat defense service policies

A service policy consists of multiple actions or rules applied to an interface or applied globally. Use Threat Defense service policies to apply services to specific traffic classes.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**, and click **Edit** ( ) for the access control policy whose Threat Defense service policy you want to edit.

Step 2 Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 3 Click **Edit** ( ) in the **Threat Defense Service Policy** group.

A dialog box opens that shows the existing policy. The policy consists of an ordered list of rules, separated between global rules (which apply to all interfaces) and interface-based rules. The table shows the interface object and extended access control list name (which combined defines the traffic class for the rule), and the services applied.

Step 4 Do any of the following:

- Click **Add Rule** to create a new rule. See Configure a service policy rule, on page 2195.
- Click **Edit** ( ) to edit an existing rule. See Configure a service policy rule, on page 2195.
- Click **Delete** ( ) to delete a rule.
- Click a rule and drag it to a new location to move it. You cannot drag rules between the interface and global lists. Instead you must edit the rule to change the interface/global setting. The first rule in the list that matches a connection is applied to the connection.

Step 5 Click **OK** when you are finished editing the policy.

Step 6 Click **Save** on the **Advanced** window. The changes are not saved until you click **Save**.

Configure a service policy rule

Service policy rules allow you to control and customize how network traffic is handled by applying specific services and connection settings to defined traffic classes.

Before you begin

Go to **Objects** > **Object Management** > **Access List** > **Extended** and create an extended access list that defines the traffic to which the rule applies. The rule is applied to any connections that match Allow rules in the extended access list. Define the ACL rules precisely, so that your service policy rule applies to only the traffic that requires the service.

If you are creating an interface-based rule, you must also have configured the interfaces on the assigned devices and added them to security zones or interface groups.

Procedure

Step 1 If you are not already in the Threat Defense service policy dialog box, choose **Policies** > **Access Control heading** > **Access Control**, edit the access control policy, select **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line, then edit the **Threat Defense Service Policy**.

Step 2 Do any of the following:

- Click **Add Rule** to create a new rule.
- Click **Edit** ( ) to edit an existing rule.

The service policy rule wizard opens to step you through the process of configuring the rule.

Step 3 In the **Interface Object** step, select the option that defines the interfaces that will use the policy.

- **Apply Globally**—Select this option to create a global rule, which applies to all interfaces.
- **Select Interface Objects**—Select this option to create an interface-based rule. Then, select the security zones or interface objects that contain the desired interfaces, and click **Add** to move them to the selected list. The service policy rule will be configured on each interface contained in the selected objects; it is not configured on the zone/group itself.

Click **Next** when the interface criterion is complete.

Step 4 In the **Traffic Flow** step, select the extended ACL object that defines the connections to which the rule applies, then click **Next**.

Step 5 In the **Connection Setting** step, configure the services to apply to this traffic class.

- **Enable TCP State Bypass** (TCP connections only)—Implement TCP state bypass. Connections subject to TCP state bypass are not inspected by any inspection engines, and they bypass all TCP state checking and TCP normalization. For detailed information, see Bypass TCP state checks for asymmetrical routing (TCP state bypass), on page 2198.

Note Use TCP state bypass for troubleshooting purposes or when asymmetric routing cannot be resolved. This feature disables multiple security features, which can cause a high number of connections if you do not implement it properly with a narrowly defined traffic class.

- **Randomize TCP Sequence Number** (TCP connections only)—Whether to enable or disable TCP sequence number randomization. Randomization is enabled by default. For more information, see Disable TCP sequence randomization, on page 2202.
- **Enable Decrement TTL** (TCP connections only)—Decrement the time-to-live (TTL) on packets that match the class. If you decrement time to live, packets with a TTL of 1 will be dropped, but a connection will be opened for the session on the assumption that the connection might contain packets with a greater TTL. Note that some packets, such as Open Shortest Path First (OSPF) hello packets, are sent with TTL = 1, so decrementing time to live can have unexpected consequences.

Note If you want the Firewall Threat Defense device to appear on traceroutes, you must configure the decrement TTL option and also set the Internet Control Message Protocol (ICMP) unreachable rate limit in the platform settings policy. See Configure the Firewall Threat Defense device to appear on traceroutes, on page 2207.

- **Connections**—Limits for the number of connections allowed for the entire class. You can configure these options:
  - **Maximum TCP and UDP** (TCP/UDP connections only)—The maximum number of simultaneous connections that are allowed, between 0 and 2000000, for the entire class. For TCP, this count applies to established connections only. The default is 0, which allows unlimited connections. Because the limit is applied to a class, one attacking host can consume all the connections and leave none for the rest of the hosts that are matched to the class. Set the per-client limit to ameliorate this problem.
  - **Maximum Embryonic** (TCP connections only)—The maximum number of simultaneous embryonic TCP connections (those that have not finished the TCP handshake) allowed, between 0 and 2000000. The default is 0, which allows unlimited connections. By setting a non-zero limit, you enable TCP intercept, which protects inside systems from a denial of service (DoS) attack perpetrated by flooding an interface with TCP SYN packets. Also set the per-client options to protect against SYN flooding. For more information, see Protect servers from a SYN flood DoS attack (TCP intercept), on page 2204.
- **Connections Per Client**—Limits for the number of connections allowed for a given client (source IP address). You can configure these options:
  - **Maximum TCP and UDP** (TCP/UDP connections only)—The maximum number of simultaneous connections allowed per client, between 0 and 2000000. For TCP, this includes established, half-open (embryonic), and half-closed connections. The default is 0, which allows unlimited connections. This option restricts the maximum number of simultaneous connections that are allowed for each host that is matched to the class.

- **Maximum Embryonic** (TCP connections only)—The maximum number of simultaneous embryonic TCP connections allowed per client, between 0 and 2000000. The default is 0, which allows unlimited connections. For more information, see Protect servers from a SYN flood DoS attack (TCP intercept), on page 2204.

- **Connections SYN Cookie MSS**—The server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit, from 48 to 65535 . The default is 1380. This setting is meaningful only if you configure **Maximum Embryonic** for connections or per-client, or both.
- **Connections Timeout**—The timeout settings to apply to the traffic class. These timeouts override the global timeouts defined in the platform settings policy. You can configure these options:
  - **Embryonic** (TCP connections only)—The timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:00:00. The default is 0:0:30.
  - **Half Closed** (TCP connections only)—The idle timeout period until a half-closed connection is closed, between 0:0:30 and 1193:0:0. The default is 0:10:0. Half-closed connections are not affected by dead connection detection (DCD). Also, the system does not send a reset when taking down half-closed connections.
  - **Idle** (TCP, UDP, ICMP, IP connections)—The idle timeout period after which an established connection of any protocol closes, between 0:0:1 and 1193:0:0. The default is 1:0:0, unless you select the TCP state bypass option, where the default is 0:2:0.
  - **Reset Connection Upon Timeout** (TCP connections only)—Whether to send a TCP RST packet to both end systems after idle connections are removed.
- **Detect Dead Connections** (TCP connections only)—Whether to enable dead connection detection (DCD). Before expiring an idle connection, the system probes the end hosts to determine if the connection is valid. If both hosts respond, the connection is preserved, otherwise the connection is freed. When operating in transparent firewall mode, you must configure static routes for the endpoints. You cannot configure DCD on connections that are also offloaded, so do not configure DCD on connections you are fast-pathing in the prefilter policy. Use the **show conn detail** command in the Firewall Threat Defense CLI to track how many DCD probes have been sent by the initiator and responder.

  Configure these options:
  - **Detection Timeout**—The time duration in hh:mm:ss format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15.

    For systems that are operating in a cluster or high-availability configuration, we recommend that you do not set the interval to less than one minute (0:1:0). If the connection needs to be moved between systems, the changes required take longer than 30 seconds, and the connection might be deleted before the change is accomplished.
  - **Detection Retries**—The number of consecutive failed retries for DCD before declaring the connection dead, from 1 to 255. The default is 5.

Step 6 Click **Finish** to save your changes.

The rule is added to the bottom of the appropriate list, either Interfaces or Global. Global rules are matched in top-down order. Rules in the Interfaces list are matched in top down order for each interface object. Place

rules for narrowly-defined traffic classes above broader rules, to ensure the right services get applied. You can move rules within each list by using drag and drop. You cannot move rules between lists.

Bypass TCP state checks for asymmetrical routing (TCP state bypass)

TCP state bypass allows traffic to bypass stateful inspection checks on Firewall Threat Defense devices.

Implementation considerations

If you have an asymmetrical routing environment in your network, where the outbound and inbound flow for a given connection can go through two different Firewall Threat Defense devices, you need to implement TCP state bypass on the affected traffic.

However, TCP state bypass weakens the security of your network, so you should apply bypass on very specific, limited traffic classes.

The asymmetrical routing problem

The asymmetrical routing problem occurs when return traffic for a connection goes through a different firewall than the outbound traffic. This causes packets to be dropped because they do not match existing connection entries in the fast path table.

Traffic inspection and fast path operation

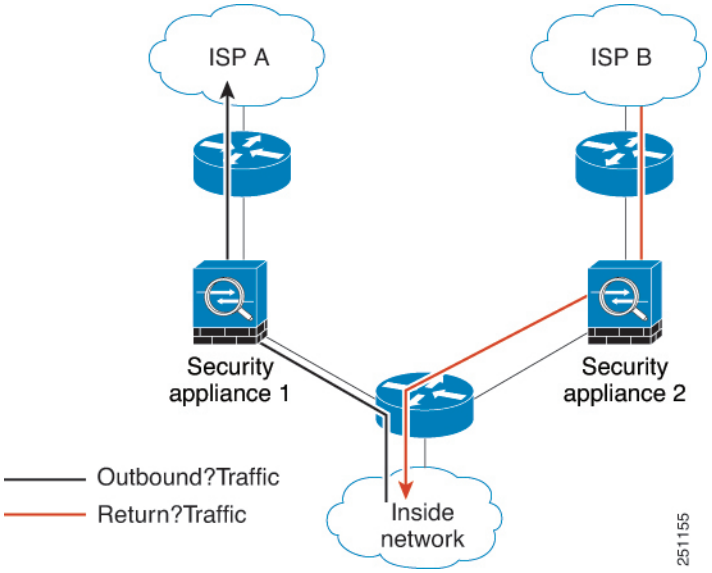
By default, the Firewall Threat Defense inspects all traffic using the Adaptive Security Algorithm. The Firewall Threat Defense allows or drops traffic based on the security policy. The Firewall Threat Defense maximizes the firewall performance by checking the state of each packet (new connection or established connection). It assigns new connection SYN packets to the session management path. It assigns established connections to the fast path. It assigns packets requiring advanced inspection to the control plane path.

The Firewall Threat Defense allows TCP packets that match existing connections to pass through via the fast path without rechecking every aspect of the security policy. This feature improves performance. However, the fast path establishment method can interfere with asymmetric routing solutions. The method uses SYN packets and performs checks such as TCP sequence number validation. Both outbound and inbound flows of a connection must pass through the same Firewall Threat Defense device.

Asymmetric routing scenario

For example, a new connection goes to Security Appliance 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through Security Appliance 1, then the packets match the entry in the fast path, and are passed through. But if subsequent packets go to Security Appliance 2, where no SYN packet went through the session management path, then no entry exists in the fast path for the connection, and Security Appliance 2 drops the packets. The following figure shows an asymmetric routing example where the outbound traffic goes through a different Firewall Threat Defense than the inbound traffic:

Figure 419: Asymmetric routing



If you have asymmetric routing configured on upstream routers and traffic alternates between two Firewall Threat Defense devices, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic similarly to a UDP connection: when a non-SYN packet matching the specified networks enters the Firewall Threat Defense device, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

Guidelines and limitations for TCP state bypass

TCP state bypass unsupported features

The system does not support these features when you use TCP state bypass:

- Application inspection—Inspection requires both inbound and outbound traffic to go through the same Firewall Threat Defense, so inspection is not applied to TCP state bypass traffic.
- Snort inspection—Inspection requires both inbound and outbound traffic to go through the same device. However, Snort inspection is not automatically bypassed for TCP state bypass traffic. You must also configure a prefilter fastpath rule for the same traffic class for which you configure TCP state bypass. Otherwise, packets might be dropped unexpectedly because the TCP Normalizer is also not engaged.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The Firewall Threat Defense does not keep track of the state of the connection, so these features are not applied.
- TCP normalization—The TCP normalizer is disabled.
- TLS server identity discovery cannot be used with TCP state bypass on an inline or inline tap interface.

TCP state bypass NAT guidelines

Because the translation session is established separately for each device, be sure to configure static NAT on both devices for TCP state bypass traffic. If you use dynamic NAT, the address chosen for the session on Device 1 will differ from the address chosen for the session on Device 2.

Configure TCP state bypass

Configure TCP state bypass to handle asymmetrical routing environments where standard TCP state checking would interfere with traffic flow.

To bypass TCP state checking in asymetrical routing environments, carefully define a traffic class that applies only to the affected hosts or networks. Then, enable TCP state bypass on the traffic class using a service policy. You must also configure a corresponding prefilter fastpath policy for the same traffic to ensure that the traffic bypasses inspection.

Because bypass reduces the security of the network, limit its application as much as possible.

Before you begin

Follow these steps to configure TCP state bypass:

Procedure

Step 1 Create the extended ACL that defines the traffic class.

For example, to define a traffic class for TCP traffic from 10.1.1.1 to 10.2.2.2, do the following:

a) Choose **Objects** > **Object Management** > **Access List** > **Extended**.
b) Click **Add Extended Access List**.
c) Enter a **Name** for the object, for example, bypass.
d) Click **Add** to add a rule.
e) Keep **Allow** for the action.
f) Enter 10.1.1.1 beneath the **Source** list and click **Add**. Then, enter 10.2.2.2 beneath the **Destination** list, and click **Add**.
g) Click **Port**, select **TCP (6)** beneath the **Selected Source Ports** list, then click **Add**. Do not enter a port number. Add TCP as the protocol. This will cover all ports.
h) In the Extended Access List Entry dialog box, click **Add** to add the rule to the ACL.
i) In the Extended Access List Object dialog box, click **Save** to save the ACL object.

Step 2 Configure the TCP state bypass service policy rule.

For example, to configure TCP state bypass for this traffic class globally, do the following:

a) Choose **Policies** > **Access Control heading** > **Access Control**, and edit the policy assigned to the devices that require this service.
b) Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line, and click **Edit** () for the **Threat Defense Service Policy**.
c) Click **Add Rule**.
d) Select **Global** and click **Next**.
e) Select the extended ACL object you created for this rule and click **Next**.
f) Select **Enable TCP State Bypass**.
g) (Optional.) Adjust the **Idle** timeout for bypassed connections. The default is 2 minutes.

h) Click **Finish** to add the rule. If necessary, drag and drop the rule to the desired position in the service policy.

Click **OK** to save the changes to the service policy.

Click **Save** on **Advanced** to save the changes to the access control policy.

Step 3 Configure a prefilter fastpath rule for the traffic class.

You cannot use the ACL object in the prefilter rule, so you need to recreate the traffic class either directly in the prefilter rule, or by first creating network objects that define the class.

This procedure assumes that you already have a prefilter policy attached to the access control policy. If you have not created a prefilter policy yet, go to **Policies** > **Prefilter** and first create the policy. You can then follow this procedure to attach it to the access control policy and create the rule.

Keeping with our example, this procedure creates a fastpath rule for TCP traffic from 10.1.1.1 to 10.2.2.2.

a) Choose **Policies** > **Access Control heading** > **Access Control**, and edit the policy that has the TCP bypass service policy rule.
b) Click the link for the **Prefilter Policy**, which is to the left immediately under the policy description.
c) In the Prefilter Policy dialog box, select the policy to assign to the device if the correct one is not already selected. Do not click OK.

Because you cannot add rules to the default prefilter policy, you must choose a custom policy.

d) In the Prefilter Policy dialog box, click **Edit** ( ). This action opens a new browser window where you can edit the policy.
e) Click **Add Prefilter Rule** and configure a rule with these properties.

- **Name**—Any name that you find meaningful will do, such as TCPBypass.
- **Action**—Select **Fastpath**.
- **Interface Objects**—If you configured TCP state bypass as a global rule, leave the default, any, for both source and destination. If you created an interface-based rule, select the same interface objects you used for rule in the **Source Interface Objects** list, and keep any as the destination.
- **Networks**—Add 10.1.1.1 to the **Source Networks** list, and 10.2.2.2 to the **Destination Networks** list. You can either use network objects or manually add the addresses.
- **Ports**—Under **Selected Source Ports**, select TCP(6), **do not enter a port**, and click **Add**. This applies the rule to all TCP traffic, regardless of TCP port number.

f) Click **Add** to add the rule to the prefilter policy.
g) Click **Save** to save your changes to the prefilter policy.

You can now close the prefilter edit window and return to the access control policy edit window.

h) In the access control policy edit window, the Prefilter Policy dialog box should still be open. Click **OK** to save your changes to the prefilter policy assignment.
i) Click **Save** on the access control policy to save the changed prefilter policy assignment, if you changed it.

You can now deploy the changes to the affected devices.

Disable TCP sequence randomization

Disable TCP initial sequence number randomization to prevent issues with data scrambling and to support specific network configurations that require non-randomized sequence numbers.

Each TCP connection has two initial sequence numbers (ISN): one generated by the client and one generated by the server. The Firewall Threat Defense device randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session. However, TCP sequence randomization effectively breaks TCP SACK (Selective Acknowledgement), as the sequence numbers the client sees are different from what the server sees.

You can disable TCP initial sequence number randomization if data is getting scrambled or if there is another necessity. This is useful in these situations:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the device, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- If you use a WAAS device that requires the device not to randomize the sequence numbers of connections.
- If you enable hardware bypass for the ISA 3000, and TCP connections are dropped when the ISA 3000 is no longer part of the data path.

Procedure

Step 1 Create the extended ACL that defines the traffic class.

For example, to define a traffic class for TCP traffic from any host to 10.2.2.2, do the following:

a) Choose **Objects** > **Object Management** > **Access List** > **Extended**.
b) Click **Add Extended Access List**.
c) Enter a **Name** for the object, for example, preserve-sq-no.
d) Click **Add** to add a rule.
e) Keep **Allow** for the action.
f) Leave the **Source** list empty, enter 10.2.2.2 beneath the **Destination** list, and click **Add**.
g) Click **Port**, select **TCP (6)** beneath the **Selected Source Ports** list, and click **Add**. Do not enter a port number, simply add TCP as the protocol, which will cover all ports.
h) Click **Add** on the Extended Access List Entry dialog box to add the rule to the ACL.
i) Click **Save** on the Extended Access List Object dialog box to save the ACL object.

Step 2 Configure the service policy rule that disables TCP sequence number randomization.

For example, to disable randomization for this traffic class globally, do the following:

a) Choose **Policies** > **Access Control heading** > **Access Control**, and edit the policy assigned to the devices that require this service.
b) Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line, and click **Edit** (✎) for the **Threat Defense Service Policy**.

c) Click **Add Rule**.
d) Select **Global** and click **Next**.
e) Select the extended ACL object you created for this rule and click **Next**.
f) Deselect **Randomize TCP Sequence Number**.
g) (Optional.) Adjust the other connection options as needed.
h) Click **Finish** to add the rule. If necessary, drag and drop the rule to the desired position in the service policy.

Click **OK** to save the changes to the service policy.

Click **Save** on **Advanced** to save the changes to the access control policy.

You can now deploy the changes to the affected devices.

Monitor service policies

You can monitor service-policy related information using the device CLI. Use these commands to get the information you need.

Commands for monitoring service policies.

- **show conn** [**detail**]

  Shows connection information. Detailed information uses flags to indicate special connection characteristics. For example, the "b" flag indicates traffic subject to TCP state bypass.

  When you use the **detail** keyword, you can see information about dead connection detection (DCD) probing, which shows how often the connection was probed by the initiator and responder. For example, the connection details for a DCD-enabled connection would look like this:

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  Shows service policy statistics, including dead connection detection (DCD) statistics.

- **show threat-detection statistics top TCP-intercept** [**all** | **detail**]

  View the top 10 protected servers under attack. The **all** keyword shows the history data of all the traced servers. The **detail** keyword shows history sampling data. The system samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.

Examples for service policy rules

This section provides examples of service policy rules to help users understand how to configure and implement service policies effectively.

Protect servers from a SYN flood DoS attack (TCP intercept)

This task configures TCP intercept to protect servers from SYN flood denial of service attacks by limiting embryonic connections and enabling monitoring statistics.

A SYN-flooding denial of service (DoS) attack occurs when an attacker sends a series of SYN packets to a host. These packets usually originate from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests from legitimate users.

You can limit the number of embryonic connections to help prevent SYN flooding attacks. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

When the embryonic connection threshold of a connection is crossed, the Firewall Threat Defense acts as a proxy for the server. It generates a SYN-ACK response to the client SYN request using the SYN cookie method. This approach prevents the connection from being added to the SYN queue of the targeted host. The SYN cookie is the initial sequence number returned in the SYN-ACK that is constructed from MSS, time stamp, and a mathematical hash of other items to essentially create a secret. If the Firewall Threat Defense receives an ACK from the client with the correct sequence number, and within the valid time window, it authenticates the client and allows the connection to the server. The component that performs the proxy is called TCP intercept.

Setting connection limits can protect a server from a SYN flood attack. You can optionally enable TCP intercept statistics and monitor the results of your policy. The following procedure explains the end-to-end process.

Before you begin

- Ensure that you set the embryonic connection limit lower than the TCP SYN backlog queue on the server that you want to protect. Otherwise, valid clients can no longer access the server during a SYN attack. To determine reasonable values for embryonic limits, carefully analyze the capacity of the server, the network, and server usage.
- The number of CPU cores affects the actual number of concurrent and embryonic connections the device can allow. Because each core manages connections, the actual counts can exceed the configured limits. In the worst case, a device with n cores can allow up to n − 1 additional connections of each type.

  For example, on a 4-core device configured for 6 concurrent connections and 4 embryonic connections, the device could allow up to 3 additional connections of each type.

  To find the number of cores for your model, enter the **show CPU core** command in the device CLI.

Procedure

Step 1 Create the extended ACL that defines the traffic class, which is the list of servers you want to protect.

For example, to define a traffic class to protect the web servers with the IP addresses 10.1.1.5 and 10.1.1.6:

a) Choose **Objects** > **Object Management** > **Access List** > **Extended**.
b) Click **Add Extended Access List**.
c) Enter a **Name** for the object, for example, protected-servers.
d) Click **Add** to add a rule.
e) Keep **Allow** for the action.
f) Leave the **Source** list empty, enter 10.1.1.5 beneath the **Destination** list, and click **Add**.
g) Also enter 10.1.1.6 beneath the **Destination** list and click **Add**.
h) Click **Port**, select **HTTP** in the available ports list, and click **Add to Destination**. If your server also supports HTTPS connections, also add that port.
i) Click **Add** to add the rule to the ACL.

Click **Save** to save the ACL object.

Step 2 Configure the service policy rule that sets embryonic connection limits.

For example, to set the total concurrent embryonic limit to 1000 connections, and the per-client limit to 50 connections, do the following:

a) Choose **Policies** > **Access Control heading** > **Access Control**, and edit the policy assigned to the devices that require this service.
b) Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line, and click **Edit** ( ) for the **Threat Defense Service Policy**.
c) Click **Add Rule**.
d) Select **Global** and click **Next**.
e) Select the extended ACL object you created for this rule and click **Next**.
f) Enter 1000 for **Connections** > **Maximum Embryonic**.
g) Enter 50 for **Connections Per Client** > **Maximum Embryonic**.

(Optional.) Adjust the other connection options as needed.

h) Click **Finish** to add the rule. If necessary, drag and drop the rule to the desired position in the service policy.

Click **OK** to save the changes to the service policy.

Click **Save** on **Advanced** to save the changes to the access control policy.

Step 3 (Optional.) Configure the rates for TCP intercept statistics.

TCP intercept uses these options to determine the rate for collecting statistics. All options have default values, so if these rates suit your needs, you can skip this step.

- Rate Interval—The size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the system samples the number of attacks 30 times.
- Burst Rate—The threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, the device generates syslog message 733104.
- Average Rate—The average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, the device generates syslog message 733105.

If you want to adjust these options, do this:

a) Choose **Objects** > **Object Management** > **FlexConfig** > **Text Object**.

b) Click **Edit** (✎) for the **threat_defense_statistics** system-defined object.
c) Although you can directly change the values, the recommended approach is to open the **Override** section and click **Add** to create a device override.
d) Select the devices to which you will assign the service policy (through the access control policy assignment) and click **Add** to move them to the selected list.
e) Click **Override**.
f) The object must have 3 entries, so click **Count** as needed until you get 3.
g) Enter the values you need, in order from 1-3, as rate interval, burst rate, and average rate. Consult the object description to verify you enter the values in the right order.
h) Click **Add** in the Object Override dialog box.
i) Click **Save** in the Edit Text Object dialog box.

Step 4 Enable TCP intercept statistics.

You must configure a FlexConfig policy to enable TCP intercept statistics.

a) Choose **Devices** > **FlexConfig**.
b) If you already have a policy assigned to the devices, edit it. Otherwise, create a new policy and assign it to the affected devices.
c) Select the **Threat_Detection_Configure** object in the **Available FlexConfig** list and click >>. The object is added to the **Selected Append FlexConfigs** list.
d) Click **Save**.
e) (Optional.) You can verify that you have the right settings by clicking **Preview Config** and selecting one of the devices.

The system generates the CLI commands that will be written to the device during the next deployment. These commands will include those needed for the service policy as well as those needed for threat detection statistics. Scroll to the bottom of the preview to see the appended CLI. The TCP intercept statistics command should look something like this, if you use the default values (line break added for clarity):

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

Step 5 You can now deploy the changes to the affected devices.

Step 6 Monitor the TCP intercept statistics from the device CLI using these commands:

- **show threat-detection statistics top TCP-intercept** [**all** | **detail**]—View the top 10 protected servers under attack. The **all** keyword shows the history data of all the traced servers. The **detail** keyword shows history sampling data. The system samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.



Note You can use the **shun** command to block attacking host IP addresses. To remove the block, use the **no shun** command.

- **clear threat-detection statistics TCP-intercept**—Erases TCP intercept statistics.

Example:

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Configure the Firewall Threat Defense device to appear on traceroutes

Make the Firewall Threat Defense device appear as a hop in traceroute results by decrementing the time-to-live on packets and adjusting ICMP rate limits.

By default, the Firewall Threat Defense device does not appear on traceroutes as a hop. To make it appear, you need to decrement the time-to-live on packets that pass through the device, and increase the rate limit on ICMP unreachable messages. To accomplish this, you must configure a service policy rule and adjust the ICMP platform settings policy.

Note If you decrement time to live, packets with a TTL of 1 will be dropped, but a connection will be opened for the session on the assumption that the connection might contain packets with a greater TTL. Note that some packets, such as OSPF hello packets, are sent with TTL = 1, so decrementing time to live can have unexpected consequences. Keep these considerations in mind when defining your traffic class.

Procedure

Step 1 Create the extended ACL that defines the traffic class for which to enable traceroute reporting.

For example, to define a traffic class for all addresses, but excluding OSPF traffic, do the following:

a) Choose **Objects** > **Object Management** > **Access List** > **Extended**.
b) Click **Add Extended Access List**.
c) Enter a **Name** for the object, for example, traceroute-enabled.
d) Click **Add** to add a rule to exclude OSPF.
e) Change the action to **Block**, click **Port**, select **OSPFIGP (89)** as the protocol beneath the **Destination Ports** list, and click **Add** to add the protocol to the selected list.
f) Click **Add** on the Extended Access List Entry dialog box to add the OSPF rule to the ACL.
g) Click **Add** to add a rule to include all other connections.
h) Keep **Allow** for the action, and leave both the Source and Destination lists empty.
i) Click **Add** on the Extended Access List Entry dialog box to add the rule to the ACL.

Ensure that the OSPF deny rule is above the Allow Any rule. Drag and drop to move the rules if necessary.

Click **Save** on the Extended Access List Object dialog box to save the ACL object.

Step 2 Configure the service policy rule that decrements the time-to-live value.

For example, to decrement time-to-live globally, do the following:

a) Choose **Policies** > **Access Control heading** > **Access Control**, and edit the policy assigned to the devices that require this service.
b) Click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line, and click **Edit** (✎) for the **Threat Defense Service Policy**.
c) Click **Add Rule**.
d) Select **Global** and click **Next**.
e) Select the extended ACL object you created for this rule and click **Next**.
f) Select **Enable Decrement TTL**.
g) (Optional.) Adjust the other connection options as needed.
h) Click **Finish** to add the rule. If necessary, drag and drop the rule to the desired position in the service policy.

Click **OK** to save the changes to the service policy.

Click **Save** on **Advanced** to save the changes to the access control policy.

You can now deploy the changes to the affected devices.

Step 3 Increase the rate limit on ICMP unreachable messages.

a) Choose **Devices** > **Platform Settings**.
b) If you already have a policy assigned to the devices, edit it. Otherwise, create a new Threat Defense platform settings policy and assign it to the affected devices.
c) Select **ICMP** from the table of contents.
d) Increase the **Rate Limit**, for example, to 50. You might also want to increase the **Burst Size**, for example, to 10, to ensure enough responses are generated within the rate limit.

You can leave the ICMP rules table empty, it is not related to this task.

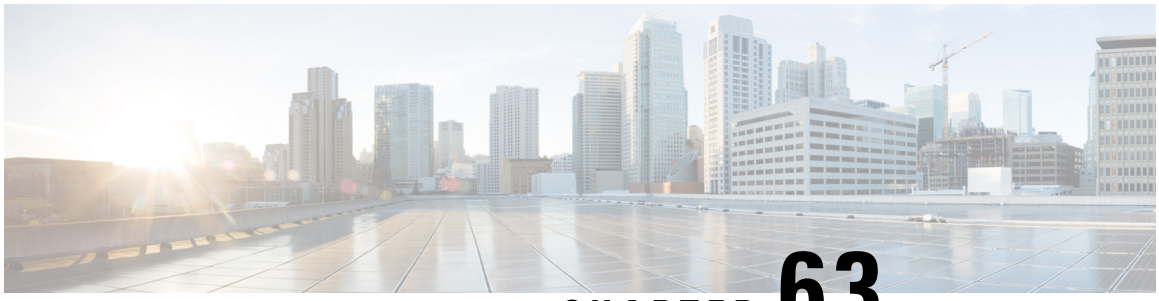
e) Click **Save**.

Step 4 You can now deploy the changes to the affected devices.

History for threat defense service policy

This reference provides a summary of feature changes by release for the service policy.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Description
Threat Defense Service Policy.	6.3	Any	You can now configure a Threat Defense service policy as part of your access control policy advanced options. You can use Threat Defense service policies to apply services to specific traffic classes. Features supported include TCP state bypass, randomizing TCP sequence numbers, decrementing the time-to-live (TTL) value on packets, dead connection detection, setting a limit on the maximum number of connections and embryonic connections per traffic class and per client, and timeouts for embryonic, half closed, and idle connections. New screen: **Policies** > **Access Control** > **Access Control**, **Advanced** tab, **Threat Defense Service Policy**. Supported platforms: Secure Firewall Threat Defense
Initiator and responder information for dead connection detection (DCD), and DCD support in a cluster.	6.5	Any	If you enable dead connection detection (DCD), you can use the **show conn detail** command to get information about the initiator and responder. Dead connection detection allows you to maintain an inactive connection, and the **show conn** output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster. New/Modified commands: **show conn** (output only). Supported platforms: Secure Firewall Threat Defense
Configure the maximum segment size (MSS) for embryonic connections.	7.1	Any	You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums. New or changed screens: **Connection Settings** in the Add/Edit Service Policy wizard.



CHAPTER 63

Threat Detection

Threat detection's portscan detector is a mechanism designed to help you detect and prevent portscan activity in all types of traffic to protect networks from eventual attacks. Portscan traffic can be detected efficiently in both allowed and denied traffic.

Portscan is a form of network reconnaissance that is often used by attackers as a prelude to an attack. In a portscan, an attacker determines the types of network protocols or services a host supports and sends specially crafted packets to a targeted host. By examining the packets that the host responds with, the attacker can often determine which ports are open on the host and, either directly or by inference, which application protocols are running on these ports.

- Portscan detection and prevention, on page 2211
- Requirements and prerequisites for threat detection, on page 2213
- Limitations for threat detection configuration, on page 2214
- Best practices for portscan prevention, on page 2214
- Configure portscan detection and prevention, on page 2215
- Monitoring threat detection, on page 2217
- History for threat detection, on page 2219

Portscan detection and prevention

Portscan detection and prevention is a threat detection system that:

- identifies port scan activity and issues events when they are found,
- optionally prevents port scans by automatically blocking scanners, and
- sends you events and also blocks the attacker for a duration that you set.

Pre-defined sensitivity levels for portscan detection

When configuring detection settings, you select from these pre-defined sensitivity levels. Except for custom, each level has pre-set values for each protocol for the number of ports (TCP, UDP), protocols (IP), or hosts (TCP, UDP, IP, ICMP) that must be scanned within a set time interval (expressed in seconds). Also, all types of scans and sweeps are enabled.

Note When counting ports or protocols, threat detection increments the number if the port or protocol in the current packet differs from the previous packet. For example, if you have an application that opens connections in 10 set ports randomly, the total number of ports scanned could mount so quickly that your port number will be exceeded within the interval. The system does not count only unique ports.

Exceeding the number within the interval can indicate a scanning attack. Portscan events are generated only when the port/protocol/host numbers are exceeded for the moving time interval window.

These sensitivity levels determine portscan detection behavior:

- **Low**—This level uses the shortest time window for portscan detection, coupled with high counts for ports, protocols, and hosts. Thus, you should see portscan events for the most aggressive scanners only. Select this sensitivity level to suppress false positives, but remember that some types of port scans, such as slow or filtered scans, might be missed. For more detail on how low sensitivity detection works, see Detection in the low sensitivity level, on page 2213.
- **Medium**—This level uses moderate values for both the interval and port/protocol/host counts. However, very active hosts such as network address translators and proxies might generate false positives. Add such hosts to the ignore scanner list. This is the default sensitivity level and a good place to start.
- **High**—This level uses a much longer time window for portscan detection, coupled with lower counts for ports, protocols, and hosts. With this level, you are most likely to see events for even the least aggressive port scans or sweeps, so you are more likely to notice all attackers. However, this level would likely result in the most portscan events issued, and potentially the highest number of false positives.
- **Custom**—If you want to configure any setting differently than one of the predefined sensitivity levels, or disable a particular type of scan or sweep, the level automatically switches to custom. If you want to adjust the options, first select the level that most closely matches what you want, then edit the values as appropriate.

Table 140: Sensitivity level settings

Setting	Low	Medium	High
Interval (TCP/UDP/IP/ICMP)	60 seconds	90 seconds	600 seconds (10 minutes)
TCP/UDP portscan - Number of Ports	120 seconds	90 seconds	60 seconds
TCP/UDP portsweep - Number of Hosts	180 seconds	150 seconds	100 seconds
IP protocol scan - Number of Protocols	30 seconds	15 seconds	10 seconds
IP protocol sweep - Number of Hosts	25 seconds	20 seconds	10 seconds
ICMP host sweep - Number of Hosts	50 seconds	30 seconds	20 seconds

Detection in the low sensitivity level

When you select the low sensitivity level, the system tracks negative responses for TCP, UDP, and ICMP initial packets. An alert is triggered only when the number of unsuccessful connections exceeds the rejection threshold (10% for low sensitivity) and the port or IP protocol count exceeds the configured threshold. This mitigates false positives.

Low sensitivity level detection behavior

Rejection threshold applies to low sensitivity (or equivalent custom settings) only; it does not apply to other sensitivity levels or their custom equivalents.

When there is a mix of allowed and blocked traffic, the number of rejected ports or hosts is calculated based on the difference between allowed and blocked traffic. In the case of only blocked traffic, the rejection threshold is not considered.

These criteria are not used for UDP/ICMP connections on interfaces configured in inline sets.

Low sensitivity level detection scenarios

In low sensitivity mode, the port count threshold is 120. Thus, the rejection count threshold is 10% of 120, which is 12. Here are examples that show how the system issues portscan events with this configuration:

- An attacker initiates connections with 131 ports of the target and the target positively acknowledges all the initiations. Port count = 131, which is greater than the threshold, but a portscan alert is not triggered because there are no negative acknowledgements.
- An attacker initiates connections with 131 ports of the target and the target positively acknowledges 121 initiations and negatively acknowledges 10 initiations. Port count = 131, which is greater than the threshold, but reject port count = 10, which is lesser than the rejection threshold. Therefore, a portscan alert is not triggered.
- An attacker initiates connections with 134 ports of the target and the target positively acknowledges 121 initiations and negatively acknowledges 13 initiations. Port count = 134, which is greater than the threshold, and reject port count = 13 is also higher than the rejection threshold. Therefore a portscan alert is triggered.

Requirements and prerequisites for threat detection

Model support

Firewall Threat Defense running version 7.2+ and Snort 3.

Supported domains

Any

User roles

Admin

Access Admin

Network Admin

Limitations for threat detection configuration

Threat detection requires Snort 3 and has specific version requirements and configuration interactions that vary by management platform.

- Threat detection requires Snort 3. The managed device must be running version 7.2 or higher. For Snort 2, or devices running versions lower than 7.2, you can configure port scan through the NAP policy. Note that the threat detection feature is not the same as the port scan feature in the NAP policy. If there are non-Snort 3 devices running version 7.2 or higher that are assigned to the access control policy, the threat detection settings are not deployed to those unsupported devices.
- If you configure port scan in the NAP policy on a device running 7.1 or lower, that configuration is not translated to the threat detection feature on upgrade to 7.2. You must manually configure threat detection. Although the NAP and threat detection port scan options are similar, they do not match one-to-one.
- If you configure threat detection, any port scan configuration in the NAP policy is ignored and not configured on the devices that support threat detection.
- The NAP port scan feature for Snort 3 is always ignored for devices running version 7.2 or higher. To configure port scanning, you must use the threat defense settings.
- Threat detection works on traffic that passes through the device only. It does not work on traffic directed to the device.
- In a high availability setup, port scanning statistics are not synchronized to the standby unit. However, blocked hosts are synchronized and continue to be blocked until the duration period expires in case of a failover.
- (Devices running Threat Defense versions 7.2 through 7.7). For nodes in a cluster, detection and prevention happen on the individual cluster node. That is, if node B detects and blocks traffic from a host, node A will not be aware of that action because port scan statistics are not synchronized across cluster nodes.
- For inline sets, or for interfaces that are configured to be part of an equal-cost multipath (ECMP) traffic zone, detection and prevention are done at the zone level. Port scan statistics for a host are accumulated across all interfaces of a zone. Similarly, when a host crosses configured thresholds, it is blocked across all interfaces of the corresponding zone.
- Although the port scan events generated by the threat detection feature are the same as the ones Snort issues for port scan, you do not need to enable port scanning intrusion rules to get the events. Threat detection works regardless of your intrusion policy implementation.

Best practices for portscan prevention

Portscan prevention mode can result in unintended traffic outage. In prevention mode, hosts are blocked from further scanning of networks on all protocols for the configured duration. Review the detection and prevention parameters carefully to ensure legitimate traffic is not blocked.

Before configuring portscan in prevention mode:

- Start using portscan in detection mode.
- Observe the generated portscan events.
- Tune the sensitivity level, monitored networks, ignore scanner list, and ignore target list. If a pre-defined sensitivity level does not work well for your situation, configure custom settings as needed.
- Repeat the process until false positives are eliminated and the event rate represents an accurate picture of port scanning in your network. Ensure that you are comfortable with blocking the remaining identified scanners.

Configure portscan detection and prevention

This task enables threat detection to watch for port scanning activity and optionally automatically block scanners for a period of time.

Portscan is a form of network reconnaissance that is often used by attackers as a prelude to an attack. In a portscan, an attacker determines the types of network protocols or services a host supports and sends specially crafted packets to a targeted host. By examining the packets that the host responds with, the attacker can often determine which ports are open on the host and, either directly or by inference, which application protocols are running on these ports.

You can enable threat detection to watch for port scanning activity and optionally, automatically block scanners for a period of time.

Before you begin

Fully Qualified Domain Name (FQDN), wildcard mask, any, any-ipv4, and any-ipv6 network objects are not supported for portscan configuration. These objects are not shown in the **Monitor**, **Ignore Scanner**, **Ignore Target**, and **Exclude** fields.

Procedure

Step 1 In the access control policy editor, click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line. Then, click **Edit** (✎) next to **Threat Detection**.

Step 2 In the **Threat Detection** window, select the **Portscan mode**:

- **Disable**—Turn off threat detection. This is the default mode. You can click **Revert to Defaults** to return to this unconfigured state.
- **Detection**—Perform portscan detection, but alert on problems only. Do not take action against potential attackers. We suggest you use this mode initially until you fine-tune the threat detection settings to avoid excessive false positives.
- **Prevention**—Perform portscan detection and actively block identified scanners, that is, hosts that are performing the port scan.

Step 3 Configure the **Traffic Selection** options.

The traffic selection options determine which networks are monitored, the type of connections monitored, and whether any scanners or target hosts should be exempted from the monitored networks. By default, the system monitors permitted connections on all networks.

- **Detection On Traffic**—Select the types of connection that will be monitored for portscan activity: **Permitted**, **Denied**, or **All** traffic. The default is **Permitted**.
- **Monitor**—Select the network objects that define the networks to monitor for portscan or sweep activity. The default is any network, IPv4 or IPv6. Use this option to limit scanning to untrusted networks.
- **Ignore Scanner**—Select the network objects that define the hosts or networks, from within the range of the monitored networks, that should be ignored. For example, if you have set up your own scanner to test your network, you can exempt the address of your scanner to avoid unnecessary reporting on the address. Do not include addresses that are outside the monitored networks, as these addresses are already ignored.
- **Ignore Target**—Select the network objects that define the hosts or networks that should be ignored as targets, that is, victims of a portscan or sweep.

Step 4 Click the **Configuration** tab and select the scanning sensitivity level.

The predefined sensitivity levels, **Low**, **Medium**, and **High**, set the port scanning options to values that are increasingly aggressive. For example, if you select low, you would expect to see fewer port scanning events, and you could potentially miss attackers more easily than if you selected medium or high. On the other hand, if you select high, you might see more events and also, potentially, more false positives. The default level is medium. For more information on these levels, see Pre-defined sensitivity levels for portscan detection, on page 2211.

As you select the levels, you can see the related values within the protocol sections: **TCP**, **UDP**, **IP**, and **ICMP**. If you change any of the preset values, or disable a type of scan, the sensitivity mode automatically changes to **Custom**.

Within each protocol section, the options are:

- **Interval**—The time range, in seconds, within which the configured values for portscan or portsweep are exceeded. For example, if you select 90 seconds, and 60 as the number of TCP portscan ports, a scanner would need to try 60 ports on a host within 90 seconds for it to be considered a portscan. The system generates events only if the number of ports, protocols, or hosts (for a portsweep) are exceeded within the specified interval.

  You can specify a range between 30 to 600 seconds. The longer the period, the more likely a host might be identified as a scanner.
- **Portscan** (TCP/UDP)—Select whether to monitor for port scanning against single hosts, and specify the number of ports that must be scanned within the interval to count as a portscan attack. The allowed range is 1-256.
- **Portsweep** (TCP/UDP)—Select whether to monitor for port sweeping against multiple hosts, and specify the number of hosts that must be scanned for a given port within the interval to count as a portsweep attack. The allowed range is 1-256.
- **Protocol Scan** (IP)—Select whether to monitor for protocol scanning against single hosts, and specify the number of protocols that must be scanned within the interval to count as a protocol scan attack. The allowed range is 1-255.
- **Protocol Sweep** (IP)—Select whether to monitor for protocol sweeping against multiple hosts, and specify the number of hosts that must be scanned for a given protocol within the interval to count as a protocol sweep attack. The allowed range is 1-256.

- **Hostsweep** (ICMP)—Select whether to monitor for ICMP host sweeping against multiple hosts, and specify the number of hosts that must be scanned within the interval to count as a hostsweep attack. The allowed range is 1-256.

Step 5 If you selected prevention mode, click the **Prevention** tab and configure the options.

In prevention mode, hosts are automatically blocked from further scanning of networks on all protocols for the configured duration. Review the detection and prevention parameters carefully to ensure legitimate traffic is not blocked.

- **Exclude**—Select the network objects that define the hosts or networks, from within the range of the monitored networks, that should be excluded from automatic blocking. Even if these hosts violate your scanning detection parameters, the system will not block them.
- **Duration**—How long, in seconds, automatically blocked scanner hosts should be prevented from sending traffic of any kind through the device. After the duration period ends, the hosts are automatically cleared and can again send traffic through the device. The allowed range is 600 to 2592000 seconds. The default is 3600 seconds (1 hour).

  If you need to manually unblock a host, SSH to the firewall that is blocking the host and use the **clear threat-detection portscan attacker** command.

Step 6 Click **OK** to save the threat detection settings.

Step 7 Click **Save** to save the access control policy.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

Monitoring threat detection

The following topics explain how to monitor portscan activity.

View portscan alerts

Portscan activity is alerted through the existing portscan-specific intrusion events. Intrusion events with generator ID (GID) 122 and Snort ID from SIDs 1 through 27 are generated. For these events, the *(port_scan)* string is prepended in the event messages. The events include packet information along with packet data containing the statistics that triggered the alert.

To viewportscan events, go to **Analysis** > **Unified Events**.

Alternatively, you can also go to **Analysis** > **Intrusions** > **Events** and view portscan events.

Portscan issues these events regardless of your intrusion policy or NAP configuration. Events are issued only when scanners exceed the number of configured ports, protocols, or hosts for the various types of scan or sweep within the configured time interval for the associated protocol. A port scan from one host generates one event per set interval as soon as the threshold is met. If the same host initiates a new port scan during the same interval, no event is reported.

Table 141: Portscan events

Portscan type	Intrusion event
TCP Regular, Decoy, Distributed Scan	122:1 (port_scan) TCP portscan
TCP Portsweep	122:3 (port_scan) TCP portsweep
TCP Distributed Scan	122:4 (port_scan) TCP distributed portscan
IP Regular, Decoy, Distributed Protocol Scan n	122:9 (port_scan) IP protocol scan
IP Protocol Sweep	122:11 (port_scan) IP protocol sweep
IP Distributed Scan	122:12 (port_scan) IP distributed protocol scan
UDP Regular, Decoy, Distributed Scan	122:17 (port_scan) UDP portscan
UDP Portsweep	122:19 (port_scan) UDP portsweep
UDP Distributed Scan	122:20 (port_scan) UDP distributed portscan
ICMP Sweep	122:25 (port_scan) ICMP sweep
Portscan Block	122:100 (port_scan) host blocked due to portscan activity

Monitor portscan on the firewall

To monitor portscan, log in to the device Command-Line Interface (CLI) and use these commands.

- **show threat-detection portscan** [**attacker** | **target** | **shun**]

  Shows the IP addresses of scanners, those that have been shunned (blocked), and hosts that have been targeted by scans or sweeps.

- **show threat-detection portscan statistics** [**host** [*ipv4_address* | *ipv6_address*]] [**protocol** {**tcp** | **udp** | **IP** | **icmp**}]

  Shows statistics related to the port scan system. You can specify host, protocol, or host and protocol to filter the output to the desired information.

- **clear threat-detection portscan** [**attacker** | **target** | **shun**] [*ipv4_address mask* | *ipv6_address/prefix*]

  Manually unblocks scanners (attackers) or identified targets. Enter the command without parameters to clear all attackers, targets, or shunned hosts.

- **clear threat-detection portscan statistics** [**host** [*ipv4_address* | *ipv6_address*]] [**protocol** {**tcp** | **udp** | **IP** | **icmp**}]

  Erases statistics related to portscan, so that you can more clearly see the current state of scanning through this device. Enter the command without parameters to clear all statistics. Alternatively, specify a host, protocol, or host and protocol, to limit the reset to the specified items.

Unblocking a host

If you configure threat detection in prevention mode and the system blocks a host that you know is not an attacker, you can manually unblock the host before the host is automatically unblocked when the duration period expires.

To manually unblock the host, log in to the device CLI where the host is blocked and enter the clear threat-detection portscan attacker command. For example:

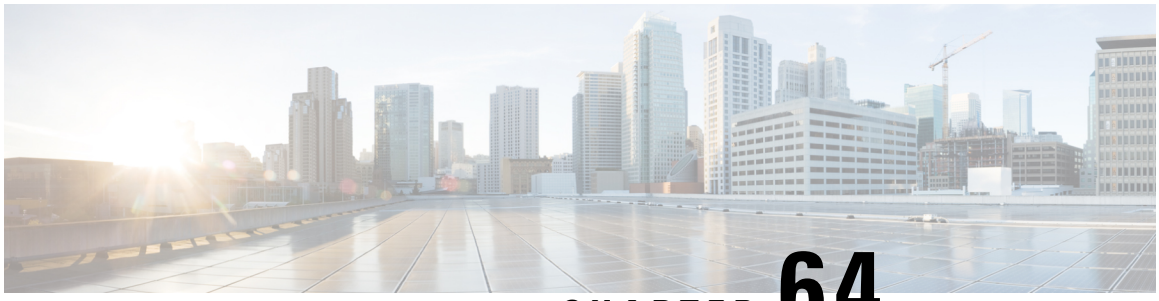
```
> clear threat-detection portscan attacker 10.2.0.100 255.255.255.255
1 tracker object deleted and 1 shun entry removed
```

Consider adding the host IP address to the exclude list in the prevention configuration.

History for threat detection

This reference provides a chronological history of changes and enhancements made to the threat detection feature across different software releases.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Description
Improved detection in low sensitivity.	7.4	7.4	The method for identifying port scans and sweeps has been improved when operating in low sensitivity level. Changes are automatic; there are no new configuration settings.
Improved portscan detection.	7.2	7.2 running Snort 3	With an improved portscan detector, you can easily configure the system to detect or prevent portscans. You can refine the networks you want to protect, set the sensitivity, and so on. For devices running Snort 2 and for devices running Version 7.1 and earlier, continue to use the network analysis policy for portscan detection. New/modified screens: We added **Threat Detection** to the access control policy's **Advanced** tab. New/Modified commands: **clear threat-detection portscan**, **show threat-detection portscan**.



CHAPTER 64

Elephant Flow Detection

Elephant flows are extremely large (in total bytes), continuous flows set up by a TCP (or other protocols) flow measured over a network link. By default, elephant flows are those larger than 1 GB/10 seconds. They can cause performance duress in Snort cores. Elephant flows are not numerous, but they can occupy a disproportionate share of the total bandwidth over a period of time. They can lead to problems, such as high CPU utilization, packet drops, and other issues.

From Firewall Management Center 7.2.0 onwards (Snort 3 devices only), you can use the elephant flow feature to detect and remediate elephant flows, which helps to reduce system stress and resolve the mentioned issues.

- Elephant flow detection and remediation, on page 2221
- Elephant flow upgrade from Intelligent Application Bypass, on page 2222
- Configure elephant flow detection, on page 2222
- Use case - Configure Elephant Flow Detection Outcomes, on page 2225

Elephant flow detection and remediation

Elephant flow detection and remediation is a feature that

- detects elephant flows in network traffic,
- applies remediation actions to manage these flows, and
- requires Snort 3 as the detection engine to function.

Remediation actions

These remediation actions can be applied:

- **Bypass elephant flow**—You can configure elephant flow to bypass Snort inspection. If this is configured, Snort does not receive any packet from that flow.
- **Throttle elephant flow**—You can apply rate-limit to the flow and continue to inspect flows. The flow rate is calculated dynamically, and the system reduces the flow rate by 10 percent. Snort sends the verdict (with QoS flow reduced by 10 percent) to the firewall engine. If you choose to bypass all applications, including unidentified applications, you cannot configure the throttle action (rate-limit) for any flow.

Elephant flow upgrade from Intelligent Application Bypass

For devices running 7.2.0 or later, you must configure elephant flow settings under the **Elephant Flow Settings** section in the access control policy (Advanced settings tab) because Intelligent Application Bypass (IAB) is deprecated from version 7.2.0 onwards for Snort 3 devices.

Post-upgrade to 7.2.0 (or later), if you are using a Snort 3 device, the elephant flow configuration settings will be picked and deployed from the **Elephant Flow Settings** section and not from the **Intelligent Application Bypass Settings** section, so if you have not migrated to Elephant Flow configuration settings, your device will lose the elephant flow configuration upon the next deployment.

This table shows the IAB or elephant flow configurations that can be applied to version 7.2.0 or later and to version 7.1.0 or earlier that are running Snort 3 or Snort 2 engines.

Firewall Management Center	Firewall Threat Defense	Elephant Flow or IAB Configuration
Firewall Management Center 7.0 or 7.1	Snort 2 device	Configuration from IAB is applicable.
	Snort 3 device	Configuration from IAB is applicable.
Firewall Management Center 7.2.0	Snort 2 device	Configuration from IAB is applicable.
	Snort 3 device (7.1.0 and earlier)	Configuration from IAB is applicable.
	Snort 3 device (7.2.0 and later)	Configuration from Elephant Flow is applicable.

Configure elephant flow detection

Configure elephant flow detection to take actions on elephant flows. This helps resolve issues such as system duress, high CPU utilization, packet drops and related performance problems.

Attention Elephant flow detection is not applicable for prefiltered, trusted, or fast-forwarded flows, which do not process through Snort. As elephant flows are detected by Snort, elephant flow detection is not applicable for encrypted traffic.

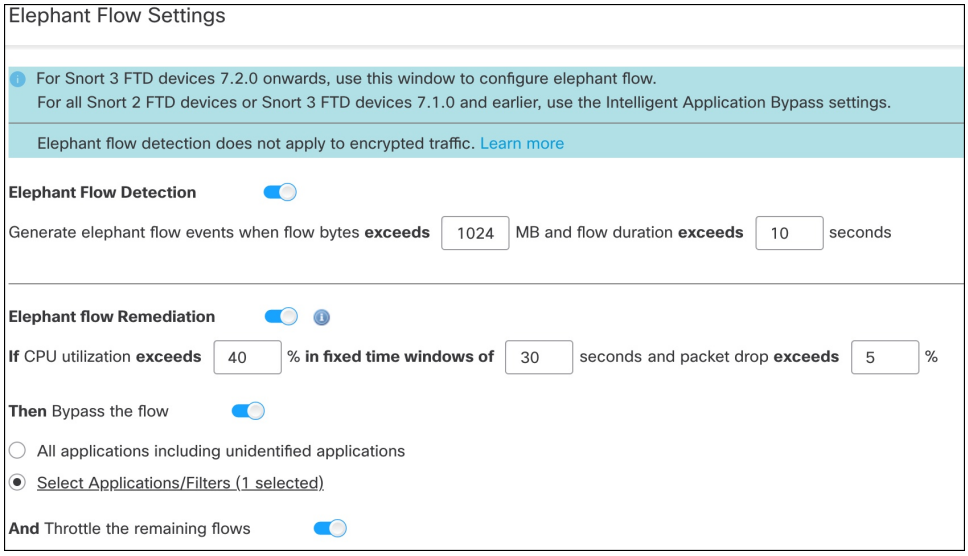
Procedure

Step 1 In the access control policy editor, click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line. Then, click **Edit** ( ) next to **Elephant Flow Settings**.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Figure 420: Configure elephant flow detection

Figure 421: Configure elephant flow detection



Step 2 Configure the values for flow bytes and flow duration for the **Elephant Flow Detection** toggle button that is enabled by default.

When they exceed your configured values, elephant flow events are generated.

Step 3 To remediate elephant flows, enable the **Elephant Flow Remediation** toggle button.

Step 4 To set the criteria for remediation of the elephant flow, configure the values for CPU utilization percentage, duration of fixed time windows, and packet drop %.

CPU utilization is calculated per elephant flow and is derived from the flow latency. If the CPU utilization crosses the configured threshold and other configurations, such as fixed time windows and packet drops, are also matched, the elephant flow remediation actions are applied. Similarly, packet drop calculation is based on the packets dropped per CPU. After the packet drop percentage exceeds the configured value on a specific CPU, the remediation actions are applied. For example, consider that configurations are set to the default, that is, CPU utilization of 40%, fixed time window of 30 seconds, and packet drop of 5%. On a specific CPU, if more than 5% of packet drops are detected and the CPU utilization per flow exceeds 40% in the fixed time frame of 30 seconds, then the flows are either bypassed or throttled.

Step 5 Configure the actions for elephant flow remediation when it meets the configured criteria.

a. **Bypass the flow**—Enable this button to bypass Snort inspection for selected applications or filters. Choose from:

- **All applications including unidentified applications**—Select this option to bypass all the application traffic. If you configure this option, you cannot configure the throttle action (rate-limit) for any flow.
- **Select Applications/Filters**—Select this option to select the applications or filters whose traffic you want to bypass; see the topic *Configuring Application Conditions and Filters* in the *Access Control Rules* chapter in the Cisco Secure Firewall Management Center Device Configuration Guide.

b. **Throttle the flow**—Enable this button to apply rate-limit to the flow and continue to inspect flows. Note that you can select the applications or filters to bypass Snort inspection and throttle the remaining flows.

Note Automatic removal of throttle from a throttled elephant flow occurs when the system is out of duress, that is, the percentage of Snort packet drops is less than your configured threshold. Consequently, rate limiting is also removed.

You can also manually remove throttling from a throttled elephant flow, using these threat defense commands:

- **clear efd-throttle <5-tuple/all> bypass**—This command removes throttling from the throttled elephant flow and bypasses Snort inspection.
- **clear efd-throttle <5-tuple/all>**—This command removes throttling from the throttled elephant flow and Snort inspection continues. Elephant flow remediation is skipped after using this command.

For more information about these commands, refer to the Cisco Secure Firewall Threat Defense Command Reference.

Note Taking action on elephant flows (bypass and throttle the flow) is not supported on Cisco Firepower 2100 series devices.

Step 6 In the **Remediation Exemption Rule** section, click **Add Rule** to configure L4 access control list (ACL) rules for flows that must be exempted from remediation.

a) In the **Add Rule** window, use the **Networks** tab to add the network details, that is the source network and the destination network. Use the **Ports** tab to add the source port and the destination port.

If an elephant flow is detected and it matches the rules that are defined, an event is generated with the reason as **Elephant Flow Exempted** in the **Reason** column header of **Connection Events**.

b) In the **Remediation Exemption Rule** section, you can view the flows that are exempt from the remediation action.

c) Click **OK** to save the elephant flow settings.

Step 7 Click **Save** to save the policy.

What to do next

Deploy configuration changes; see Deploy configuration changes, on page 135.

After configuring your elephant flow settings, monitor your connection events to see if any flows are detected, bypassed, or throttled. You can view this in the **Reason** field of your connection event. The three reasons for elephant flow connections are:

- Elephant Flow
- Elephant Flow Throttled
- Elephant Flow Trusted

Attention Enabling elephant flow detection alone does not cause generation of connection events for elephant flows. If a connection event is already logged for another reason and the flow is also an elephant flow, then the **Reason** field contains this information. However, to ensure that you are logging all elephant flows, you must enable connection logging in the applicable access control rules.

Refer to Cisco Secure Firewall Elephant Flow Detection for more information.

Use case - Configure Elephant Flow Detection Outcomes

This use case provides a sample scenario for configuring outcomes and system responses that detect elephant flows in network traffic to optimize performance and resource usage.

Elephant flows

An elephant flow is an extremely large network connection that

- consists of long-running connections set up by TCP or other protocols measured over a network link,
- measures larger than 1 GB per 10 seconds by default, and
- can cause performance duress or issues in Snort cores by consuming excessive CPU resources.

Impact on system performance

Elephant flows can potentially consume an excessive amount of CPU resources and impact other competing flows for detection resources and cause issues, such as increased latency or packet drops.

Benefits of elephant flow detection and remediation

- Elephant flow configuration allows customization and the option to bypass or even throttle elephant flows.
- You can choose to bypass or throttle flows that are based on your chosen applications to provide Snort inspection of suspect traffic, while bypassing more trusted traffic.
- Elephant flow remediation helps prioritize and free up more bandwidth for your internal applications, depending on your specific requirements.

How elephant flows work

Summary

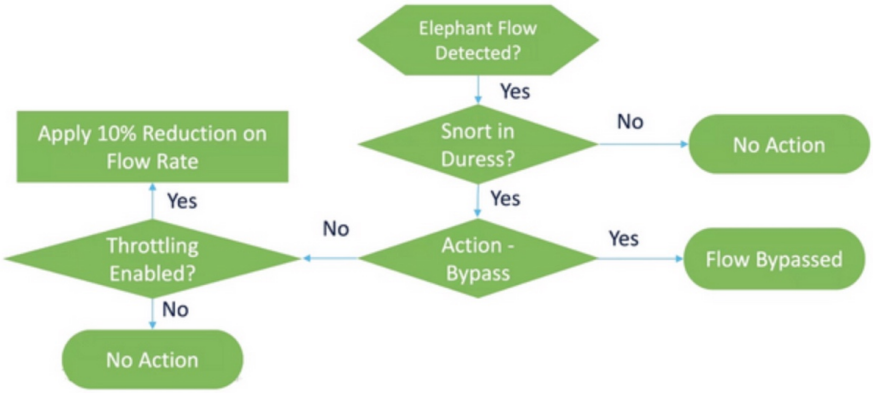
The key components involved in the elephant flow process are:

- System detection: Monitors for Snort duress conditions based on configured parameters.
- Flow identification: Determines when a flow qualifies as an elephant flow.

- CPU monitoring: Tracks CPU utilization against configured thresholds.
- Bypass action: Allows traffic for trusted applications to pass without Snort inspection.
- Throttle action: Reduces the flow throughput in 10 percent increments until CPU utilization drops below the threshold.

Workflow

Figure 422: Elephant flow workflow



These stages describe how elephant flows are processed:

1. The system continuously monitors traffic flows and applies intrusion policy processing to all flows, including potential elephant flows, ensuring that attacks are detected early in connections.
2. When an elephant flow is detected based on configured parameters, the system evaluates whether a Snort duress condition exists by checking CPU utilization and time window parameters.

   No action is taken unless the system detects a Snort duress condition (performance issue). The system does not throttle or bypass a flow just because it is large.
3. If duress conditions are met, the system determines whether to bypass or throttle the elephant flow based on configuration settings.

   The actions of throttle and bypass are mutually exclusive. This means that you can either bypass or throttle a flow, but not both.
4. For bypass actions, if configured for specific applications only, the system allows trusted application flows to pass without Snort inspection while throttling remaining flows causing duress.

   This ensures that other non-trusted application flows still receive full Snort inspection, although their bandwidth is reduced.
5. For throttle actions, the system reduces flow throughput in 10 percent increments until CPU utilization reduces to below the configured threshold.

Sample business scenarios

In a data center, several activities are happening, such as replication of data between clusters, virtual machine integration, and database backup. Users in an organization could be watching videos on an OTT service or

downloading them. Bandwidth utilization for such activities might result in elephant flows that slow down the network and impact the performance of important tasks. As a network administrator (and depending on your specific requirements), you want visibility into such large flows that are causing bandwidth issues and remediate them.

As an example, let's see how you can configure elephant flow parameters to bypass Snort inspection for WebEx traffic (which your organization uses for real-time video conferencing) and throttle the remaining applications or connections, including videos, movies, and so on.

Prerequisites

Ensure that you are running management center 7.2.0 or later and that the managed threat defense is also 7.2.0 or later.

When you enable only elephant flow detection, no additional connection events are generated. The system adds the Elephant Flow notation to matching connections that are already logged to the management center. **To log these events, you must enable connection logging in your access control policy.** You can do that for specific rules or add a Monitor rule that logs all connections, including elephant flows.

Configure elephant flow parameters

Configure elephant flow detection and remediation settings to identify high-bandwidth connections, and manage them through bypassing or throttling to maintain optimal system performance during high CPU utilization.

Elephant flows are high-bandwidth, long-duration connections that can impact system performance. By configuring elephant flow parameters, you can detect these flows and apply appropriate remediation actions such as bypassing trusted applications from inspection or throttling flows that cause system duress.

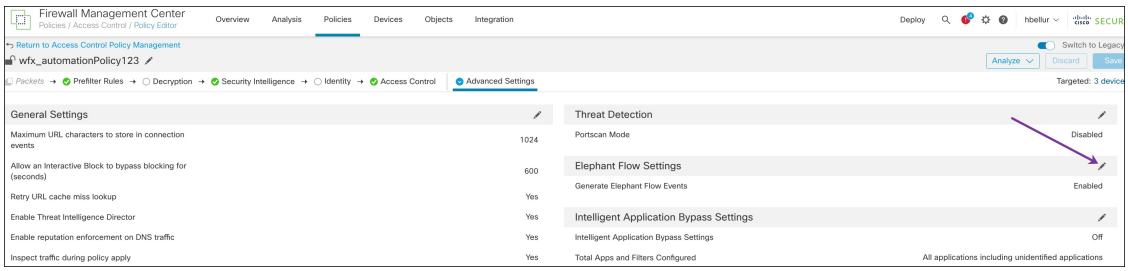
Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy that you want to edit.

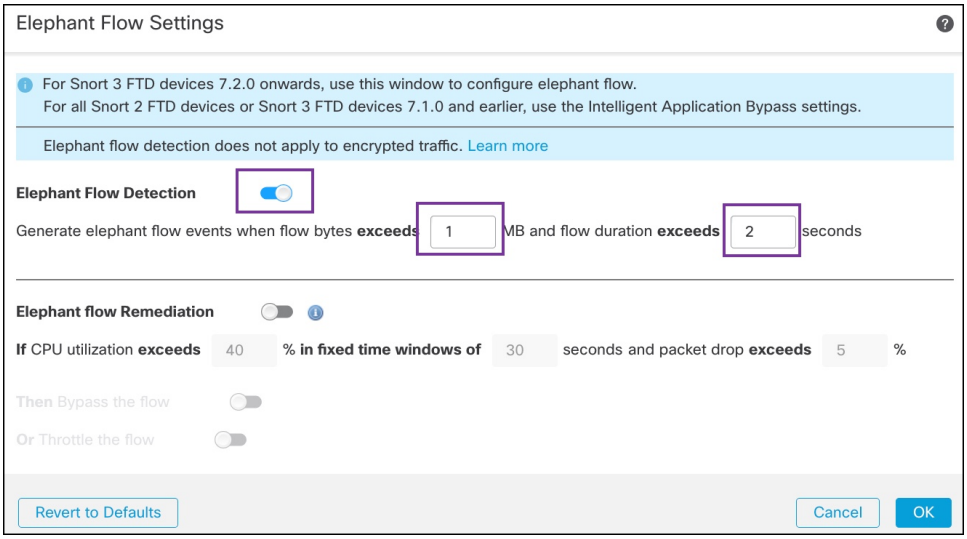
Step 3 Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 Click **Edit** (✎) next to **Elephant Flow Settings**.



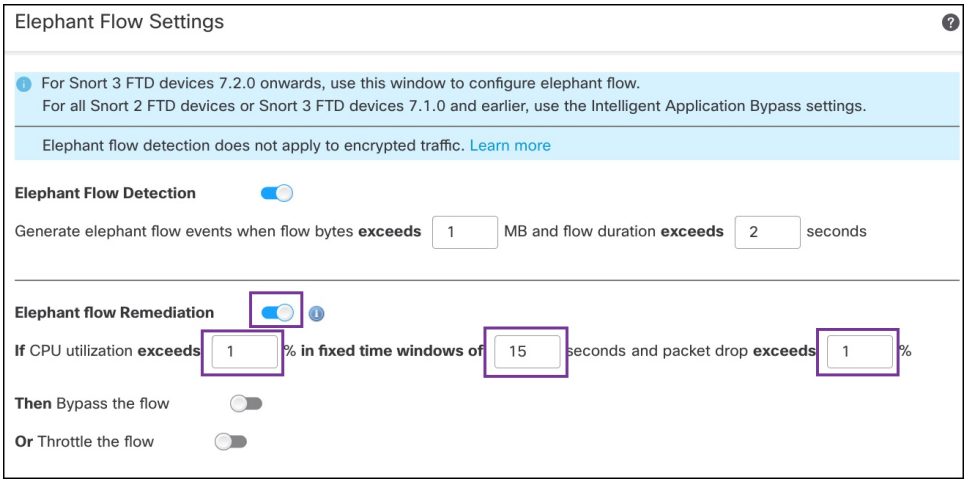
Step 5 The **Elephant Flow Detection** toggle button is enabled by default. The default setting enables detection only and no default action is configured. The detection settings allow you to adjust the flow bytes and duration so that you can identify the elephant flows in your system.

As a test setting, configure the flow bytes and duration parameters, as shown in the following figure.

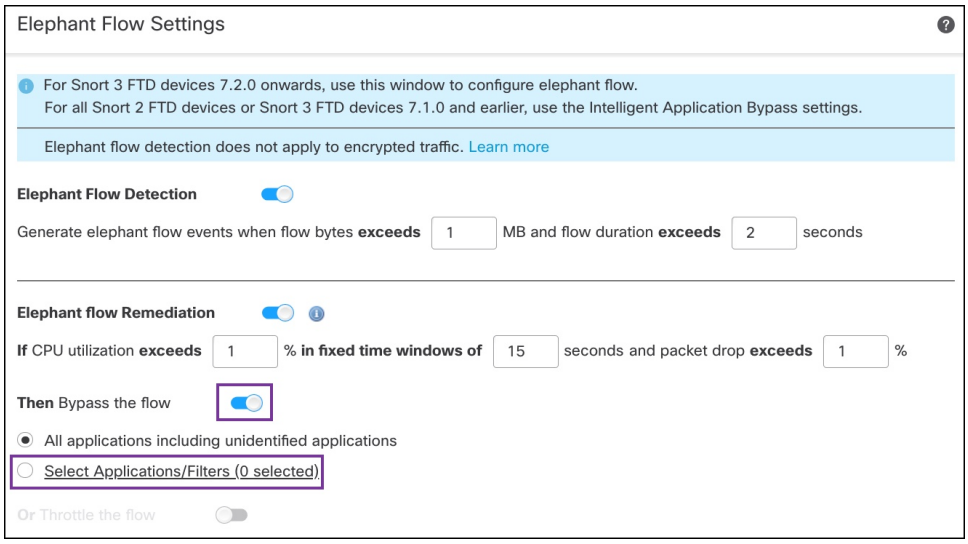


Step 6 Enable the **Elephant Flow Remediation** toggle button. When an elephant flow is detected, you can choose to bypass or throttle the flow. Bypassing a flow means that the traffic is allowed to pass without Snort inspection. Throttling indicates that the flow throughput is reduced. This rate reduction is done in 10 percent increments until the CPU utilization decreases to less than the configured threshold.

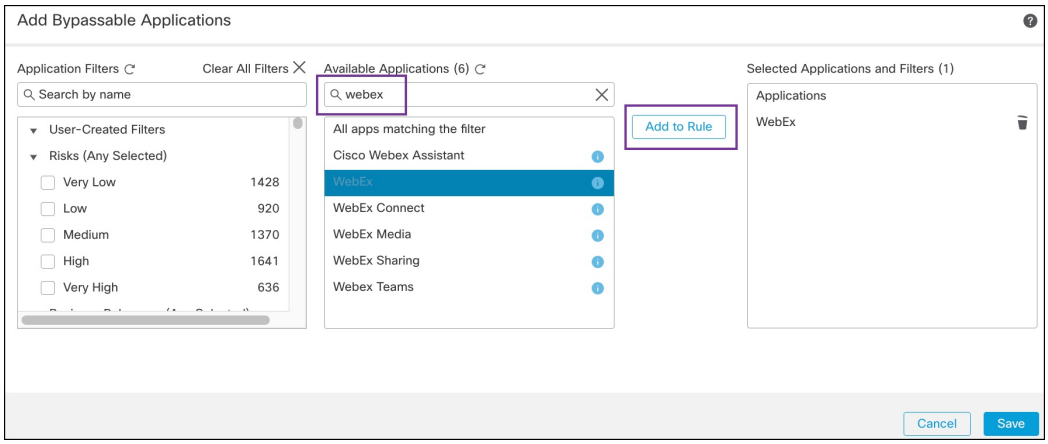
As a test setting, configure the elephant flow remediation parameters as shown in the following figure.



Step 7 Enable the **Bypass the flow** toggle button and click the **Select Applications/Filters** radio button.



Step 8 Under **Application Filters**, search for and select the **WebEx** application, add it to the rule, and click **Save**. This means that WebEx connections are trusted and prioritized. These connections will skip Snort inspection if detected as elephant flows based on the configured parameters.



Step 9 Enable the **Throttle** toggle button to throttle the remaining flows (causing duress). This ensures that all the other flows are slowed down in 10 percent increments until the Snort duress condition is met.

Click **OK** and then **Save**.

What to do next

Deploy configuration changes.

View events for elephant flows

This task enables you to monitor elephant flow connection events to track flow detection, bypass, and throttling activities through the Reason field in connection events.

After configuring your elephant flow settings, monitor your connection events to see if any flows are detected, bypassed, or throttled. You can see this information in the **Reason** field of your connection events. The three types for elephant flow connections are:

- Elephant Flow
- Elephant Flow Throttled
- Elephant Flow Trusted

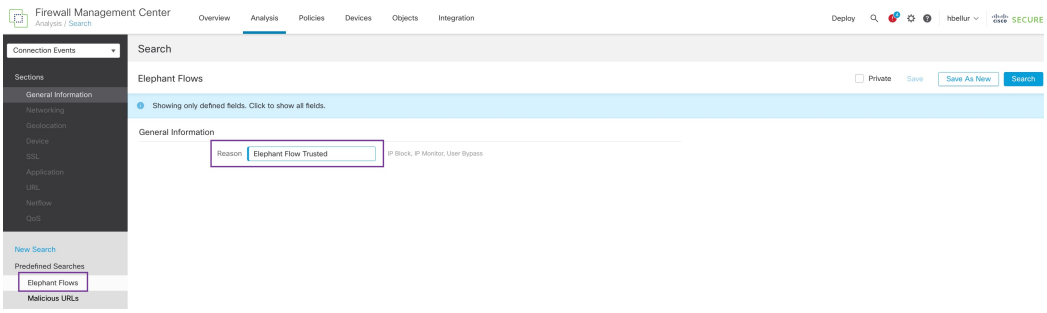
Procedure

Step 1 Choose **Analysis** > **Connections** > **Events**. You can also view the events from the **Unified Events** viewer.

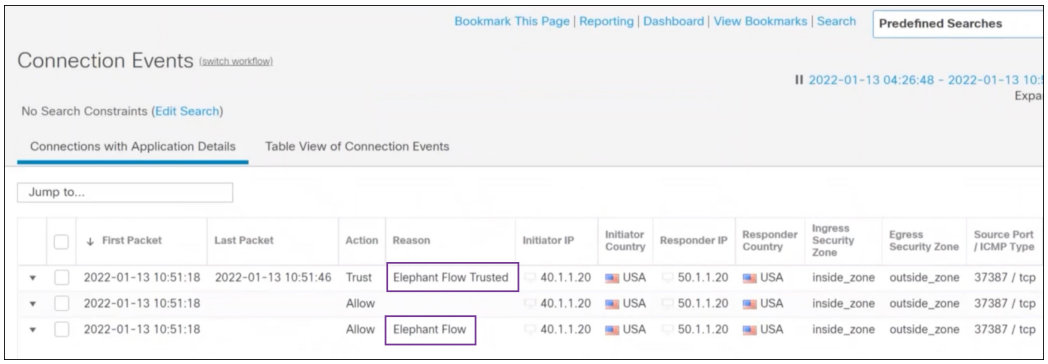
Step 2 In the **Connection Events** page, from the **Predefined Search** drop-down list, choose **Elephant Flows** to display elephant flow events.



Tip To see **Elephant Flow Trusted** or **Elephant Flow Throttled** event types, click the **Edit Search** link on the top-left corner of the page and in the **Reason** field, choose **Elephant Flows** in the left panel. Enter **Elephant Flow Trusted** or **Elephant Flow Throttled**, depending on what you want to search.



Step 3 View the elephant flow that was detected mid-flow and the **Reason** field shows **Elephant Flow**. At the end of the flow, it was bypassed and the **Reason** field shows **Elephant Flow Trusted**.



Configure elephant flow remediation exemption

This task allows you to create exemption rules for specific flows that should not be subject to remediation actions even when detected as elephant flows.

You can configure L4 access control list (ACL) rules for flows that must be exempted from remediation. If a flow is detected as an elephant flow and it matches the rules that are defined, that flow is exempted from remediation.

Before you begin

You must be running management center version 7.4.0 or later and the managed threat defense must also be on version 7.4.0 or later.

Follow these steps to configure elephant flow remediation exemption.

Procedure

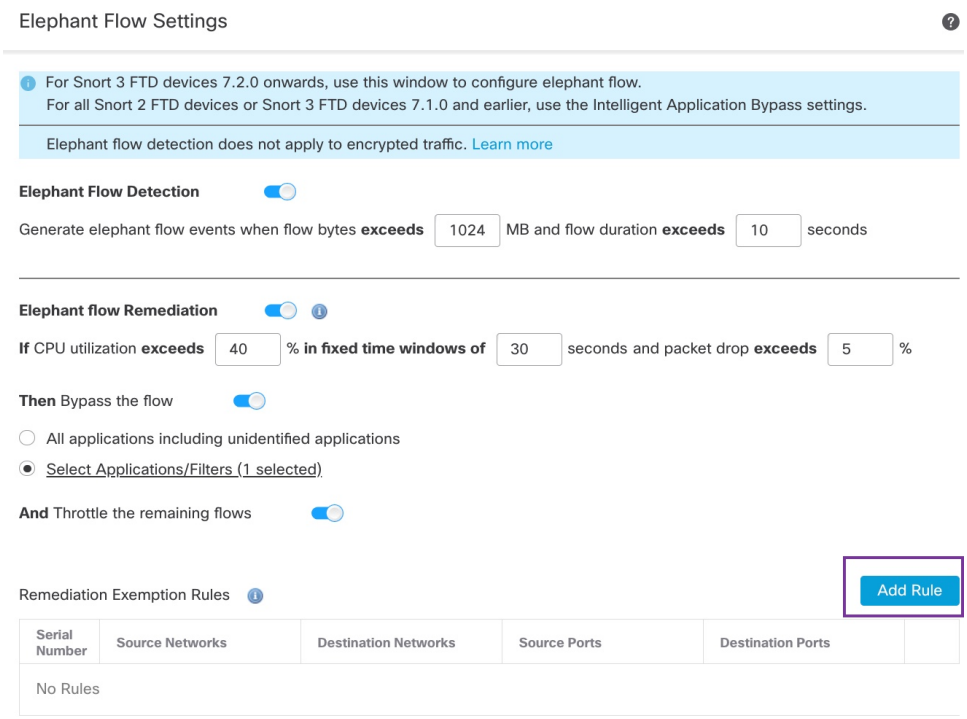
Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

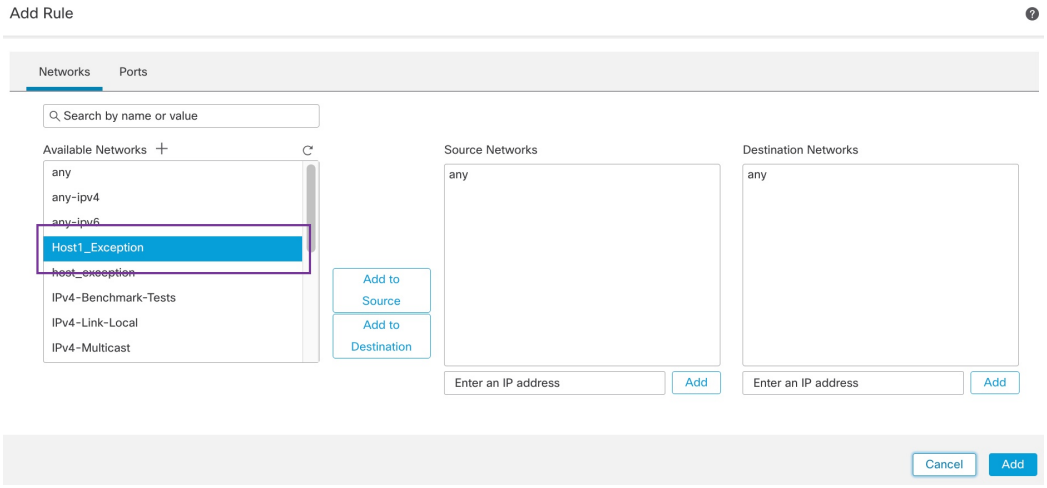
Step 3 Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 Click **Edit** (✎) next to **Elephant Flow Settings**. Ensure that you have configured the elephant flow detection and remediation parameters. See Configure elephant flow parameters, on page 2227.

Step 5 Click the **Add Rule** button next to **Remediation Exemption Rules**.



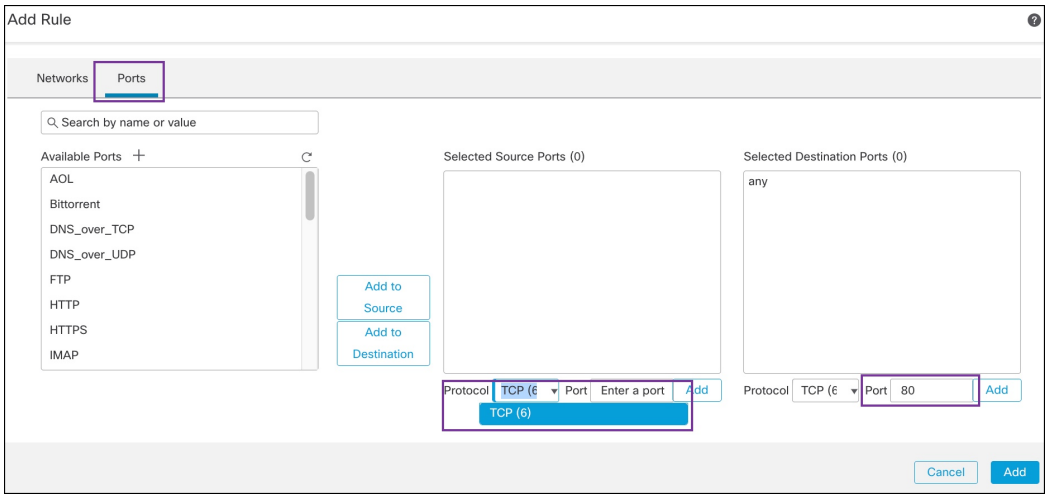
Step 6 From the list of **Available Networks**, choose the configured host to exempt from elephant flow remediation. For the purposes of this example, we have created a host called "Host1_Exception."



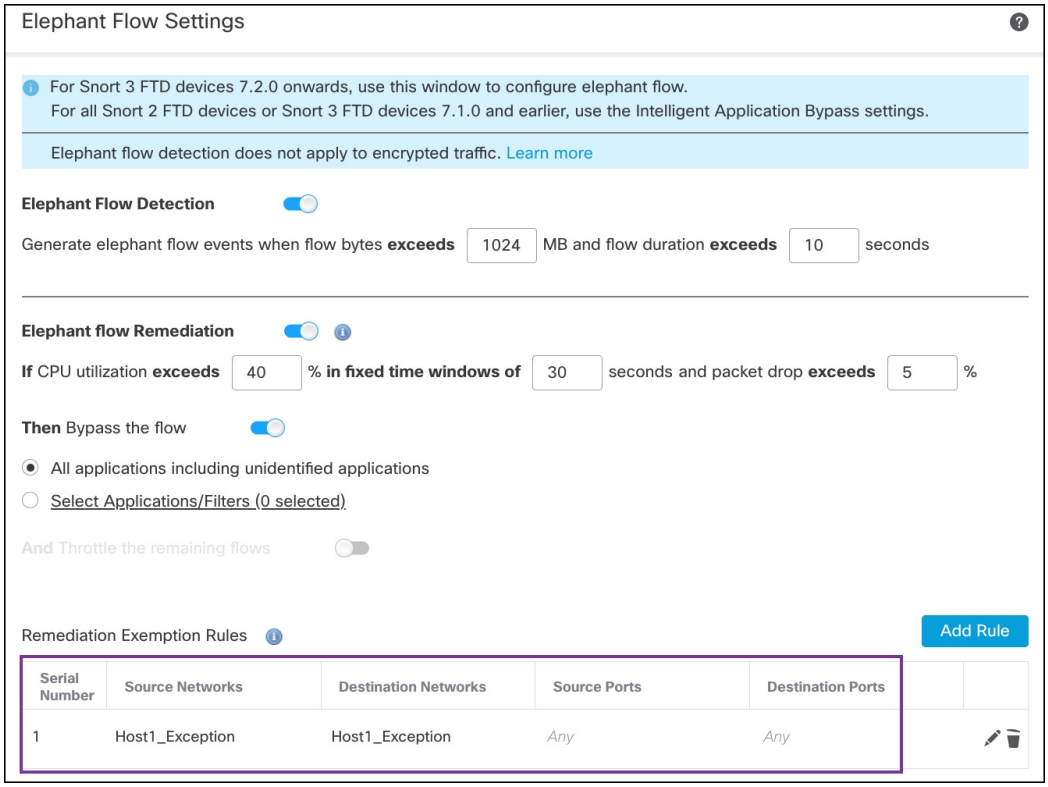
Step 7 Click **Add to Source** or **Add to Destination** as needed to add this host to the source or destination.

Step 8 Click the **Ports** tab.

a) For the source port, choose **Protocol** as TCP, enter **80** as the destination port, then click **Add**.



b) Click **OK**.



Step 9 Click **Save**.

What to do next

Deploy configuration changes.

View events for elephant flow remediation exemption

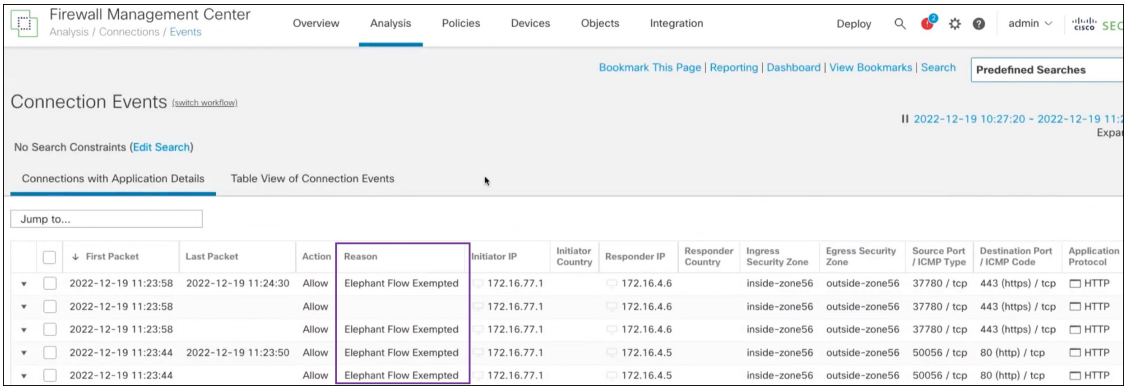
This task allows you to monitor and review elephant flows that have been exempted from remediation to understand network traffic patterns and exemption reasons.

Elephant flows are high-volume network connections that may require special handling. When these flows are exempted from remediation, you can view the exemption events to track and analyze the decision.

Procedure

Step 1 Choose **Analysis** > **Connections** > **Events**. You can also view the events from the **Unified Events** viewer.

Step 2 View the elephant flows that were exempted from remediation. The **Reason** field shows **Elephant Flow Exempted**.



Additional references

For detailed conceptual information, see the Elephant Flow Detection for Snort 3 chapter in this guide or the content in the following link:

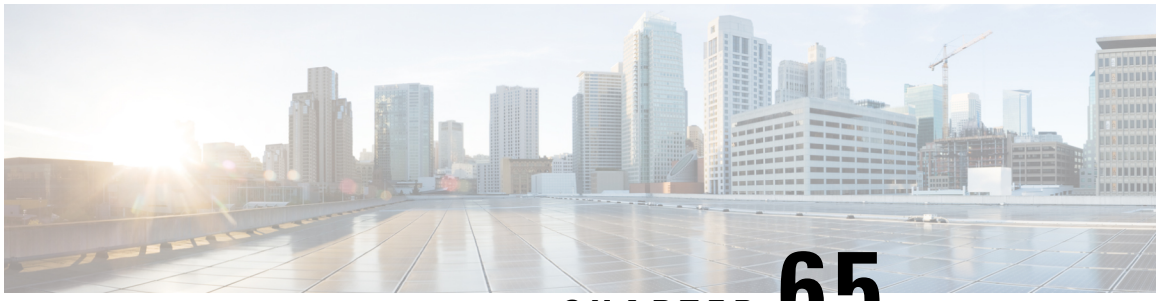
- Elephant Flow Detection



PART XII

Network Discovery

- Network discovery overview, on page 2237
- Host identity sources, on page 2247
- Application detection, on page 2283
- Network Discovery Policies, on page 2305



CHAPTER 65

Network discovery overview

Network discovery is the automated process for identifying active devices and their connections within a network to maintain an accurate inventory.

- Detection of host, application, and user data, on page 2237
- Host and application detection fundamentals, on page 2238

Detection of host, application, and user data

Detection of host, application, and user data is a network monitoring capability that

- collects host and application data using host identity sources and application detectors according to network discovery policy settings,
- gathers user data through user identity sources according to network discovery and identity policy configurations, and
- enables comprehensive network asset mapping, forensic analysis, behavioral profiling, access control, and vulnerability mitigation.

Host, application, and user data collection

The system uses *network discovery* and *identity* policies to collect host, application, and user data for traffic on your network. The system analyzes discovery and identity data to create a detailed map of network assets, perform forensic analysis, behavioral profiling, access control, and respond to potentials vulnerabilities and hazards to your organization.

The system collect various types of data to enhance network security and performance analytics:

- Host and Application Data: Collected by host identity sources and application detectors according to the settings in your network discovery policy. Managed devices observe traffic on the network segments you specify.

  For more information about fundamentals of host and application data, refer to Host and application detection fundamentals, on page 2238
- User Data: Collected by user identity sources according to the settings in your network discovery and identity policies. Use the data for user awareness and user control.

  For more information about user identity, refer to User identity, on page 1819.

Logging discovery and identity data allows you to take advantage of many features in the system, including:

- Viewing the network map, which is a detailed representation of your network assets and topology that you can view by grouping hosts and network devices, host attributes, application protocols, or vulnerabilities.
- Performing application and user controls using access control rules with application conditions, realm conditions, user conditions, user group conditions, and ISE attribute conditions.
- Viewing complete profiles for detected hosts.
- Monitoring network assets and user activity through dashboards.
- Viewing detailed information on the discovery events and user activity.

  Logging and using NetFlow connections, if applicable.
- Associate hosts, servers, and clients with susceptible exploits to identify and mitigate vulnerabilities.

  Evaluate the impact that intrusion events have on your network, and tune intrusion rule states so that they provide maximum protection for your network assets.
- Receiving alerts by email, SNMP trap, or syslog when the system generates either an intrusion event with a specific impact flag, or a specific type of discovery event.
- Monitoring your organization's compliance with an allow list of allowed operating systems, clients, application protocols, and protocols.
- Creating correlation policies with rules that trigger and generate correlation events when the system generates discovery events or detects user activity.

Host and application detection fundamentals

The network discovery policy is a feature that serves multiple purposes. You can:

- enable device identification,
- monitor network devices and services, and
- configure detection settings to track performance.

For more information on host and application detection, refer to Host data collection overview, on page 2247 and Application detection, on page 2283.

Passive detection of operating system and host data

Passive detection is a network mapping method that

- analyzes network traffic and any exported NetFlow data to populate the network map,
- provides contextual information about network assets, such as operating systems and running applications, and
- serves as the system's default detection method.

Operating system determination process

If traffic from a monitored host does not offer conclusive evidence of the host's operating system, the network map displays the most likely operating system. For example, a NAT device may appear to be running several operating systems because of the hosts "behind" the NAT device. To make this most-likely determination, the system uses a confidence value it assigns to each detected operating system, and the amount of corroborating data among detected operating systems.



Note The system does not consider reported "`unknown`" applications and operating systems in its determination.

If passive detection inaccurately identifies your network assets, consider the placement of your managed devices. You can also augment the system's passive detection capabilities with custom operating-system fingerprints and custom application detectors. Or, you can use *active detection*, which is not based on traffic analysis, but instead allows you to directly update the network map using scan results or other information sources.

Active detection of operating system and host data

Active detection is a network discovery capability that

- adds host information collected by active sources to network maps,
- discovers operating systems and applications on hosts using tools like Nmap Scanner, and
- allows active addition of host input data to network maps.

Host input data is categorized into:

- *User input data*—Data added through the system user interface, permitting modification of the host's operating system or application identity.
- *Host import input data*—Data imported using a command line utility.

Identity retention and priority behavior

The system retains one identity for each active source. For example, when you run an Nmap scan instance, previous results are updated with the new scan data. However, replacing scan results with data from a client whose results are imported through the command line, the system retains both the identities. The system then uses the priorities set in the network discovery policy to determine which active identity to use as the current identity.

User input supersedes other identities, regardless of the source. For example, if UserA sets the operating system through the host profile, and then UserB changes that definition through the host profile, the definition set by UserB is retained. User input overrides all other active sources and is used as the current identity if it exists.

Current identities for applications and operating systems

A *current identity* is an identity determination for an application or operating system that

- represents the identity that the system finds most likely to be correct,

- is used for vulnerability assignments and impact assessments, and
- is determined by source priorities when multiple identities exist for the same host.

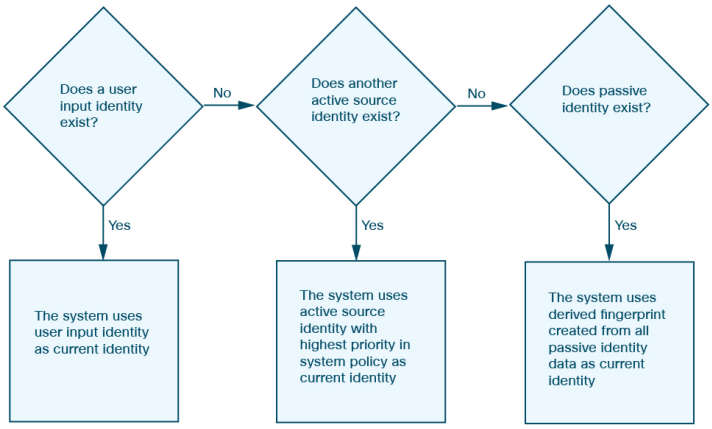
Current identity uses

The system uses the current identity for an operating system or application for these purposes:

- Assign vulnerabilities to a host
- Assess impact
- Evaluate correlation rules relating to operating system identifications, host profile qualifications, and compliance allow lists
- Display in the Hosts and Servers table views in workflows
- Display in the host profile
- Calculate the operating system and application statistics on the Discovery Statistics page

The system uses source priorities to determine which active identity should be used as the current identity for an application or operating system.

Figure 423: Current identity determination process



The database may retain information from multiple sources for an operating system or for a specific application on a host.

The system treats an operating system or application identity as the current identity when the source for the data has the highest source priority. Possible sources have this priority order:

1. User
2. Scanner and application (set in the Network Discovery Policy)
3. Managed devices
4. NetFlow records

If a new higher priority application identity has less detail than the current identity, it will not override the current application identity.

In addition, when an identity conflict occurs, the resolution of the conflict depends on settings in the network discovery policy or on your manual resolution.

Operating system assignment as current identity

For example, if a user sets the operating system to Windows 2003 Server on a host, Windows 2003 Server becomes the current identity and attacks targeting Windows 2003 Server vulnerabilities on that host are given a higher impact. The vulnerabilities listed for that host in the host profile include Windows 2003 Server vulnerabilities.

Current user identities

A current user identity is a system determination that:

- identifies the last authoritative user login as the current user when multiple users log into the same host
- assumes only one user is logged into any given host at a time
- records the first login for a user on a specific host and disregards subsequent logins by the same user, and
- reports the last user detected by the server to the Firewall Management Center when multiple users are logged in through remote sessions.

User login tracking behavior

The system uses specific rules to determine current user identity:

- When the system detects multiple logins to the same host by different users, the system assumes that only one user is logged into any given host at a time, and that the current user of a host is the last authoritative user login. If only non-authoritative user logins have been logged into the host, the last non-authoritative user login is considered the current user. If multiple users are logged in through remote sessions, the last user reported by the server is the user reported to the Firewall Management Center.
- When the system detects multiple logins to the same host by the same user, the system records the first time that a user logs into a specific host and disregards subsequent logins. If an individual user is the only person who logs into a specific host, the only login that the system records is the original login.
- If another user logs into that host, however, the system records the new login. Then, if the original user logs in again, his or her new login is recorded.

Application and operating system identity conflicts

An *identity conflict* is a system condition that

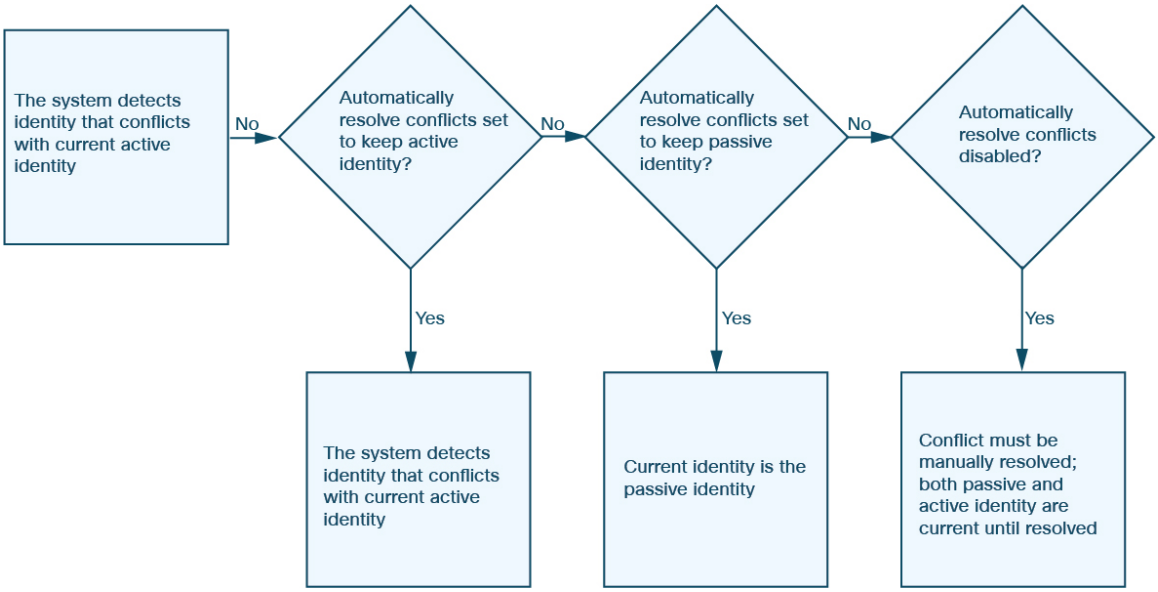
- occurs when the system reports a new passive identity that conflicts with the current active identity and previously reported passive identities
- results in both conflicting identities being listed as current and used for impact assessment until the conflict is resolved, and
- can be resolved automatically by choosing to always use the passive identity or always use the active identity.

Identity conflict behavior and resolution

When an identity conflict exists for the identity of the host's operating system or one of the applications on the host, the system lists both conflicting identities as current and uses both for impact assessment until the conflict is resolved.

A user with Administrator privileges can resolve identity conflicts automatically by choosing to always use the passive identity or always use the active identity. Unless you disable automatic resolution of identity conflicts, identity conflicts are always automatically resolved.

A user with Administrator privileges can also configure the system to generate an event when an identity conflict occurs. That user can then set up a correlation policy with a correlation rule that uses an Nmap scan as a correlation response. When an event occurs, Nmap scans the host to obtain updated host operating system and application data.



Operating system identity conflict scenario

The previous passive identity for an operating system is reported as Windows 2000, then an active identity of Windows XP becomes current. Next, the system detects a new passive identity of Ubuntu Linux 8.04.1. The Windows XP and the Ubuntu Linux identities are in conflict.

NetFlow data

NetFlow data is a collection of network flow statistics that

- provides statistics on packets flowing through a router through a Cisco IOS application
- is available on Cisco networking devices and can also be embedded in Juniper, FreeBSD, and OpenBSD devices, and
- stores records of flows in a database on the device called the NetFlow cache when NetFlow is enabled on a network device.

NetFlow data processing and usage

A flow, called a *connection* in the system, is a sequence of packets that represents a session between a source and destination host, using specific ports, protocol, and application protocol. The network device can be configured to export this NetFlow data. In this documentation, network devices configured in this way are called *NetFlow exporters*.

Managed devices can be configured to collect records from NetFlow exporters, generate unidirectional end-of-connection events based on the data in those records, and finally send those events to the Firewall Management Center to be logged in the connection event database. You can also configure the network discovery policy to add host and application protocol information to the database based on the information in NetFlow connections.

You can use this discovery and connection data to supplement the data gathered directly by your managed devices. This is especially useful if you have NetFlow exporters monitoring networks that your managed devices cannot monitor.

Requirements for using NetFlow data (principle)

NetFlow device configuration

Before you configure the system to analyze NetFlow data, you **must** enable the NetFlow feature on the routers or other NetFlow-enabled network devices you plan to use. Configure the devices to broadcast NetFlow data to a destination network where the sensing interface of a managed device is connected.

NetFlow version and field specifications

The system can parse both NetFlow version 5 and NetFlow version 9 records. NetFlow exporters **must** use one of those versions if you export data. Ensure the exported NetFlow templates and records contain specific fields like IN_BYTES, IN_PKTS, PROTOCOL, among others. If your NetFlow exporters are using version 9, which you can customize, you **must** make sure that the exported templates and records contain these fields, in any order:

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Managed device deployment

Your deployment must include at least one managed device that can monitor NetFlow exporters. Connect at least one sensing interface on that managed device to a network for collecting exported NetFlow data. The system does not support the direct collection due to lack of IP addresses on sensing interfaces.

Sampled NetFlow considerations

Sampled NetFlow feature available on some network devices collects NetFlow statistics on only a subset of packets that pass through the devices. While enabling this feature improves CPU utilization, it may affect the NetFlow data collected for system analysis.

Differences between NetFlow and managed device data

NetFlow and managed device data differences are analytical distinctions that

- result from converting exported NetFlow records into connection logs and host and application protocol data rather than directly analyzing traffic,
- affect statistics on detected connections, operating system information, and application data, and
- impact the identification of connection initiators and responders.

Key differences in data collection and analysis

The traffic represented by NetFlow data is not directly analyzed. Instead, it converts exported NetFlow records into connection logs and host and application protocol data.

As a result, there are several differences between converted NetFlow data and the discovery and connection data gathered directly by your managed devices. You should keep these differences in mind when performing analysis that requires:

- Statistics on the number of detected connections
- Operating system and other host-related information (including vulnerabilities)
- Application data, including client information, web application information, and vendor and version server information
- Knowing which host in a connection is the initiator and which is the responder

Network discovery policy versus access control policy:

You configure NetFlow data collection, including connection logging, using rules in the network discovery policy. Contrast this with connection logging for connections detected by managed devices, which you configure per access control rule.

Types of connection events:

- Because NetFlow data collection is linked to networks rather than access control rules, you do not have granular control over which NetFlow connections the system logs.
- NetFlow data cannot generate Security Intelligence events.
- NetFlow-based connection events can be stored in the connection event database only; you cannot send them to the system log or an SNMP trap server.

Number of connection events generated per monitored session:

For connections detected directly by managed devices, you can configure the access control rule to log a bidirectional connection event at the beginning or end of a connection, or both.

In contrast, because exported NetFlow records contain unidirectional connection data, the system generates at least two connection events for each NetFlow record it processes. This also means that a summary's connection count is incremented by two for every connection based on NetFlow data, providing an inflated count of the number of connections that are actually occurring on your network.

Because the NetFlow exporter outputs records at regular intervals, even during an ongoing connection, long-running sessions can result in multiple exported records, each of which generates a connection event. For example, if the NetFlow exporter exports every five minutes, and a particular connection lasts twelve minutes, the system generates six connection events for that session:

- One pair of events for the first five minutes
- One pair for the second five minutes
- A final pair when the connection is terminated

Host and operating system data:

Hosts added to the network map from NetFlow data do not have operating system, NetBIOS, or host type (host vs network device) information. However, using the host input feature, you can manually set a host's operating system identity.

Application data:

For connections detected directly by managed devices, the system can identify application protocols, clients, and web applications by examining the packets in the connection.

When the system processes NetFlow records, the system uses a port correlation in `/etc/sf/services` to extrapolate application protocol identity. However, there is no vendor or version information for those application protocols, nor do connection logs contain information on client or web applications used in the session. You can, however, manually provide this information using the host input feature.

Note that a simple port correlation means that application protocols running on non-standard ports may be unidentified or misidentified. Additionally, if no correlation exists, the system marks the application protocol as `unknown` in connection logs.

Vulnerability mappings:

The system cannot map vulnerabilities to hosts monitored by NetFlow exporters, unless you use the host input feature to manually set either a host's operating system identity or an application protocol identity. Note that because there is no client information in NetFlow connections, you cannot associate client vulnerabilities with hosts created from NetFlow data.

Initiator and responder information in connections:

For connections detected directly by managed devices, the system can identify which host is the initiator, or source, and which is the responder, or destination. However, NetFlow data does not contain initiator or responder information.

When the System processes NetFlow records, it uses an algorithm to determine this information based on the ports each host is using, and whether those ports are well-known:

- If both or neither port being used is a well-known port, the system considers the host using the lower-number port to be the responder.
- If only one of the hosts is using a well-known port, the system considers that host to be the responder.

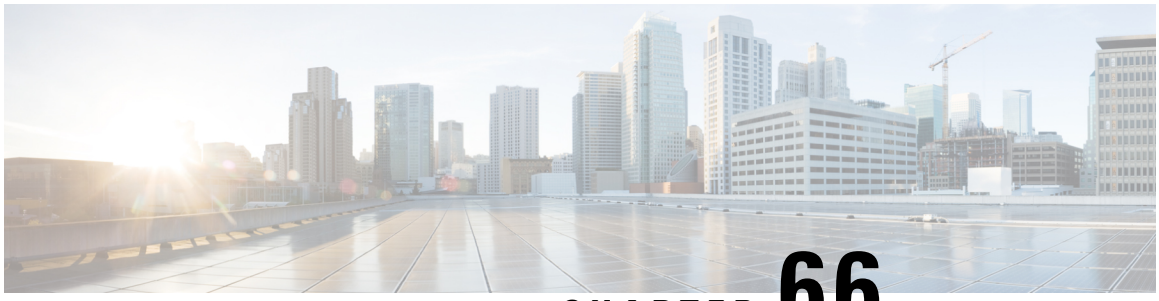
For this purpose, a well-known port is any port that is either numbered from 1 to 1023,or any port that the system considers a server port, regardless of number.

NetFlow byte counts

Connection events based on unidirectional NetFlow records contain only one byte count, which the system assigns to either **Initiator Bytes** or **Responder Bytes**, depending on the port-based algorithm. The system sets the other field to 0. Note that if you are viewing connection summaries (aggregated connection data) of NetFlow records, both fields may be populated.

NetFlow-only connection event fields

A small number of fields are present only in connection events generated from NetFlow records; refer to *Information Available in Connection Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide*.



CHAPTER 66

Host identity sources

These topics provide information on host identity sources.

- Host data collection overview, on page 2247
- Requirements and prerequisites for host identity sources, on page 2248
- Determine which host operating systems the system can detect, on page 2248
- Identifying host operating systems, on page 2249
- Custom fingerprinting, on page 2249
- Host input data, on page 2257
- Nmap scanning, on page 2264
- History for host identity sources, on page 2282

Host data collection overview

Host data collection is a passive monitoring mechanism that

- compares specific packet header values and other unique data from network traffic against established definitions called *fingerprints*,
- determines information about the hosts on your network, and
- identifies network topology and system characteristics through traffic analysis.

Host information collected

The system determines this information about hosts on your network:

- The number and types of hosts (including network devices such as bridges, routers, load balancers, and NAT devices).
- Basic network topology data, including the number of hops from the discovery point on the network to the hosts.
- The operating systems running on the hosts.
- Applications on the hosts and users associated with these applications.

If the system cannot identify a host's operating system, you can create custom client or server fingerprints. The system uses these fingerprints to identify new hosts. You can map fingerprints to systems in the

vulnerability database (VDB) to allow the appropriate vulnerability information to be displayed whenever a host is identified using the custom fingerprint.

Note In addition to collecting host data from monitored network traffic, the system can collect host data from exported NetFlow records, and you can actively add host data using Nmap scans and the host input feature.

Requirements and prerequisites for host identity sources

This topic provides the necessary requirements and prerequisites to manage host identity sources:

Requirement	Details
Model support	Any.
Supported domains	Any, with the exception of custom fingerprinting, which is Leaf only.
User roles	• Admin • Discovery Admin, except for third-party data and custom mappings.

Determine which host operating systems the system can detect

To verify the exact operating systems that the system can fingerprint, you can view the list of available fingerprints during the process of creating a custom operating system fingerprint. This helps you understand which operating systems the system is capable of identifying.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Custom Operating Systems**.

Step 3 Click **Create Custom Fingerprint**.

Step 4 In the **OS Vulnerability Mappings** section, view the options available in the drop-down lists. These options represent the operating systems that the system can fingerprint.

What to do next

For more information, refer to Identifying host operating systems, on page 2249.

Identifying host operating systems

If the system does not correctly identify a host operating system (for example, it shows in the Host Profile as Unknown or is incorrectly identified), try the strategies listed here.

Procedure

Try one of these strategies:

- Check the Network Discovery Identity Conflict Settings.
- Create a custom fingerprint for the host.
- Run an Nmap scan against the host.
- Import data into the network map, using the host input feature.
- Manually enter operating system information.

Custom fingerprinting

The system includes operating system *fingerprints* that the system uses to identify the operating system on each host it detects. However, sometimes the system cannot identify a host operating system or misidentifies it because no fingerprints exist that match the operating system. To correct this problem, you can create a *custom fingerprint*. This fingerprint provides a pattern of operating system characteristics unique to the unknown or misidentified operating system and supplies the name of the operating system for identification purposes

Operating system identification and vulnerability mapping

If the system cannot match the operating system of a host, it cannot identify the vulnerabilities for the host, because the system derives the list of vulnerabilities for each host from its operating system fingerprint. For example, if the system detects a host running Microsoft Windows, it adds a stored Microsoft Windows vulnerability list to the host's profile based on the detected operating system.

As an example, if you have several devices on your network running a new beta version of Microsoft Windows, the system cannot identify that operating system or map vulnerabilities to the hosts. However, knowing that the system has a list of vulnerabilities for Microsoft Windows, you may want to create a custom fingerprint for one of the hosts to help identify the other hosts running the same operating system. You can include a mapping of the vulnerability list for Microsoft Windows in the fingerprint to associate it with each host that matches the fingerprint.

When you create a custom fingerprint, the Firewall Management Center lists the set of vulnerabilities associated with that fingerprint for any hosts running the same operating system. If the custom fingerprint does not contain any vulnerability mappings, the system uses the fingerprint to assign the custom operating system information you provide. When the system sees new traffic from a previously detected host, it updates the

host with the new fingerprint information. The system also uses the new fingerprint to identify any new hosts with that operating system the first time they are detected.

Before you create a custom fingerprint, determine why the host is not being identified correctly to decide whether custom fingerprinting is a viable solution.

You can create two types of fingerprints with the system:

- Client fingerprints, which identify operating systems based on the SYN packet that the host sends when it connects to a TCP application running on another host on the network.
- Server fingerprints, which identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application.

Note If both a client and server fingerprint match the same host, the client fingerprint is used.

After creating fingerprints, you must activate them before the system can associate them with hosts.

Manage fingerprints

After a fingerprint is created and activated, you can edit a fingerprint to make changes or add vulnerability mappings.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Custom Operating Systems**.

If the system is waiting for data to create a fingerprint, it refreshes the page every 10 seconds until the fingerprint is created.

Step 3 Manage your custom fingerprints using these options:

- **Activate/Deactivate**: Activate or deactivate a fingerprint as described in Activate and deactivate fingerprints, on page 2250.
- **Create**: Create fingerprints as described in Create a custom fingerprint for clients, on page 2252 and Create a custom fingerprint for servers, on page 2254.
- **Edit**: Edit a fingerprint as described in Edit an active fingerprint, on page 2251 and Edit an inactive fingerprint, on page 2252.
- **Delete**: Click **Delete** ( ) next to the fingerprint you want to delete, and click **OK** to confirm. You can only delete deactivated fingerprints.

Activate and deactivate fingerprints

You must activate a custom fingerprint before the system can use it to identify hosts. After the new fingerprint is activated, the system uses it to re-identify previously discovered hosts and discover new hosts.

If you want to stop using a fingerprint, you can deactivate it. Deactivating a fingerprint prevents the system from using it, but the fingerprint remains on the system. When you deactivate a fingerprint, the operating system is marked as unknown for hosts that use the fingerprint. If these hosts are detected again and match a different active fingerprint, they are then identified by that active fingerprint.

Deleting a fingerprint removes it from the system completely. After deactivating a fingerprint, you can delete it.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Custom Operating Systems**.

Step 3 Click the slider next to the fingerprint you want to activate or deactivate.

Note The activate option is only available if the fingerprint you created is valid. If the slider is not available, try creating the fingerprint again.

Edit an active fingerprint

If a fingerprint is *active*, you can modify the fingerprint name, description, and custom operating system display. You can also map additional vulnerabilities to it.

You can modify the fingerprint name, description, custom operating system display, and map additional vulnerabilities to it.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Custom Operating Systems**.

Step 3 Click **Edit** ( ) next to the fingerprint you want to edit.

Step 4 Modify the fingerprint name, description, and custom OS display, if necessary.

Step 5 If you want to delete a vulnerability mapping, click **Delete** next to the mapping in the **Pre-Defined OS Product Maps** section of the page.

Step 6 If you want to add additional operating systems for vulnerability mapping, choose the **Product** and, if applicable, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** and then click **Add OS Definition**.

The vulnerability mapping is added to the **Pre-Defined OS Product Maps** list.

Step 7 Click **Save**.

Edit an inactive fingerprint

If a fingerprint is *inactive*, you can modify all elements of the fingerprint and resubmit it to the Secure Firewall Management Center. This includes all properties you specified when creating the fingerprint, such as fingerprint type, target IP addresses and ports, vulnerability mappings, and so on.

When you edit and submit an inactive fingerprint, the system resubmits it. If it is a client fingerprint, you must resend traffic to the appliance before activating it. Note that you can choose only a single vulnerability mapping for an inactive fingerprint. After you activate the fingerprint, you can map additional operating systems and versions to its vulnerabilities list.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Custom Operating Systems**.

Step 3 Click **Edit** ( ) next to the fingerprint you want to edit.

Step 4 Make changes to the fingerprint as necessary:

- If you are modifying a client fingerprint, refer to Create a custom fingerprint for clients, on page 2252.
- If you are modifying a server fingerprint, refer to Create a custom fingerprint for servers, on page 2254.

Step 5 Click **Save**.

What to do next

If you modified a client fingerprint, remember to send traffic from the host to the appliance gathering the fingerprint.

Create a custom fingerprint for clients

Client fingerprints identify the operating system by analyzing the SYN packet a host sends when it connects to a TCP application on another network host.

If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a device that is managed by the Firewall Management Center and is closest to the host you intend to fingerprint when specifying client fingerprint properties.

Before you begin

Before you begin the fingerprinting process, obtain these details about the host you want to fingerprint:

- The number of network hops between the host and the Firewall Management Center or the device you use to obtain the fingerprint. (Cisco strongly recommends that you directly connect the Firewall Management Center or the device to the same subnet that the host is connected to.)
- The network interface (on the Firewall Management Center or the device) that is connected to the network where the host resides.
- The actual operating system vendor, product, and version of the host.
- Access to the host in order to generate client traffic.

Procedure

Step 1 Choose **Policies** > **Network Discovery**. Click **Custom Operating Systems**, and then **Create Custom Fingerprint**.

Step 2 From the **Device** drop-down list, choose the Firewall Management Center or the device that you want to use to collect the fingerprint. Then, enter a **Fingerprint Name**, **Fingerprint Description** and from the **Fingerprint Type** list, choose **Client**.

Step 3 In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

Note The fingerprint is based exclusively on traffic to and from the specified host IP address. Traffic from other IP addresses assigned to the host is not included.

Step 4 In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

Caution This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

Step 5 From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

Note Use the management interface or any other available network interfaces that is configured as the sensing interface on your device to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

Step 6 If you want to display custom information in the host profile for fingerprinted hosts (or if the host you want to fingerprint does not reside in the **OS Vulnerability Mappings** section), choose **Use Custom OS Display** and provide the values you want to display for these fields:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.
- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.
- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

Step 7 In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify **Vendor** and **Product** values in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the **Vendor** and **Product** values.

Note Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

Example:

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the major version.

Example:

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

Step 8 Click **Create**.

The status briefly shows `New`, then switches to `Pending`, where it remains until traffic is seen for the fingerprint. Once traffic is seen, it switches to `Ready`.

The Custom Fingerprint status page refreshes every ten seconds until it receives data from the host in question.

Step 9 Using the IP address you specified as the target IP address, access the host you are trying to fingerprint and initiate a TCP connection to the appliance.

To create an accurate fingerprint, traffic **must** be seen by the appliance collecting the fingerprint. If you are connected through a switch, traffic to a system other than the appliance may not be seen by the system.

Example:

Access the web interface of the Firewall Management Center from the host you want to fingerprint or SSH into the Firewall Management Center from the host. If you are using SSH, use the command below, where localIPv6address is the IPv6 address specified in step 7 that is currently assigned to the host and DCmanagementIPv6address is the management IPv6 address of the Firewall Management Center. The Custom Fingerprint page should then reload with a “Ready” status.

```
ssh -b localIPv6address DCmanagementIPv6address
```

Create a custom fingerprint for servers

Server fingerprints identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application.

Before you begin, you should obtain this information about the host you want to fingerprint:

- The number of network hops between the host and the appliance you use to obtain the fingerprint. Cisco strongly recommends that you directly connect an unused interface on the appliance to the same subnet that the host is connected to.
- The network interface (on the appliance) that is connected to the network where the host resides.
- The actual operating system vendor, product, and version of the host.

- An IP address that is not currently in use and is authorized on the network where the host is located.

Tip If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a managed device that is closest to the host you intend to fingerprint when specifying server fingerprint properties.

Procedure

Step 1 Choose **Policies** > **Network Discovery**. Click **Custom Operating Systems** and then, click **Create Custom Fingerprint**.

Step 2 From the **Device** list, choose the Firewall Management Center or the managed device that you want to use to collect the fingerprint and enter a **Fingerprint Name**. Enter a **Fingerprint Description** and from the **Fingerprint Type** list, choose **Server** to display the server fingerprinting options. In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

Note that the fingerprint will only be based on traffic to and from the host IP address you specify, not any of the host's other IP addresses (if it has any).

Caution You can capture IPv6 fingerprints only with appliances running Version 5.2 and later.

Step 3 In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

Caution This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

Step 4 From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

Caution Cisco recommends that you do **not** use the sensing interface on a managed device for fingerprinting for several reasons. First, fingerprinting does not work if the sensing interface is on a span port. Also, if you use the sensing interface on a device, the device stops monitoring the network for the amount of time it takes to collect the fingerprint. You can, however, use the management interface or any other available network interfaces to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

Step 5 Click **Get Active Ports**. In the **Server Port** field, enter the port that you want the device chose to collect the fingerprint to initiate contact with, or choose a port from the **Get Active Ports** drop-down list.

You can use any server port that you know is open on the host (for instance, 80 if the host is running a web server).

Step 6 In the **Source IP Address** field, enter an IP address that should be used to attempt to communicate with the host.

You should use a source IP address that is authorized for use on the network but is not currently being used, for example, a DHCP pool address that is currently not in use. This prevents you from temporarily knocking another host offline while you create the fingerprint.

You should exclude that IP address from monitoring in your network discovery policy while you create the fingerprint. Otherwise, the network map and discovery event views will be cluttered with inaccurate information about the host represented by that IP address.

Step 7 In the **Source Subnet Mask** field, enter the subnet mask for the IP address you are using. If the **Source Gateway** field appears, enter the default gateway IP address that should be used to establish a route to the host. If you want to display custom information in the host profile for fingerprinted hosts or if the fingerprint name you want to use does not exist in the OS Definition section, choose **Use Custom OS Display** in the Custom OS Display section.

Provide the values you want to appear in host profiles for these fields:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.
- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.
- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

Step 8 In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify a Vendor and Product name in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the vendor and product name.



Note Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

Example:

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Example:

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

Click **Create**.

Step 9 Click **Create**.
The Custom Fingerprint status page refreshes every ten seconds and should reload with a "Ready" status.

Note If the target system stops responding during the fingerprinting process, the status shows an `ERROR: No Response` message. If you see this message, submit the fingerprint again. Wait three to five minutes (the time period may vary depending on the target system), click **Edit** ( ) to access the Custom Fingerprint page, and then click **Create**.

What to do next

Activate the fingerprint as described in Activate and deactivate fingerprints, on page 2250.

Host input data

You can augment the network map by importing network map data from third parties. You can also use the host input feature by modifying operating system or application identities or deleting application protocols, protocols, host attributes, or clients using the web interface.

The system may reconcile data from multiple sources to determine the current identity of an operating system or application.

All data except third-party vulnerabilities is discarded when the affected host is removed from the network map. For more information on setting up scripts or import files, see the *Firepower System Host Input API Guide*.

To include imported data in impact correlations, you must map the data to the operating system and application definitions in the database.

Requirements for using third-party data

You can import discovery data from third-party systems on your network. However, to enable features where intrusion and discovery data are used together, such as Cisco recommendations, adaptive profile updates, or impact assessment, you should map as many elements of it as possible to corresponding definitions. Consider the following requirements for using third-party data:

- If you have a third-party system that has specific data on your network assets, you can import that data using the host input feature. However, because third parties may name the products differently, you must map the third-party vendor, product, and versions to the corresponding Cisco product definition. After you map the products, you must enable vulnerability mappings for impact assessment in the Firewall Management Center configuration to allow impact correlation. For versionless or vendorless application protocols, you need to map vulnerabilities for the application protocols in the Firewall Management Center configuration.
- If you import patch information from a third party and you want to mark all vulnerabilities fixed by that patch as invalid, you must map the third-party fix name to a fix definition in the database. All vulnerabilities addressed by the fix will then be removed from hosts where you add that fix.
- If you import operating system and application protocol vulnerabilities from a third party and you want to use them for impact correlation, you must map the third-party vulnerability identification string to vulnerabilities in the database. Note that although many clients have associated vulnerabilities, and clients

are used for impact assessment, you cannot import and map third-party client vulnerabilities. After the vulnerabilities are mapped, you must enable third-party vulnerability mappings for impact assessment in the Firewall Management Center configuration. To cause application protocols without vendor or version information to map to vulnerabilities, an administrative user must also map vulnerabilities for the applications in the Firewall Management Center configuration.

- If you import application data and you want to use that data for impact correlation, you must map the vendor string for each application protocol to the corresponding Cisco application protocol definition.

Third-party product mappings

When you add data from third parties to the network map through the user input feature, you must map the vendor, product, and version names used by the third party to the Cisco product definitions. Mapping the products to Cisco definitions assigns vulnerabilities based on those definitions.

Similarly, if you are importing patch information from a third party, such as a patch management product, you must map the name for the fix to the appropriate vendor and product and the corresponding fix in the database.

Map third-party products

If you import data from a third party, you must map the Cisco product to the third-party name to assign vulnerabilities and perform impact correlation using that data. Mapping the product associates Cisco vulnerability information with the third-party product name, which allows the system to perform impact correlation using that data.

If you import data using the host input import feature, you can also use the AddScanResult function to map third-party products to operating system and application vulnerabilities during the import.

For example, if you import data from a third party that lists Apache Tomcat as an application and you know it is version 6 of that product, you could add a third-party map where:

- **Vendor Name** is set to `Apache`.
- **Product Name** is set to `Tomcat`.
- **Apache** is chosen from the **Vendor** drop-down list.
- **Tomcat** is chosen from the **Product** drop-down list.
- **6** is chosen from the **Version** drop-down list

This mapping would cause any vulnerabilities for Apache Tomcat 6 to be assigned to hosts with an application listing for Apache Tomcat.

Note that for versionless or vendorless applications, you must map vulnerabilities for the application types in the Secure Firewall Management Center configuration. Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot import and map third-party client vulnerabilities.

Tip If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

Follow these steps to map third-party products:

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **User Third-Party Mappings**.

Step 3 You have two choices:

- **Create**: To create a new map set, click **Create Product Map Set**.
- **Edit**: To edit an existing map set, click **Edit** ( ) next to the map set you want to modify. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Mapping Set Name**.

Step 5 Enter a **Description**.

Step 6 You have two choices:

- **Create**: To map a third-party product, click **Add Product Map**.
- **Edit**: To edit an existing third-party product map, **Edit** ( ) next to the map set you want to modify. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 7 Enter the **Vendor String**, **Product String**, and **Version String** used by the third-party product.

Step 8 In the Product Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping from the **Vendor**, **Product**, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** fields.

Example:

If you want a host running a product whose name consists of third-party strings to use the vulnerabilities from Red Hat Linux 9, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Step 9 Click **Save**.

Map third-party product fixes

Mapping a fix name to a set of fixes in the database allows you to import data from a third-party patch management application and apply the fix to specified hosts. When the fix name is imported to a host, the system marks all vulnerabilities addressed by the fix as invalid for that host.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **User Third-Party Mappings**.

Step 3 You have two choices:

- Create — To create a new map set, click **Create Product Map Set**.

- Edit — To edit an existing map set, click **Edit** ( ) next to the map set you want to modify. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Mapping Set Name**.

Step 5 Enter a **Description**.

Step 6 You have two choices:

- Create — To map a third-party product, click **Add Fix Map.**
- Edit — To edit an existing third-party product map, click **Edit** ( ) next to it. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 7 Enter the name of the fix you want to map in the **Third-Party Fix Name** field.

Step 8 In the **Product Mappings** section, choose the operating system, product, and versions you want to use for fix mapping from these fields:

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **Build**
- **Patch**
- **Extension**

Example:

If you want your mapping to assign the fixes from Red Hat Linux 9 to hosts where the patch is applied, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

Step 9 Click **Save** to save the fix map.

Map third-party vulnerabilities

To add vulnerability information from a third party to the VDB, you must map the third-party identification string for each imported vulnerability to any existing SVID, Bugtraq, or SID. After you create a mapping for the vulnerability, the mapping works for all vulnerabilities imported to hosts in the network map and allows impact correlation for those vulnerabilities.

You must enable impact correlation for third-party vulnerabilities to allow correlation to occur. For versionless or vendorless applications, you must also map vulnerabilities for the application types in the Secure Firewall Management Center configuration.

Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot use third-party client vulnerabilities for impact assessment.

Tip If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **User Third-Party Mappings**.

Step 3 You have two choices:

- Create — To create a new vulnerability set, click **Create Vulnerability Map Set**.
- Edit — To edit an existing vulnerability set, click **Edit** ( ) next to the vulnerability set. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Click **Add Vulnerability Map**.

Step 5 Enter the third-party identification for the vulnerability in the **Vulnerability ID** field.

Step 6 Enter a **Vulnerability Description**.

Step 7 Optionally:

- Enter a Snort ID in the **Snort Vulnerability ID Mappings** field.
- Enter a legacy vulnerability ID in the **SVID Mappings** field.
- Enter a Bugtraq identification number in the **Bugtraq Vulnerability ID Mappings** field.

Step 8 Click **Add**.

Custom product mappings

A custom product mapping is a network configuration feature that - ensures servers input by a third party are associated with the appropriate Cisco definitions - applies to all servers or clients on monitored hosts that have the mapped vendor strings, and - enables mapping vulnerabilities for all servers in the network map with a particular vendor string instead of explicitly setting the vendor, product, and version for the server.

Create custom product mappings

Custom product mappings allow you to manually create mappings when the system cannot automatically map a server to a vendor and product in the VDB. When you activate a custom product mapping, the system maps vulnerabilities for the specified vendor and product to all servers in the network map where that vendor string occurs.

Note Custom product mappings apply to all occurrences of an application protocol, regardless of the source of the application data (such as Nmap, the host input feature, or the system itself). However, if third-party vulnerability mappings for data imported using the host input feature conflicts with the mappings you set through a custom product mapping, the third-party vulnerability mapping overrides the custom product mapping and uses the third-party vulnerability mapping settings when the input occurs.

You create lists of product mappings and then enable or disable use of several mappings at once by activating or deactivating each list. When you specify a vendor to map to, the system updates the list of products to include only those made by that vendor.

After you create a custom product mapping, you must activate the custom product mapping list. After you activate a list of custom product mappings, the system updates all servers with occurrences of the specified vendor strings. For data imported through the host input feature, vulnerabilities update unless you have already explicitly set the product mappings for this server.

If, for example, your company modifies the banner for your Apache Tomcat web servers to read `Internal Web Server`, you can map the vendor string `Internal Web Server` to the vendor **Apache** and the product **Tomcat**, then activate the list containing that mapping, all hosts where a server labeled `Internal Web Server` occurs have the vulnerabilities for Apache Tomcat in the database.

Tip You can use this feature to map vulnerabilities to local intrusion rules by mapping the SID for the rule to another vulnerability.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **Custom Product Mappings**, and then **Create Custom Product Mapping List**.

Step 3 Enter a **Custom Product Mapping List Name**.

Step 4 Click **Add Vendor String**.

Step 5 In the **Vendor String** field, enter the vendor string that identifies the applications that should map to the chosen vendor and product values.

Step 6 Choose the vendor you want to map to from the **Vendor** drop-down list.

Step 7 Choose the product you want to map to from the **Product** drop-down list.

Step 8 Click **Add** to add the mapped vendor string to the list.

Step 9 Optionally, repeat steps 4 to 8 as needed to add additional vendor string mappings to the list.

Step 10 Click **Save**.

What to do next

- Activate the custom product mapping list. For more information, see Activate and deactivate custom product mappings, on page 2263.

Edit custom product mapping lists

You can modify existing custom product mapping lists by adding or removing vendor strings or changing the list name.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **Custom Product Mappings**.

Step 3 Click **Edit** ( ) next to the product mapping list you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Make changes to the list as described in Create custom product mappings, on page 2261.

Step 5 When you finish, click **Save**.

Activate and deactivate custom product mappings

Activating custom product mappings allows you to enable or disable use of an entire list of custom product mappings at once, providing centralized control over application detection across your network.

After you activate a custom product mapping list, each mapping on that list applies to all applications with the specified vendor string, whether detected by managed devices or imported through the host input feature.

Procedure

Step 1 Choose **Policies** > **Application Detectors**.

Step 2 Click **Custom Product Mappings**.

Step 3 Click the slider next to the custom product mapping list to activate or deactivate it.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Configure the host input client

The host input feature allows you to update the Firewall Management Center's network map from a client program running on another appliance. For example, you can add or delete hosts from the network map, or update the host OS and service information. For more information, see the *Firepower System Host Input API Guide*.

Before you can run a remote client, you must add the client to the Firewall Management Center's peers database from the Host Input Client page. You must also copy the authentication certificate generated by the Firewall

Management Center to the client. After completing these steps the client can connect to the Firewall Management Center.

In a multidomain deployment, you can create a client in any domain. The authentication certificate allows the client to submit network map updates for any leaf domains associated with the client certificate's domain. If you create a certificate for an ancestor domain (or if your certificate domain later becomes an ancestor domain after adding descendant domains), any clients using that certificate must specify a target leaf domain with every transaction, as described in the *Firepower System Host Input API Guide*.

The Host Input Client shows only clients associated the current domain, so if you want to download or revoke a certificate, switch to the domain where the client was created.

This connection uses TLS 1.2.

Before you begin

Follow these steps to configure the host input client:

Procedure

Step 1 Choose **Integration** > **Other Integrations**.

Step 2 Click **Host Input Client**.

Step 3 Click **Create Client**.

Step 4 In the **Hostname** field, enter the host name or IP address of the host running the host input client.

Note If you have not configured DNS resolution, use an IP address.

Step 5 If you want to encrypt the certificate file, enter a password in the **Password** field.

Step 6 Click **Save**.
The host input service allows the host to access port 8307 on the Firewall Management Center and creates an authentication certificate to use during client-server authentication.

Step 7 Click **Download** ( ) next to the certificate file.

Step 8 Save the certificate file to the directory used by your client for SSL/TLS authentication.

Step 9 To revoke access for a client, click **Delete** ( ) next to the host you want to remove.

Nmap scanning

The system builds network maps through passive analysis of traffic on your network. Information obtained through this passive analysis can occasionally be incomplete, depending on system conditions. However, you can actively scan a host to obtain complete information.

If a host has a server running on an open port but the server has not received or sent traffic during the time that the system has been monitoring your network, the system does not add information

about that server to the network map. If you scan the host using an active scanner, you can detect the server.

You can use Nmap, an open source active scanner, to explore your network and audit its security.

When you scan a host using Nmap, the system:

- Adds servers found on previously undetected open ports are added to the Servers list in the host profile. The host profile lists any servers detected on filtered or closed TCP ports or on UDP ports in the **Scan Results** section. By default, Nmap scans more than 1660 TCP ports.

  If the system recognizes a server identified in an Nmap scan and has a corresponding server definition, the system maps the names Nmap uses for servers to the corresponding Cisco server definitions.

- Compares the results of the scan to over 1500 known operating system fingerprints to determine the operating system and assigns scores to each. The operating system assigned to the host is the operating system fingerprint with the highest score.

  The system maps Nmap operating system names to Cisco operating system definitions.

- Vulnerabilities are assigned to the host for any added servers and operating systems.

Note

- A host must exist in the network map before Nmap can append its results to the host profile.
- If the host is deleted from the network map, any Nmap scan results for that host are discarded.

Tip Scanning options like port scans can put a heavy load on networks with low bandwidth. Run these scans when your network traffic is low.

For more information on the underlying Nmap technology used to scan, refer to the Nmap documentation at http://insecure.org/.

Nmap remediation options

You define the settings for an Nmap scan by creating an Nmap remediation. An Nmap remediation can be used in a correlation policy, initiated on demand, or scheduled for a specific time.

Note Nmap-supplied server and operating system data remain static until you run another Nmap scan. If you plan to scan a host for operating system and server data using Nmap, schedule regular scans to keep Nmap-supplied data and server data up-to-date.

Table 142: Nmap remediation options

Option	Description	Corresponding Nmap option
Scan which addresses from the event?	When you use an Nmap scan as a response to a correlation rule, select one of the following options to control which address in the event is scanned: that of the source host, the destination host, or both: • **Scan Source and Destination Addresses** scans the hosts represented by the source IP address and the destination IP address in the event. • **Scan Source Address Only** scans the host represented by the event's source IP address. • **Scan Destination Address Only** scans the host represented by the event's destination IP address.	N/A
Scan types	Select how Nmap scans ports: • The **TCP Syn** scan connects quickly to thousands of ports without using a complete TCP handshake. This option allows you to scan quickly in stealth mode on hosts where the `admin` account has raw packet access or where IPv6 is not running, by initiating TCP connections but not completing them. If a host acknowledges the Syn packet sent in a TCP Syn scan, Nmap resets the connection. • The **TCP Connect** scan uses the `connect()` system call to open connections through the operating system on the host. You can use the TCP Connect scan if the `admin` user on the Firewall Management Center or managed device does not have raw packet privileges on a host or you are scanning IPv6 networks. In other words, use this option in situations where the TCP SYN scan cannot be used. • The **TCP ACK** scan sends an ACK packet to check whether ports are filtered or unfiltered. • The **TCP Window** scan works in the same way as a TCP ACK scan but can also determine whether a port is open or closed. • The **TCP Maimon** scan identifies BSD-derived systems using a FIN/ACK probe.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
Scan for UDP ports	Enable this option to scan UDP ports as well as TCP ports. Scanning UDP ports may be time consuming, so avoid using this option if you want to scan quickly.	`-sU`

Option	Description	Corresponding Nmap option
Use port from event	If you plan to use the remediation as a response in a correlation policy, enable to cause the remediation to scan only the port specified in the event that triggers the correlation response. • Select **On** to scan the port in the correlation event, rather than the ports you specify during Nmap remediation configuration. If you scan the port in the correlation event, note that the remediation scans the port on the IP addresses that you specify during Nmap remediation configuration. These ports are also added to the remediation's dynamic scan target. • Select **Off** to scan only the ports you specify Nmap remediation configuration. You can also control whether Nmap collects information about operating system and server information. Enable the **Use Port From Event** option to scan the port associated with the new server.	N/A
Scan from reporting detection engine	Enable this option to scan a host from the appliance where the detection engine that reported the host resides. • To scan from the appliance running the reporting detection engine, select **On**. • To scan from the appliance configured in the remediation, select **Off**.	N/A
Fast port scan	Enable this option to scan only the TCP ports listed in the `nmap-services` file located in the `/var/sf/nmap/share/nmap/nmap-services` directory on the device that does the scanning, ignoring other port settings. You cannot use this option with the **Port Ranges and Scan Order** option. • To scan only the ports listed in the `nmap-services` file located in the `/var/sf/nmap/share/nmap/nmap-services` directory on the device that does the scanning, ignoring other port settings, select **On**. • To scan all TCP ports, select **Off**.	`-F`
Port ranges and scan order	Set the specific ports you want to scan and the order in which you want to scan them using Nmap port specification syntax. Note that you cannot use this option with the **Fast Port Scan** option.	`-p`
Probe open ports for vendor and version information	Enable to detect server vendor and version information. If you probe open ports for server vendor and version information, Nmap obtains server data that it uses to identify servers. Nmap then replaces the Cisco server data for that server. • Select **On** to scan open ports on the host for server information to identify server vendors and versions. • Select **Off** to continue using Cisco server information for the host.	`-sV`

Option	Description	Corresponding Nmap option
Service version intensity	Select the intensity of Nmap probes for service versions. • To use more probes for higher accuracy with a longer scan, select a higher number. • To use fewer probes for less accuracy with a faster scan, select a lower number.	`--version-intensity` <intensity>
Detect operating system	Enable to detect operating system information for the host. If you configure detection of the operating system for a host, Nmap scans the host and uses the results to create a rating for each operating system that reflects the likelihood that the operating system is running on the host. • Select **On** to scan the host for information to identify the operating system. • Select **Off** to continue using Cisco operating system information for the host.	`-O`
Treat all hosts as online	Enable to skip the host discovery process and run a port scan on every host in the target range. Note that when you enable this option, Nmap ignores settings for **Host Discovery Method** and **Host Discovery Port List**. • To skip the host discovery process and run a port scan on every host in the target range, select **On**. • To perform host discovery using the settings for **Host Discovery Method** and **Host Discovery Port List** and skip the port scan on any host that is not available, select **Off**.	`-PN`
Host discovery method	Select to perform host discovery for all hosts in the target range, over the ports listed in the **Host Discovery Port List**, or if no ports are listed, over the default ports for that host discovery method. Note that if you also enabled **Treat All Hosts As Online**, however, the **Host Discovery Method** option has no effect and host discovery is not performed. Select the method to be used when Nmap tests to see if a host is present and available: • The **TCP SYN** option sends an empty TCP packet with the SYN flag set and recognizes the host as available if a response is received. TCP SYN scans port 80 by default. Note that TCP SYN scans are less likely to be blocked by a firewall with stateful firewall rules. • The **TCP ACK** option sends an empty TCP packet with the ACK flag set and recognizes the host as available if a response is received. TCP ACK also scans port 80 by default. Note that TCP ACK scans are less likely to be blocked by a firewall with stateless firewall rules. • The **UDP** option sends a UDP packet and assumes host availability if a port unreachable response comes back from a closed port. UDP scans port 40125 by default.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`

Option	Description	Corresponding Nmap option
Host discovery port list	Specify a customized list of ports, separated by commas, that you want to scan when doing host discovery.	port list for host discovery method
Default NSE scripts	Enable to run the default set of Nmap scripts for host discovery and server and operating system and vulnerability detection. or a list of default scripts, refer to https://nmap.org/nsedoc/categories/default.html. • To run the default set of Nmap scripts, select **On**. • To skip the default set of Nmap scripts, select **Off**.	`-sC`
Timing template	Select the timing of the scan process; the higher the number you select, the faster and less comprehensive the scan.	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap scanning guidelines

While active scanning can obtain valuable information, overuse of a tool such as Nmap may overload your network resources or even crash important hosts. When you use any active scanner, create a scanning strategy to scan only the hosts and ports you need.

Selecting appropriate scan targets

When you configure Nmap, you can create scan targets that identify which hosts you want to scan. A scan target includes a single IP address, a CIDR block, an octet range of IP addresses, an IP address range, or a list of IP addresses or ranges to scan. You can also select the ports on the host or hosts.

You can specify targets in various ways:

- For IPv6 hosts: An exact IP address (for example, `2001:DB8:1::178:ABCD`).
- For IPv4 hosts:
  - An exact IP address (for example, `192.168.x.x`) or a list of IP addresses separated by commas or spaces.
  - An IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between 192.168.x.x and 192.168.x.x, inclusive).
  - An IP address range using octet range addressing (for example, `198.51.0-255.1-254` scans all addresses in the 198.51.x.x range, except those that end in .0 and or .255).
  - An IP address range using hyphenation (for example, `192.168.x.x-192.168.x.x` scans the six hosts between 192.168.x.x and 192.168.x.x, inclusive).

- A list of addresses or ranges separated by commas or spaces (for example, `192.168.1.0/24, 194.168.1.0/24` scans the 254 hosts between 192.168.x.x and 192.168.x.x, inclusive and the 254 hosts between 194.168.x.x and 194.168.x.x, inclusive).

Ideal scan targets for Nmap scans include hosts with operating systems that the system is unable to identify, hosts with unidentified servers, or hosts recently detected on your network. Remember that Nmap results cannot be added to the network map for hosts that do not already exist in the network map.

Caution

- Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans.
- If a host is deleted from the network map, any Nmap scan results are discarded.
- Make sure you have permission to scan your targets. Scanning Nmap hosts not owned by you or your company may be illegal.

Selecting appropriate ports to scan

For each scan target you configure, you can select the ports you want to scan. You can designate individual port numbers, port ranges, or a series of port numbers and port ranges to identify the exact set of ports that should be scanned on each target.

By default, Nmap scans TCP ports 1 through 1024. If you plan to use the remediation as a response in a correlation policy, you can configure the remediation to scan only the port specified in the event that triggers the correlation response. If you run remediation on demand, or as a scheduled task, or if you do not use the port from the event, you can use other port options to determine which ports are scanned. You can choose to scan only the TCP ports listed in the `nmap-services` file, ignoring other port settings. You can also scan UDP ports in addition to TCP ports. Scanning for UDP ports may take longer. Use this option only if you do not require a quick scan. To select the specific ports or range of ports to scan, use Nmap port specification syntax to identify ports.

Setting host discovery options

You can decide whether to perform host discovery before starting a port scan for a host, or you can assume that all the hosts you plan to scan are online. If you choose not to treat all hosts as online, you can choose what method of host discovery to use and, if needed, customize the list of ports scanned during host discovery. Host discovery does not probe the ports listed for operating system or server information; it uses the response over a particular port only to determine whether a host is active and available. If you perform host discovery and a host is not available, Nmap does not scan ports on that host.

Example: Use Nmap to resolve unknown operating systems

This example walks through an Nmap configuration designed to resolve unknown operating systems. For a complete look at Nmap configuration, see Manage Nmap scanning, on page 2272.

If the system cannot determine the operating system on a host on your network, you can use Nmap to actively scan the host. Nmap uses the information it obtains from the scan to rate the possible operating systems. It then uses the operating system that has the highest rating as the host operating system identification.

Using Nmap to challenge new hosts for operating system and server information deactivates the system's monitoring of that data for scanned hosts. If you use Nmap to discover the host and server operating system

for hosts marked as unknown by the systems, you may identify groups of similar hosts. You can then create a custom fingerprint using one of these hosts to associate the fingerprint with the operating system you identified through Nmap scan. Whenever possible, create a custom fingerprint rather than inputting static data through a third-party source like Nmap because the custom fingerprint allows the system to continue to monitor the host operating system and update it as needed.

Procedure

Step 1 Configure a scan instance as described in Add an Nmap scan instance, on page 2273.

Step 2 Create an Nmap remediation using the following settings:

- Enable **Use Port From Event** to scan the port associated with the new server.
- Enable **Detect Operating System** to detect operating system information for the host.
- Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
- Enable **Treat All Hosts as Online**, because you know the host exists.

Step 3 Create a correlation rule that triggers when the system detects a host with an unknown operating system.

The rule should trigger when **a discovery event occurs** and **the OS information for a host has changed** and it meets the following conditions: **OS Name is unknown**.

Step 4 Create a correlation policy that contains the correlation rule.

Step 5 In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.

Step 6 Activate the correlation policy.

Step 7 Purge the hosts on the network map to force network discovery to restart and rebuild the network map.

Step 8 After a day or two, search for events generated by the correlation policy.

Analyze the Nmap results for the operating systems detected on the hosts to see if there is a particular host configuration on your network that the system does not recognize.

Step 9 If you find hosts with unknown operating systems whose Nmap results are identical, create a custom fingerprint for one of those hosts and use it to identify similar hosts in the future.

Example: Using Nmap to respond to new hosts

This example walks through an Nmap configuration designed to respond to new hosts. For a complete look at Nmap configuration, see Manage Nmap scanning, on page 2272.

When the system detects a new host in a subnet where intrusions may be likely, you may want to scan that host to make sure you have accurate vulnerability information for it.

You can accomplish this by creating and activating a correlation policy that detects when a new host appears in this subnet, and that launches a remediation that performs an Nmap scan on the host.

Procedure

Step 1 Configure a scan instance as described in Add an Nmap scan instance, on page 2273.

Step 2 Create an Nmap remediation using the following settings:

- Enable **Use Port From Event** to scan the port associated with the new server.
- Enable **Detect Operating System** to detect operating system information for the host.
- Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
- Enable **Treat All Hosts as Online**, because you know the host exists.

Step 3 Create a correlation rule that triggers when the system detects a new host on a specific subnet.

The rule should trigger when **a discovery event occurs** and **a new host is detected**.

Step 4 Create a correlation policy that contains the correlation rule.

Step 5 In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.

Step 6 Activate the correlation policy.

Step 7 When you are notified of a new host, check the host profile to see the results of the Nmap scan and address any vulnerabilities that apply to the host.

After you activate the policy, you can periodically check the remediation status view (**Analysis** > **Correlation** > **Status**) to see when the remediation launched. The remediation's dynamic scan target should include the IP addresses of the hosts it scanned as a result of the server detection. Check the host profile for those hosts to see if there are vulnerabilities that need to be addressed for the host, based on the operating system and servers detected by Nmap.



Caution If you have a large or dynamic network, detection of a new host may be too frequent an occurrence to respond to using a scan. To prevent resource overload, avoid using Nmap scans as a response to events that occur frequently. In addition, note that using Nmap to challenge new hosts for operating system and server information deactivates Cisco monitoring of that data for scanned hosts.

Manage Nmap scanning

To use Nmap scanning, you must, at minimum, configure an Nmap scan instance and an Nmap remediation. Configuring an Nmap scan target is optional.

Procedure

Step 1 Configure the Nmap scan:

- Add an Nmap scan instance as described in Add an Nmap scan instance, on page 2273.
- Create an Nmap remediation as described in Create an Nmap remediation, on page 2276.
- Optionally, add an Nmap scan target as described in Add an Nmap scan target, on page 2275.

Step 2 Run the Nmap scan:

- Run an on-demand Nmap scan as described in Run an on-demand Nmap scan, on page 2279.
- Configure automatic Nmap scans as described in *Nmap Scan Automation* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Schedule automatic Nmap scans as described in *Scheduling an Nmap Scan* in the *Cisco Secure Firewall Management Center Administration Guide*.

What to do next

- Monitor the Nmap scan in progress by viewing the related task; see *Viewing Task Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Optionally, refine the scan:
  - Edit an Nmap scan instance as described in Edit an Nmap scan instance, on page 2274.
  - Edit an Nmap scan target as described in Edit an Nmap scan target, on page 2276.
  - Edit an Nmap remediation as described in Edit an Nmap remediation, on page 2278.

Add an Nmap scan instance

You can set up a separate scan instance for each Nmap module that you want to use to scan your network for vulnerabilities. You can set up scan instances for the local Nmap module on the Secure Firewall Management Center and for any devices you want to use to run scans remotely. The results of each scan are always stored on the Firewall Management Center where you configure the scan, even if you run the scan from a remote device. To prevent accidental or malicious scanning of mission-critical hosts, you can create a blacklist for the instance to indicate the hosts that should never be scanned with the instance.

You cannot add a scan instance with the same name as any existing scan instance.

Procedure

Step 1 Access the list of Nmap scan instances using either of the following methods:

- Choose **Policies** > **Actions** > **Instances**.
- Choose **Policies** > **Actions** > **Scanners**.

Step 2 Add the remediation:

- If you accessed the list via the first method above, locate the Add a New Instance section, choose the Nmap Remediation module from the drop-down list, and click **Add**.
- If you accessed the list via the second method above, click **Add Nmap Instance**.

Step 3 Enter an **Instance Name**.

Step 4 Enter a **Description**.

Step 5 Optionally, in the **Exempted hosts** field, specify any hosts or networks that should *never* be scanned with this scan instance, using the following syntax:

- For IPv6 hosts, an exact IP address (for example, `2001:DB8::fedd:eeff`)
- For IPv4 hosts, an exact IP address (for example, `192.168.1.101`) or an IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between `192.168.1.1` and `192.168.1.254`, inclusive)
- Note that you cannot use an exclamation mark (!) to negate an address value.



Note If you specifically target a scan to a host that is in a blacklisted network, that scan will not run.

Step 6 Optionally, to run the scan from a remote device instead of the Firewall Management Center, specify the IP address or name of the device as it appears in the Information page for the device in the Firewall Management Center web interface, in the **Remote Device Name** field.

Step 7 Click **Create**.
When the system is done creating the instance, it displays it in edit mode.

Step 8 Optionally, add an Nmap remediation to the instance. To do so, locate the Configured Remediations section of the instance, click **Add**, and create a remediation as described in Create an Nmap remediation, on page 2276.

Step 9 Click **Cancel** to return to the list of instances.



Note If you accessed the list of Nmap scan instances via the **Scanners** option, the system does not display the instance you added unless you also added a remediation to the instance. To view any instances to which you have not yet added remedations, use the **Instances** menu option to access the list.

Edit an Nmap scan instance

When you edit a scan instance, you can view, add, and delete remediations associated with the instance. If you no longer need the Nmap module in this scan instance, delete the Nmap scan instance. When you delete a scan instance, you also remove any remediations that use this instance.

Procedure

Step 1 To access the list of Nmap scan instances, use one of these methods:

- Choose **Policies** > **Actions** > **Instances**.
- Choose **Policies** > **Actions** > **Scanners**.

Step 2 Click **View** ( ) next to the instance you want to edit.

Step 3 Make changes to the scan instance settings as described in Add an Nmap scan instance, on page 2273.

Step 4 Click **Save**.

Step 5 Click **Done**.

What to do next

- To add a new remediation to the scan instance; refer to Create an Nmap remediation, on page 2276.
- To edit a remediation associated with the instance; refer to Edit an Nmap remediation, on page 2278.
- To delete a remediation associated with the instance; refer to Run an on-demand Nmap scan, on page 2279.
- You can delete the scan instance by clicking **Delete** ( ) next to it.

Add an Nmap scan target

Create and save scan targets that identify the hosts and ports you want to target when you perform an on-demand or a scheduled scan, so that you do not have to construct a new scan target every time.

A scan target includes a single IP address or a block of IP addresses. It also specifies the ports on the host or hosts. For Nmap targets, you can also use Nmap octet range addressing or IP address ranges. For more information on Nmap octet range addressing, see the Nmap documentation at https://insecure.org/.

Note

- Scans for targets containing a large number of hosts can take a long time. As a workaround, scan fewer hosts at a time.
- Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans. If a host is deleted from the network map, any Nmap scan results are discarded.

Procedure

Step 1 Choose **Policies** > **Actions** > **Scanners**.

Step 2 On the toolbar, click **Targets**.

Step 3 Click **Create Scan Target**.

Step 4 In the **Name** field, enter the name you want to use for this scan target.

Step 5 In the **IP Range** text box, specify the host or hosts you want to scan using the syntax described in Nmap scanning guidelines, on page 2269.

Note If you use a comma in a list of IP addresses or ranges in a scan target, the comma converts to a space when you save the target.

Step 6 In the **Ports** field, specify the ports you want to scan.

You can enter any of these values from 1 to 65535:

- A port number.
- A list of ports separated by commas.
- A range of port numbers separated by a dash.
- Range of port numbers separated by dashes, and commas.

Step 7 Click **Save**.

Edit an Nmap scan target

Edit a remediation's dynamic scan target to exclude a specific IP address, but the IP address was added to the target because the host was involved in a correlation policy violation that launched the remediation.

Delete a scan target if you no longer want to scan the hosts listed in it.

Procedure

Step 1 Choose **Policies** > **Actions** > **Scanners**.

Step 2 On the toolbar, click **Targets**.

Step 3 Click **Edit** ( ) next to the scan target you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Make modifications as necessary. For more information, see Add an Nmap scan target, on page 2275.

Step 5 Click **Save**.

Step 6 Delete the scan target by clicking **Delete** ( ) next to it.

Create an Nmap remediation

An Nmap remediation can only be created by adding it to an existing Nmap scan instance. You can use the remediation as a response in a correlation policy, run it on demand, or schedule it to run at a specific time.

Nmap-supplied server and operating system data remains static until another Nmap scan is run. To keep data updated, regularly schedule scans if you plan to scan a host using Nmap. If a host is deleted from the network map, any existing Nmap scan results are discarded.

For general information about Nmap functionality, refer to the Nmap documentation at https://insecure.org.

Before you begin

Add an Nmap scan instanceas described in Add an Nmap scan instance, on page 2273 .

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Click **View** ( ) next to the instance to which you want to add the remediation.

Step 3 In the Configured Remediations section, click **Add**.

Step 4 Enter a **Remediation Name**.

Step 5 Enter a **Description**.

Step 6 If you plan to use this remediation in response to a correlation rule that triggers on an intrusion event, a connection event, or a user event, configure the **Scan Which Address(es) From Event?** option.

Tip If you plan to use this remediation in response to a correlation rule that triggers on a discovery event or a host input event, by default the remediation scans the IP address of the host involved in the event; you do not need to configure this option.

Note Do **not** assign an Nmap remediation as a response to a correlation rule that triggers on a traffic profile change.

Step 7 Configure the **Scan Type** option.

Step 8 To scan UDP ports in addition to TCP ports, choose **On** for the **Scan for UDP ports** option.

Tip A UDP portscan takes more time than a TCP portscan. To speed up your scans, leave this option disabled.

Step 9 If you plan to use this remediation in response to correlation policy violations, configure the **Use Port From Event** option.

Step 10 If you plan to use this remediation in response to correlation policy violations and want to run the scan using the appliance running the detection engine that detected the event, configure the **Scan from reporting detection engine** option.

Step 11 Configure the **Fast Port Scan** option.

Step 12 In the **Port Ranges and Scan Order** field, enter the ports you want to scan by default, using Nmap port specification syntax, in the order you want to scan those ports.

Use this format:

- Specify values from 1 to 65535.
- Separate ports using commas or spaces.
- Use a hyphen to indicate a port range.
- When scanning for both TCP and UDP ports, preface the list of TCP ports you want to scan with a T and the list of UDP ports with a U.

Note The **Use Port From Event** option overrides this setting when the remediation is launched in response to a correlation policy violation, as described in step 8.

Example:

To scan ports 53 and 111 for UDP traffic, then scan ports 21-25 for TCP traffic, enter **U:53,111,T:21-25**.

Step 13 To probe open ports for server vendor and version information, configure **Probe open ports for vendor and version information**.

Step 14 If you choose to probe open ports, set the number of probes used by choosing a number from the **Service Version Intensity** drop-down list.

Step 15 To scan for operating system information, configure **Detect Operating System** settings.

Step 16 To determine whether host discovery occurs and whether port scans are only run against available hosts, configure **Treat All Hosts As Online**.

Step 17 To set the method you want Nmap to use when it tests for host availability, choose a method from the **Host Discovery Method** drop-down list.

Step 18 If you want to scan a custom list of ports during host discovery, enter a list of ports appropriate for the host discovery method you chose, separated by commas, in the **Host Discovery Port List** field.

Step 19 Configure the **Default NSE Scripts** option to control whether to use the default set of Nmap scripts for host discovery and server, operating system, and vulnerability discovery.

Tip See https://nmap.org/nsedoc/categories/default.html for the list of default scripts.

Step 20 To set the timing of the scan process, choose a timing template number from the **Timing Template** drop-down list.

Choose a higher number for a faster, less comprehensive scan and a lower number for a slower, more comprehensive scan.

Step 21 Click **Create**.
When the system is done creating the remediation, it displays it in edit mode.

Step 22 Click **Done** to return to the related instance.

Step 23 Click **Cancel** to return to the instance list.

Edit an Nmap remediation

Edit an Nmap remediation to modify scan settings or remove it when it is no longer required.

Modifications you make to Nmap remediations do not affect scans in progress. The new settings take effect when the next scan starts. Delete an Nmap remediation if you no longer need it.

Procedure

Step 1 Access the list of Nmap scan instances using one of these methods:

- Choose **Policies** > **Actions** > **Instances**.
- Choose **Policies** > **Actions** > **Scanners**.

Step 2 Access the remediation you want to edit by performing one of these actions:

- If you accessed the list via the first method above, click **View** ( ) next to the relevant instance, and then click it again next to the remediation you want to edit in the Configured Remediations section.
- If you accessed the list via the second method above, click **View** ( ) next to the remediation you want to edit.

Step 3 Make any necessary modifications as described in Create an Nmap remediation, on page 2276.

Step 4 Click **Save** if you want to save your changes, or click **Done** to exit without saving.

Step 5 Delete the remediation by clicking **Delete** ( ) next to it.

Run an on-demand Nmap scan

You can launch on-demand Nmap scans whenever needed. You can specify the target for an on-demand scan by entering the IP addresses and ports you want to scan or by choosing an existing scan target.

Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans. If a host is deleted from the network map, any Nmap scan results are discarded.

Before you begin

Optionally, add an Nmap scan target; for more information, refer to Add an Nmap scan target, on page 2275 section.

Procedure

Step 1 Choose **Policies** > **Actions** > **Scanners**.

Step 2 Next to the Nmap remediation you want to use to perform the scan, click **Scan** ( ).

Step 3 To scan using a saved scan target, choose a target from the **Saved Targets** drop-down list, and click **Load**.

Step 4 In the **IP Range(s)** field, specify the IP address for hosts you want to scan or modify the loaded list.

Note

- For hosts with IPv4 addresses, you can specify multiple IP addresses separated by commas or use CIDR notation. You can also negate IP addresses by preceding them with an exclamation point (!).
- For hosts with IPv6 addresses, use an exact IP address. Ranges are not supported.

Step 5 In the **Ports** field, specify the ports you want to scan or modify the loaded list.

You can enter a port number, a list of ports separated by commas, or a range of port numbers separated by a dash.

Step 6 Click **Scan Now**.

What to do next

- Monitor the task status; see *Viewing Task Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.

Nmap scan results

You can manage, monitor, and analyze Nmap scan data to gain insights into your network configuration.

Nmap scan result viewing options

You can monitor Nmap scans in progress. You can import results from scans previously performed through the system, or import results performed outside the system. You can also view and analyze scan results.

You can view scan results that you create using the local Nmap module as a rendered page in a pop-up window. You can also download the Nmap results file in raw XML format.

You can also view operating system and server information detected by Nmap in host profiles and in the network map. If a scan of a host produces server information for servers on filtered or closed ports, or if a scan collects information that cannot be included in the operating system information or the servers section, the host profile includes those results in an Nmap Scan Results section.

View Nmap scan results

You can view the scan results in tabular format after the Nmap scan is completed and use the results view to find specific information.

When an Nmap scan is complete, you can view a table of scan results.

You can customize the results view depending on the information you are looking for. The page you see when you access scan results differs, based on the workflow. The predefined workflow includes a table view of scan results. You can also create a custom workflow that displays only the information that matches your specific needs.

You can download and view the Nmap results using the Nmap Version 1.01 DTD, available at http://insecure.org.

You can also clear scan results.

Procedure

Step 1 Choose **Policies** > **Actions** > **Scanners**.

Step 2 On the toolbar, click **Scan Results**.

Step 3 You have the following choices:

- Adjust the time range as described in *Event Time Constraints* in the *Cisco Secure Firewall Management Center Administration Guide*.

- To use a different workflow, including a custom workflow, click **(switch workflows)** by the workflow title.
- To view the scan results as a rendered page in a pop-up window, click **View** next to the scan job.
- To save a copy of the scan results file so that you can view the raw XML code in any text editor, click **Download** next to the scan job.
- To sort scan results, click the column title. Click the column title again to reverse the sort order.
- To constrain the columns that appear, click **Close** ( ) in the column heading that you want to hide. In the pop-up window that appears, click **Apply**.

Tip To hide or show other columns, check or clear the appropriate check boxes before you click **Apply**. To add a disabled column back to the view, Click the expand arrow to expand the search constraints, then click the column name under **Disabled Columns**.

- To drill down to the next page in the workflow, see *Using Drill-Down Pages* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To configure scan instances and remediations, click **Scanners** in the toolbar and see Manage Nmap scanning, on page 2272.
- To navigate within and between workflow pages, see *Workflow Page Navigation Tools* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To navigate to other event views to view associated events, choose the name of the event view you want to see from the **Jump to** drop-down list.
- To search for scan results, enter your search criteria in the appropriate fields.

Nmap scan results fields

When you run an Nmap scan, the Firewall Management Center collects the scan results in a database. The following table describes the fields in the scan results table that can be viewed and searched.

Table 143: Scan results fields

Field	Description
Start Time	The date and time that the scan that produced the results started.
End Time	The date and time that the scan that produced the results ended.
Target	The IP address (or host name, if DNS resolution is enabled) of the scan target for the scan that produced the results.
Scan Type	Either `Nmap` or the name of the third-party scanner to indicate the type of the scan that produced the results.

Field	Description
Scan Mode	The mode of the scan that produced the results: • `On Demand`: results from scans run on demand. • `Imported`: results from scans on a different system and imported onto the Firewall Management Center. • `Scheduled`: results from scans run as a scheduled task.
Results	The results of the scan.
Domain	The domain of the scan target. This field is only present in a multidomain deployment.

Import Nmap scan results

You can import XML results files created by an Nmap scan performed outside of the system. You can also import XML results files that you previously downloaded from the system. To import Nmap scan results, the results file must be in XML format and adhere to the Nmap Version 1.01 DTD. For more information on creating Nmap results and on the Nmap DTD, refer to the Nmap documentation at https://insecure.org.

A host must already exist in the network map before Nmap can append its results to the host profile.

Procedure

Step 1 Choose **Policies** > **Actions** > **Scanners**.

Step 2 On the toolbar, click **Import Results**.

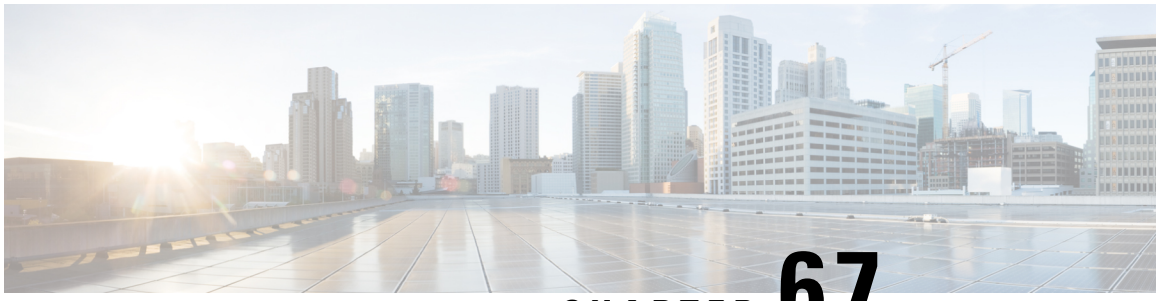
Step 3 Click **Browse** to navigate to the results file.

Step 4 After you return to the Import Results page, click **Import** to import the results.

History for host identity sources

This reference provides the version history for Host Identity Sources features, including security improvements and version compatibility information.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Security improvement to the host input data feature	6.5	Any	TLS 1.2 is now used for communication between your Firewall Management Center and the host input client. The topic Configure the host input client, on page 2263has been updated with this information.



CHAPTER 67

Application detection

Application detection is a process that

- identifies network traffic by application type,
- classifies network traffic to facilitate granular management, and
- enhances security.

Application detection provides administrators visibility into network usage patterns and enhances control over network management and policy enforcement.

- Application detection, on page 2283
- Requirements and prerequisites for application detection, on page 2289
- Custom application detectors, on page 2289
- View or download detector details, on page 2298
- Sort the detector list, on page 2299
- Filter the detector list, on page 2299
- Navigate to other detector pages, on page 2301
- Activate and deactivate detectors, on page 2301
- Edit custom application detectors, on page 2302
- Deleting detectors, on page 2303

Application detection

Application detection is a system capability that

- analyzes IP traffic to identify commonly used applications on your network,
- provides application awareness crucial for application control, and
- identifies applications according to characteristics specified in detectors.

Application detection types and sources

The system detects three types of applications:

- *application protocols* such as HTTP and SSH, representing communications between hosts
- *clients* such as web browsers and email clients, representing software running on the host

- *web applications* such as MPEG video and Facebook, representing the content or requested URL for HTTP traffic

The system identifies applications in network traffic according to the characteristics specified in the detector. For example, applications may be identified using ASCII patterns in packet headers. SSL protocol detectors use session information to identify the applications.

Application detectors come from two sources:

- *System-provided detectors* detect web applications, clients, and application protocols based on system software version and VDB. Professional Services can import individual detectors. Release notes provide information on updated detectors.
- *Custom application protocol detectors* are user-created to detect web applications, clients, and application protocols.

Implied application protocol detection, infers the existence of an application protocol based on client detection.

You can identify applications only if they originate from monitored network hosts as defined in your network discovery policy. If an internal host accesses an FTP server at an unmonitored remote site, the system does not identify the application protocol as FTP. However, if a remote or internal host accesses an FTP server on a monitored host, the system can identify the application protocol.

If the system identifies the client used by a monitored host to connect to a non-monitored server, it identifies the client's application protocol. However, it does not add this protocol to the network map. Client sessions must include a response from the server to occur for application detection.

The system characterizes each application that it detects; see Application rule conditions, on page 1322. The system uses these characteristics to create groups of applications, called *application filters*. Application filters are used to perform access control and to constrain search results and data used in reports and dashboard widgets.

You can also supplement application detector data using exported NetFlow records, Nmap active scans, and the host input feature.

Related Topics

Application detectors, on page 2284

Application detectors

An application detector is a tool used in network analysis that

- identifies commonly used applications on your network by analyzing traffic patterns,
- provides customizable detection capabilities through different detector types, and
- operates only when active to analyze application traffic.

Application detector types and characteristics

Application detectors identify commonly used applications on your network. Use the Detectors page (**Policies** > **Application Detectors**) to view the detector list and customize detection capabilities.

Modify a detector or change its state (active or inactive) based on its type. The system uses only active detectors to analyze application traffic.

Note

- Cisco-provided detectors may change with system and VDB updates. Refer to the release notes for updates.
- For firepower application identification, we intentionally do not list the ports. The application's associate ports are not reported for any of Cisco's applications because most of the applications are port-agnostic. Our platform's detection capabilities can identify services running at any port in the network.

- *Internal detectors* are a special category of detectors for client, web application, and application protocol traffic. Internal detectors are delivered with system updates and are always on.

  If an application matches internal detectors for client-related activity and no specific client detector exists, it reports a generic client.
- *Client detectors* detect client traffic and are delivered via VDB or system update. These detectors are provided for import by Cisco Professional Services. You can activate and deactivate client detectors. You can export a client detector only if you import it.
- *Web application detectors* detect web applications in HTTP traffic payloads and are delivered via VDB or system update. Web application detectors are always on.
- *Port-based application protocol detectors* use well-known ports to identify network traffic. They are delivered via VDB or system update, or are provided for import by Cisco Professional Services. You can activate and deactivate application protocol detectors, and view a detector definition to use it as the basis for a custom detector.
- *Firepower-based application protocol detectors* analyze network traffic using Firepower application fingerprints and are delivered via VDB or system update. You can activate and deactivate application protocol detectors.
- *Custom application detectors* are pattern-based. They detect patterns in packets from client, web application, or application protocol traffic. You have full control over imported and custom detectors.

Identification of application protocols in the web interface

This table shows how the web interface system identifies application protocols:

Table 144: System identification of application protocols

Identification	Description
Application protocol name	The Firewall Management Center lists the protocol name if it is: • Positively identified by the system • Identified using NetFlow data and a correlation exists in `/etc/sf/services` • Manually identified using the host input feature • Identified by Nmap or an active source

Identification	Description
`pending`	The Firewall Management Center identifies an application protocol as `pending` if the system can neither positively nor negatively identify the application. The system usually needs to collect and analyze more connection data to identify a pending application. In the Application Details and Servers tables and in the host profile, the `pending` status appears only where specific application protocol traffic is detected, not inferred from detected client or web application traffic.
`unknown`	The Firewall Management Center identifies an application protocol as `unknown` if: • the application does not match any of the system's detectors. • the application protocol was identified using NetFlow data, but no port-application protocol correlation exists in `/etc/sf/services`. • Snort has closed the session, but the session still persists in the device. Here, the traffic is allowed to pass through the firewall, but the application is not detected.
blank	All available detected data has been examined, but no application protocol was identified. In the Application Details and Servers tables and in the host profile, the application protocol is left blank for generic client traffic without HTTP connections.

Implied application protocol detection from client detection

Implied application protocol detection is a process that

- occurs when the system can identify the client used by a monitored host to access a non-monitored server,
- allows the Firewall Management Center to infer that the connection uses the application protocol that corresponds with the client, and
- provides application protocol information for connections where monitored hosts access non-monitored servers.

Consequences of implied application protocol detection

This process has these consequences:

- The system does not generate a New TCP Port or New UDP Port event for these servers, preventing their appearance in the Servers table. Additionally, the detection of these application protocols cannot trigger discovery event alerts or correlation rules.
- The application protocol is not associated with a host. Its details cannot be viewed in host profiles, its server identity is not set, and its information is not used in host profile qualifications for traffic profiles or correlation rules. In addition, the system does not associate vulnerabilities with hosts based on this type of detection.

You can trigger correlation events when application protocol information is present in a connection. You can also use the application protocol information in connection logs to create connection trackers and traffic profiles.

Host limits and discovery event logging

The system generates a discovery event when it detects a client, server, or web application, unless the associated host has reached its maximum number of clients, servers, or web applications.

Each host profile displays up to 16 clients, 100 servers, and 100 web applications.

Actions that depend on the detection of clients, servers, or web applications are not affected by this limit. Access control rules set to activate on a server will continue to log connection events.

Special considerations for application detection

Special considerations for application detection are network traffic analysis requirements that

- define specific conditions needed for accurate detection of certain application protocols,
- address limitations in detecting encrypted or proxy-based traffic, and
- establish rules for identifying applications that use referral mechanisms or certificate-based identification.

Application-specific detection requirements

Different applications require specific detection approaches:

- **SFTP**: To detect SFTP traffic, the same rule must also detect SSH.
- **Squid**: The system identifies Squid server traffic when either the system detects a connection from a host on your monitored network to a Squid server where proxy authentication is enabled, or the system detects a connection from a Squid proxy server on your monitored network to a target system, like the the destination server where the client is requesting information or another resource.

The system cannot identify Squid service traffic if:

- proxy authentication is disabled, or
- the Squid proxy server is configured to strip through header fields from its HTTP responses

SSL application detection:

The system uses session information from a Secure Socket Layers (SSL) session to identify the application protocol, client application, or web application in the session.

When the system detects an encrypted connection, it marks that connection as either a generic HTTPS connection or as a specific secure protocols, like SMTPS, when applicable. When the system detects an SSL session, it adds `SSL client` to the **Client** field in connection events for the session. If it identifies a web application for the session, the system generates discovery events for the traffic.

For SSL application traffic, managed devices can also detect the common name from the server certificate and match that against a client or web application from an SSL host pattern. When the system identifies a specific client, it replaces `SSL client` with the name of the client.

Because the SSL application traffic is encrypted, the system can use only information in the certificate for identification, not application data within the encrypted stream. For this reason, SSL host patterns can sometimes only identify the company that authored the application, so SSL applications produced by the same company may have the same identification.

In some instances, such as when an HTTPS session is launched from within an HTTP session, managed devices detect the server name from the client certificate in a client-side packet.

To enable SSL application identification, you must create access control rules that monitor responder traffic. Those rules must have either an application condition for the SSL application or URL conditions using the URL from the SSL certificate. For network discovery, the responder IP address does not have to be in the networks to monitor in the network discovery policy; the access control policy configuration determines whether the traffic is identified. To identify detections for SSL applications, you can filter by the `SSL protocol` tag, in the application detectors list or when adding application conditions in access control rules.

Referred web applications:

Web servers sometimes refer traffic to other websites, which are often advertisement servers. To help you understand referred traffic on your network, the system lists the referring web application in the **Web Application** field for the referred sessio eventsn. The VDB contains a list of known referred sites. When the system detects traffic from one of those sites, the referring site is stored with the event for that traffic. For example, if an advertisement accessed via Facebook is actually hosted on Advertising.com, the detected Advertising.com traffic is associated with the Facebook web application. The system can also detect referring URLs in HTTP traffic, such as when a website provides a simple link to another site; in this case, the referring URL appears in the HTTP Referrer event field.

In events, if a referring application exists, it is listed as the web application for the traffic, while the URL is that for the referred site. In the example above, the web application for the connection event for that traffic would be Facebook, but the URL would be Advertising.com. A referred application may appear as the web application if no referring web application is detected, if the host refers to itself, or if there is a chain of referrals. In the dashboard, connection and byte counts for web applications include sessions where the web application is associated with traffic referred by that application.

Note When creating a rule for referred traffic, add a condition for the referred application instead of the referring application. To block Advertising.com traffic referred from Facebook, for example, add an application condition to your access control rule specific to Advertising.com.

Disable application detection in Snort 3

Disable application detection in Snort 3 by removing application rules and related policies that enable application monitoring.

Note Snort 3 is now at parity with Snort 2, with respect to enabling AppID inspection exclusively on particular network subnets that are defined in the Network Discovery policy filters **if** no other configuration in the AC policy requires AppID to monitor all traffic.

Snort 3 always enables application detection for all networks by default.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**, click edit policy and delete the application rules.

Step 2 Choose **Policies** > **Access Control heading** > **Decryption**, click delete to delete the SSL policy.

Step 3 Choose **Policies** > **Network Discovery**, click delete to delete the network discovery policy.

Step 4 Choose **Policies** > **Access Control heading** > **Access Control**, click **Edit** ( ) to the policy you want to edit and then click the **Security Intelligence** > **URLs** tab to delete the URLs Allow or Block list.

Step 5 As you cannot delete default DNS rules, choose **Policies** > **Access Control heading** > **DNS**, click edit, and uncheck the enabled box to disable the DNS policy.

Step 6 In the access control policy, under the **Advanced** settings, disable the *Enable Threat Intelligence Director* and the *Enable reputation enforcement on DNS traffic* options.

Step 7 Save and deploy the access control policy.

Application detection is disabled in Snort 3, stopping any network monitoring for application identification.

Requirements and prerequisites for application detection

This reference provides the requirements and prerequisites for application detection, including model support, supported domains, and required user roles.

Model support

Any.

Supported domains

Any

User roles

- Admin
- Discovery Admin

Custom application detectors

A custom application detector is a network monitoring tool that

- provides the system with information needed to identify custom applications on your network
- can be created as a custom web application, client, or application protocol detector, and
- is determined by your selections in the **Protocol**, **Type**, and **Direction** fields.

Custom application detector requirements and limitations

The system detects application protocols in server traffic when client sessions include a responder packet from the server. For UDP traffic, the system designates the server as the source of the responder packet.

If you have already created a detector on another Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported detector to suit your needs.

You can export and import both custom detectors and those provided by Cisco Professional Services. However, you **cannot** export or import any other type of Cisco-provided detectors.

Custom application detector and user-defined application fields

Use these fields to configure custom application detectors and user-defined applications.

Custom application detector fields: general

You should use these fields to configure basic and advanced custom application detectors.

Table 145: General custom application detector fields

Field	Description
Application Protocol	The application protocol you want to detect. This can be a system-provided application or a user-defined application. If you want the application to be available for exemption from active authentication (configured in your identity rules), you should select or create an application protocol with the **`User-Agent Exclusion`** tag.
Description	A description for the application detector.
Name	A name for the application detector.
Detector Type	The type of detector, **`Basic`** or **`Advanced`**. Basic application detectors are created in the web interface as a series of fields. Advanced application detectors are created externally and uploaded as custom .lua files.

Custom application detector fields: detection patterns

Use these fields to configure the detection patterns for basic custom application detectors.

Table 146: Detection pattern fields

Field	Description
Direction	The source of the traffic the detector should inspect, **`Client`** or **`Server`**.
Offset	The location in a packet, in bytes from the beginning of the packet payload, where the system should begin the pattern search. Because packet payloads start at byte 0, calculate the offset by subtracting 1 from the number of bytes you want to move forward from the beginning of the packet payload. For example, to look for the pattern in the fifth bit of the packet, type `4` in the **Offset** field.
Pattern	The pattern string associated with the **Type** you selected.
Ports	The port of the traffic the detector should inspect.

Field	Description
Protocol	The protocol you want to detect. Your protocol selection determines whether the **Type** or the **URL** field displays. The protocol (and, in some cases, your subsequent selections in the **Type** and **Direction** fields) determine the type of application detector you create: web application, client, or application protocol.
Type	The type of pattern string you entered. The options you see are determined by the **Protocol** you selected. If you selected **`RTMP`** as the protocol, the **URL** field displays instead of the **Type** field. **Note** If you select **`User Agent`** as the **Type**, the system automatically sets the **Tag** for the application to **`User-Agent Exclusion`**.
URL	Either a full URL or a section of a URL from the swfURL field within the C2 message of a RTMP packet. This field displays instead of the **Type** field when you select **`RTMP`** as the **Protocol**. **Note** The detector assumes that the string you enter is a complete section of the URL. For example, entering **`cisco.com`** would match **`www.cisco.com/support`** and **`www.cisco.com`**, but not **`www.wearecisco.com`**.

Table 147: Application detector types by protocol and configuration

Detector Type	Protocol	Type or Direction
Web Application	HTTP	**Type** is **`Content Type`** or **`URL`**
	RTMP	Any
	SSL	Any
Client	HTTP	**Type** is **`User Agent`**
	SIP	Any
	TCP or UDP	**Direction** is **`Client`**
Application Protocol	TCP or UDP	**Direction** is **`Server`**

Table 148: Pattern string types and characteristics

Type Selection	String Characteristics
`ASCII`	The string is ASCII encoded.
`Common Name`	The string is the value in the commonName field within the server response message.
`Content Type`	The string is the value in the content-type field within the server response header.

Type Selection	String Characteristics
Hex	The string is in hexadecimal notation.
Organizational Unit	The string is the value in the organizationName field within the server response message.
SIP Server	The string is the value in the From field within the message header.
SSL Host	The string is the value in the server_name field within the ClientHello message.
URL	The string is a URL. **Note** The detector assumes that the string you enter is a complete section of the URL. For example, entering **cisco.com** would match **www.cisco.com/support** and **www.cisco.com**, but not **www.wearecisco.com**.
User Agent	The string is the value in the user-agent field within the GET request header. It is also available for the SIP protocol and indicates that the string is the value in the User-Agent field within the SIP message header.

User-defined application fields

Use these fields to configure user-defined applications within basic and advanced custom application detectors.

Table 149: User-defined application configuration fields

Field	Description
Business Relevance	The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally: **Very High**, **High**, **Medium**, **Low**, or **Very Low**. Select the option that best describes the application.
Categories	A general classification for the application that describes its most essential function.
Description	A description for the application.
Name	A name for the application.
Risk	The likelihood that the application is used for purposes that might be against your organization's security policy: **Very High**, **High**, **Medium**, **Low**, or **Very Low**. Select the option that best describes the application.
Tags	One or more predefined tags that provide additional information about the application. If you want an application to be available for exemption from active authentication (configured in your identity rules), you must add the **User-Agent Exclusion** tag to your application.

Configure custom application detectors

Configure custom application detectors to identify specific applications and protocols not covered by the default detectors, enabling more accurate traffic analysis and control.

Configure basic or advanced custom application detectors.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Click **Create Custom Detector**.

Step 3 Enter a **Name** and a **Description**.

Step 4 Choose an **Application Protocol** from the application drop-down list.

You have these options:

- If you are creating a detector for an existing application protocol (for example, if you want to detect a particular application protocol on a non-standard port), select the application protocol from the drop-down list.
- If you are creating a detector for a user-defined application, follow the procedure outlined in Create a user-defined application, on page 2294.

Step 5 Click **Detector Type** as **Basic** or **Advanced** and click **OK**.

Step 6 Configure **Detection Patterns** or **Detection Criteria** or **Encrypted Visibility Engine Process Assignments**:

- If you are configuring a basic detector, specify preset **Detection Patterns** as described in Specifying detection patterns in basic detectors, on page 2295.
- If you are configuring an advanced detector, specify custom **Detection Criteria** as described in Specify detection criteria in advanced detectors, on page 2296.
- If you are configuring an encrypted visibility engine (EVE) detector, specify custom EVE process assignments as described in *Specifying EVE Process Assignments* section in this chapter.

Caution Advanced custom detectors are complex; ensure your knowledge of .lua files is adequate. Incorrect configuration can negatively impact performance or detection.

Step 7 Optionally, use **Packet Captures** to test the new detector as described in Testing a custom application protocol detector, on page 2298.

Step 8 Click **Save**.

Note If you include the application in an access control rule, the detector is automatically activated and cannot be deactivated while it's in use.

The custom application detector is created and is ready for activation in access control rules and policies.

What to do next

Activate the detector as described in Activate and deactivate detectors, on page 2301.

Related Topics

Custom application detector and user-defined application fields, on page 2290

Create a user-defined application

Creating an application protocol detector to identify traffic that is not recognized by default system detectors. Applications, categories, and tags created here can be used in access control rules and application filters.

Caution Creating a user-defined application immediately restarts the Snort process without going through the deploy process. The system warns that continuing will restart the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Before you begin

Begin configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293.

Follow these steps to create a user-defined application:

Procedure

Step 1 On the **Create A Custom Application Detector** dialog box, click **Add** (+) next to the **Application** field.

Step 2 Type a **Name**.

Step 3 Type a **Description**.

Step 4 Select a **Business Relevance**.

Step 5 Select a **Risk**.

Step 6 Click **Add** next to Categories to add a category and type a new category name, or select an existing category from the **Categories** drop-down list.

Step 7 (Optional) Click **Add** next to Tags to add a tag and type a new tag name, or select an existing tag from the **Tags** drop-down list.

Step 8 Click **OK**.

The user-defined application is created and is ready to be configured as part of your custom application protocol detector.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Custom application detector and user-defined application fields, on page 2290

Specifying detection patterns in basic detectors

Configure a custom application protocol detector to search application protocol packet headers for a specific pattern string. You can also configure detectors to search for multiple patterns; requiring the application protocol traffic to match all patterns for positive identification.

Application protocol detectors can search for ASCII or hexadecimal patterns, using any offset.

Before you begin

Configure your custom application protocol detector as described in Configure custom application detectors, on page 2293.

Follow these steps to specify detection patterns in basic detectors:

Procedure

Step 1 On the **Create Detector** page, in the **Detection Patterns** section, click **Add**.

Step 2 Choose protocol type from the **Application** drop-down list.

Step 3 Choose pattern type from the **Type** drop-down list.

Step 4 Type a **Pattern** string that matches the **Type** you specified.

Step 5 Optionally, type the **Offset** (in byte).

Step 6 Optionally, to identify application protocol traffic based on the port it uses, type a port from 1 to 65535 in the **Port(s)** field. To use multiple ports, separate them by commas.

Step 7 Click a **Direction**: `Client` or `Server`.

Step 8 Click **OK**.

Tip If you want to delete a pattern, click **Delete** ( ) next to the pattern you want to delete.

The detection pattern is successfully added to your custom application protocol detector configuration.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Specify detection criteria in advanced detectors, on page 2296

Specify detection criteria in advanced detectors

Upload a custom .lua file to specify detection criteria for advanced custom application detectors.

Caution

- Advanced custom detectors are complex and require outside knowledge to construct valid .lua files. Incorrectly configured detectors could have a negative impact on performance or detection capability.
- Do not upload .lua files from untrusted sources.

Custom .lua files contain your custom application detector settings. Creating custom .lua files requires advanced knowledge of the lua programming language and experience with Cisco's C-lua API. Cisco strongly recommends you use these references to prepare .lua files:

- Third-party instruction and reference material for the lua programming language
- The Open Source Detectors Developers Guide: https://www.snort.org/downloads
- OpenAppID Snort community resources: http://blog.snort.org/search/label/openappid

Note The system does not support .lua files that reference system calls or file I/O.

Before you begin

- Begin configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293.
- Prepare to create a valid .lua file by downloading and studying the .lua files for comparable detectors. For more information about downloading detector files, refer to View or download detector details, on page 2298.
- Create a valid .lua file that contains your custom application detector settings.

Follow these steps to specify detection criteria in advanced detectors:

Procedure

Step 1 On the **Create Detector** page for an advanced custom application detector, in the **Detection Criteria** section, click **Add**.

Step 2 Click **Browse...** to navigate to the `.lua` file and upload it.

Step 3 Click **OK**.

The .lua file is uploaded and the detection criteria are specified for your advanced custom application detector.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Specifying detection patterns in basic detectors, on page 2295

Specifying EVE process assignments

Configure custom application detectors to map processes detected by the encrypted visibility engine (EVE) to applications.

Before you begin

Configure your custom application protocol detector as described in the relevant section on Configure custom application detectors, on page 2293.

Follow these steps to specify EVE process assignments:

Procedure

Step 1 On the Create Detector page, in the Encrypted Visibility Engine Process Assignments section, click **Add**.

Step 2 Enter the **Process Name** and **Minimum Process Confidence** value.

Note You can enter text in the **Process Name** field, and this is case-sensitive. The value should match the exact process name detected by EVE. The **Minimum Process Confidence** value ranges from 0 to 100. This is the number displayed in the **Encrypted Visibility Process Confidence Score** field in Connection Events.

For information about the **Encrypted Visibility Process Confidence Score** field, refer to the section *Connection and Security Intelligence Event Fields* in the Cisco Firepower Management Center Administration Guide.

Step 3 Click **Save**.

Step 4 In the Application Detector listing page, activate the detector that you created. For more information, refer to Activate and deactivate detectors, on page 2301. When you activate the detector, the system pushes the detector files to all the FTDs registered on the Firewall Management Center.

Your EVE process assignments are set for your custom application detector, effectively mapping processes to the specified applications.

What to do next

Continue the configuration of your custom application protocol detector as described in Configure custom application detectors, on page 2293 to enable system traffic analysis.

Testing a custom application protocol detector

Test a custom application protocol detector against packet capture (pcap) files to verify that the detector accurately identifies the intended application traffic before deploying it in your network environment.

If you have a packet capture (pcap) file that contains packets with traffic from the application protocol you want to detect, test it using a custom application protocol detector. Use a simple pcap file free of unnecessary traffic.

Pcap files must be 256 KB or smaller. If you test your detector with a larger pcap file, the Firewall Management Center automatically truncates it and tests the incomplete file. You must fix the unresolved checksums in a pcap before using the file to test a detector.

Before you begin

Configure your custom application protocol detector as described in Configure custom application detectors, on page 2293.

Follow these steps to test a custom application protocol detector:

Procedure

Step 1 On the Create Detector page, in the **Packet Captures** section, click **Add**.

Step 2 Browse to the pcap file in the pop-up window and click **OK**.

Step 3 Click **Evaluate** next to the pcap file to test your detector against the contents of the pcap file. The system displays a message shwoing if the test was successful.

Step 4 Optionally, repeat steps 1 to 3 to test the detector against additional pcap files.

Tip To delete a pcap file, click **Delete** ( ) next to the file you want to delete.

The system evaluates your custom application protocol detector against the chosen pcap files and displays test results indicating the detector's success in identifying traffic.

What to do next

Continue configuring your custom application protocol detector as described in Configure custom application detectors, on page 2293. You must save and activate the detector before the system can use it to analyze traffic.

View or download detector details

Use the detectors list to view details for all application detectors and to download details for custom application detectors, supporting network security analysis and configuration management.

Procedure

Step 1 To view application detector details, choose from the available options:

- Refer to the *Cisco Firepower Application Detector Reference* for the relevant VDB version at https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html
- a. Select **Policies** > **Application Detectors**.

  b. Filter the list to find a particular detector.

  c. Click **Information** ( )

Step 2 To download detector details for a custom application detector, click **Download** ( ).

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have the necessary permissions.

You can access application detector information either through the reference documentation or the management interface and download custom detector details.

Sort the detector list

Organize detectors in a specific order to make them easier to locate and manage by sorting the detector list.

By default, the Detectors page lists detectors alphabetically by name. An up or down arrow placed next to a column heading shows the sort direction.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Click the appropriate column heading.

The detector list is sorted according to the selected column, with an arrow indicator showing the sort direction.

Filter the detector list

Use filters to narrow down the detector list. Focus on specific types of detectors or detector characteristics relevant to your analysis or configuration needs.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Expand one of the filter groups described in Filter groups for the detector list, on page 2300 and select the check box next to a filter. To select all filters in a group, right-click the group name and select **Check All**.

Step 3 If you want to remove a filter, click **Remove** (×) in the name of the filter in the **Filters** field or disable the filter in the filter list. To remove all filters in a group, right-click the group name and select **Uncheck All**.

Step 4 If you want to remove all filters, click **Clear all** next to the list of filters applied to the detectors.

The system updates the detector list displaying only those detectors that match your selected criteria.

Filter groups for the detector list

You can use several filter groups, separately or in combination, to filter the list of detectors.

Name

Locate detectors using string-matching in names or descriptions. All alphanumeric and special characters are allowed.

Custom filter

Locates detectors using custom filters set up on the object management page.

Author

Filter detectors based on their creator, such as:

- Individual user: Custom detectors created or imported by a user
- Cisco: All detectors provided by Cisco, *except* imported add-on detectors (you are the author for any detector that you import)
- **Any User**: Detectors not provided by Cisco.

State

Filters detectors based on their status, either **Active** or **Inactive**.

Type

Filters detectors by type, as described in Application detectors, on page 2284.

Protocol

Identifies detectors based on the inspected traffic protocol.

Category

Finds detectors based on the application categories they target.

Tag

Locates detectors by the tags assigned to applications.

Risk

Filters detectors based on the application risk levels: **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Business relevance

Filters detectors according to the business relevance of applications: **Very High**, **High**, **Medium**, **Low**, and **Very Low**.

Navigate to other detector pages

Detector pages display large amounts of data across multiple pages. Use the navigation controls to move efficiently between pages.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 If you want to view the next page, click **Right Arrow** ( ).

Step 3 If you want to view the previous page, click **Left Arrow** ( ).

Step 4 If you want to view a different page, type the page number and press Enter.

Step 5 If you want to jump to the last page, click **Right End Arrow** ( ).

Step 6 If you want to jump to the first page, click **Left End Arrow** ( ).

You can now navigate efficiently between detector pages using the available navigation controls.

Activate and deactivate detectors

Activate detectors to analyze network traffic or deactivate unused detectors to improve performance.

You must activate a detector before you can use it to analyze network traffic. By default, all Cisco-provided detectors are activated.

You can activate multiple application detectors for each port to enhance detection.

If you include an application in an access control rule in a policy and that policy is deployed without an active detector for that application, one or more detectors automatically activate. You cannot deactivate a detector while an application is in use in a deployed policy if doing so leaves no active detectors for that application.

Tip For improved performance, deactivate any application protocol, client, or web application detectors you do not intend to use.

Caution Activating or deactivating a system or custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Click the slider next to the detector you want to activate or deactivate. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Note Some application detectors are required by other detectors. If you deactivate one of these detectors, a warning appears to indicate that the detectors that depend on it are also disabled.

The detector activation status changes immediately. When you activate or deactivate a system or custom application detector, the Snort process automatically restarts.

Edit custom application detectors

Use this procedure to modify the custom application detectors already configured in your system.

Before you begin

Follow these steps to edit custom application detectors:

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Click **Edit** ( ) next to the detector you want to modify. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Make changes to the detector as described in Configure custom application detectors, on page 2293.

Step 4 Choose an appropriate saving options based on the state of the detector:

- To save an inactive detector, click **Save**.
- To save an inactive detector as a new, inactive detector, click **Save as New**.
- To save an active detector and immediately start using it, click **Save and Reactivate**.

Caution Saving and reactivating a custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing will restart the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

- To save an active detector as a new, inactive detector, click **Save as New**.

The custom application detector is modified and saved based on your selected option.

Deleting detectors

You can delete custom detectors as well as individually imported add-on detectors provided by Cisco Professional Services. You cannot delete any of the other Cisco-provided detectors, though you can deactivate many of them.

Note While a detector is in use in a deployed policy, you cannot delete the detector.

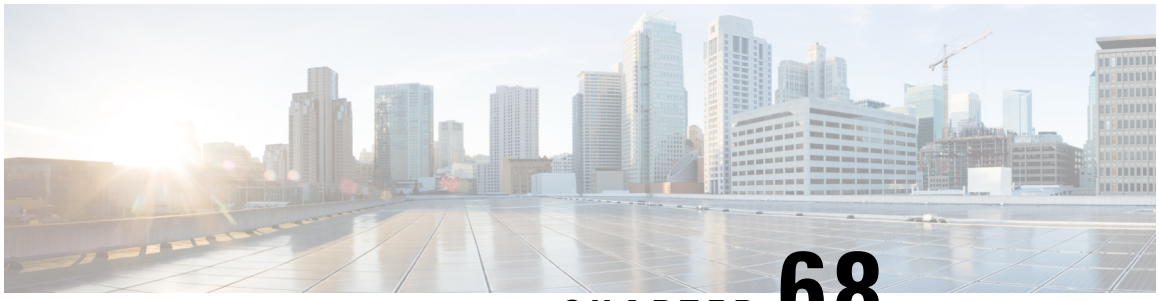
Caution Deleting an activated custom application detector immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel; the restart occurs on any managed device in the current domain or in any of its child domains. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Procedure

Step 1 Select **Policies** > **Application Detectors**.

Step 2 Click **Delete** ( ) next to the detector you want to delete. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click **OK**.



CHAPTER 68

Network Discovery Policies

The following topics describe how to create, configure, and manage network discovery policies:

- Network discovery policies overview, on page 2305
- Requirements and prerequisites for network discovery policies, on page 2306
- Network discovery customization, on page 2306
- Network discovery rules, on page 2307
- Configure advanced network discovery options, on page 2316
- Troubleshoot your network discovery strategy, on page 2325

Network discovery policies overview

The network discovery policy on the Firewall Management Center controls how the system collects data on the network assets of your organization and which network segments and ports are monitored.

Discovery rule configuration

Discovery rules in the policy specify which networks and ports you monitor to collect discovery data from traffic, and the zones where you deploy the policy. Within a rule, choose whether to discover hosts, applications, and non-authoritative users. Create rules to exclude networks and zones from discovery that you do not want to monitor. Set up discovery for data from NetFlow exporters as needed. You can also restrict which protocols on your network are used for discovering user data.

By default, the network discovery policy has a single rule that discovers applications from all observed traffic without excluding any networks, zones, or ports. Host and user discovery is not enabled, nor is NetFlow exporter monitoring. The policy is deployed automatically to managed devices when you register them to the Firewall Management Center. To collect host or user data, add or modify discovery rules and deploy the policy to a device.

If you want to adjust the scope of network discovery, you can create additional discovery rules and modify or remove the default rule.

The access control policy for each managed device determines which traffic you permit and, therefore, the traffic you can monitor with network discovery. If you block certain traffic with access control, the system does not examine that traffic for host, user, or application activity. For example, when you block access to social networking applications in an access control policy, discovery data is not collected on those applications.

Enable traffic-based user detection in your discovery rules to detect non-authoritative users based on login activity in traffic across specific application protocols. Disable discovery in certain protocols across all rules

if necessary. Disabling some protocols helps prevent reaching the user limit for your Firewall Management Center model and reserves user count for other protocols.

Use advanced network discovery settings to control what data is logged, how discovery data is stored, which indications of compromise (IOC) rules are active, how you map vulnerabilities for impact assessment, and how you resolve conflicting discovery data from multiple sources.

You can also add sources for host input and NetFlow exporters to monitor.

Requirements and prerequisites for network discovery policies

The following requirements and prerequisites apply to network discovery policies:

Requirement	Description
Model support	Any
Supported domains	Only Leaf domains are supported
User roles	• Admin • Discovery Admin

Network discovery customization

The information about your network traffic collected by the system is most valuable to you when the system can correlate this information to identify the hosts on your network that are most vulnerable and most important.

As an example, if you have several devices on your network running a customized version of SuSE Linux, the system cannot identify that operating system and so cannot map vulnerabilities to the hosts. However, knowing that the system has a list of vulnerabilities for SuSE Linux, you may want to create a custom fingerprint for one of the hosts that can then be used to identify the other hosts running the same operating system. You can include a mapping of the vulnerability list for SuSE Linux in the fingerprint to associate that list with each host that matches the fingerprint.

Customization capabilities

The system also allows you to input host data from third-party systems directly into the network map, using the host input feature. However, third-party operating system or application data does not automatically map to vulnerability information. If you want to see vulnerabilities and perform impact correlation for hosts using third-party operating system, server, and application protocol data, you must map the vendor and version information from the third-party system to the vendor and version listed in the vulnerability database (VDB). You also may want to maintain the host input data on an ongoing basis. Note that even if you map application data to system vendor and version definitions, imported third-party vulnerabilities are not used for impact assessment for clients or web applications.

If the system cannot identify application protocols running on hosts on your network, you can create user-defined application protocol detectors that allow the system to identify the applications based on a port or a pattern. You can also import, activate, and deactivate certain application detectors to further customize the application detection capability.

You can also replace detection of operating system and application data using scan results from the Nmap active scanner or augment the vulnerability lists with third-party vulnerabilities. The system may reconcile data from multiple sources to determine the identity for an application.

Configure the network discovery policy

Configure the Network Discovery Policy to establish how the system identifies and monitors network resources, user traffic, and host operating systems in your environment.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Configure the following components of your policy:

- Discovery rules — See Configure network discovery rules, on page 2308.
- Traffic-based detection for users — See Configure Traffic-Based user detection, on page 2315.
- Advanced network discovery options — See Configure advanced network discovery options, on page 2316.
- Custom operating system definitions (fingerprints) — See Create a custom fingerprint for clients, on page 2252 and Create a custom fingerprint for servers, on page 2254.

Network discovery rules

Network discovery rules allow you to tailor the information discovered for your network map to include only the specific data you want. Rules in your network discovery policy are evaluated sequentially. You can create rules with overlapping monitoring criteria, but doing so may affect your system performance.

Network discovery rule behavior

When you exclude a host or a network from monitoring, the host or network does not appear in the network map and no events are reported for it. However, when the host discovery rules for the local IP are disabled, the detection engine instances are impacted by a higher processing load, as it builds data from each flow afresh rather than using the existing host data.

We recommend that you exclude load balancers (or specific ports on load balancers) and NAT devices from monitoring. These devices may create excessive and misleading events, filling the database and overloading the Firewall Management Center. For example, a monitored NAT device might exhibit multiple updates of its operating system in a short period of time. If you know the IP addresses of your load balancers and NAT devices, you can exclude them from monitoring.

Tip The system can identify load balancers and NAT devices by examining your network traffic.

In addition, if you need to create a custom server fingerprint, you should temporarily exclude from monitoring the IP address that you are using to communicate with the host you are fingerprinting. Otherwise, the network

map and discovery event views will be cluttered with inaccurate information about the host represented by that IP address. After you create the fingerprint, you can configure your policy to monitor that IP address again.

Cisco also recommends that you **not** monitor the same network segment with NetFlow exporters and managed devices. Although ideally you should configure your network discovery policy with non-overlapping rules, the system does drop duplicate connection logs generated by managed devices. However, you **cannot** drop duplicate connection logs for connections detected by both a managed device and a NetFlow exporter.

Configure network discovery rules

You can configure discovery rules to tailor the discovery of host and application data to your needs.

Tip In most cases, we recommend restricting discovery to the addresses in RFC 1918.

Before you begin

- Make sure you are logging connections for the traffic where you want to discover network data ; see *Best Practices for Connection Logging* in the *Cisco Secure Firewall Management Center Administration Guide*.
- If you want to collect exported NetFlow records, add a NetFlow Exporter as described in Add NetFlow exporters to a network discovery policy, on page 2321.
- If you will want to view discovery performance graphs, you must enable hosts, users, and applications in your discovery rule. Note that this may impact system performance.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Add Rule**.

Step 3 Set the **Action** for the rule as described in Actions and discovered assets, on page 2309.

Step 4 Set optional discovery parameters:

- Restrict the rule action to specific networks; see Restrict the monitored network, on page 2310.
- Restrict the rule action to traffic in specific zones; see Configuring zones in network discovery rules, on page 2313.
- Exclude ports from monitoring; see Exclude ports in network discovery rules, on page 2312.
- Configure the rule for NetFlow data discovery; see Configure rules for NetFlow data discovery, on page 2310.

Step 5 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Actions and discovered assets

When you configure a discovery rule, you must select an action for the rule. The effect of that action depends on whether you are using the rule to discover data from a managed device or from a NetFlow exporter.

The table describes what assets are discovered by rules with the specified action settings in those two scenarios.

Table 150: Discovery rule actions

Action	Option	Managed Device	NetFlow Exporter
Exclude	--	Excludes the specified network from monitoring. If the source or destination host for a connection is excluded from discovery, the connection is recorded but discovery events are not created for excluded hosts.	Excludes the specified network from monitoring. If the source or destination host for a connection is excluded from discovery, the connection is recorded but discovery events are not created for excluded hosts.
Discover	Hosts	Adds hosts to the network map based on discovery events. (Optional, unless user discovery is enabled, then required.)	Adds hosts to the network map and logs connections based on NetFlow records.
Discover	Applications	Adds applications to the network map based on application detectors. Note that you cannot discover hosts or users in a rule without also discovering applications.	Adds application protocols to the network map based on NetFlow records and the port-application protocol correlation in `/etc/sf/services`.
Discover	Users	Adds users to the users table and logs user activity based on traffic-based detection on the user protocols configured in the network discovery policy.	n/a
Log NetFlow Connections	--	n/a	Logs NetFlow connections only. Does not discover hosts or applications.

If you want the rule to monitor managed device traffic, application logging is required. If you want the rule to monitor users, host logging is required. If you want the rule to monitor exported NetFlow records, you cannot configure it to log users, and logging applications is optional.

Note The system detects connections in exported NetFlow records based on the **Action** settings in the network discovery policy. The system detects connections in managed device traffic based on access control policy settings.

Monitored networks

A discovery rule causes discovery of monitored assets only in traffic to and from hosts in the specified networks. For a discovery rule, discovery occurs for connections that have at least one IP address within the networks specified, with events generated only for IP addresses within the networks to monitor. The default discovery rule discovers applications from all observed traffic (`0.0.0.0/0` for all IPv4 traffic, and `::/0` for all IPv6 traffic).

If you configure a rule to handle NetFlow discovery and log only connections data, the system also logs connections to and from IP addresses in the specified networks. Note that network discovery rules provide the only way to log NetFlow network connections.

You can also use network object or object groups to specify the networks to monitor.

Restrict the monitored network

Network discovery rules require at least one network to be specified for monitoring purposes. This task enables you to define which networks should be included in the discovery process.

Every discovery rule must include at least one network.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Add Rule**.

Step 3 Click **Networks**, if it is not already open.

Step 4 Add network objects to the Available Networks list as described in Create network objects during discovery rule configuration, on page 2311.

If you modify a network object used in the network discovery policy, the changes do not take effect for discovery until you deploy the configuration changes.

Step 5 Specify a network:

- Choose a network from the **Available Networks** list. If the network does not immediately appear on the list, click **Reload** ( ).
- Enter the IP address into the text box below the Available Networks label.

Step 6 Click **Add**.

Step 7 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure rules for NetFlow data discovery

The system can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.

If you choose a NetFlow exporter in a discovery rule, the rule is limited to discovery of NetFlow data for the specified networks. Choose the NetFlow device to monitor before you configure other aspects of rule behavior, as the available rule actions change when you choose a NetFlow device. You cannot configure port exclusions for monitoring NetFlow exporters.

Before you begin

- Add NetFlow-enabled devices to the network discovery policy; see Add NetFlow exporters to a network discovery policy, on page 2321.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Add Rule**.

Step 3 Choose **NetFlow Device**.

Step 4 From the **NetFlow Device** drop-down list, choose the IP address of the NetFlow exporter to be monitored.

Step 5 Specify the type of NetFlow data you want the system managed device to collect:

- Connection only — Choose `Log NetFlow Connections` from the **Action** drop-down list.
- Host, Application, and Connection — Choose `Discover` from the **Action** drop-down list. The system automatically checks the **Hosts** check box and enables collection of connection data. Optionally, you can check the **Application** check box to collect application data.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Create network objects during discovery rule configuration

You can add new network objects to the list of available networks that appears in a discovery rule by adding them to the list of reusable network objects and groups.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 In **Networks**, click **Add Rule**.

Step 3 Click **Add** (+) next to **Available Networks**.

Step 4 Create a network object as described in Create a network object, on page 2388.

Step 5 Finish adding the network discovery rule as described in Configure network discovery rules, on page 2308.

Port exclusions

Just as you can exclude hosts from monitoring, you can exclude specific ports from monitoring.

Port exclusion use cases

Port exclusions are useful in these scenarios:

- Load balancers can report multiple applications on the same port in a short period of time. You can configure your network discovery rules so that they exclude that port from monitoring, such as excluding port 80 on a load balancer that handles a web farm.
- Your organization may use a custom client that uses a specific range of ports. If the traffic from this client generates excessive and misleading events, you can exclude those ports from monitoring. Similarly, you may decide that you do not want to monitor DNS traffic. In that case, you could configure your rules so that your discovery policy does not monitor port 53.

When adding ports to exclude, you can decide whether to use a reusable port object from the Available Ports list, add ports directly to the source or destination exclusion lists, or create a new reusable port and then move it into the exclusion lists.

Note You cannot exclude ports in rules handling NetFlow data discovery.

Exclude ports in network discovery rules

Excluding ports in network discovery rules allows you to prevent the system from monitoring traffic on specific source and destination ports, helping to optimize network discovery performance and focus on relevant traffic patterns.

You cannot exclude ports in rules handling NetFlow data discovery.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Add Rule**.

Step 3 Click **Port Exclusions**.

Step 4 Optionally, add port objects to the Available Ports list as described in Create port objects during discovery rule configuration, on page 2313.

Step 5 Exclude specific source ports from monitoring, using either of these methods:

- Choose a port or ports from the **Available Ports** list and click **Add to Source**.
- To exclude traffic from a specific source port without adding a port object, under the **Selected Source Ports** list, choose a **Protocol**, enter a **Port** number (a value from 1 to 65535), and click **Add**.

Step 6 Exclude specific destination ports from monitoring, using either of these methods:

- Choose a port or ports from the **Available Ports** list and click **Add to Destination**.
- To exclude traffic from a specific destination port without adding a port object, under the **Selected Destination Ports** list, choose a **Protocol**, enter a **Port** number, and click **Add**.

Step 7 Click **Save** to save the changes you made.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Create port objects during discovery rule configuration

You can add new port objects to the list of available ports that appears in a discovery rule by adding them to the list of reusable port objects and groups that can be used anywhere in the system.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 In Networks, click **Add Rule**.

Step 3 Click **Port Exclusions**.

Step 4 To add a port to the Available Ports list, click **Add** (+).

Step 5 Enter **Name**.

Step 6 In the **Protocol** field, specify the protocol of the traffic you want to exclude.

Step 7 In the **Port** field, enter the ports you want to exclude from monitoring.

You can specify a single port, a range of ports using the dash (-), or a comma-separated list of ports and port ranges. Allowed port values are from 1 to 65535.

Step 8 Click **Save**.

Step 9 If the port does not immediately appear on the list, click **Refresh**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Zones in network discovery rules

To improve performance, discovery rules can be configured so that the zones in the rule include the sensing interfaces on your managed devices that are physically connected to the networks-to-monitor in the rule.

Unfortunately, you may not always be kept informed of network configuration changes. A network administrator may modify a network configuration through routing or host changes without informing you, which may make it challenging to stay on top of proper network discovery policy configurations. If you do not know how the sensing interfaces on your managed devices are physically connected to your network, leave the zone configuration as the default. This default causes the system to deploy the discovery rule to all zones in your deployment. (If no zones are excluded, the system deploy the discovery policy to all zones.)

Configuring zones in network discovery rules

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Add Rule**.

Step 3 Click **Zones**.

Step 4 Choose a zone or zones from the **Available Zones** list.

Step 5 Click **Save** to save the changes you made.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Traffic-based detection identity sources

Traffic-based detection is the only non-authoritative identity source supported by the system. When configured, managed devices detect LDAP, AIM, POP3, IMAP, Oracle, SIP (VoIP), FTP, HTTP, MDNS, and SMTP logins on the networks you specify. The data gained from traffic-based detection can be used only for user awareness. Unlike authoritative identity sources, you configure traffic-based detection in your network discovery policy as described in Configure Traffic-Based user detection, on page 2315.

Traffic-based detection limitations

- Traffic-based detection interprets only Kerberos logins for LDAP connections as LDAP authentications. Managed devices cannot detect encrypted LDAP authentications using protocols such as SSL or TLS.
- Traffic-based detection detects AIM logins using the OSCAR protocol only. They cannot detect AIM logins using TOC2.
- Traffic-based detection cannot restrict SMTP logging. This is because users are not added to the database based on SMTP logins; although the system detects SMTP logins, the logins are not recorded unless there is already a user with a matching email address in the database.

Traffic-based detection also records failed login attempts. A failed login attempt does not add a new user to the list of users in the database. The user activity type for detected failed login activity detected by traffic-based detection is **Failed User Login**.

Note The system cannot distinguish between failed and successful HTTP logins. To see HTTP user information, you must enable **Capture Failed Login Attempts** in the traffic-based detection configuration.

Caution Enabling or disabling non-authoritative, traffic-based user detection over the HTTP, FTP, or MDNS protocols, using the network discovery policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

Traffic-based detection data

When a device detects a login using traffic-based detection, it sends the following information to the Firewall Management Center to be logged as user activity:

- The user name identified in the login.
- The time of the login.

- The IP address involved in the login, which can be the IP address of the user's host (for LDAP, POP3, IMAP, and AIM logins), the server (for HTTP, MDNS, FTP, SMTP and Oracle logins), or the session originator (for SIP logins).
- The user's email address (for POP3, IMAP, and SMTP logins).
- The name of the device that detected the login.

If the user was previously detected, the Firewall Management Center updates that user's login history. Note that the Firewall Management Center can use the email addresses in POP3 and IMAP logins to correlate with LDAP users. This means that, for example, if the Firewall Management Center detects a new IMAP login, and the email address in the IMAP login matches that for an existing LDAP user, the IMAP login does not create a new user; rather, it updates the LDAP user's history.

If the user was previously undetected, the Firewall Management Center adds the user to the users database. Unique AIM, SIP, and Oracle logins always create new user records, because there is no data in those login events that the Firewall Management Center can correlate with other login types.

The Firewall Management Center does **not** log user activity or user identities in the following cases:

- If you configured the network discovery policy to ignore that login type
- If a managed device detects an SMTP login, but the users database does not contain a previously detected LDAP, POP3, or IMAP user with a matching email address

The user data is added to the users table.

Traffic-based detection strategies

You can restrict the protocols where user activity is discovered to reduce the total number of detected users so you can focus on users likely to provide the most complete user information. Limiting protocol detection helps minimize user name clutter and preserve storage space on your Firewall Management Center.

Consider these factors when selecting traffic-based detection protocols:

- Obtaining user names through protocols such as AIM, POP3, and IMAP may introduce user names not relevant to your organization due to network access from contractors, visitors, and other guests.
- AIM, Oracle, and SIP logins may create extraneous user records. This occurs because these login types are not associated with any of the user metadata that the system obtains from an LDAP server, nor are they associated with any of the information contained in the other types of login that your managed devices detect. Therefore, the Firewall Management Center cannot correlate these users with other types of users.

Configure Traffic-Based user detection

Configure traffic-based user detection to automatically enable host discovery and monitor user login activities across various protocols in your network.

When you enable traffic-based user detection in a network discovery rule, host discovery is automatically enabled. For more information about traffic-based detection, see Traffic-based detection identity sources, on page 2314.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Users**.

Step 3 Click **Edit** ( ).

Step 4 Check the check boxes for protocols where you want to detect logins, or clear check boxes for protocols where you do not want to detect logins. Then choose whether you want to **Capture Failed Login Attempts**.

Step 5 Click **Save**.

Traffic-based user detection is configured for the selected protocols, enabling the system to monitor user login activities and automatically discover hosts in your network.

What to do next

Caution Enabling or disabling non-authoritative, traffic-based user detection over the HTTP, FTP, or MDNS protocols, using the network discovery policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. Refer to Snort restart traffic behavior, on page 129.

- Configure network discovery rules to discover users as described in Configure network discovery rules, on page 2308.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure advanced network discovery options

The **Advanced** section of the network discovery policy allows you to configure policy-wide settings. You can define which events are detected, how long discovery data is retained, how often it is updated, which vulnerability mappings are used for impact correlation, and how operating system and server identity conflicts are resolved. In addition, you can add host input sources and NetFlow exporters to allow import of data from other sources.

Note Database event limits for discovery and user activity events are set in system configuration.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** ( ) or **Add** ( ) next to the setting you want to modify:

- Data Storage Settings — Update the settings as described in Configure network discovery data storage, on page 2323.
- Event Logging Settings — Update the settings as described in Configure network discovery event logging, on page 2324.
- General Settings — Update the settings as described in Configuring network discovery general settings, on page 2318.
- Identity Conflict Settings — Update the settings as described in Configure network discovery identity conflict resolution, on page 2319.
- Indications of Compromise Settings — Update the settings as described in Enable indications of compromise rules, on page 2321.
- NetFlow Exporters — Update the settings as described in Add NetFlow exporters to a network discovery policy, on page 2321.
- OS and Server Identity Sources — Update the settings as described in Add network discovery OS and server identity sources, on page 2324.
- Vulnerabilities to use for Impact Assessment — Update the settings as described in Enable network discovery vulnerability impact assessment, on page 2320.

Step 4 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Network discovery general settings

The general settings control how often the system updates network maps and whether server banners are captured during discovery.

Capture banners

Select this check box if you want the system to store header information from network traffic that advertises server vendors and versions (“banners”). This information can provide additional context to the information gathered. You can access server banners collected for hosts by accessing server details.

Update interval

The interval at which the system updates information (such as when any of a host's IP addresses was last seen, when an application was used, or the number of hits for an application). The default setting is 3600 seconds (1 hour).

Note Setting a lower interval for update timeouts provides more accurate information in the host display, but generates more network events.

Configuring network discovery general settings

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** (✎) next to **General Settings**.

Step 4 Update the settings as described in Network discovery general settings, on page 2317.

Step 5 Click **Save** to save the general settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Network discovery identity conflict settings

The system identifies the operating system and applications running on a host by matching fingerprints for operating systems and servers against patterns in traffic. It collects fingerprint information from several sources to give you reliable operating system and server identity information.

The system uses all passive data to derive operating system identities and assign a confidence value.

By default, unless there is an identity conflict, identity data added by a scanner or third-party application overrides identity data detected by the system. You can use the Identity Sources settings to rank scanner and third-party application fingerprint sources by priority. The system retains one identity for each source, but only data from the highest priority third-party application or scanner source is used as the current identity.

Note User input data overrides scanner and third-party application data, regardless of priority.

An identity conflict occurs when the system detects an identity that conflicts with an existing identity from active scanner, third-party application sources listed in the Identity Sources settings, or a system user. By default, identity conflicts are not automatically resolved and you must resolve them through the host profile or by rescanning the host or re-adding new identity data to override the passive identity. However, you can set your system to automatically resolve the conflict by keeping either the passive identity or the active identity.

Generate identity conflict event

Specifies whether the system generates an event when an identity conflict occurs.

Automatically resolve conflicts

From the **Automatically Resolve Conflicts** drop-down list, choose one of these options:

- **Disabled** if you want to force manual conflict resolution of identity conflicts.

- **Keep Passive Identity** if you want the system to use the passive fingerprint when an identity conflict occurs.
- **Keep Active Identity** if you want the system to use the current identity from the highest priority active source when an identity conflict occurs.

Configure network discovery identity conflict resolution

Network discovery may encounter conflicts when multiple sources provide different information about the same network device or host. Configure these settings to define how the system resolves such conflicts.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** ( ) next to **Identity Conflict Settings**.

Step 4 Update the settings in the Edit Identity Conflict Settings pop-up window as described in Network discovery identity conflict settings, on page 2318.

Step 5 Click **Save** to save the identity conflict settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Network discovery vulnerability impact assessment options

You can configure how the system performs impact correlation with intrusion events.

Your choices are:

- Check the **Use Network Discovery Vulnerability Mappings** check box if you want to use system-based vulnerability information to perform impact correlation.
- Check the **Use Third-Party Vulnerability Mappings** check box if you want to use third-party vulnerability references to perform impact correlation. For more information, see the *Firepower System Host Input API Guide*.

You can check either or both of the check boxes. If the system generates an intrusion event and the host involved in the event has servers or an operating system with vulnerabilities in the selected vulnerability mapping sets, the intrusion event is marked with the Vulnerable (level 1: red) impact icon. For any servers which do not have vendor or version information, note that you need to enable vulnerability mapping in the Firewall Management Center configuration.

If you clear both check boxes, intrusion events will **never** be marked with the Vulnerable (level 1: red) impact icon.

Related Topics

Map third-party vulnerabilities, on page 2260

Enable network discovery vulnerability impact assessment

Configure network discovery vulnerability impact assessment. This configuration determines which vulnerabilities are evaluated when you assess the potential impact of security threats on your network assets.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** (✎) next to **Vulnerabilities to use for Impact Assessment**.

Step 4 Update the settings in the Edit Vulnerability Settings pop-up window as described in Network discovery vulnerability impact assessment options, on page 2319.

Step 5 Click **Save** to save the vulnerability settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Indications of compromise

An indication of compromise (IOC) tag is a security detection marker that

- signifies a host is likely compromised by malicious means,
- is generated based on IOC rules that correlate network and host activity, and
- specifies the nature and type of potential compromise, aiding investigation and remediation.

IOC tagging conditions

The Firewall Management Center can tag the host and user involved when one of these things occurs:

- The system correlates data gathered about your monitored network and its traffic, using intrusion, connection, Security Intelligence, and file or malware events, and determines that a potential IOC has occurred.
- The Firewall Management Center can import IOC data from your Secure Endpoint deployments via the AMP cloud. Because this data examines activity on a host itself, such as actions taken by or on individual programs, it can provide insights into possible threats that network-only data cannot. For your convenience, the Firewall Management Center automatically obtains any new IOC tags that Cisco develops from the AMP cloud.

To configure this feature, refer to Enable indications of compromise rules, on page 2321.

You can also write correlation rules against host IOC data and compliance allow lists that account for IOC-tagged hosts.

To investigate and work with tagged IOCs, see *Cisco Secure Firewall Management Center Administration Guide*.

Enable indications of compromise rules

Tip To disable IOC rules for individual hosts or their associated users, see the *Discovery Events* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

Before you begin

Because IOC rules trigger based on data provided by other components of the system and by Secure Endpoint, those components must be correctly licensed and configured for IOC rules to set IOC tags. Enable the system features associated with the IOC rules you plan to enable, such as intrusion detection and prevention (IPS) and Advanced Malware Protection (AMP). If an IOC rule's associated feature is not enabled, no relevant data is collected and the rule cannot trigger.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** (✎) next to **Indications of Compromise Settings**.

Step 4 To toggle the entire IOC feature off or on, click the slider next to **Enable IOC**.

Step 5 To globally enable or disable individual IOC rules, click the slider in the rule's **Enabled** column.

Step 6 Click **Save** to save your IOC rule settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Add NetFlow exporters to a network discovery policy

Use this procedure to add NetFlow exporters.

Note You cannot delete an exporter if it is currently in use in a disocvery rule.

Before you begin

- Review prerequisites: Refer to Requirements for using NetFlow data (principle), on page 2243.
- Configure NetFlow exporters: Refer to NetFlow data, on page 2242.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Add** (+) next to **NetFlow Devices**.

Step 4 Enter the **IP Address** of the exporter.

Step 5 Click **Save**.

What to do next

- Configure a network discovery rule to monitor NetFlow traffic: Refer to Configure network discovery rules, on page 2308.
- Deploy configuration changes; see Deploy configuration changes, on page 135.

Network discovery data storage settings

Discovery data storage settings include the host limit and timeout settings.

When host limit reached

The number of hosts a Secure Firewall Management Center can monitor, and therefore store in the network map, depends on its model. The **When Host Limit Reached** option controls what happens when you detect a new host after you reach the host limit. You can:

Drop hosts

The system drops the host that has remained inactive for the longest time, then adds the new host. This is the default setting.

Don't insert new hosts

The system does not track any newly discovered hosts. Only after the host count falls below the limit does the system resume tracking new hosts. This can occur if an administrator increases the domain's host limit, manually deletes hosts from the network map, or the system identifies hosts as timed out due to inactivity.

Table 151: Reaching the host limit with multitenancy

Setting	Domain Host Limit Set?	Domain Host Limit Reached	Ancestor Domain Host Limit Reached
Drop hosts	yes	Drops oldest host in the constrained domain.	Drops the oldest host among all descendant leaf domains configured to drop hosts. If no host can be dropped, does not add the host.
	no	n/a	Drops the oldest host among all descendant leaf domains configured to drop hosts and that share the general pool.
Don't insert new hosts	yes or no	Does not add the host.	Does not add the host.

Host timeout

The amount of time that passes, in minutes, before the system drops a host from the network map due to inactivity. The default setting is 10080 minutes (one week). Individual host IP and MAC addresses can time out individually, but a host does not disappear from the network map unless all its associated addresses time out.

To avoid premature timeout of hosts, make sure that the host timeout value is longer than the update interval in the network discovery policy general settings.

Server timeout

The amount of time that passes, in minutes, before the system drops a server from the network map due to inactivity. The default setting is seven days (10,080 minutes).

To avoid premature timeout of servers, make sure that the service timeout value is longer than the update interval in the network discovery policy general settings.

Client application timeout

The amount of time that passes, in minutes, before the system drops a client from the network map due to inactivity. The default setting is 10080 minutes (one week).

To ensure optimal performance, set the client timeout value to exceed the update interval in the network discovery policy general settings.

Related Topics

Host limits, on page 1830

Configure network discovery data storage

Configure network discovery data storage settings to control how the system stores and manages network discovery information, including retention policies and storage limits.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** (✎) next to **Network Discovery Data Storage Settings**.

Step 4 Update the settings in the Data Storage Settings dialog as described in Network discovery data storage settings, on page 2322.

Step 5 Click **Save** to save the data storage settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Configure network discovery event logging

The Event Logging Settings control whether discovery and host input events are logged. If you do not log an event, you cannot retrieve it in event views or use it to trigger correlation rules.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** (✎) next to **Event Logging Settings**.

Step 4 Check or clear the check boxes next to the discovery and host input event types you want to log in the database , described in the *Discovery Events* chapter of the *Cisco Secure Firewall Management Center Administration Guide*.

Step 5 Click **Save** to save the event logging settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Add network discovery OS and server identity sources

In **Advanced** section of the network discovery policy, add new active sources or change the priority or timeout settings for existing sources.

Adding a scanner to this page does not add the full integration capabilities that exist for the Nmap scanners, but does allow integration of imported third-party application or scan results.

If you import data from a third-party application or scanner, make sure that you map vulnerabilities from the source to the vulnerabilities detected in your network.

Procedure

Step 1 Choose **Policies** > **Network Discovery**.

Step 2 Click **Advanced**.

Step 3 Click **Edit** ( ) next to **OS and Server Identity Sources**.

Step 4 To add a new source, click **Add Source**.

Step 5 Enter a **Name**.

Step 6 Choose the input source **Type** from the drop-down list:

- Choose **Scanner** if you plan to import scan results using the AddScanResult function.
- Choose **Application** if you do not plan to import scan results.

Step 7 To indicate the duration of time that should elapse between the addition of an identity to the network map by this source and the deletion of that identity, choose **Hours**, **Days**, or **Weeks** from the **Timeout** drop-down list and enter the appropriate duration.

Step 8 Optionally:

- To promote a source and cause the operating system and application identities to be used in favor of sources below it in the list, choose the source and click the up arrow.
- To demote a source and cause the operating system and application identities to be used only if there are no identities provided by sources above it in the list, choose the source and click the down arrow.
- To delete a source, click **Delete** ( ) next to the source.

Step 9 Click **Save** to save the identity source settings.

What to do next

- Deploy configuration changes; see Deploy configuration changes, on page 135.

Related Topics

Map third-party vulnerabilities, on page 2260

Troubleshoot your network discovery strategy

Before you make any changes to the system's default detection capabilities, you should analyze what hosts are not being identified correctly and why, so you can decide what solution to implement.

Are your managed devices correctly placed?

If network devices such as load balancers, proxy servers, or NAT devices reside between the managed device and the unidentified or misidentified host, place a managed device closer to the misidentified host rather than using custom fingerprinting. Custom fingerprinting is not recommended in this scenario.

Do unidentified operating systems have a unique TCP stack?

If the system misidentifies a host, you should investigate why the host is misidentified to help you decide between creating and activating a custom fingerprint or substituting Nmap or host input data for discovery data.



Caution If you encounter misidentified hosts, contact your support representative before creating custom fingerprints.

- If a host is running an operating system that is not detected by the system by default and does not share identifying TCP stack characteristics with existing detected operating systems, you should create a custom fingerprint.
- For example, if you have a customized version of Linux with a unique TCP stack that the system cannot identify, you would benefit from creating a custom fingerprint, which allows the system to identify the host and continuing monitoring it, rather than using scan results or third-party data, which require you to actively update the data yourself on an ongoing basis.
- Note that many open source Linux distributions use the same kernel, and as such, the system identifies them using the Linux kernel name. If you create a custom fingerprint for a Red Hat Linux system, you may see other operating systems (such as Debian Linux, Mandrake Linux, Knoppix, and so on) identified as Red Hat Linux, because the same fingerprint matches multiple Linux distributions.
- Do not use a fingerprint in every situation.

  For example:

  - A modification may have been made to a host's TCP stack so that it resembles or is identical to another operating system.
  - If an Apple Mac OS X host is altered, making its fingerprint identical to a Linux 2.4 host, causing the system to identify it as Linux 2.4 instead of Mac OS X. If you create a custom fingerprint for the Mac OS X host, it may cause all legitimate Linux 2.4 hosts to be erroneously identified as Mac OS X hosts. In this case, if Nmap correctly identifies the host, you could schedule regular Nmap scans for that host.

Third-party data integration

If you import data from a third-party system using host input, you must map the vendor, product, and version strings that the third party uses to describe servers and application protocols to the Cisco definitions for those products. Note that even if you map application data to system vendor and version definitions, imported third-party vulnerabilities are not used for impact assessment for clients or web applications.

- The system may reconcile data from multiple sources to determine the current identity for an operating system or application.
- For Nmap data, you can schedule regular Nmap scans. For host input data, you can regularly run the Perl script for the import or the command line utility. However, note that active scan data and host input data may not be updated with the frequency of discovery data.

Can the system identify all applications?

If a host is correctly identified by the system but has unidentified applications, create a user-defined detector to provide the system with port and pattern matching information to help identify the application.

If the system correctly identifies a host but cannot identify some applications, create a user-defined detector that provides the system with port and pattern matching information. This will help the system identify the application.

Have you applied patches that fix vulnerabilities?

If the system correctly identifies a host but does not reflect applied fixes, you can use the host input feature to import patch information. When you import patch information, you must map the fix name to a fix in the database.

Do you want to track third-party vulnerabilities?

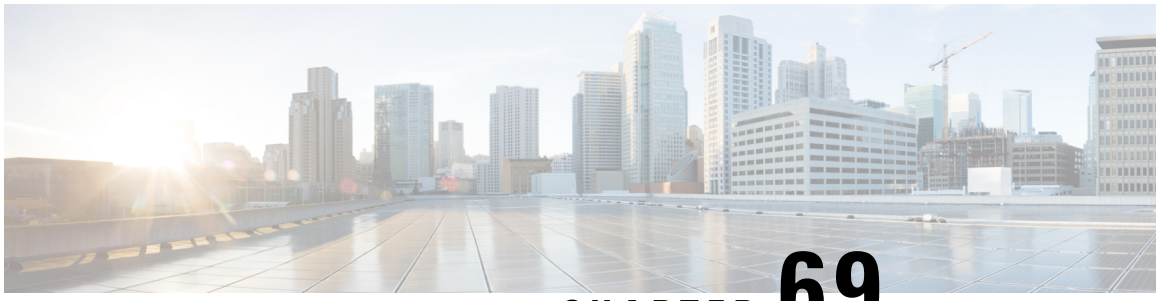
If you have vulnerability information from a third-party system that you want to use for impact correlation, you can map the third-party vulnerability identifiers for servers and application protocols to vulnerability identifiers in the Cisco database and then import the vulnerabilities using the host input feature. For more information on using the host input feature, see the *Firepower System Host Input API Guide*. Note that even if you map application data to system vendor and version definitions, imported third-party vulnerabilities are not used for impact assessment for clients or web applications.



PART XIII

Objects and Certificates

- Object Management, on page 2331
- Certificates, on page 2481



CHAPTER 69

Object Management

This chapter describes how to manage reusable objects.

- Objects, on page 2332
- Use the object manager, on page 2334
- AAA servers, on page 2345
- Access lists, on page 2351
- Configure address pools, on page 2356
- Create an application filter, on page 2357
- Configure an AS PATH object, on page 2357
- Configure a BFD template, on page 2358
- Cipher suite lists, on page 2359
- Configure a community list, on page 2360
- DHCP IPv6 pools, on page 2363
- Distinguished names, on page 2364
- DNS server groups, on page 2366
- External attributes, on page 2367
- File lists, on page 2377
- FlexConfig objects, on page 2382
- Geolocation objects, on page 2382
- Interfaces, on page 2383
- Key chains, on page 2384
- Networks, on page 2386
- PKI objects, on page 2389
- Configure a policy list, on page 2409
- Ports, on page 2411
- Prefix lists, on page 2413
- Configure a route map, on page 2415
- Security intelligence, on page 2418
- Sinkhole objects, on page 2432
- Configure an SLA monitor, on page 2433
- Time ranges, on page 2435
- Time zones, on page 2436
- Tunnel zones, on page 2437
- URLs, on page 2437

- Variable sets, on page 2439
- VLAN tags, on page 2456
- VPN, on page 2456
- History for object management , on page 2477

Objects

An object is a configuration element that

- associates a name with a value for increased flexibility and ease of use in the web interface,
- enables reuse of configurations across policies, rules, event searches, reports, and dashboards, and
- can be managed, grouped, and overridden as needed within the system.

Object management and usage

The system uses named objects to simplify configuration and management. Use the object manager to create and manage objects. Many configurations that use objects also allow you to create objects as needed. The object manager enables you to:

- View the policies, settings, and other objects where a network, port, VLAN, or URL object is used; see View objects and their usage, on page 2338.
- Group objects to reference multiple objects with a single configuration; see Object groups, on page 2340.
- Override object values for selected devices; see Object overrides, on page 2342.

After editing an object used in an active policy, you must redeploy the changed configuration for your changes to take effect. You cannot delete an object that is in use by an active policy.

Note The system configures an object on a managed device only when a policy assigned to that device uses the object. If you remove an object from all policies assigned to a given device, the object is also removed from the device configuration on the next deployment, and subsequent changes to the object are not reflected in the device configuration.

Object types

This table lists the objects you can create in the system, and indicates whether each object type can be grouped or configured to allow overrides.

Object type	Groupable?	Allows overrides?
Network	yes	yes
Port	yes	yes

Object type	Groupable?	Allows overrides?
Interface: • Security Zone • Interface Group	no	no
Tunnel Zone	no	no
Application Filter	no	no
VLAN Tag	yes	yes
External Attribute: Security Group Tag (SGT) and Dynamic Object	no	no
URL	yes	yes
Geolocation	no	no
Time Range	no	no
Variable Set	no	no
Security Intelligence: Network, DNS, and URL lists and feeds	no	no
Sinkhole	no	no
File List	no	no
Cipher Suite List	no	no
Distinguished Name	yes	no
Public Key Infrastructure (PKI): • Internal and Trusted CA • Internal and External Certs	yes	no
Key Chain	no	yes
DNS Server Group	no	no
SLA Monitor	no	no
Prefix List: IPv4 and IPv6	no	yes
Route Map	no	yes
Access List: Standard and Extended	no	yes
AS Path	no	yes
Community List	no	yes

Object type	Groupable?	Allows overrides?
Policy List	no	yes
FlexConfig: Text and FlexConfig objects	no	yes

Objects and multi-tenancy

In a multidomain deployment, you can create objects in Global and descendant domains with the exception of Security Group Tag (SGT) objects, which you can create only in the Global domain. The interface shows objects created in the current domain, which you can edit. It also presents objects created in ancestor domains, which you cannot edit, except for security zones and interface groups.



Note Security zones and interface groups are tied to device interfaces, which you configure at the leaf level. Administrators in descendant domains can view and edit security zones and groups created in ancestor domains. Subdomain users can add and delete interfaces from ancestor zones and groups, but cannot delete or rename these zones or groups.

Object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

For objects that support grouping, you can group objects in the current domain with objects inherited from ancestor domains.

Object overrides allow you to define device-specific or domain-specific values for certain types of object, including network, port, VLAN tag, and URL. In a multidomain deployment, you can define a default value for an object in an ancestor domain, but allow administrators in descendant domains to add override values for that object.

Use the object manager

The object manager provides capabilities for creating and managing objects and object groups, viewing them in paginated lists, filtering results, and refreshing the displayed information.

- The object manager enables creation and management of objects and object groups.
- The object manager displays 20 objects or groups per page. If you have more than 20 of any type of object or group, use the navigation links at the bottom of the page to view additional pages. You can also go to a specific page or click **Refresh** ( ) to refresh your view.
- Access the page using **Objects** > **Object Management**. You can alternatively access the page using **Objects** > **Other FTD Objects**.
- By default, objects and groups are listed alphabetically by name. You can filter objects by name or value.

Import objects

Import objects into the system by uploading a properly formatted comma-separated values file. This task enables bulk addition of supported object types, streamlining object management.

Objects can be quickly imported into the system using a properly formatted CSV file. Up to 1000 objects can be imported in a single operation. The format and required columns vary depending on object type.

Object TYPE	Rules

Individual object	• The column header must be mentioned in capital letters.
	• The file must have the following columns headers:
	  • NAME
	  • DN
	• Both NAME and DN column entries are mandatory to import an entry.
	• You can import individual objects directly into an existing distinguished NAME object group.

Network object	• The column header must be mentioned in capital letters.
	• The file must have the following columns headers:
	  • NAME
	  • DESCRIPTION
	  • TYPE
	  • VALUE
	  • LOOKUP
	• To import a host, range, or network object type, provide entries for both NAME and VALUE columns.
	• For an FQDN object, specify "FQDN" in the TYPE column entry, and enter "IPv4," "IPv6," or "IPv4/IPv6" in the LOOKUP column entry.
	• If you leave the LOOKUP column entry for the FQDN object empty, the system saves the object with ipv4_ipv6 as the VALUE.

Object TYPE	Rules

PORT	• The column header must be mentioned in capital letters.
	• The file must have the following columns headers:
	  • NAME
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• The NAME column entry is mandatory.
	• The PORT column entry is mandatory for 'tcp' and 'udp' PROTOCOL types.
	• The ICMPCODE and ICMPTYPE column entries are mandatory for 'icmp' and 'icmp6' PROTOCOL types.

URL	• The column header must be mentioned in capital letters.
	• The file must have the following columns headers:
	  • NAME
	  • DESCRIPTION
	  • URL
	• You must provide entries for the NAME and URL columns to import an object.

VLAN TAG	• The column header must be mentioned in capital letters.
	• The file must have these columns headers:
	  • NAME
	  • DESCRIPTION
	  • TAG
	• The NAME and TAG column entries are mandatory to import an entry.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose one of these object types from the left pane:

- **Distinguished Name** > **Individual Objects**
- **Network Object**
- **PORT**
- **URL**
- **VLAN TAG**

Step 3 Choose **Import Object** from the **Add [Object TYPE]** drop-down list.

Note If you have selected **Individual Objects** in the previous step, click **Import**.

Step 4 Click **Browse**.

Step 5 Locate and select the comma-separated file on your system.

Step 6 Click **Open**.

Note While importing **Distinguished Name** objects, you can optionally check the **Add imported Distinguished Name objects to the below object group** check box and select the group name from the drop-down box to import the objects directly to an existing distinguished name object group.

Step 7 Click **Import**.

Edit objects

Edit network objects and groups to update their settings or manage variable sets as required for your deployment.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose an object type from the list; see Objects, on page 2332.

Step 3 Click **Edit** ( ) next to the object you want to edit.

If **View** ( ) appears instead, the object belongs to an ancestor domain and has been configured not to allow overrides, or you do not have permission to modify the object.

Step 4 Modify the object settings as desired.

Step 5 If you are editing a variable set, manage the variables in the set; see Manage variables, on page 2452.

Step 6 For objects that can be configured to allow overrides:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344. You can change this setting only for objects that belong to the current domain.

- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 7 Click **Save**.

Step 8 If you are editing a variable set, and that set is in use by an access control policy, click **Yes** to confirm that you want to save your changes.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

View objects and their usage

This task enables you to view where objects are used within your system, helping you understand object dependencies and usage across policies and settings.

You can view usage details of objects on the Object Management page. Firewall Management Center provides this functionality for many object types. However, some object types are not supported.

Before you begin

No prerequisites are required to view object usage details.

Follow these steps to view objects and their usage:

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose one of the following supported object types:

- Access List > Extended
- Access List > Standard
- AS Path
- Community List
- Interface
- Network
- Policy List
- Port
- Prefix List > IPv4 Prefix List
- Prefix List > IPv6 Prefix List
- Route Map

- SLA Monitor
- URL
- VLAN Tag

Step 3 Click the **Find Usage** ( ) icon next to the object.

The Object Usage window displays a list of all the policies, objects, and other settings where the object is in use. Click any of the listed items to know more about the object usage. For policies and some other settings where the object is used, you can click the corresponding links to visit the respective UI pages.

After completing these steps, you will be able to see where each object is used within your system, allowing you to manage and audit object usage efficiently.

Filter objects or object groups

Use this task when working with large configurations or when you need to identify and manage unused objects or object groups.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Enter your filter criteria in the **Filter** field.

The page updates as you type to display matching items.

You can use these wildcards:

- The asterisk (*) matches zero or more occurrences of a character.
- The caret (^) matches content at the beginning of a string.
- The dollar sign ($) matches content at the end of a string.

Step 3 To identify and review unused objects or object groups, check the **Show Unused Object** check box.

Note

- If an object is a part of an unused object group, the object is considered as used. However, the unused object group is displayed when the **Show Unused Object** check box is checked.
- The **Show Unused Object** check box is available only for network, port, URL, and VLAN tag object types.

Object groups

An object group is a configuration grouping that

- enables referencing multiple objects with a single configuration,
- allows objects and object groups to be used interchangeably in the web interface, and
- supports grouping of network, port, VLAN tag, URL, and PKI objects.

Object group usage and management

The system allows you to use objects and object groups interchangeably in the web interface. For example, anywhere you would use a port object, you can also use a port object group.

Network object groups can be nested. You can add a network object group to another network object group, up to 10 levels deep.

Objects and object groups of the same type cannot have the same name.

Edit an object group used in a policy, such as a network object group in an access control policy. Then, re-deploy the configuration for your changes to take effect.

Deleting a group does not delete the objects in the group; only their association with each other. Additionally, you cannot delete a group that is in use in an active policy. For example, you cannot delete a VLAN tag group that is used in a VLAN condition in a saved access control policy.

Object references and literal entries in object groups

Object groups can contain either object references or literal entries.

- Object references are links to existing Host/Network Objects. When the original object is modified (for example, an IP address change), all object groups containing references to that object are automatically updated to reflect the change.
- Literal entries are manually created entries within an object group. Unlike object references, literal entries are independent configuration entities and are not dynamically linked to existing Host/Network Objects. Therefore, changes made to a Host/Network Object do not propagate to object groups containing literal entries.

For example, an administrator may manually add a literal entry with the same name and IP address as an existing Host/Network Object. Although the entries appear identical, the literal entry remains independent of the original object. If the original Host/Network Object is modified, only object groups containing a reference to that object are updated.

Modifying a Host/Network Object updates only those object groups that contain a reference to that object. Object groups containing literal entries continue to display their original configuration unless the literal entries are manually modified.

Group reusable objects

Group reusable objects to simplify configuration and management in Secure Firewall Management Center.

- Organize object types such as Network, Port, URL, VLAN Tag, Distinguished Name, and PKI into groups for easier policy application.

This task is relevant when you need to manage multiple reusable objects and apply them efficiently in firewall policies.

Grouping objects allows for streamlined configuration and reduces manual effort when deploying or updating policies.

- Use this task when creating or editing object groups for policy deployment in Secure Firewall Management Center.

Before you begin

No explicit prerequisites are stated. Ensure you have access to Secure Firewall Management Center and the necessary permissions to manage objects.

- Identify the object types you want to group before starting the task.

Follow these steps to group reusable objects:

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 If the object type you want to group is **Network**, **Port**, **URL**, or **VLAN Tag**:

a) Choose the object type from the list of object types.
b) Choose **Add Group** from the **Add [Object Type]** drop-down list.

Step 3 If the object type you want to group is **Distinguished Name**:

a) Expand the **Distinguished Name** node.
b) Choose **Object Groups**.
c) Click **Add Distinguished Name Group**.

Step 4 If the object type you want to group is **PKI**:

a) Expand the **PKI** node.
b) Choose one of the following:
   - **Internal CA Groups**
   - **Trusted CA Groups**
   - **Internal Cert Groups**
   - **External Cert Groups**
c) Click **Add [Object Type] Group**.

Step 5 Enter a unique **Name**.

Step 6 Choose one or more objects from the list, and click **Add**.

You can also:

- Use the filter field **Search** ( ) to search for existing objects to include, which updates as you type to display matching items. Click **Reload** ( ) above the search field or click **Clear** ( ) in the search field to clear the search string.

- Click **Add** (+) to create objects on the fly if no existing objects meet your needs.

Step 7 Optionally for **Network**, **Port**, **URL**, and **VLAN Tag** groups:

- Enter a **Description**.
- Check the **Allow Overrides** check box to allow overrides for this object group; see Allow object overrides, on page 2344.

Step 8 Click **Save**.

After completing these steps, the object group is created and available for use in firewall policies. You can reference the group in active policies and deploy configuration changes as needed.

What to do next

- If an active policy references your object group, deploy configuration changes; see Deploy configuration changes, on page 135.

Object overrides

An object override is a configuration mechanism that

- enables the definition of alternate values for objects, which the system applies to specified devices,
- lets administrators create a smaller set of shared policies that can be used across devices without losing the flexibility to modify policies for individual devices, and
- allows modifications to an object for devices or domains that require different definitions.

Object override usage and supported object types

Administrators can create an object whose definition works for most devices and use overrides to specify modifications for those devices needing different definitions. You may also need to override an object for all devices. This approach allows you to create a single policy that applies everywhere. Object overrides allow you to use fewer shared policies and customize them for individual devices when necessary.

You can target overrides to a specific domain. The override value applies to all devices in that domain unless you set a device-specific override. The object manager enables selection of objects that can be overridden and allows listing device-level or domain-level overrides for each object.

Supported object types for overrides include:

- Network
- Port
- VLAN tag
- URL
- SLA Monitor

- Prefix List
- Route Map
- Access List
- AS Path
- Community List
- Policy List
- Cert Enrollment (PKI)
- Key Chain

In the object manager, the **Override** column flags objects that support overrides:

- Green checkmark: Overrides can be created, and none have been added yet.
- Red X: Overrides are not supported for the object.
- Number: Indicates the count of overrides added for the object (for example, "2" means two overrides have been defined).

Object override example

For example, to deny ICMP traffic to different departments, each connected to a different network, you can define an access control policy that includes a network object called Departmental Network. By enabling overrides for this object, it's possible to create policy variations on each relevant device that specify the actual network associated with that device.

Manage object overrides

Object overrides are used when you need to adjust the behavior of reusable objects for specific use cases, such as applying different values in different domains or policies. Use this task when you want to add, allow, delete, or edit object overrides in the Secure Firewall Management Center.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose from the list of object types; see Objects, on page 2332.

Step 3 Click **Edit** ( ) next to the object you want to edit.

If **View** ( ) appears instead, the object belongs to an ancestor domain and has been configured not to allow overrides, or you do not have permission to modify the object.

Step 4 Manage the object overrides:

- Add—Add object overrides; see Add object overrides, on page 2344.
- Allow—Allow object overrides; see Allow object overrides, on page 2344.
- Edit—Edit object overrides; see Edit an object override, on page 2345.
- Delete—In the object editor, click **Delete** ( ) next to the override you want to remove.

Step 5 Click **Save**.

Allow object overrides

Enable the Allow Overrides option for an object so that you can specify override values as required for different use cases.

Procedure

Step 1 In the object editor, check the **Allow Overrides** check box.

Step 2 Click **Save** to apply your changes.

What to do next

Add object override values; see Add object overrides, on page 2344.

Add object overrides

Add or adjust object overrides so that network objects or groups can have different values assigned in specific domains or to specific devices, making configuration more flexible without modifying the base object.

Use this task when you need to assign different settings or values to the same object across multiple domains or devices—for example, when different parts of your organization require different configurations for the same network object.

Before you begin

Ensure that object overrides are allowed in your environment. See Allow object overrides, on page 2344.

Procedure

Step 1 In the object editor, expand the **Override** section.

Step 2 Click **Add**.

Step 3 On **Targets**, choose domains or devices in the **Available Devices and Domains** list and click **Add**.

Step 4 On the Override tab, enter a **Name**.

Step 5 Optionally, enter a **Description**.

Step 6 Enter an override value.

Example:

```
For a network object, enter a network value.
```

Step 7 Click **Add**.

Step 8 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Edit an object override

This task enables you to edit the description and value of an existing object override to update its configuration as needed.

You can modify the description and the value of an existing override, but you cannot modify the existing target list. Add a new override with new targets to replace the existing override.

Procedure

Step 1 In the object editor, expand the **Override** section.

Step 2 Click **Edit** ( ) next to the override you want to modify.

Step 3 Optionally, modify the **Description**.

Step 4 Modify the override value.

Step 5 Click **Save** to save the override.

Step 6 Click **Save** to save the object.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

AAA servers

An AAA server is a network authentication, authorization, and accounting component that

- enables centralized management of user credentials
- supports policy enforcement, and
- provides accounting for user activities.

Add a RADIUS server group

RADIUS Server Group objects contain one or more references to RADIUS servers. These servers are used to authenticate users logging in through Remote Access VPN connections.

You can apply these objects to compatible Firewall Threat Defense devices.

Before you begin

Note You cannot override RADIUS Server Group Objects.

Procedure

Step 1 Select **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group**.

All currently configured RADIUS Server Group objects will be listed. Use the filter to narrow down the list.

Step 2 Choose and edit a listed RADIUS Server Group object, or add a new one.

See Configure RADIUS server options, on page 2347 and RADIUS server group configuration options, on page 2346 to configure this object.

Step 3 Click **Save**.

RADIUS server group configuration options

The configuration options for a RADIUS server group enable integration with identity policies and VPN authentication. This topic lists each option and describes its purpose, required settings, and usage notes.

Navigation path

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group**. Choose and edit a configured RADIUS Server Group object or add a new one.

Fields

- **Name** and **Description**—Enter a name and optionally, a description to identify this RADIUS Server Group object.
- **Group Accounting Mode**—Defines how accounting messages are sent to the RADIUS servers. Choose one of these:
  - **Single**—Sends accounting messages to a single server (default).
  - **Multiple**—Sends accounting messages to all servers in the group simultaneously.
- **Retry Interval**—Sets the interval (1–10 seconds) between attempts to contact RADIUS servers.
- **Realms**(Optional)—Specify the Active Directory (AD) realm associated with this RADIUS server group. The selected realm is referenced in identity policies to determine VPN authentication identity sources

for relevant traffic flows. This realm effectively provides a bridge from the identity policy to this RADIUS server group. If no realm is associated with this RADIUS server group, the RADIUS server group cannot be reached to determine the VPN authentication identity source for a traffic flow in an identity policy.

Note This field is mandatory if you use remote access VPN with User Identity and RADIUS as the identity source.

- **Enable authorize only**—If the group is used only for authorization or accounting (not authentication), enable authorize-only mode. This mode omits the RADIUS server password from Access-Request messages; the configured password for individual RADIUS servers is ignored.
- **Enable interim account update** and **Interval**—Enables the generation of interim accounting update messages to notify the RADIUS server of newly assigned IP addresses. The Interval option sets the period (1 to 120 hours; default is 24 hours) between updates.
- **Enable Dynamic Authorization** and **Port**— Enables the RADIUS dynamic authorization or change of authorization (CoA) services for this RADIUS server group. Specify the listening port for RADIUS CoA requests in the **Port** field. The valid range is 1024 to 65535 and the default value is 1700. Once defined, the corresponding RADIUS server group will be registered for CoA notification and it listens to the port for the CoA policy updates from the Cisco Identity Services Engine (ISE).
- **Merge Downloadable ACL with Cisco AV Pair ACL**—Enables merging a downloadable access control list (dACL) with a Cisco attribute-value (AV) pair ACL.

  A downloadable ACL defines and updates access control lists in Cisco ISE. Administrators can then download the updated ACLs to all applicable controllers. For more information about using dACLs in Cisco ISE, see the chapter on Segmentation, section on authorization policies, in the *Cisco ISE Administrator Guide*.

  A Cisco AV pair ACL can be utilized to define specific authentication, authorization, and accounting elements for each individual session. For more information about using dACLs in Cisco ISE, see the chapter on Segmentation, section on authorization profile settings, in the *Cisco ISE Administrator Guide*.

  If you select **Merge Downloadable ACL with Cisco AV Pair ACL**, you can choose the following options:

  - **After Cisco AV Pair ACL**—Place downloadable ACL entries after AV pair entries.
  - **Before Cisco AV Pair ACL**—Place downloadable ACL entries before AV pair entries.

- **RADIUS Servers**—For server-specific configuration options, see Configure RADIUS server options, on page 2347.

Related Topics

Add a RADIUS server group, on page 2346

Configure RADIUS server options

Use this topic to configure a RADIUS server, including authentication, accounting, connectivity, and security settings.

Navigation path

Objects > **Object Management** > **AAA Server** > **RADIUS Server Group**. Choose and edit a listed RADIUS Server Group object, or add a new one. In the RADIUS Server Group dialog, choose and edit a RADIUS Server or add a new server.

Fields

- **IP Address/Hostname**—Specify the hostname or IP address (IPv4 or IPv6) of the RADIUS server that receives authentication requests. Only one server may be selected. To add servers, add more RADIUS Server entries to the RADIUS Server Group list.
- **RADIUS Server-Enabled Message Authenticator**—Message authenticators safeguard server-to-client communication and are required for a secure connection between your RADIUS server and firewall devices. Disabling message authenticators may expose your firewalls to potential attacks.

  Your RADIUS server must support and be configured for Message-Authenticator. Requires Firewall Threat Defense Version 7.0.7+, 7.2.10+, or 7.4.3+. For the Firepower 4100/9300, this feature may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.
- **Authentication Port**—The port on which RADIUS authentication and authorization are performed. The default is 1812.
- **Key** and **Confirm Key**—Enter the shared secret to encrypt data between the managed device (client) and the RADIUS server.

  The key is a case-sensitive, alphanumeric string of up to 127 characters. Special characters are permitted.

  Enter the same key in this field and on the RADIUS server. Enter the shared secret again in the Confirm field.
- **Accounting Port**—Enter the port number for RADIUS accounting. The default port is 1813.
- **Timeout**—Specify the session timeout for authentication.

  Set the timeout value to 60 seconds or more for RADIUS two-factor authentication. The default timeout value is 10 seconds.
- **Connect Using** —Select the method to connect the device to a RADIUS server using either a route lookup or a specific interface.
  - Click the **Routing** radio button to use the routing table.
  - Click the **Specific Interface** radio button and choose a security zone/interface group or the Management interface (the default) from the drop-down list. If you want to use Management, you must choose it specifically; it is not available when using a route lookup. You cannot specify any other management-only interface as the RADIUS source.You can also choose a loopback interface group.
- **Redirect ACL**—Select the redirect ACL from the list or add a new one.

  Use the ACL name from the device to control redirected traffic. The Redirect ACL name here must be the same as the *redirect-ACL* name in ISE server. When you configure the ACL object, ensure that you select Block action for ISE and DNS servers, and Allow action for the rest of the servers.

Related Topics

Add a RADIUS server group, on page 2346

RADIUS server group configuration options, on page 2346

Add a single sign-on server

Add a single sign-on (SSO) server to integrate SAML-based authentication for remote access VPN users. This task enables secure user authentication through your identity provider.

Use this task when you need to configure SAML single sign-on for remote access VPN, allowing users to authenticate using an external identity provider. You typically need to perform this configuration when you integrate with SAML IdPs, such as Microsoft Azure.

Before you begin

Obtain the following from your SAML identity provider:

- Identity Provider Entity ID URL
- Sign-in URL
- Sign-out URL
- Identity provider certificate and enroll the certificate in Firewall Threat Defense using the Firewall Management Center web interface (**Devices** > **Certificates**)

For more information, see Configuring a SAML Single Sign-On Authentication, on page 1508.

Follow these steps to add a single sign-on server:

Procedure

Step 1 Choose **Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**.

Step 2 Click **Add Single Sign-on Server** and provide the following details:

Field	Description
Name	Enter the name for the SAML single sign-on server object.
Identity Provider Entity ID	Enter the URL that the SAML IdP defines to uniquely identify a service provider. Enter the URL for a metadata XML page that describes how the SAML Issuer responds to requests.
SSO URL	Enter the URL for signing in to the SAML identity provider server.
Logout URL	Enter the URL for signing out of the SAML identity provider server.
Base URL	Enter the URL that redirects users back to Firewall Threat Defense after the identity provider authenticates them. This should be the access interface URL configured for the Firewall Threat Defense remote access VPN.

Field	Description
Identity Provider Certificate	Enter the IdP certificate enrolled into the Firewall Threat Defense to verify the signed messages. Select an identity provider certificate from the list or click **Add** to create a new certificate enrollment object. For more information, see Manage Firewall Threat Defense certificates, on page 2483. You must enroll all of the Microsoft Azure registered application CA certificates as Trustpoints on the Firewall Threat Defense. The Microsoft Azure SAML identity provider is configured on Firewall Threat Defense for the initial application. All connection profiles are mapped to the configured MS Azure SAML identity provider. For each of the MS Azure applications (other than the default), you can choose the required trustpoint(CA certificate) in the connection profile configuration of the remote access VPN. For details, see Configure AAA Settings for Remote Access VPN, on page 1439.
Service Provider Certificate	Firewall Threat Defense certificate, which will be used to sign the requests and build circle of trust with IdP. If you have not enrolled internal Firewall Threat Defense certificates, click + to add and enroll a certificate. For more information, see Manage Firewall Threat Defense certificates, on page 2483.
Request Signature	Select the encryption algorithm to sign the SAML single sign-on requests. The signatures are listed from weakest to strongest: SHA1, SHA256, SHA384, SHA512. Select None to disable encryption.
Request Timeout	Specify how long users can complete the single sign-on request (SAML assertion validity duration). The SAML IdP has two time outs: *NotBefore* and *NotOnOrAfter*. The Firewall Threat Defense validates if its current time is within the time range of (lower limit) *NotBefore* and (upper limit) the smaller of *NotBefore* plus *timeout* and *NotOnOrAfter*. Thus, if you set a timeout longer than the IdP's *NotOnOrAfter* timeout, the specified timeout is ignored and the *NotOnOrAfter* timeout is selected. If the sum of the specified timeout and the *NotBefore* timeout is less than the *NotOnOrAfter* time, Firewall Threat Defense timeout overrides the timeout. The timeout range is 1-7200 seconds; the default is 300 seconds.
Enable IdP only accessible on Internal Network	Select this option if the SAML IdP resides on the internal network. Firewall Threat Defense acts as a gateway and establishes communication between the users and IdP using an anonymous webvpn session.
Request IdP re-authentication on Login	Select this option to authenticate user at each login even if the previous IdP session is valid.
Allow Overrides	Select this check box to allow overrides for this single sign-on server object.

Step 3 Click **Save**.

The single sign-on server is added and configured for SAML authentication. Users can now authenticate to the remote access VPN using the specified identity provider.

Access lists

An access list is a traffic selection object that

- identifies and selects traffic to which a service will apply
- is used when configuring features such as route maps for Firewall Threat Defense devices, and
- distinguishes between allowed and blocked traffic, where blocked traffic is excluded from the service but not necessarily dropped altogether.

Types of access lists

You can configure these types of ACL:

- Extended: Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses, which you can mix in a given rule.
- Standard: Identifies traffic based on destination address only. Supports IPv4 only.

Each access list is composed of one or more access control entries (ACEs), or rules. The order of ACEs is important.

1. When the ACL is evaluated, a packet is tested against each ACE in the order listed.
2. After a match is found, no more ACEs are checked.
3. Place more specific rules at the top of an ACL for correct behavior.

Place the most specific rules at the top of the ACL so it works as expected

Configure an extended ACL object

Configure extended ACL objects to define traffic classification rules based on source and destination addresses, protocols, ports, application groups, or IPv6 traffic. This enables granular control over network traffic for security and policy enforcement.

Use extended ACL objects when you want to match traffic based on source and destination addresses, protocol and port, application group, or if the traffic is IPv6. These objects are useful for policy-based routing and direct internet access scenarios, and provide flexibility in defining access control entries for various network requirements.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Access List** > **Extended** from the table of contents.

Step 2 Do one of the following:

- Click **Add Extended Access List** to create a new object.
- Click **Edit** ( ) to edit an existing object.

Step 3 In the **New Extended Access List Object** dialog box, enter a name for the object (no spaces allowed) and configure the access control entries:

a) Do one of the following:

- Click **Add** to create a new entry.
- Click **Edit** ( ) to edit an existing entry.

b) Select the **Action**, whether to Allow (match) or Block (not match) the traffic criteria.

Note The **Logging**, **Log Level**, and **Log Interval** options are used for access rules only (ACLs attached to interfaces or applied globally). Because ACL objects are not used for access rules, leave these values at their defaults.

c) Configure the source and destination addresses on the **Network** tab using any of the following techniques:

- Select the desired network objects or groups from the Available list and click **Add to Source** or **Add to Destination**. You can create new objects by clicking the + button above the list. You can mix IPv4 and IPv6 addresses.
- Type an address in the edit box below the source or destination list and click **Add**. You can specify a single host address (such as 10.100.10.5 or 2001:DB8::0DB8:800:200C:417A), or a subnet (in 10.100.10.0/24 or 10.100.10.0 255.255.255.0 format, or for IPv6, 2001:DB8:0:CD30::/60).

d) Click the **Port** tab and configure the service using any of the following techniques.

- Select the desired port objects from the Available list and click **Add to Source** or **Add to Destination**. You can create new objects by clicking the + button above the list. The object can specify TCP/UDP ports, ICMP/ICMPv6 message types, or other protocols (including “any”). However, the source port, which you typically would leave empty, accepts TCP/UDP only. You cannot select port groups.

  For TCP/UDP, note that you must use the same protocol in both the source and destination fields, if you specify both. For example, you cannot specify a UDP source port and a TCP destination port.
- Type or select a port or protocol in the edit box below the source or destination list and click **Add**.

Note To get an entry that applies to all IP traffic, select a destination port object that specifies “all” protocols.

e) Click the **Application** tab and choose the applications that are to be grouped for the direct internet access policy.

Important

- You cannot configure applications for cluster devices. Hence, this tab is not applicable for cluster devices.
- Use extended ACL with applications only in policy-based routing. Do not use it in other policies as its behavior is unknown and not supported. Ensure migration of the realm/ISE configuration for policy-based routing that uses User Identity and SGT in extended ACL.

Note

- The **Available Applications** list displays a fixed set of pre-defined applications. This list is a subset of the applications that are available on the Access Control policy as only they can be detected by their first packet (FQDN end-points resolved to IP addresses and port). The application definitions are updated through the VDB updates and are pushed to Firewall Threat Defense during subsequent deployments.
- User-defined custom applications or group of applications are not supported.
- Currently, Firewall Management Center neither supports user-defined custom applications or group of applications nor allows you to modify the pre-defined applications list.
- You can use the filter options provided under the **Application Filters** to refine this list.

f) Click the **Users** tab and choose the users, user groups, or both that are to be classified for the Policy Based Routing (PBR).

Important

Use extended ACL with users, user groups, or both only for Policy Based Routing. Do not use it in other policies as its behavior is unknown and not supported.

Note

- The **Available Realms** list displays the configured active directory/LDAP realms. For information on creation of realm and managing them, see Create an LDAP realm or an Active Directory realm and realm directory, on page 1860 and Manage a realm, on page 1876 respectively.

  Note Local realms and Azure AD realms are not supported.

- The **Available Users** list displays the downloaded users and user groups of the selected AD/LDAP realms. To download the users, user groups, or both, navigate to **Integrations** > **Other Integrations** > **Realms**, and then click **Download** against the relevant active directory/LDAP realms.

  Note Threat defense can support a maximum of 512 user groups and 64000 user-IP mappings.

- The user to IP mapping and user group membership information are updated and pushed to the Firewall Threat Defense from the Firewall Management Center during the user login or logouts, and changes in the group memberships.

g) Click the **Security Group Tag** tab and choose the source SGT tags to be classified for the direct internet access policy.

Important Use extended ACL with SGTs only for Policy Based Routing. Do not use it in other policies as its behavior is unknown and not supported.

Note

- The **Available Security Group Tags** list displays the configured security group tags. You can choose to use the ISE SGTs or create custom SGTs.
- To use ISE SGTs, ensure that ISE is integrated with Firewall Management Center with **Session Directory Topic** and SXP Topic subscribed.

  Note The supported ISE versions are 3.2, 3,1, 3.0, and 2.7 patch 2+.

- For information on creating custom SGTs, see Create a security group tag object, on page 2376.

h) Select the required application, and click **Add to Rule**.

Note

- Do not configure destination networks and applications in the extended ACL object.
- The selected applications (Network Service objects) in each of the access control entries, form a Network Service Group (NSG) and this group is deployed on the Firewall Threat Defense. The NSG is used in direct internet access to classify traffic based on the match with the selected application group.

i) Click **Add** to add the entry to the object.

Troubleshooting Tips

If necessary, click and drag the entry to move it up or down in the rule order to the desired location. Repeat the process to create or edit additional entries in the object.

Step 4 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 5 Click **Save**.

Configure a standard ACL object

Use standard ACL objects when you only need to match traffic based on destination IPv4 address. Extended ACLs allow more granularity if needed.

Procedure

Step 1 Select **Objects** > **Object Management** > **Access List** > **Standard** from the table of contents.

Step 2 Do one of the following:

- Click **Add Standard Access List** to create a new object.
- Click **Edit** (✎) to edit an existing object.

Step 3 In the **New Standard Access List Object** dialog box, enter a name for the object (no spaces allowed), and configure the access control entries:

a) Do one of the following:

- Click **Add** to create a new entry.
- Click **Edit** (✎) to edit an existing entry.

b) For each access control entry, configure the following properties:

- **Action**—Whether to allow (match) or block (not match) the traffic criteria.
- **Network**—Add the IPv4 network objects or groups that identify the destination of the traffic.

c) Click **Add** to add the entry to the object.

d) If necessary, click and drag the entry to move it up or down in the rule order to the desired location.

Repeat the process to create or edit additional entries in the object.

Step 4 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 5 Click **Save**.

Configure address pools

You can configure IP address pools for both IPv4 and IPv6 that can be used for clustering or for VPN remote access profiles.

Procedure

Step 1 Select **Objects** > **Object Management** > **Address Pools**.

Step 2 Click **IPv4 Pools** and then **Add IPv4 Pools**, and configure the following fields.

- **Name**—Enter the name of the address pool. It can be up to 64 characters.
- **Description**—Add an optional description for this pool.
- **IP Address**—Enter a range of addresses available in the pool. Use dotted decimal notation and a dash between the beginning and the end address, for example: 10.10.147.100-10.10.147.177.
- **Mask**—Identifies the subnet on which this IP address pool resides.
- **Allow Overrides**—Check this check box to enable object overrides. Click the expand arrow to show the **Overrides** table. You can add a new override by clicking **Add**. See Object overrides, on page 2342 for more information.

Step 3 Click **Save**.

Step 4 Click **IPv6 Pools** and then **Add IPv6 Pools**, and configure the following fields.

- **Name**—Enter the name of the address pool. It can be up to 64 characters
- **Description**—Add an optional description for this pool.
- **IPv6 Address**—Enter the first IP address available in the configured pool and the prefix length in bits. For example: 2001:DB8::1/64.
- **Number of Addresses**—Identifies the number of IPv6 addresses, starting at the Starting IP Address, that are in the pool.
- **Allow Overrides**—Check this check box to enable overrides. Click the expand arrow to show the **Overrides** table. You can add a new override by clicking **Add**. See Object overrides, on page 2342 for more information.

Step 5 Click **Save**.

Create an application filter

An application filter is a reusable object that allows you to organize and manage applications efficiently for use in policies that require application matching.

An application filter does these:

- Simplifies application control and policy management.
- Groups applications based on type, risk, business relevance, category, and tags.
- Supports policies such as access control, QoS, intelligent application bypass, and decryption.

Application filter configuration options

- Use the system-provided filters to find applications. Select the desired applications and click **Add to Rule**.
- To remove an application from the filter, click the delete icon next to it.
- Click the info icon next to an application to view its information.

For detailed information on application characteristics, refer to Application rule conditions, on page 1322.

Configure an AS PATH object

Enable control over BGP routing updates and filtering by specifying a sequence of autonomous system (AS) numbers.

An AS Path is a mandatory attribute to set up BGP. It is a sequence of AS numbers through which a network can be accessed. AS path is a sequence of intermediate AS numbers between source and destination routers that form a directed route for packets to travel. Neighboring autonomous systems (ASes) use BGP to exchange and update messages about how to reach different AS prefixes. After each router makes a new local decision on the best route to a destination, it sends the route and associated path information, including distance metrics and path attributes, to its peers. As this information travels through the network, each router along the path prepends its unique AS number to a list of ASes in the BGP message. This list is the route's AS-PATH.

An AS path, along with an AS prefix, provides a specific handle for a one-way transit route through the network. Use the Configure AS Path page to create, copy, and edit autonomous system (AS) path policy objects. Create AS path objects to use when configuring route maps, policy maps, or BGP Neighbor Filtering. An AS path filter allows you to filter the routing update message by using regular expressions.

You can use this object with Firewall Threat Defense devices.

Procedure

Step 1 Choose **Objects** > **Object Management** > **AS Path** from the table of contents.

Step 2 Click **Add AS PATH**.

Step 3 Enter a name for the AS PATH object in the **Name** field. Valid values are between 1 and 500.

Step 4 Click **Add** on the **New AS PATH Object** window.

a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.

b) Specify the regular expression that defines the AS PATH filter in the **Regular Expression** field.

c) Click **Add**.

Step 5 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 6 Click **Save**.

Configure a BFD template

Configure a BFD template to define BFD interval values and authentication settings for single-hop or multi-hop sessions. This enables flexible and reusable BFD configurations across interfaces.

The BFD template specifies a set of BFD interval values. BFD interval values as configured in the BFD template are not specific to a single interface. You can also configure authentication for single-hop and multi-hop sessions. Echo mode is disabled by default. You can enable Echo mode on single-hop only.

Before you begin

No prerequisites are required to configure a BFD template.

Procedure

Step 1 Choose **Objects** > **Object Management** > **BFD Template**.

Step 2 Click **Add BFD Template** or **Edit**.

Note If you are editing a template, you cannot modify its name and type.

Step 3 On the **Template** tab, configure the following:

- **Template Name**—The name of this BFD template. You must assign a name in order to configure the rest of the parameters in the template. The template name cannot have spaces and cannot have only numbers.
- **Type**—Click the **Single-Hop** or **Multi-Hop** radio button.
- **Enable Echo**—(Optional) Enables Echo for the single-hop template.

If the Echo function is not negotiated, BFD control packets are sent at a high rate to meet the detection time. If the Echo function is negotiated, BFD control packets are sent at a slower, negotiated rate and self-directed echo packets are sent at a high rate. We recommend that you use Echo mode, if possible.

Step 4 On the **Interval** tab, configure the following:

a) From the **Interval Type** drop-down list, select **Microseconds** or **Milliseconds**.

b) In the **Multiplier** field, enter the value to be used for computing the hold down time. This value indicates the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The range is 3 to 50. The default is 3.

c) In the **Minimum Transmit** field, enter the minimum transmit interval capability. The range is 50 to 999 milliseconds or 50000 to 999000 microseconds.

d) In the **Minimum Receive** field, enter the minimum receive interval capability. The range is 50 to 999 milliseconds or 50000 to 999000 microseconds.

Step 5 On the **Authentication** tab, configure the following:

- **Authentication Type**—Select **NONE**, **md5**, **meticulous-sha-1**, **meticulous-md5**, or **sha-1** from the drop-down list.
- **Encrypted Password**—(Optional) Enables encryption of the authentication password.
- **Password**—The authentication password that must be sent and received in the packets using the routing protocol being authenticated. The valid value is a string containing 1 to 29 uppercase and lowercase alphanumeric characters, except that the first character cannot be a digit or a digit followed by a whitespace. For example, '1password' or '0 password' is invalid.
- **Key ID**—The shared key ID that matches the key value. The range is 0 to 255.

Step 6 Click **OK**.

Step 7 Click **Apply** to save the BFD template configuration.

The BFD template is configured with the specified interval values, authentication settings, and echo mode options. The template can now be applied to interfaces as needed.

Cipher suite lists

A cipher suite list is an object that

- contains several cipher suites,
- enables negotiation of SSL or TLS encrypted sessions, and
- can be used in SSL rules to control encrypted traffic based on the negotiated cipher suite.

Usage of cipher suite lists in SSL rules

You can use cipher suites and cipher suite lists in SSL rules to control encrypted traffic. These rules evaluate whether the client and server negotiated the SSL session using that cipher suite. If you add a cipher suite list to an SSL rule, and if an SSL session negotiates with any cipher suite from the list, the rule matches the session.

Note You can use cipher suites in the web interface wherever you use cipher suite lists. However, you cannot add, change, or remove cipher suites.

Create a cipher suite list

Create a custom cipher suite list to control which cipher suites are available for use in your environment.

Use this task when defining or updating the set of cipher suites to align with security policies or updated encryption standards.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Cipher Suite List** from the list of object types.

Step 2 Click **Add Cipher Suites**.

Step 3 Enter a **Name**.

Step 4 Choose one or more cipher suites from the **Available Ciphers** list.

Step 5 Click **Add**.

Step 6 Optionally, click **Delete** ( ) next to any cipher suites in the **Selected Ciphers** list that you want to remove.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Configure a community list

Configure a community list to group BGP destinations that share common attributes for route tagging and policy enforcement. This task enables you to create, copy, and edit community list policy objects for use in route maps or policy maps.

Community lists allow marking sets of prefixes for common routing policies, such as filtering or assigning local preference.

A community is an optional transitive BGP attribute used for route tagging. Communities are numerical values assigned to prefixes. They are advertised to neighbors. Upstream providers use these markers to apply routing policies, such as filtering or modifying attributes.

Use the Configure Community Lists page to create, copy, and edit community list policy objects. You can use this object with Firewall Threat Defense devices.

Community lists are used in match clauses of route maps and consist of ordered matching statements. Each destination is compared against the rules. The system stops processing further rules when it finds a match.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Community List** from the table of contents.

Step 2 Click **Add Community List**.

Step 3 In the **Name** field, specify a name for the community list object.

Step 4 Click **Add** on the **New Community List Object** window.

Step 5 Select the **Standard** radio button to indicate the community rule type.

Standard community lists are used to specify well-known communities and community numbers.

Note You cannot have entries using Standard and entries using Expanded community rule types in the same Community List object.

a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.
b) In the **COMMUNITIES** field, specify a community number. Valid values can be from 1 to 4294967295 or from 0:1 to 65534:65535.
c) Select the appropriate **Route Type**.

- Internet—Select to specify the Internet well-known community. Routes with this community are advertised to all peers (internal and external).
- No Advertise—Select to specify the no-advertise well-known community. Routes with this community are not advertised to any peer (internal or external).
- No Export—Select to specify the no-export well-known community. Routes with this community are advertised to only peers in the same autonomous system or to only other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

Step 6 Select the **Expanded** radio button to indicate the community rule type.

Expanded community lists filter communities with regular expressions, which specify patterns used to match community attributes.

a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.
b) Specify the regular expression in the **Expressions** field.

Step 7 Click **Add**.

Step 8 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 9 Click **Save**.

Configure an extended community list

Create an extended community list to organize destinations by shared attributes, enabling precise BGP route filtering and policy object use.

An extended community is a larger group of destinations that share some common attribute. The BGP extended community list has attributes that can be used to mark a set of prefixes that share a common attribute. These markers are used in the match clause of a route map to filter the routes for implementing route leaks among virtual routers. You can also define policy list objects with the extended community list for filtering. Matching statements are organized in an ordered list within the extended community list. Routes are matched against the rules until a match is found with the specified route target (standard rule type) or regular expression

(expanded rule type). Create and edit extended community list policy objects using the Extended Community page.

Note The extended community lists are applicable only for configuring import or export of routes.

You can use this object with Firewall Threat Defense devices.

Procedure

Step 1 Select **Objects** > **Object Management** > **Community List** > **Extended Community**, and then click **Add Extended Community List**.

Step 2 In the **Name** field, specify a name for the extended community list object. You can enter up to 80 characters for the name.

Step 3 Select the extended community rule type:

- To specify one or more route targets, click the **Standard** radio button .
- To specify regular expressions, click the **Expanded** radio button.

Note Use either Standard or Expanded extended community rule type in each Extended Community List object.

Step 4 Click **Add**.

Step 5 If you have selected **Standard** as the extended community rule type, specify the following:

a) In the **Sequence No** field, enter the order in which you want the rule to be executed.

The sequence number must be unique in the list.

b) From the **Action** drop-down list, if you want to permit routes that have matching route target that is specified here, select **Allow**; if you want to deny routes that have matching route target that is specified here, select **Block**.

c) In the **Route Target** field, specify a route target.

- You can add a single route target or a set of route targets separated by commas in a single entry. For example, *1:2,1:4,1:6*.
- Valid values can be from 1:1 to 65534:65535.
- You can have a maximum of 8 route targets in an entry.
- You cannot have redundant route target set across multiple entries. For example, say you want to configure *seq1* with *1:200,100:100,1:300* route targets, and *seq2* with *1:300,100:100,1:200* route targets. This results in redundant route target set and cannot be deployed.

Step 6 If you have selected **Expanded** as the extended community rule type, specify the following:

a) In the **Sequence No** field, enter the order in which you want the rule to be executed.

The sequence number must be unique in the list.

b) From the **Action** drop-down list, if you want to permit routes that have matching regular expression that is specified here, select **Allow**; if you want to deny routes that have matching regular expression that is specified here, select **Block**.

c) Specify the regular expression in the **Expressions** field.

- You can add a single route target or a set of route targets separated by a space in a single entry. For example, *^((16) | (18)):(.)$*.
- You can add a maximum of 16 regular expressions to an entry.
- You cannot have redundant regular expression set across multiple entries. For example, say you want to configure *seq1* with *^((16) | (18)):(.)$ ^4_[0-9]*$* route targets, and *seq2* with *^4_[0-9]*$ ^((16) | (18)):(.)$* route targets. This results in redundant regular expression set and cannot be deployed.

For details on BGP regular expressions, see here.

Step 7 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 8 Click **Save**.

The extended community list can be referenced in the match clause of the Route Map object or Policy List object:

- In the Route Map object, the name of the extended community list is displayed in the **Add Route Map Entry** > **Match Clause** > **BGP** > **Community List** > **Add Extended Community List** dialog. For more details on configuring BGP settings in a route map, see Configure a route map, on page 2415.
- In the Policy List object, the name of the extended community list is displayed in the **Add Policy List** > **Community Rule** > **Add Extended Community List** dialog. For more details on configuring BGP settings in a policy list, see Configure a policy list, on page 2409.

DHCP IPv6 pools

A DHCP IPv6 pool is a configuration element that

- defines a range of IPv6 addresses for DHCP assignment,
- is referenced when configuring DHCPv6 services, and
- enables address allocation to IPv6 clients.

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature (Enable the IPv6 prefix delegation client, on page 703), you can configure the Firewall Threat Defense to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the Firewall Threat Defense by defining a DHCP IPv6 Pool and assigning it to the DHCPv6 server. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

To add a pool, see Create a DHCP IPv6 pool, on page 833.

Distinguished names

A distinguished name is a certificate attribute that

- represents the subject or issuer for a public key certificate,
- can be used in rules to control encrypted traffic based on certificate negotiation, and
- consists of attributes such as country code, common name, organization, and organizational unit.

A *distinguished name group* is a named collection of existing distinguished name objects.

Distinguished name attributes and usage

Distinguished name objects and distinguished name groups can be used in TLS/SSL rules to control encrypted traffic based on whether the client and server negotiated the TLS/SSL session using a server certificate with the distinguished name as subject or issuer.

A distinguished name can include a country code, common name, organization, and organizational unit. In most cases, the certificate includes only a common name. For example, the common name in the certificate for `https://www.cisco.com` is `cisco.com`. The certificate can include multiple Subject Alternative Names (SANs). You can use these names as distinguished names (DNs) in a rule condition. For detailed information about SANs, see RFC 5280, section 4.2.1.6.

The format of a distinguished name object that references a common name is `CN=`*`name`*. If you add a DN rule condition without `CN=`, the system prepends `CN=` before saving the object.

The system uses Server Name Indication (SNI) to match the DN in the TLS/SSL rule whenever possible.

You can also add a distinguished name with one of each of the attributes listed in this table, separated by commas.

Table 152: Distinguished name attributes

Attribute	Description	Allowed Values
C	Country Code	two alphabetic characters
CN	Common Name	up to 64 alphanumeric, backslash (/), hyphen (-), quotation ("), or asterisk (*) characters, or spaces
O	Organization	up to 64 alphanumeric, backslash (/), hyphen (-), quotation ("), or asterisk (*) characters, or spaces
OU	Organizational Unit	up to 64 alphanumeric, backslash (/), hyphen (-), quotation ("), or asterisk (*) characters, or spaces

DN rule conditions

- When the system first detects an encrypted session to a new server, DN data is not available for ClientHello processing. As a result, the first session might not be decrypted.

If the server requests TLS 1.3, the setting for TLS server identity discovery can help by making sure the server certificate is known before making decryption policy decisions. For more information, see TLS server identity discovery, on page 2173.

- You *cannot* configure a distinguished name condition if you also choose the **Decrypt - Known Key** action. Because that action requires you to choose a server certificate to decrypt traffic, the certificate already matches the traffic.

Wildcard examples

You can define one or more asterisks (*****) as wildcards in an attribute. In a common name attribute, you can define one or more asterisks per domain name label. Wildcards match only in that label, but you can define multiple labels with wildcards. See this table for examples.

Table 153: Common name attribute wildcard examples

Attribute	Matches	Does not match
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

Note The DN object `CN=amp.cisco.com` would *not* match a CN like `CN=auth.amp.cisco.com`, which is why wildcards are recommended in these cases.

For more information and examples, see Conditions for distinguished name rules in decryption policies, on page 1765.

Related Topics

Conditions for distinguished name rules in decryption policies, on page 1765

Create a distinguished name object

Enables you to create distinguished name objects, which uniquely identify and reference network entities within Secure Firewall Management Center.

Distinguished name objects are used to specify unique identifiers for certificates or access policies. Perform this task when configuring objects that require a distinguished or common name for identification.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **Distinguished Name** node, and choose **Individual Objects**.

Step 3 Click **Add Distinguished Name**.

Step 4 Enter a **Name**.

Step 5 In the **DN** field, enter a value for the distinguished name or common name. You have the following options:

- If you add a distinguished name, you can include one of each attribute listed in Distinguished names, on page 2364 separated by commas.
- If you add a common name, you can include multiple labels and wild cards.

Step 6 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

DNS server groups

A DNS server group is a network configuration object that

- contains multiple Domain Name System (DNS) servers
- resolves fully qualified domain names (FQDNs), such as `www.example.com`, to IP addresses, and
- enables efficient domain name resolution within a network.

Create a DNS server group object

Create and manage a group of DNS servers for use in network policies to simplify DNS server assignments.

DNS server group objects allow you to define multiple DNS servers that can be referenced by other configuration elements. Use this task to centralize DNS server assignments for interfaces or policies.

Procedure

Step 1 Choose **Objects** > **Object Management** > **DNS Server Group** from the network objects list.

Step 2 Click **Add DNS Server Group**.

Step 3 Enter a **Name**.

Step 4 Optionally, enter the **Default Domain** that will be used to append to the host names that are not fully-qualified.

This setting is only used for the default server group.

Step 5 The default **Timeout** and **Retries** values are pre-populated. Change these values if necessary.

- Retries—Specify how many times (0 to 10) to retry contacting DNS servers if there is no response. Default is 2.
- Timeout—Specify how many seconds (1 to 30) to wait before trying the next DNS server. Default is 2 seconds; this timeout doubles with each retry.

Step 6 Enter the **DNS Servers** IP addresses (IPv4 or IPv6), separated by commas. *(Maximum of 6 servers per group.)*

Step 7 Click **Save**.

What to do next

Assign the configured DNS server group to interface objects in the DNS platform settings. For more information, see Configure DNS server settings, on page 852.

External attributes

Dynamic objects

A dynamic object is a network object that

- specifies one or many IP addresses retrieved using REST API calls or the Dynamic Attributes Connector from cloud sources,
- can be used in access control rules without deploying dynamic changes, and
- automatically updates object values on managed devices after being pushed by the Dynamic Attributes Connector.

Kinds of dynamic objects

There are these kinds of dynamic objects:

- Connector-created dynamic objects: The system pushes dynamic objects created using the dynamic attributes connector to the Firewall Management Center as soon as you create them. The system updates them at regular intervals.

- API-created dynamic objects have the following characteristics:
  - Are IP addresses, with or without classless inter-domain routing (CIDR), that can be used in access control rules much like a network object.
  - Do not support fully-qualified domain names or address ranges.
  - You must update these objects using an API.

For more information about API-created dynamic objects, see API-created dynamic objects, on page 2375.

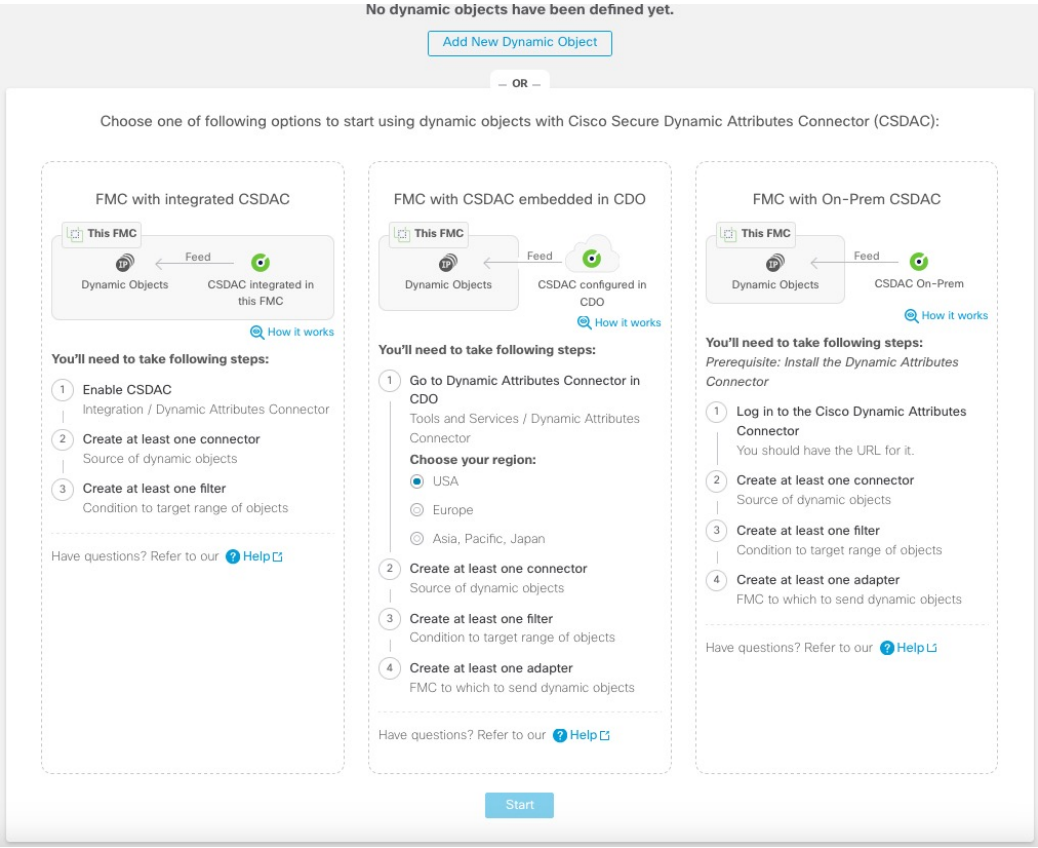
Note Unlike most other objects, dynamic objects do not have to be deployed to managed devices to take effect. Add a dynamic object to the **Dynamic Attributes** tab in a rule and deploy the rule. The object values are automatically updated on the managed device as soon as possible after being pushed by the Dynamic Attributes Connector.

Create dynamic objects for the first time

This topic explains how to create dynamic objects for the first time, describes the informational page displayed when no dynamic objects exist, and outlines the steps to begin the configuration process using the secure firewall manager or dynamic attributes connector.

The page available at **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** is displayed as follows if you have not configured any dynamic objects yet.

If you have already created some dynamic objects, see Dynamic objects page features, on page 2374.



To use this page:

- Select the section that matches how you plan to deploy the dynamic attributes connector.

  Deployment method and outcome:

Method	Outcome
Cloud-Delivered Firewall Management Center with CSDAC Embedded	Access dashboard and configure within application
Cloud-Delivered Firewall Management Center with or CSDAC	Download connector and follow guided configuration
Management Center with Integrated CSDAC	Enable and configure connector within on-prem manager

- Click **How it works** to view diagrams and get more help with that type of deployment.

  The following topics provide more information.

  - Create dynamic objects with embedded Dynamic Attributes Connector, on page 2370
  - Dynamic objects with Security Cloud Control, on page 2371
  - Create dynamic objects with on-premises Dynamic Attributes Connector, on page 2372

- Click **Start** to begin the configuration process in the related application:

- If you clicked the **FMC with Integrated CSDAC** method, **Start** takes you to **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** where you can enable and configure the Dynamic Attributes Connector.

  For more information, see Enable the dynamic attributes connector, on page 2063.

- If you clicked the **FMC with CSDAC embedded in** Security Cloud Control method, **Start** starts Security Cloud Control.

  For more information, see the guide titled *Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Security Cloud Control*.

- If you clicked the **FMC with On-Prem CSDAC** method, **Start** enables you to download the Dynamic Attributes Connector if you have not done so already.

  For more information, see the *Cisco Secure Dynamic Attributes Connector Configuration Guide*.

Create dynamic objects with embedded Dynamic Attributes Connector

A dynamic object is a firewall configuration element that

- enables integration with the embedded Dynamic Attributes Connector
- allows retrieval of IP addresses from cloud services, and
- supports use in access control and DNS rules within the Secure Firewall Management Center.

Integration and configuration details

The Dynamic Attributes Connector is already integrated with the Secure Firewall Management Center (**Integration** > **Dynamic Attributes Connector**).

To use the dynamic attributes connector included with the secure firewall manager, enable it (Integration > Dynamic Attributes Connector), configure connectors that receive dynamic objects, and set up dynamic attributes filters that determine what dynamic objects are sent to this secure firewall manager.

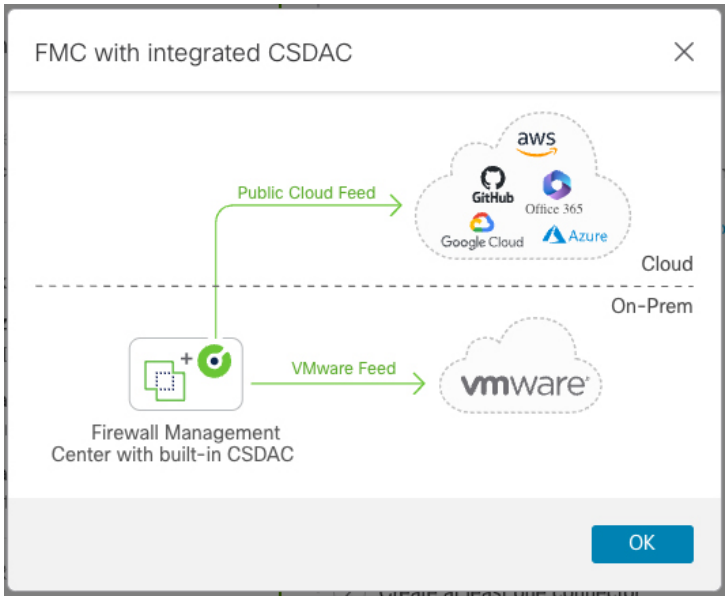
To use this type of deployment:

1. Enable the Dynamic Attributes Connector as discussed in Enable the dynamic attributes connector, on page 2063.
2. Configure connectors, which retrieve IP addresses from cloud services.

   For more information, see Connectors, on page 2072.
3. Configure dynamic attributes filters, which determine what IP addresses to send to the management center.

   For more information, see Create dynamic attributes filters, on page 2092.
4. View your dynamic objects at **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.
5. Use dynamic objects in access control rules (**Policies** > **Access Control heading** > **Access Control**, then click the **Dynamic Attributes** tab).

Figure 424: Dynamic attributes connector integration

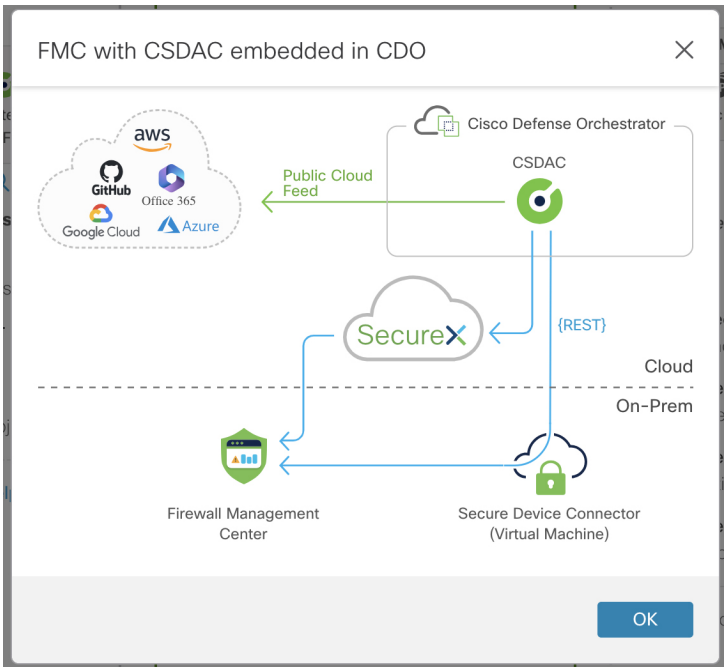


Dynamic objects with Security Cloud Control

A dynamic object is a network management feature that

- enables the retrieval of IP addresses from cloud services using connectors,
- allows you to create dynamic attributes filters to determine which objects are sent, and
- supports integration with secure firewall management centers through adapters.

This page is displayed if you configure the Dynamic Attributes Connector provided with Security Cloud Control.



The diagram includes details about configuring Security Cloud Control that are not discussed in this guide. For more information, see Secure Device Connector (SDC) or SecureX and Security Cloud Control.

To use this type of deployment:

1. Configure connectors to retrieve IP addresses from cloud services. For instructions, see Connectors, on page 2072.
2. Define dynamic attribute filters to specify which IP addresses are sent to the management center.

   For more information, see Create dynamic attributes filters, on page 2092.
3. Set up adapters to send IP addresses to a Secure Firewall Management Center or Cloud-Delivered Firewall Management Center.

   For more information, see the section on creating adapters in the *Cisco Security Cloud Control: Secure Firewall Threat Defense Management*.
4. Log in to the Secure Firewall Management Center that you defined as an adapter.

   If the Secure Firewall Management Center is managed by Security Cloud Control, access the **Cloud-Delivered FMC**.
5. View your dynamic objects at **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.
6. Use dynamic objects in access control rules (**Policies** > **Access Control heading** > **Access Control**, then click the **Dynamic Attributes** tab).

Create dynamic objects with on-premises Dynamic Attributes Connector

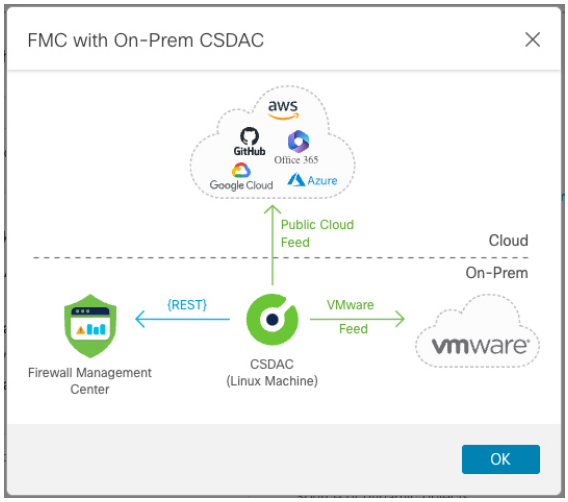
A dynamic object deployment is a configuration method that

- installs the Dynamic Attributes Connector on a supported Linux virtual machine,

- configures connectors, adapters, and dynamic attributes filters to retrieve and send IP addresses to a management center, and
- enables use of dynamic objects in access control and DNS rules.

This page appears if you indicated that you are configuring the on-premises Dynamic Attributes Connector to send dynamic objects to a Secure Firewall Management Center or Cloud-Delivered Firewall Management Center.

Figure 425: Dynamic attributes connector configuration



The on-premises Dynamic Attributes Connector can send dynamic objects to a Secure Firewall Management Center or Cloud-Delivered Firewall Management Center.

To use this type of deployment, complete these steps:

1. Install the Dynamic Attributes Connector on a supported Linux virtual machine.
2. Configure connectors, which retrieve IP addresses from cloud services.

   For more information, see the section on creating connectors in the *Cisco Secure Dynamic Attributes Connector Configuration Guide*.
3. Configure adapters, which send IP addresses to a Secure Firewall Management Center or Cloud-Delivered Firewall Management Center.

   For more information, see the section on creating adapters in the *Cisco Secure Dynamic Attributes Connector Configuration Guide*.
4. Configure dynamic attributes filters, which determine what IP addresses to send to the management center.

   For more information, see the section on configuring dynamic attributes filters in the *Cisco Secure Dynamic Attributes Connector Configuration Guide*.
5. You can view your dynamic objects at **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.
6. Use dynamic objects in access control rules (**Policies** > **Access Control heading** > **Access Control**, then click the **Dynamic Attributes** tab).

For more information, see the *Cisco Secure Dynamic Attributes Connector Configuration Guide*.

Dynamic objects page features

The Dynamic Objects page displays all dynamic objects created using the API or the Cisco Secure Dynamic Attributes Connector. You can edit, delete, or view IP address mappings on this page. The page enables you to view or download IP addresses associated with each object.

The page available at **Objects** > **Object Management** > **External Attributes** > **Dynamic Object** is displayed similar to this if you have already configured some dynamic objects.



This page displays information about each dynamic object and enables you to view or download IP addresses associated with that object. For more information, see Dynamic object mappings, on page 2374.

Dynamic object mappings

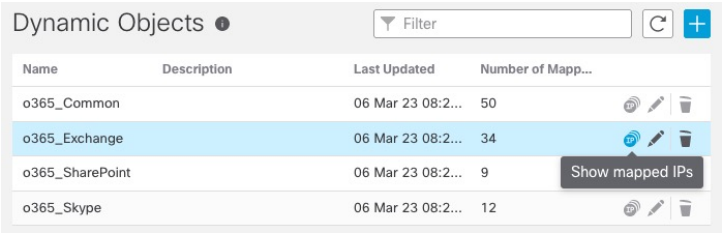
A dynamic object mapping is a configuration feature that

- enables connectors to send IPs matching dynamic attribute filters to the Firewall Management Center,
- allows users to view or download a current list of mapped IP addresses, and
- updates IP addresses dynamically over time to reflect changes in access control rules.

Mapped IP address information

If you configured dynamic objects through the API or by using the dynamic attributes connector, the connectors send IPs that match dynamic attribute filters to the Firewall Management Center at regular intervals.

To view or download a current list of these IP addresses, click **Show Mapped IDs** in the Firewall Management Center, as illustrated.



IP addresses are added dynamically over time. Review the mapped IP addresses regularly, especially if the access control rules do not behave as expected.

Related topics

- API-created dynamic objects, on page 2375
- About the dynamic attributes connector , on page 2061

API-created dynamic objects

An API-created dynamic object is a network object that

- specifies one or more IP addresses retrieved using REST API calls or the Dynamic Attributes Connector,
- can be used in access control rules without deploying dynamic changes to the objects, and
- updates IP addresses from cloud sources.

For more information about the dynamic attributes connector, see the *Cisco Secure Dynamic Attributes Configuration Guide* (link to guide).

Differences between dynamic objects and network objects

- Dynamic objects created using the dynamic attributes connector are pushed to the Firewall Management Center as soon as they are created. These objects are then updated at regular intervals.
- API-created dynamic objects:
  - are IP addresses, with or without classless inter-domain routing (CIDR), that can be used in access control rules much like a network object,
  - do not support fully-qualified domain names or address ranges, and
  - must be updated using an API.

Add or edit an API-created dynamic object

This task enables you to add or edit a dynamic object using the API, allowing you to group IP addresses for use in access control rules. Dynamic objects help automate address management and streamline policy configuration.

A dynamic object is a group of IP addresses, with or without classless inter-domain routing (CIDR). You can use dynamic objects in access control rules much like a network object. This procedure is relevant when you need to manage dynamic address groups via the API instead of manually creating static objects.



Note This procedure is not necessary if you use the Dynamic Attributes Connector because it automatically creates dynamic objects for you.

Before you begin

Consult the *Firepower Management Center REST API Quick Start Guide* for information about how to use the object services REST API to populate the IP object with an address. Dynamic objects do not require deployment.

Follow these steps to add or edit an API-created dynamic object:

Procedure

Step 1 Click **Objects** > **Object Management**.

Step 2 Click **External Attributes** > **Dynamic Objects**.

Step 3 Click **Add Dynamic Object** or **Edit** ( ).

Step 4 Enter a **Name** for the object and an optional **Description**.

Step 5 From the **Type** list, click **IP**.

What to do next

If necessary, update the dynamic object using the API. Deployment is not required.

Security group tags

A security group tag is a network security object that

- specifies a single SGT value,
- is used in rules to control traffic with SGT attributes not assigned by Cisco ISE, and
- cannot be grouped or overridden.

Related Topics

Autotransition from custom SGTs to ISE SGTs
Custom SGT conditions
ISE SGTs versus custom SGT rule conditions

Create a security group tag object

This task allows you to add a security group tag object to enforce network access policies based on SGT.

You can create security group tag objects only in the global domain. A Control license is required for Classic devices. Any Smart License provides coverage for Smart Licensed devices.

Before you begin

- Disable ISE or ISE-PIC connections because custom SGT objects cannot be created if either is used as an identity source.

  Click **Integration** > **Other Integrations** > **Identity Sources**, click **None**, then click **Save**.

- See Best practices for ISE/ISE-PIC integration, on page 1914 for guidelines for using the identity source.

Follow these steps to create a security group tag object:

Procedure

Step 1 Click **Objects** > **Object Management**.

Step 2 Click **External Attributes** > **Security Group Tag**.

Step 3 Click **Add Security Group Tag**.

Step 4 Enter a **Name**.

Step 5 Optionally, enter a **Description**.

Step 6 In the **Tag** field, enter a single SGT.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

File lists

A file list is a threat management feature that

- allows you to manually specify files using unique SHA-256 hash values,
- overrides AMP cloud verdicts to improve detection accuracy within your environment, and
- supports categorization into clean or custom detection lists, enabling precise control over file treatment.

If you use malware defense and the AMP cloud incorrectly identifies a file's disposition, you can add the file to a file list to improve future detection. Specify these files using SHA-256 hash values. You can add up to 10,000 unique SHA-256 values in each file list.

File list categories

File lists are organized into two predefined categories.

- **Clean list**: If you add a file to this list, the system treats it as if the AMP cloud assigned a clean disposition.
- **Custom detection list**: If you add a file to this list, the system treats it as if the AMP cloud assigned a malware disposition.

Because you manually specify the blocking behavior for the files included in these lists, the system does not query the AMP cloud for these files' dispositions. You must configure a rule in the file policy with either the **Malware Cloud Lookup** or **Block Malware** action and a matching file type to calculate a file's SHA value.

Caution Do **not** include malware on the clean list. The clean list overrides both the AMP cloud disposition and the custom detection list.

Source files for file lists

Source files allow you to add multiple SHA-256 values to a file list by uploading a comma-separated value (CSV) file. The system validates the contents and populates the file list with valid SHA-256 values. Upload source files must meet the following requirements:

- The source file must be a simple text file with a .CSV extension.
- Any header must start with a pound sign; it is treated as a comment and will not be uploaded.

- Each entry should contain a single SHA-256 value followed by a description, and must end with either LF or CR+LF newline character.
- The system ignores any additional information present in the entry.

Note the following behaviors and limitations:

- Deleting a source file from the file list also removes all associated SHA-256 hashes from the list.
- You cannot upload multiple files to a file list if the upload would result in more than 10,000 distinct SHA-256 values in the list.
- The system truncates descriptions exceeding 256 characters to the first 256 characters when uploading. If the description contains commas, you must use an escape character (`\,`). If no description is provided, the source file name is used instead.
- All non-duplicate SHA-256 values are added to the file list. If a SHA-256 value already exists, it is not modified by subsequent uploads. Any threat name or description is derived from the individual SHA-256 value in related events.
- Invalid SHA-256 values in a source file are not uploaded.
- If multiple uploaded source files contain entries for the same SHA-256 value, the system uses the most recent value.
- If a source file contains multiple entries for the same SHA-256 value, the system uses the last entry.
- You cannot edit a source file directly within the object manager. To make changes, edit your local source file, delete the existing file from the system, then upload the revised file.
- The number of entries associated with a source file refers to the number of distinct SHA-256 values. Deleting a source file decreases the file list's SHA-256 entries by the number of valid entries in the deleted file.

Add individual SHA-256 values to file lists

Add unique SHA-256 values to file lists to enhance file detection and management within the system.

You must have the Malware Defense license for this procedure.

Adding SHA-256 values identifies files for detection and prevents duplicates by ensuring only unique values are included.

Before you begin

- Right-click a file or malware event from the event view, choose **Show Full Text** in the context menu, and copy the full SHA-256 value for pasting into the file list.

Follow these steps to add individual SHA-256 values to file lists:

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **File List** from the list of object types.

Step 3 Click **Edit** ( ) next to the clean list or custom detection list where you want to add a file.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 Choose `Enter SHA Value` from the **Add by** drop-down list.

Step 5 Enter a description of the source file in the **Description** field.

Step 6 Enter or paste the file's entire value in the **SHA-256** field. The system does not support matching partial values.

Step 7 Click **Add**.

Step 8 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Note After configuration changes are deployed, the system no longer queries the AMP cloud for files on the list.

Upload an individual file to a file list

You must have the Malware Defense license for this procedure.

If you have a copy of the file you want to add to a file list, you can upload the file to the Secure Firewall Management Center for analysis. The system automatically calculates the file's SHA-256 value on upload. No file size limit applies for SHA-256 calculation.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **File List** from the list of object types.

Step 3 Click **Edit** ( ) next to the clean list or custom detection list where you want to add a file.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 From the **Add by** drop-down list, choose **Calculate SHA**.

Step 5 (Optional) Enter a description of the file in the **Description** field. If you leave this field blank, the file name becomes the description during upload.

Step 6 Click **Browse**, and choose a file to upload.

Step 7 Click **Calculate and Add SHA** to upload the file and calculate the SHA-256 value.

Step 8 Click **Save**.

After completing these steps, the file is uploaded, its SHA-256 value is calculated, and the file is added to the selected file list for analysis.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Note After you deploy configuration changes, the system no longer queries the AMP cloud for files on the list.

Upload source files to file lists

This task enables you to upload source files to file lists, allowing for efficient management and use of file data within the system.

You must have the Malware Defense license for this procedure.

Use this task when you need to add values from a source file to an existing file list in the system.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Click **File List**.

Step 3 Click **Edit** ( ) next to the file list where you want to add values from a source file.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 In the **Add by** drop-down list, choose `List of SHAs`.

Step 5 (Optional) Enter a description of the source file in the **Description** field. If you do not enter a description, the system uses the file name.

Step 6 Click **Browse** to browse to the source file, then click **Upload and Add List**.

Step 7 Click **Save**.

After you complete these steps, the system uploads the source file and adds its values to the selected file list.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Note After you deploy the policies, the system stops querying the AMP cloud for files on the list.

Edit SHA-256 values in file lists

You must have the Malware Defense license for this procedure.

You can edit or delete individual SHA-256 values on a file list. However, you cannot directly edit a source file within the object manager. To make changes, first modify your source file, delete the copy on the system, and then upload the modified file.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Click **File List**.

Step 3 Click **Edit** ( ) next to the clean list or custom detection list where you want to modify a file.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 You can:

- Click **Edit** ( ) next to the SHA-256 value you want to change, and modify the **SHA-256** or **Description** values as desired.
- Click **Delete** ( ) next to the SHA-256 value you want to delete.

Step 5 Click **Save** to update the file entry in the list.

Step 6 Click **Save** to save the file list.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Note After configuration changes are deployed, the system no longer queries the AMP cloud for files on the list.

Download source files from a file list

This task allows you to download source files from file lists, enabling you to obtain files for analysis or operational needs.

You must have the Malware Defense license for this procedure.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **File List** from the list of object types.

Step 3 Click **Edit** ( ) next to the clean list or custom detection list where you want to download a source file.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 Next to the source file you want to download, click **View** ( ).

Step 5 Click **Download SHA List** and follow the prompts to save the source file.

Step 6 Click **Close**.

FlexConfig objects

A FlexConfig object is a configuration element that

- provides customized configuration of features on Firewall Threat Defense devices
- enables configuration of features not otherwise available through Secure Firewall Management Center, and
- uses policy objects in FlexConfig policies to customize device behavior.

FlexConfig object types

You can configure these types of objects for FlexConfig.

- **Text objects** define free-form text strings used as variables in a FlexConfig object. These objects can have a single value or multiple values. Several predefined text objects are included in FlexConfig objects. To customize device behavior, edit the contents of the text object when using a FlexConfig object. When editing a predefined object, create device overrides for each device instead of changing the default values. This helps prevent configuration issues for other users who use the same FlexConfig object. For information on configuring text objects, see Configure FlexConfig text objects, on page 950.
- **FlexConfig objects** include device configuration commands, variables, and scripting language instructions. During deployment, the system processes these instructions to create configuration commands with customized parameters for the target devices. You can add instructions at the beginning (prepended) of the configuration or at the end (appended), based on your requirements. Append any FlexConfig that depends on Secure Firewall Management Center-configured objects (for example, a network object) to the configuration deployment. This ensures the necessary objects are configured before the FlexConfig refers to them. For more information on configuring FlexConfig objects, see Configure FlexConfig objects, on page 945.

Geolocation objects

A geolocation object is a network policy element that

- represents one or more countries or continents identified as the source or destination of traffic on your monitored network,

- can be used in various places in the system's web interface, including access control policies, SSL policies, remote access VPN, and event searches, and
- enables you to write access control rules that block traffic to or from certain countries.

Geolocation database updates

To ensure that you are using up-to-date information to filter your network traffic, we strongly recommend that you regularly update your Geolocation Database (GeoDB).

Create a geolocation object

Create a geolocation object to define groups of countries and continents for use in security policies.

Use geolocation objects in access control and policy rules to manage network traffic based on geographic criteria.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **Geolocation** from the list of object types.

Step 3 Click **Add Geolocation**.

Step 4 Enter a **Name**.

Step 5 Select the countries and/or continents to include.

- Selecting a continent includes all countries within that continent, including future additions via GeoDB updates.
- You can select any combination of countries and continents.

Step 6 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Interfaces

An interface is a network connection point that

- can be assigned to a *security zone*, an *interface group*, or both,
- enables application of security policies based on zones or groups, and
- supports flexible traffic control between different network segments.

Security zone and interface group assignments

Each interface can be assigned to a *security zone*, an *interface group*, or both. Apply your security policy based on zones or groups. For example, assign the "inside" interface to the "inside" zone and the "outside" interface to the "outside" zone. Configure the access control policy to allow traffic from inside to outside and block traffic from outside to inside. Some policies support only security zones. Other policies support both zones and groups.

For more information about interface objects, see Security zones and interface groups, on page 607.

To add interface objects, see Create security zone and interface group objects, on page 610.

Key chains

Key chains help you rotate authentication keys for IGP peers to enhance data security, prevent unauthorized users from guessing routing protocol authentication keys, and maintain uninterrupted, secure communication by allowing overlapping key lifetimes.

Key chain authentication and key management

Use rotating keys in key chains, with a duration of 180 days or less, to protect your devices and data. Rotating keys apply only to the OSPFv2 protocol.



Note Only the MD5 cryptographic algorithm is used for authentication.

Each key in a key chain has two lifetimes:

- Accept lifetime: The time interval within which the device accepts the key during key exchange with another device.
- Send lifetime: The time interval within which the device sends the key during key exchange with another device.

During a key's send lifetime, the device sends routing update packets using that key. If the key is not within the accept lifetime, the device does not accept communication from other devices.

If lifetimes are not configured, the system treats the configuration as using an MD5 authentication key without defined timelines.

When configuring authentication for routing protocols that provide key chains, configure the keys in your key chain with overlapping lifetimes to prevent losing secure communication if no active key is available.

Key selection in a key chain is determined as follows:

- When a key chain has more than one valid key, OSPF selects the key with the longest lifetime.
- The system prefers a key with an infinite lifetime.
- If keys have the same lifetime, then key with the higher key ID is preferred.

Create a key chain object

Create key chain objects that securely manage and organize authentication keys for devices on your network.

Use this task when you need to define and manage key chains for secure authentication. Key chains enable secure key exchange, helping prevent unauthorized access and ensuring reliable communication between devices.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **Key Chain** from the list of object types, and then click **Add Key Chain**.

Step 3 In the Add Key Chain Object dialog box, do the following:

a. Enter a name for the key chain in the **Name** field.

The name must start with an underscore or letter, followed by alphanumeric characters or one of the following special characters: hyphen, underscore, plus sign, or period.

b. Add a key to the key chain, click **Add**.

c. Specify the key identifier (between 0 and 255; use 0 only to signal an invalid key) in the **Key ID** field.

d. The **Algorithm** field and the **Crypto Encryption Type** field displays the supported algorithm and the encryption type, namely MD5 and Plain Text.

e. Enter the password in the **Crypto Key String** field and confirm it in the appropriate field. Passwords can be up to 80 characters and must not be a single digit or start with a digit followed by a space (e.g., "0 pass" or "1" are invalid).

f. Set the **Accept Lifetime** and **Send Lifetime** values to define the time intervals for key exchange. The times default to UTC. When specifying start and end lifetimes, ensure that the start is earlier than the end and is never left blank if the end is entered.

g. Click **Add** to create keys. Create at least two keys with overlapping lifetimes to prevent loss of secure communication.

Repeat steps 3b to 3g to create keys.

Step 4 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.
- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 5 Click **Save**.

After you save, you can use the key chain object in device authentication and secure communication configurations.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Networks

A network object is a network entity that

- represents one or more IP addresses,
- can be used in access control policies, network variables, identity rules, network discovery rules, event searches, and reports, and
- is filtered automatically to show only valid objects for each configuration option.

Network object types

You can define a network object as one of these types:

- **Host**: A single IP address.

  IPv4 example:

  `209.165.200.225`

  IPv6 example:

  `2001:DB8::0DB8:800:200C:417A` or `2001:DB8:0:0:0DB8:800:200C:417A`

- **Range**: A range of IP addresses.

  IPv4 example:

  `209.165.200.225-209.165.200.250`

  IPv6 example:

  `2001:db8:0:cd30::1-2001:db8:0:cd30::1000`

- **Network**: An address block, also known as a subnet.

  IPv4 example:

  `209.165.200.224/27`

  IPv6 example:

  `2001:DB8:0:CD30::/60`

Note Security Intelligence ignores IP address blocks using a `/0` netmask.

- **FQDN**: A single fully-qualified domain name (FQDN). You can limit FQDN resolution to IPv4 address only, IPv6 address only, or both types. FQDNs must begin and end with a digit or letter. They can contain only letters, digits, and hyphens internally.

Example:

```
www.example.com
```

Note You can use FQDN objects in access control rules and prefilter rules, or manual NAT rules, only. The rules match the IP address obtained for the FQDN through a DNS lookup. To use an FQDN network object, ensure you have configured the DNS server settings in DNS server groups, on page 2366 and the DNS platform settings in Configure DNS server settings, on page 852.

You *cannot* use FDQN network objects in identity rules.

- **Group**: A group of network objects or other network object groups. You can create nested groups by adding a network object group to another. Nesting is supported up to 10 levels.

Note You can add up to 100 network literals in a network object. Each nested network object group contains up to 100 network literals.

Network wildcard masks

A network wildcard mask is an IP address mask that

- uses a discontinuous mask of bits to define network objects,
- enables you to create network objects with expanded subnet IP addresses, and
- appears as **Network Wildcard** in the **Type** column of the network object list.

Network wildcard mask usage and support

You can create and manage wildcard mask objects from the Network Wildcard Mask page in **Objects** > **Object Management** .

Standard network objects use contiguous masks, while wildcard network objects use discontinuous masks.

This table shows examples of IP addresses and indicates whether they are considered network wildcard objects:

Table 154: Network wildcard mask examples

Example IP address	Network wildcard?	Object type
192.0.0.0/8	No	Network
10.10.0.0/255.255.0.0	No	Network
10.10.0.10/255.255.0.255	Yes	Network Wildcard
72.0.240.10/255.255.240.255	Yes	Network Wildcard

Note Network wildcard objects and groups containing network wildcard objects are allowed only when configuring these policies:

- Prefilter policy
- Access control policy
- NAT policy

Guidelines and limitations

- To create network wildcard objects, in the Firewall Management Center UI, choose **Objects** > **Object Management** > **Network** and click **Add Network** and then **Add Object**. Select the **Network** option and enter the value as expanded subnet mask fotmat, such as 10.0.10.10 or 255.255.0.255.
- Features supported: Object override, group object support, group object override, wildcard literals, and wildcard object import.
- Network wildcard objects are supported only for IPv4 addresses.
- Network wildcard objects are supported from Firewall Management Center and Firewall Threat Defense versions 7.1 onwards.
- Network wildcard objects are supported only for Snort-3.

Create a network object

Create network objects to define network addresses, address ranges, or groups that can be used in security policies and access rules.

Network objects allow you to efficiently manage and reuse network definitions across your security policies. This task is relevant when you need to add, clone, or modify network objects in your management center.

Procedure

Step 1 Choose **Objects** > **Object Management**, and then Choose **Network** from the list of object types.

Step 2 Choose **Add Object** from the **Add Network** drop-down menu.

Step 3 Alternatively, you can clone an existing network object and edit the parameters to create a new network object. Click the **Clone** icon on the existing network object that you want to clone.

Step 4 Enter a **Name** and optionally, enter a **Description**.

Step 5 In the **Network** field, select the required option and enter an appropriate value; see Networks, on page 2386.

Note You can add up to 100 network literals in a network object. Additionally, each nested network object group can contain a maximum of 100 network literals.

Step 6 (FQDN objects only) Select the DNS resolution from the **Lookup** drop-down menu to determine whether you want the IPv4, IPv6, or both IPv4 and IPv6 addresses associated with the FQDN.

Step 7 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.
- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 8 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Import network objects

For details on importing network objects, see Import objects, on page 2334.

PKI objects

PKI objects are public key certificates and paired private keys that

- represent the security components required to support your deployment
- consist of certificate authority certificates for internal and trusted CA objects
- consist of server certificates for internal and external certificate objects, and
- contain private keys paired with certificates for internal objects.

PKI object usage for applications and SSL rules

PKI objects support various security configurations across your network deployment.

You can use PKI objects for these applications:

- ISE/ISE-PIC identity source: Use trusted certificate authority objects and internal certificate objects to configure a connection to ISE/ISE-PIC as an identity source.
- Captive portal authentication: Use internal certificate objects to authenticate the identity of your captive portal device when connecting to users' web browsers.
- Secure LDAP or AD connections: Use trusted certificate authority objects to configure realms for secure connections to LDAP or AD servers.

If you use PKI objects in SSL rules, you can match traffic encrypted with:

- the certificate in an external certificate object
- a certificate either signed by the CA in a trusted CA object, or within the CA's chain of trust

If you use PKI objects in SSL rules, you can decrypt:

- outgoing traffic by re-signing the server certificate with an internal CA object
- incoming traffic using the known private key in an internal certificate object

You can manually input certificate and key information, upload a file containing that information, or in some cases, generate a new CA certificate and private key.

When you view a list of PKI objects in the object manager, the system displays the certificate's Subject distinguished name as the object value. Hover your pointer over the value to view the full certificate Subject distinguished name. To view other certificate details, edit the PKI object.



Note The Firewall Management Center and managed devices encrypt all private keys stored in internal CA objects and internal certificate objects with a randomly generated key before saving them. If you upload private keys that are password protected, the appliance decrypts the key using the user-supplied password, then reencrypts it with the randomly generated key before saving it.

PKI objects for certificate enrollment

A certificate enrollment object is a PKI configuration item that

- contains the Certification Authority (CA) server information and enrollment parameters required for creating Certificate Signing Requests (CSRs)
- obtains identity certificates from the specified CA, and
- may include certificate revocation information.

Internal certificate authority objects

An internal certificate authority object is a security certificate object that

- represents the CA public key certificate of a CA your organization controls
- consists of the object name, CA certificate, and paired private key, and
- can be used in SSL rules to decrypt outgoing encrypted traffic by re-signing the server certificate with the internal CA.

Internal certificate authority object usage and management

You can create an internal certificate authority object in these ways:

- import an existing RSA-based or elliptic curve-based CA certificate and private key
- generate a new self-signed RSA-based CA certificate and private key
- generate an unsigned RSA-based CA certificate and private key. You must submit a certificate signing request (CSR) to another CA to sign the certificate before using the internal CA object.

Note If you reference an internal CA object in a **Decrypt - Resign** SSL rule and the rule matches an encrypted session, the user's browser may warn that the certificate is not trusted while negotiating the SSL handshake. To avoid this, add the internal CA object certificate to either the client or domain list of trusted root certificates.

After you create an internal CA object containing a signed certificate, you can download the CA certificate and private key. The system encrypts downloaded certificates and private keys with a user-provided password.

Whether system-generated or user-created, you can modify the internal CA object name, but cannot modify other object properties.

You cannot delete an internal CA object that is in use. Additionally, after you edit an internal CA object used in an SSL policy, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

CA certificates and private key import

A CA certificate and private key import is a security configuration process that

- enables uploading of X.509 v3 CA certificates and private keys,
- supports files encoded in DER or PEM formats, and
- validates that the certificate and key are properly paired before saving the object.

Supported file formats and import details

You can configure an internal CA object by importing an X.509 v3 CA certificate and private key. You can upload files encoded in one of these supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the private key file is password-protected, you can supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

The system only allows you to upload files that contain proper certificate or key information. It also ensures the certificate and key are paired with each other. The system validates the pair before saving the object.

Note If you configure a rule with the **Decrypt - Resign** action, the rule matches traffic based on the referenced internal CA certificate's encryption algorithm type, in addition to any configured rule conditions. You must upload an elliptic curve-based CA certificate to decrypt outgoing traffic encrypted with an elliptic curve-based algorithm, for example.

Import a CA certificate and private key

Use this task when you need to add a new internal CA to your Secure Firewall Management Center for certificate management.

Administrators typically perform this task during initial setup or when updating trusted certificate authorities. It is relevant for those managing PKI infrastructure within Secure Firewall Management Center.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal CAs**.

Step 3 Click **Import CA**.

Step 4 Enter a **Name**.

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 Above the **Key** field, click **Browse** to upload a DER or PEM-encoded paired private key file.

Step 7 If the uploaded file is password-protected, check the **Encrypted, and the password is:** check box, and enter the password.

Step 8 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Generate a new CA certificate and private key

Generate a self-signed RSA-based CA certificate and accompanying private key by configuring an internal CA object.

Use this task to establish a trusted CA for your environment. The CA certificate enables secure signing and validation of other certificates and will be valid for ten years, with the **Valid From** date starting one week before creation.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal CAs**.

Step 3 Click **Generate CA**.

Step 4 Enter a **Name**.

Step 5 Enter your identification attributes.

Step 6 Click **Generate self-signed CA**.

Signed certificates

A signed certificate is a digital security credential that

- is obtained from a certificate authority (CA)
- enables configuration of an internal CA object, and
- allows referencing the internal CA object in an SSL rule if it contains a signed certificate.

Certificate configuration steps

You can configure an internal CA object by obtaining a signed certificate from a CA. This process consists of these actions:

- Provide identification information to configure the internal CA object. This action generates an unsigned certificate, produces a paired private key, and creates a certificate signing request (CSR) to a specified CA.
- Upload the signed certificate issued by the CA to the internal CA object. The internal CA object now contains a signed certificate instead of the unsigned certificate.

Only reference an internal CA object in an SSL rule if it contains a signed certificate.

Create an unsigned CA certificate and CSR

Create an unsigned CA certificate and generate a certificate signing request (CSR) to enable secure certificate management in Secure Firewall Management Center.

Perform this task when you need to generate a new unsigned CA certificate and CSR, typically for setting up internal certificate authorities or renewing certificates for secure communications. Always complete this task before uploading a signed certificate issued by a certificate authority.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal CAs**.

Step 3 Click **Generate CA**.

Step 4 Enter a **Name**.

Step 5 Enter the identification attributes.

Step 6 Click **Generate CSR**.

Step 7 Copy the CSR to submit to a CA.

Step 8 Click **OK**.

What to do next

- Upload a signed certificate issued by a CA as described in Upload a signed certificate issued in response to a CSR, on page 2394

Upload a signed certificate issued in response to a CSR

Perform this task after receiving a signed certificate from a certificate authority (CA) in response to a CSR generated by the system. Once uploaded, the certificate is available for referencing in SSL rules.

Before you begin

Obtain the signed certificate file (DER or PEM-encoded X.509 v3 CA certificate) that was issued in response to the CSR.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal CAs**.

Step 3 Click **Edit** (✎) next to the CA object containing the unsigned certificate awaiting the CSR.

Step 4 Click **Install Certificate**.

Step 5 Click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 If the uploaded file is password protected, check the **Encrypted, and the password is:** check box, and enter the password.

Step 7 Click **Save** to upload a signed certificate to the CA object.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

CA certificates and private key downloads

A CA certificate and private key download is a security operation that

- enables you to back up or transfer a CA certificate and its paired private key by downloading a file from an internal CA object,
- requires the system to decrypt the private key before creating the downloadable file, and
- uses a password provided by the user to encrypt the downloaded file for secure storage.

Encryption and storage of downloaded CA certificates and private keys

When you download a CA certificate and its private key, the system decrypts the private key before generating the file. Provide a password to encrypt the downloaded file. This helps keep it safe during storage and transfer. The system also encrypts the private key in the CA object with a randomly generated key before saving it to disk.



Caution Store downloaded key information in a secure location.

Caution If you download private keys as part of a system backup, they are decrypted and stored in the unencrypted backup file.

Download a CA certificate and private key

Obtain a CA certificate and private key required for certificate backup, migration, or integration within your secure firewall environment.

You can download CA certificates for both the current domain and ancestor domains. Use this task when you need to obtain the CA certificate and private key for backup, migration, or integration purposes.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal CAs**.

Step 3 Select the internal CA object whose certificate and private key you want to download. Click **Edit** ( ).

Step 4 Click **Download**.

Step 5 Enter an encryption password in the **Password** and **Confirm Password** fields.

Step 6 Click **OK**.

Trusted certificate authority objects

A trusted certificate authority object is a security configuration item that

- represents a CA public key certificate belonging to a trusted CA,
- consists of the object name and CA public key certificate, and
- can be used in SSL policy, realm configurations, and integration with ISE or ISE-PIC.

Usage scenarios for trusted certificate authority objects

You can use trusted certificate authority objects and groups in the following configurations:

- SSL policy: Control traffic encrypted with a certificate signed either by the trusted CA, or any CA within the chain of trust.
- Realm configurations: Establish secure connections to LDAP or Active Directory (AD) servers.
- ISE or ISE-PIC connection: Select trusted certificate authority objects for the pxGrid Server CA and MNT Server CA fields.

After you create the trusted CA object, you can modify the name and add certificate revocation lists (CRL), but cannot modify other object properties. There is no limit on the number of CRLs you can add to an object. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

Note Adding a CRL to an object has no effect when the object is used in your ISE or ISE-PIC integration configuration.

You cannot delete a trusted CA object that is in use. Additionally, after you edit a trusted CA object that is in use, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

Trusted CA objects

A trusted CA object is a security object that:

- enables configuration of an external CA object by uploading an X.509 v3 CA certificate
- supports uploading files encoded in DER or PEM formats, and
- requires the system to validate the certificate before saving the object.

You can upload a file encoded in one of these supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the file is password-protected, you must supply the decryption password. If the certificate is encoded in the PEM format, you can also copy and paste the certificate information.

You can upload a CA certificate only if the file contains proper certificate information; the system validates the certificate before saving the object.

Add a trusted CA object

Add a trusted CA object so the system can validate certificates issued by a Certificate Authority (CA).

Use this task when you need to import a new trusted CA certificate into the system, such as when enabling secure communications or integrating with external certificate authorities.

Before you begin

- Have the DER or PEM-encoded X.509 v3 CA certificate file available.
- If the file is password-protected, ensure you have the password ready.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Trusted CAs**.

Step 3 Click **Add Trusted CAs**.

Step 4 Enter a **Name**.

Step 5 Click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 If the file is password-protected, check the **Encrypted, and the password is:** check box, and enter the password.

Step 7 Click **Save**.

The trusted CA object is added and available for use in certificate validation processes.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Certificate revocation lists in trusted CA objects

A certificate revocation list is a security file that

- can be uploaded to a trusted CA object
- enables control of encrypted traffic based on whether the issuing CA has revoked a certificate, and
- supports files encoded in Distinguished Encoding Rules (DER) or Privacy-enhanced Electronic Mail (PEM) formats.

Certificate revocation list usage in trusted CA objects

You can upload CRLs to a trusted CA object. If you reference that trusted CA object in an SSL policy, you can control encrypted traffic based on whether the CA that issued the session encryption certificate subsequently revoked the certificate.

Supported file formats for CRLs include:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

After you add the CRL, you can view the list of revoked certificates. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

You can upload only files that contain a proper CRL. There is no limit to the number of CRLs you can add to a trusted CA object. However, you must save the object each time you upload a CRL, before adding another CRL.



Note Adding a CRL to an object has no effect when the object is used in your ISE/ISE-PIC integration configuration.

Add a certificate revocation list to a trusted CA object

Add a certificate revocation list (CRL) to a trusted certificate authority (CA) object. This step ensures that revoked certificates are recognized during certificate validation.

Add a CRL to a trusted CA object to ensure that Secure Firewall Management Center validates client certificates against a list of revoked certificates.

Note Adding a CRL to an object has no effect when the object is used in your ISE/ISE-PIC integration configuration.

Before you begin

Ensure you have a DER or PEM-encoded CRL file available for upload.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Trusted CAs**.

Step 3 Click **Edit** ( ) next to a trusted CA object.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Click **Add CRL** and upload your DER or PEM-encoded CRL file.

Step 5 Click **OK** to save the changes.

The certificate revocation list is added to the trusted CA object, updating it with the new CRL information.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

External certificate objects

An external certificate object is a certificate management item that

- represents a server public key certificate that does not belong to your organization,
- consists of the object name and certificate, and
- can be used in SSL rules to control traffic that is encrypted with the server certificate. For example, you can upload a self-signed server certificate that you trust, but cannot verify by using a trusted CA certificate.

Supported certificate formats

You can configure an external certificate object by uploading an X.509 v3 server certificate. The supported file formats include:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

The system validates the file before saving the object, ensuring your certificate is correctly processed. If the certificate is encoded in the PEM format, you can also copy and paste the information.

Add external certificate objects

Add external certificate objects to facilitate secure certificate management and integration with external systems.

Use this task when you need to import and manage external X.509 v3 server certificates in Secure Firewall Management Center for PKI integration.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **External Certs**.

Step 3 Click **Add External Cert**.

Step 4 Enter a **Name**.

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 server certificate file.

Step 6 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Internal certificate objects

An internal certificate object is a server public key certificate representation that

- belongs to your organization and consists of the object name, public key certificate, and paired private key
- supports SSL rule traffic decryption using the known private key, and
- enables authentication for ISE connections and captive portal configurations.

Internal certificate object usage and configuration

You can use internal certificate objects and groups in:

- your SSL rules to decrypt traffic incoming to one of your organization's servers using the known private key.
- your ISE/ISE-PIC connection. Select an internal certificate object for the **MC Server Certificate** field.
- your captive portal configuration to authenticate the identity of your captive portal device when connecting to users' web browsers. Select an internal certificate object for the **Server Certificate** field.

You can configure an internal certificate object by uploading an X.509 v3 RSA-based or elliptic curve-based server certificate and paired private key. You can upload a file in one of these supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the file is password-protected, you must supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

You can upload only files that contain proper certificate or key information, and that are paired with each other. The system validates the pair before saving the object.

After you create the internal certificate object, you can modify the name, but cannot modify other object properties.

You cannot delete an internal certificate object that is in use. Additionally, after you edit an internal certificate object that is in use, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

Add internal certificate objects

Add and manage internal certificate objects for secure handling of server certificates and associated private keys within the system.

Use this task when you need to upload and manage DER or PEM-encoded X.509 v3 server certificates and their corresponding private keys for internal use. This is typically required for secure communication and authentication within your environment.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **PKI** node, and choose **Internal Certs**.

Step 3 Click **Add Internal Cert**.

Step 4 Enter a **Name**.

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 server certificate file.

Step 6 Above the **Key** field, or click **Browse** to upload a DER or PEM-encoded paired private key file.

Step 7 If the uploaded private key file is password-protected, check the **Encrypted, and the password is:** check box, and enter the password.

Step 8 Click **Save**.

Certificate enrollment objects

A certificate enrollment object is a PKI configuration item that

- contains the Certification Authority (CA) server information and enrollment parameters required for creating Certificate Signing Requests (CSRs)
- obtains identity certificates from the specified CA, and
- may include certificate revocation information.

Certificate enrollment object reference information

Trustpoints let you manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one, enrolled identity certificate.

This section describes how to use and manage certificate enrollment objects in your PKI infrastructure.

- Certificate enrollment objects are used to enroll managed devices into your PKI infrastructure and create trustpoints (CA objects) on devices that support VPN connections.
- To manage certificate enrollment objects, go to **Objects** > **Object Management** > **PKI** > **Certificate Enrollment**. The following information is shown:
  - Existing certificate enrollment objects are listed in the **Name** column. Use the search field (the magnifying glass) to filter the list.
  - The enrollment type of each object is shown in the **Type** column. These enrollment methods can be used:
    - **Self Signed**—The managed device generates its own self signed root certificate.
    - **EST**—Enrollment over Secure Transport is used by the device to obtain an identity certificate from the CA.
    - **SCEP**—(Default) Simple Certificate Enrollment Protocol (SCEP) is used by the device to obtain an identity certificate from the CA.
    - **Manual**—The process of enrolling is carried out manually by the administrator.
    - **PKCS12 File**—Import a PKCS12 file on a Threat Defense managed device that supports VPN connectivity. A PKCS#12, or PFX or P12 file holds the server certificate, any intermediate certificates, and the private key in one encrypted file. Enter the **Passphrase** value for decryption.
  - The **Override** column indicates whether the object allows overrides (a green check mark) or not (a red X). If a number is displayed, it is the number of overrides in place. Use the Override option to customize the object settings for each device that is part of the VPN configuration. Overriding makes each device's trustpoint details unique. Typically the Common Name or Subject is overridden for each device in the VPN configuration. See Object overrides, on page 2342 for details and procedures on overriding objects of any type.
  - **Edit** a previously created certificate enrollment object by clicking on the edit icon (a pencil). Editing can only be done if the enrollment object is not associated with any managed devices. Refer to the adding instructions for editing a certificate enrollment object. Failed enrollment objects can be edited.
  - **Delete** a previously created certificate enrollment object by clicking on the delete icon (a trash can). You cannot delete a certificate enrollment object if it is associated with any managed device.

1. Define parameters for CA authentication and enrollment in a certificate enrollment object. Specify shared parameters and use the override facility to specify unique object settings for different devices.
2. Associate and install this object on each managed device that requires the identity certificate. On the device, it becomes a trustpoint.

   When a certificate enrollment object is associated with and then installed on a device, the process of certificate enrollment starts immediately. The process is automatic for self-signed, SCEP, EST, and

PKCS12 file enrollment types, meaning it does not require any additional administrator action. Manual certificate enrollment requires extra administrator action.

3. Specify the created trustpoint in your VPN configuration.

Press ( )**Add Cert Enrollment** to open the **Add Cert Enrollment** dialog and configure a certificate enrollment object, see Add certificate enrollment objects, on page 2402. Then install the certificate on each managed, headend device.

For more information on PKI, digital certificates, and certificate enrollment see PKI infrastructure and digital certificates, on page 1337.

Add certificate enrollment objects

Add certificate enrollment objects to manage device trustpoints and enable secure certificate enrollment for Firewall Threat Defense devices.

- Support multiple enrollment protocols, including SCEP, EST, Manual, and PKCS12 file import.

Use these objects to enable secure certificate management and device trustpoint enrollment. You must have Admin or Network Admin privileges to do this task.

Procedure

Step 1 Open the **Add Certificate Enrollment** dialog:

- Directly from Object Management: In the **Objects** > **Object Management** > **PKI** > **Certificate Enrollment** from the navigation pane, and click **Add Certificate Enrollment**.
- While configuring a managed device: In the **Devices** > **Certificates** screen, choose **Add** > **Add New Certificate** and click ( ) for the **Certificate Enrollment** field.

Step 2 Enter the **Name**. When enrollment is complete, this name is used as the trustpoint name on the managed devices with which it is associated. Click the **CA Information** tab, and then choose the **Enrollment Type**.

- **Self-Signed Certificate**—The managed device, acting as a CA, generates its own self-signed root certificate. No other information is needed in this pane.

Note When enrolling a self-signed certificate you must specify the Common Name (CN) in the certificate parameters.

- **EST**—Enrollment over Secure Transport protocol. Specify the EST information. See EST enrollment configuration options in Certificate Enrollment Object , on page 2404.
- **SCEP**—(Default) Simple Certificate Enrollment Protocol. Specify the SCEP information. See Certificate Enrollment Object SCEP options , on page 2405.
- **Manual**
  - **CA Only**—Check this check box to create only the CA certificate from the selected CA. An identity certificate will not be created for this certificate.

    If you do not select this check box, a CA certificate is not mandatory. You can generate the CSR without having a CA certificate and obtain the identity certificate.

- **CA Certificate**—Paste the CA certificate in the PEM format in the box. You can also obtain a CA certificate by copying it from another device.

  You can leave this box empty if you choose to generate a CSR without the CA certificate.

- **PKCS12 File**—Import a PKCS12 file on a Firewall Threat Defense managed device that supports VPN connectivity. A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file. Enter the **Passphrase** value for decryption.

Step 3 **Skip Check for CA flag in basic constraints of the CA Certificate**—Check this check box if you want to skip checking the basic constraints extension and the CA flag in a trustpoint certificate.

Step 4 **Validation Usage**—Choose from the options to validate the certificate during a VPN connection:

- **IPsec Client**—Validate an IPsec client certificate for a site-to-site VPN connection.
- **SSL Client**—Validate an SSL client certificate during a remote access VPN connection attempt.
- **SSL Server**—Select to validate an SSL server certificate, such as a Cisco Umbrella server certificate.

Step 5 (Optional) Click the **Certificate Parameters** tab and specify the certificate contents. Refer to Certificate Enrollment Object certificate parameters in certificate requests , on page 2406.

This information is placed in the certificate and is readable by any party who receives the certificate from the router.

Step 6 (Optional) Click the **Key** tab and specify the Key information. Refer to Certificate Enrollment Object key options , on page 2407.

Step 7 (Optional) Click the **Revocation** tab and specify the revocation options: Refer to Certificate Enrollment Object revocation options , on page 2408.

Step 8 **Allow Overrides** of this object if desired.

When you allow overrides in the PKCS12 certificate enrollment object, update the**Passphrase** for the certificate on the device where you override it.

See Object overrides, on page 2342 for a full description of object overrides.

Step 9 Click **Save**.

What to do next

Associate and install the enrollment object on a device to create a trustpoint on that device.

Related Topics

Install a certificate using self-signed enrollment, on page 2486
Install a certificate using EST enrollment, on page 2487
Install a certificate using SCEP enrollment, on page 2487
Install a certificate using manual enrollment, on page 2488
Install a certificate using a PKCS12 file, on page 2489

Add a certificate enrollment

A valid IdP certificate ensures that your system can securely authenticate users through an identity provider. This is essential for secure communications and compliance.

Procedure

Step 1 Enter the **Name**.

Step 2 Paste the certificate information in the **IdP Certificate** field in PEM format.

Note If the certificate is dependent on a root or intermediate certificate, you must install the dependent certificates. See Certificates, on page 2481.

Step 3 Click **Save**.

EST enrollment configuration options in Certificate Enrollment Object

This topic describes the EST enrollment options and the required fields for configuring EST certificate enrollment in the Secure Firewall Management Center.

Secure Firewall Management Center navigation path

Objects > **Object Management** > **PKI** > **Certificate Enrollment**. Click **Add Certificate Enrollment** to open the **Add Certificate Enrollment** dialog, and select the **CA Information** tab.

Fields

Enrollment Type—set to **EST**.

Note
- EST enrollment type does not support EdDSA key.
- EST's ability to auto-enroll a device when its certificate expires is not supported.

Enrollment URL—Enter the URL of the CA server to which devices should attempt to enroll.

Use an HTTPS URL in the form of **https://CA_name:port**, where *CA_name* is the host DNS name or IP address of the CA server. The *port* number is mandatory.

Username—The username required to access the CA server.

Password / Confirm Password—The password required to access the CA server.

Fingerprint—Optionally, enter the fingerprint of the CA server certificate. Verifying the fingerprint helps ensure you are connecting to the legitimate CA server and not a substitute. Enter the fingerprint in hexadecimal format. If the fingerprint does not match, the certificate is rejected. Obtain the fingerprint directly from the CA server.

Source Interface—The interface that interacts with the CA server. By default, the diagnostic interface is displayed. To configure a data interface as the source interface, choose the respective security zone or interface group object.

Ignore EST Server Certificate Validations—By default, EST server certificate validation is enabled. Check the check box to ignore Firewall Threat Defense validating EST server certificate.

Certificate Enrollment Object SCEP options

This topic describes the SCEP enrollment options and fields available when adding a certificate enrollment object in Secure Firewall Management Center.

Secure Firewall Management Center navigation path

Objects > **Object Management** > **PKI** > **Certificate Enrollment**. Click **Add Certificate Enrollment** to open the **Add Certificate Enrollment** dialog, and select the **CA Information** tab.

Fields

Enrollment Type—Set to **SCEP**.

Enrollment URL—Enter the URL of the CA server to which devices should attempt to enroll.

Use an HTTP URL in the format **`http://CA_name:port,`** . The CA_name is the DNS name or IP address of the CA server, and the port number is mandatory.



Note If the SCEP Server is referred with hostname/FQDN, configure the DNS Server using FlexConfig object.

If the CA cgi-bin script location at the CA is not the default (/cgi-bin/pkiclient.exe) include the nonstandard script location in the URL, in the form of http://CA_name:port/script_location, where script_location is the full path to the CA scripts.

Challenge Password / Confirm Password—The password used by the CA server to validate the identity of the device. You can obtain the password by contacting the CA server directly or by entering the following address in a web browser: **`http://URLHostName/certsrv/mscep/mscep.dll`**. Because the password is valid for only 60 minutes, deploy it as soon as possible after creation.

Retry Period—The interval (in minutes) between certificate request attempts. Values range from 1 to 60 minutes. The default is 1 minute.

Retry Count—The number of retries that should be made if no certificate is issued on the first request. Value can be 1 to 100. The default is 10.

CA Certificate Source—Specifies how the CA certificate will be obtained.

- **Retrieve Using SCEP** (default and only supported option)—Retrieve the certificate from the CA server using the Simple Certificate Enrollment Process (SCEP). Using SCEP requires a connection between your device and the CA server. Ensure a network route exists between your device and the CA server before beginning enrollment.

Fingerprint—When retrieving the CA certificate using SCEP, you may enter the fingerprint for the CA server. Using the fingerprint to verify the authenticity of the CA server's certificate helps prevent an unauthorized party from substituting a fake certificate in place of the real one. Enter the **Fingerprint** for the CA server in hexadecimal format. If the value you enter does not match the fingerprint on the certificate, the certificate is rejected. Obtain the CA's fingerprint by contacting the server directly, or by opening: **`http://<URLHostName>/certsrv/mscep/mscep.dll`**.

Certificate Enrollment Object certificate parameters in certificate requests

When sending a certificate request to a CA server, you can specify additional information that is placed into the certificate and is viewable by recipients. All information should follow the standard LDAP X.500 format.

Secure Firewall Management Center navigation path

Objects > **Object Management** > **PKI** > **Certificate Enrollment**. Click **Add Certificate Enrollment** to open the **Add Certificate Enrollment** dialog box, and select the **Certificate Parameters** tab.

Fields

Field	Description
Include FQDN	Whether to include the device's fully qualified domain name (FQDN) in the certificate request. You can select from these options: • **Use Device Hostname as FQDN** • **Don't use FQDN in certificate** • **Custom FQDN**—Select this and then specify it in the **Custom FQDN** field that displays.
Include Device's IP Address	Specify the interface whose IP address you want to include in the certificate request.
Common Name (CN)	Specify the X.500 common name to include in the certificate. **Note** When enrolling a self-signed certificate you must specify the Common Name (CN) in the certificate parameters.
Organization Unit (OU)	Specify the name of the organization unit (for example, a department name) to include in the certificate.
Organization (O)	Specify the organization or company name to include in the certificate.
Locality (L)	Specify the state or province to include in the certificate.
State (ST)	The state or province to include in the certificate.
County Code (C)	The country to include in the certificate. These codes conform to ISO 3166 country abbreviations, for example "US" for the United States of America.
Email (E)	Specify the email address to include in the certificate.
Include Device's Serial Number	Specify whether to include the device's serial number in the certificate. The CA uses the serial number to authenticate certificates or to later associate a certificate with a particular device. If you are unsure, include the serial number, because it is useful for debugging purposes.

Certificate Enrollment Object key options

This topic describes the available key options and their settings when adding certificate enrollment and selecting the Key tab in the Certificate Enrollment Object dialog box.

Secure Firewall Management Center navigation path

Objects > **Object Management** > **PKI** > **Certificate Enrollment**, and click **Add Certificate Enrollment** to open the **Add Certificate Enrollment** dialog box, and select the **Key** tab.

Fields

- **Key Type**: Choose RSA, ECDSA, EdDSA.

Note

- EdDSA is not supported for EST enrollment type.
- EdDSA is supported only in Site-to-Site VPN topologies.
- EdDSA is not supported as an identity certificate for Remote Access VPN.

- **Key Name**: Specifies the name of the key pair. If the key pair already exists, this field refers to the existing name. If not, it defines the name for a new key pair to be generated during enrollment. If no name is specified, the fully qualified domain name (FQDN) key pair is used instead.
- **Key Size**: When generating a new key pair, defines the desired key size (modulus) in bits. The recommended size is 2048 bits. Larger modulus sizes offer more security but require more time (a minute or more when larger than 512 bits) to generate and process.

Important

- On Firewall Management Center and Firewall Threat Defense Versions 7.0 and higher, you cannot enroll certificates with RSA key sizes smaller than 2048 bits and keys using SHA-1 with the RSA Encryption algorithm.
- You can use the PKI Enrollment of Certificates with Weak-Crypto to allow certificates with SHA-1 and smaller key size.
- You cannot generate RSA keys with sizes smaller than 2048 bits for Firewall Threat Defense 7.0, even when you enable the weak-crypto option.

- **Advanced Settings**: Select **Ignore IPsec Key Usage** if you do not want to validate values in the key usage and extended key usage extensions of IPsec remote client certificates. You can suppress key usage checking on IPsec client certificates. By default, this option is not enabled.

Note For site-to-site VPN connection, if you use a Windows Certificate Authority (CA), the default Application Policies extension is **IP security IKE intermediate**. If you are using this default setting, you must select the **Ignore IPsec Key Usage** option for the object you select. Otherwise, the endpoints cannot complete the site-to-site VPN connection.

Enroll PKI certificates with weak-crypto

Certificates that use weak cryptography (such as SHA-1 signatures or RSA keys smaller than 2048 bits) have restricted support on Firewall Management Center and Firewall Threat Defense devices. This reference details the conditions under which weak-crypto certificates may be enrolled and the required steps for enabling their use.

SHA-1 hashing signature algorithm, and RSA key sizes that are smaller than 2048 bits for certification are not supported on Firewall Management Center and Firewall Threat Defense Version 7.0 and later. You cannot enroll certificates with RSA key sizes that are smaller than 2048 bits.

To override these restrictions on Firewall Management Center 7.0 managing Firewall Threat Defenses running Versions earlier than 7.0, use the enable weak-crypto option on the Firewall Threat Defense. Do not permit weak-crypto keys, because, such keys are not as secure as the ones with larger key sizes.

Note Firewall Threat Defense 7.0 or later does not support generating RSA keys with sizes smaller than 2048 bits even when you permit weak-crypto.

To enable weak-crypto on the device, navigate to the **Devices** > **Certificates** page. Click the **Enable Weak-Crypto**() button provided against the Firewall Threat Defense device. When the weak-crypto option is enabled, the button changes to . By default, the weak-crypto option is disabled.

Note When a certificate enrollment fails due to weak cipher usage, the Firewall Management Center displays a warning message prompting you to enable the weak-crypto option. Similarly, when you turn on the enable weak-crypto button, the Firewall Management Center displays a warning message before enabling weak-crypto configuration on the device.

Upgrade earlier versions to Firewall Threat Defense 7.0

When you upgrade to Firewall Threat Defense 7.0, the existing certificate configurations are retained. However, if those certificates have RSA keys smaller than 2048 bits and use SHA-1 encryption algorithm, they cannot be used to establish VPN connections. You must either procure a certificate with RSA key size of at least 2048 bits or enable the permit weak-crypto option for VPN connections.

Certificate Enrollment Object revocation options

Specify whether to check the revocation status of a certificate by choosing and configuring the method. Revocation checking is off by default. The system does not check either method (CRL or OCSP).

Secure Firewall Management Center navigation path

Objects > **Object Management** > **PKI** > **Certificate Enrollment**, and click () **Add Cert Enrollment** to open the **Add Cert Enrollment** dialog, and select the **Revocation** tab.

Fields

- **Enable Certificate Revocation Lists**—Check to enable CRL checking.

- **Use CRL distribution point from the certificate**—Check to obtain the revocation lists distribution URL from the certificate.
- **Use static URL configured**—Check this to add a static, predefined distribution URL for revocation lists. Then add the URLs.

  CRL Server URLs—Specify the URL of the LDAP server from which the CRL can be downloaded.

  URLs must start with **`http://`**. Include a port number in the URL. Enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

- **Enable Online Certificate Status Protocol (OCSP)**—Check to enable OCSP checking.

  OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks.

  URLs must start with **`http://`**. Enclose IPv6 addresses in square brackets, for example: *http://[0:0:0:0:0.18:0a01:7c16]*.

- **Consider the certificate valid if revocation information cannot be reached**—Checked by default. Uncheck if you do not want to allow this.

Configure a policy list

Configure a policy list to group and manage multiple match statements for use in route maps. This allows for efficient policy management and flexible routing decisions.

Use the Configure Policy List page to create, copy, and edit policy list objects. You can create policy list objects to use when you are configuring route maps. When a policy list is referenced within a route map, all of the match statements in that policy list are evaluated and processed. With a route map, you can configure two or more policy lists. A policy list can coexist with other match and set statements that are configured in the same route map but outside the policy list. When multiple policy lists perform matching within a route map entry, only the incoming attribute is matched by all policy lists.

You can use this object with Firewall Threat Defense devices.

Procedure

Step 1 Select **Objects** > **Object Management** > **Policy List**.

Step 2 Click **Add Policy List**. Specify these values:

a. Enter a name for the policy list object in the **Name** field. Object names are not case-sensitive.

b. Select whether to allow or block access for matching conditions from the **Action** drop-down list.

Step 3 Enter the details in each of these tabs:

Tabs	Details
Interface	Use this tab to distribute routes that have their next hop out of one of the interfaces specified. In the **Zones/Interfaces** list, add the zones that contain the interfaces through which the device communicates with the management station. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. The host will be configured on a device only if the device includes the selected interfaces or zones.
Address	Use this tab to redistribute any routes that have a destination address that is permitted by a standard access list or prefix list. Choose whether to use an **Access List** or **Prefix List** for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.
Next Hop	Use this tab to redistribute any routes that have a next hop router address passed by one of the access lists or prefix lists specified. Choose whether to use an **Access List** or **Prefix List** for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.
Route Source	Use this tab to redistribute routes that have been advertised by routers and access servers at the address specified by the access lists or prefix list. Choose whether to use an **Access List** or **Prefix List** for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.
AS Path	Use this tab to match a BGP autonomous system path. If you specify more than one AS path, then the route can match either AS path.
Community Rule	Use this tab to enable matching of the BGP community or extended community with the specified community list objects or the extended community list objects respectively. If you specify more than one rule, the routes are verified against the rules until a matching permit or deny is met. **a.** To specify a community list to the rule, click **Edit** ( ) given in the **Selected Community List** field. The community lists appear under **Available Community List**. Select the required list, click **Add**, and then click **Ok**. To enable matching the BGP community exactly with the specified community, check the **Match the specified community exactly** check box. **b.** To add the extended community list, click **Edit** ( ) given in the **Selected Extended Community List** field. The extended community lists appear under the **Available Extended Community List**. Select the required list, click **Add**, and then click **Ok**. **Note** The extended community lists are applicable only for configuring import or export of routes.

Tabs	Details
Metric & tag	Use this tab to match the metric and security group tag of a route. **a.** Enter the metric values to use for matching in the **Metric** field. You can enter multiple values, separated by commas. This setting allows you to match any routes that have a specified metric. The metric values can range from 0 to 4294967295. **b.** Enter the tag values to use for matching in the **Tag** field. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified security group tag. The tag values can range from 0 to 4294967295.

Step 4 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 5 Click **Save**.

Ports

A port object is a network configuration element that

- represents different protocols, such as TCP, UDP, ICMP, and others, in distinct ways
- can specify protocol numbers, port numbers or ranges, and optional type and code for certain protocols, and
- is used to define access and monitoring rules within the system's web interface.

Port object representations and usage

Port objects represent protocols differently depending on their type.

- **TCP and UDP**: Port objects represent these transport layer protocols by specifying the protocol number, and may include an associated port or port range. For example: `TCP(6)/22`.
- **ICMP and ICMPv6 (IPv6-ICMP)**: Port objects represent these Internet layer protocols by specifying the protocol number and optional type and code. For example: `ICMP(1):3:3`.

  Restrict an ICMP or IPV6-ICMP port object by type and, if needed, code. Learn more about ICMP types and codes at:

  - ICMP Types and Codes: http://www.iana.org/assignments/ICMP-parameters/ICMP-parameters.xml
  - ICMPv6 Types and Codes: http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

- **Other protocols**: Port objects can represent protocols that do not use ports.

The system provides default port objects for well-known ports. Default objects are read-only and always available for use. You can create custom port objects or groups in addition to the default ones.

Port objects and groups can be used throughout the system's web interface in access control policies, identity rules, network discovery rules, port variables, and event searches. For example, you can configure a network

discovery policy to exclude monitoring ports used by a custom client if it generates excessive or misleading events.

Guidelines for using port objects

- You cannot add any protocol other than TCP or UDP for source port conditions in access control rules.
- Set source and destination port conditions in a rule using only one transport protocol.
- Add only supported protocols to a port object group used in a source port condition so that the rule takes effect on the managed device when you deploy the configuration.
- To add a destination port, create a port object using only TCP or only UDP ports for the source port condition in a rule. Similarly, to add a source port, create a port object using only TCP or only UDP ports as the destination port condition.

Create port objects

Create port objects to specify protocol and port information for network traffic management in Secure Firewall Management Center.

Use this task to add or modify port objects in access control or other security policies within Secure Firewall Management Center. Port objects allow you to specify which network traffic is allowed or blocked based on protocol and port criteria. They are critical when you set up or update security rules.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **Port** from the object types list.

Step 3 Choose **Add Object** from the **Add Port** drop-down list.

Alternatively, clone an existing port object and edit its parameters to create a new port object. Click the **Clone** icon on the existing port object that you want to clone.

Step 4 Enter a **Name**.

Step 5 Choose a **Protocol**.

Step 6 Depending on the protocol you chose, constrain by **Port**, or choose an ICMP **Type** and **Code**.

You can enter ports from `1` to `65535`. Use a hyphen to specify a port range. You must constrain the object by port if you chose to match **All** protocols, using the **Other** drop-down list.

Step 7 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.
- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 8 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Import port objects

To import port objects, refer to Import objects, on page 2334.

Prefix lists

A prefix list is a route filtering object that

- defines IPv4 and IPv6 address ranges
- is used when configuring route maps, policy maps, OSPF filtering, or BGP neighbor filtering, and
- enables control over which routes are permitted or denied.

Configure an IPv6 prefix list

Use IPv6 prefix lists in Firewall Threat Defense devices to specify which IPv6 routes are allowed or blocked during redistribution. This enhances routing policy control for protocols such as OSPF and BGP.

Procedure

Step 1 Select **Objects** > **Object Management** > **Prefix Lists** > **IPv6 Prefix List** from the table of contents.

Step 2 Click **Add Prefix List**.

a. Enter a name for the prefix list object in the **Name** field

b. Click **Add**.

Step 3 Select the appropriate action, Allow or Block, from the **Action** drop-down list to indicate the redistribution access.

Step 4 Enter a unique number that indicates the position a new prefix list entry will have in the list of prefix list entries already configured for this object, in the **Sequence No.** field. If left blank, the sequence number will default to five more than the largest sequence number currently in use.

Step 5 Specify the IPv6 address in the IP address/mask length format in the **IP address** field. The mask length must be a valid value between 1 and 128.

Step 6 Enter the minimum prefix length in the **Minimum Prefix Length** field and the maximum prefix length in the **Maximum Prefix Length** field.

The minimum prefix length value must be greater than the mask length and less than or equal to the Maximum Prefix Length, if specified.

If the Minimum Prefix Length is present, the maximum prefix length value must be greater than or equal to it. If the Minimum Prefix Length is not specified, the maximum value must be greater than the mask length.

Step 7 Click **Add**.

Step 8 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 9 Click **Save**.

Configure an IPv4 prefix list

Use the Configure IPv4 Prefix list page to manage prefix list objects. These objects can be used when configuring route maps, policy maps, OSPF filtering, or BGP neighbor filtering.

You can use this object with Firewall Threat Defense devices.

Procedure

Step 1 Select **Objects** > **Object Management** > **Prefix Lists** > **IPv4 Prefix List** from the table of contents.

Step 2 Click **Add Prefix List**.

a. Enter a name for the prefix list object in the **Name** field

b. Click **Add**.

Step 3 Select the appropriate action, Allow or Block, from the **Action** drop-down list to indicate the redistribution access.

Step 4 Enter a unique number in the **Sequence No.** field to specify the position of the new prefix list entry. If the field is left blank, the system assigns a sequence number that is five higher than the largest one currently in use.

Step 5 Specify the IPv4 address in the IP address/mask length format in the **IP address** field. The mask length must be a valid value between 1 and 32.

Step 6 Enter the minimum prefix length in the **Minimum Prefix Length** field and the maximum prefix length in the **Maximum Prefix Length** field.

The minimum prefix length value must be greater than the mask length and less than or equal to the Maximum Prefix Length, if specified.

If the Minimum Prefix Length is present, the maximum prefix length value must be greater than or equal to it. If the Minimum Prefix Length is not specified, the maximum value must be greater than the mask length.

Step 7 Click **Add**.

Step 8 If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 9 Click **Save**.

Configure a route map

Route maps are used to manage route redistribution between routing protocols and to control default route generation. Route maps can specify which routes are permitted or denied and apply rules for matching route attributes.

You can use this object with Firewall Threat Defense devices.

Configure a route map to create or edit route map entries in a Route Map object.

Before you begin

A Route Map can use one or more of these objects. It is not mandatory to add all of them. Create and use any of these objects as required to configure your route map.

- Add ACLs.
- Add Prefix Lists.
- Add AS Path.
- Add Community Lists.
- Add Extended Community Lists.

Note The extended community lists apply only to configuring import or export of routes.

- Add Policy Lists.

Procedure

Step 1 Select **Objects** > **Object Management** > **Route Map**.

Step 2 Click **Add Route Map**.

Step 3 Click **Add** on the **New Route Map Object** window.

Step 4 In the **Sequence No.** field, enter a number, from 0 through 65535, that indicates the position a new route map entry has in the list of route maps entries already configured for this route map object.

Note We recommend that you number clauses in intervals of at least 10 to reserve numbering space in case you want to insert clauses in the future.

Step 5 Select Allow or Block from the **Redistribution** drop-down list, to indicate the redistribution access.

Step 6 Click the **Match Clauses** tab to match routes or traffic based on the following criteria, which you select in the table of contents:

- **Security Zones** —Match traffic based on the (ingress/egress) interfaces. You can select zones and add them, or type in interface names and add them.
- **IPv4**— Match IPv4 (routes/traffic) based on the following criteria; select the tab to define the criteria.
  a. Click the **Address** tab to match routes based on the route address. For IPv4 addresses, choose whether to use an Access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.
  b. Click the **Next Hop** tab to match routes based on the next hop address of a route. For IPv4 addresses, choose whether to use an access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.
  c. Click the **Route Source** tab to match routes based on the advertising source address of the route. For IPv4 addresses, choose whether to use an access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.
- **IPv6** —Match IPv6 (routes/traffic) based on the route address, next-hop address or advertising source address of route.
- **BGP**—Match BGP (routes/traffic) based on the following criteria; select the tab to define the criteria.
  a. Click the **AS Path** tab to enable matching the BGP autonomous system path access list with the specified path access list. If you specify more than one path access list, then the route can match either path access list.
  b. Click the **Community List** tab to enable matching of the BGP community or extended community with the specified community list objects or the extended community list objects respectively.
     - To specify a community list to the rule, click **Edit** ( ) given in the **Selected Community List** field. The community lists appears under **Available Community List**. Select the required list, click **Add**, and then click **Ok**. For information on how to create community list objects, see Configure a community list, on page 2360
     - To add the extended community list, click **Edit** ( ) given in the **Selected Extended Community List** field. The extended community lists appears under the **Available Extended Community List**. Select the required list, click **Add**, and then click **Ok**. For information on how to create extended community list objects, see Configure an extended community list, on page 2361.

     To enable matching the BGP community exactly with the specified community list objects, check the **Match the specified community exactly** check box. This option is not applicable for the extended community list.

Note If you specify more than one rule, the routes are verified against the rules until a matching permit or deny condition is met. Any route that does not match at least one Match community will not be advertised for outbound route maps.

  c. Click the **Policy List** tab to configure a route map to evaluate and process a BGP policy. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

- **Others** —Match routes or traffic based on the following criteria.

a. Enter the metric values to use for matching in the **Metric Route Value** field, to enable matching the metric of a route. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified metric. The metric values can range from 0 to 4294967295.

b. Enter the tag values to use for matching in the **Tag Values** field. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified security group tag. The tag values can range from 0 to 4294967295.

c. Check the appropriate **Route Type** option to enable matching of the route type. Valid route types are External1, External2, Internal, Local, NSSA-External1, and NSSA-External2. You can choose more than one route type from the list.

Step 7 Click the **Set Clauses** tab to set routes/traffic based on the following criteria, which you select in the table of contents:

- **Metric Values**—Set either Bandwidth, all of the values or none of the values.

  a. Enter a metric value or bandwidth in Kbits per second in the **Bandwidth** field. Valid values are an integer value in the range from 0 to 4294967295.

  b. Select to specify the type of metric for the destination routing protocol, from the **Metric Type** drop-down list. Valid values are: internal, type-1, or type-2.

- **BGP Clauses** —Set BGP routes based on the following criteria; select the tab to define the criteria.

  a. Click the **AS Path** tab to modify an autonomous system path for BGP routes.

     1. Enter an AS path number in the **Prepend AS Path** field to prepend an arbitrary autonomous system path string to BGP routes. Usually the local AS number is prepended multiple times, increasing the autonomous system path length. If you specify more than one AS path number then the route can prepend either AS number.

     2. Enter an AS path number in the **Prepend Last AS to AS Path** field to prepend the AS path with the last AS number. Enter a value for the AS number from 1 to 10.

     3. Check the **Convert route tag into AS path** check box to convert the tag of a route into an autonomous system path.

  b. Click the **Community List** tab to set the community attributes:

     Under **Specific Community**:

     1. Click the **None** radio button, to remove the community attribute from the prefixes that pass the route map.

     2. Click the **Specific Community** radio button, to enter a community number, if applicable. Valid values are from 1 to 4294967295.

     3. Check the **Add to existing communities** check box, to add the community to the already existing communities.

     4. Select the **Internet**, **No-Advertise**, or **No-Export** check-boxes to use one of the well-known communities.

     Under **Specific Extended Community**, in the **Route Target** field, enter the route target number in *ASN:nn* format:

- You can enter values that ranges from 1:1 to 65534:65535.

  You can add a single route target or a set of route targets separated by commas in a single entry. For example, *1:2,1:4,1:6*.

- You can have a maximum of 8 route targets in an entry.
- You cannot have redundant route target entries across route maps.

c. Click the **Others** tab to set additional attributes.

1. Check the **Set Automatic Tag** check-box to automatically compute the tag value.
2. Enter a preference value for the autonomous system path in the **Set Local Preference** field. Enter a value between 0 and 4294967295.
3. Enter a BGP weight for the routing table in the **Set Weight** field. Enter a value between 0 and 65535.
4. Select to specify the BGP origin code. Valid values are **Local IGP** and **Incomplete**.
5. In the IPv4 Settings section, specify a next hop IPv4 address of the next hop to which packets are output. It need not be an adjacent router. If you specify more than one IPv4 address then the packets can output at either IP address.

   Select to specify an IPv4 prefix list in the **Prefix List** drop-down list.
6. In the IPv6 Settings section, specify a next hop IPv6 address of the next hop to which packets are output. It need not be an adjacent router. If you specify more than one IPv6 address, then the packets can output at any of the IP addresses.

   Select to specify an IPv6 prefix in the **Prefix List** drop-down list.

Step 8 Click **Add**.

If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.

Step 9 Click **Save**.

After completing these steps, the route map is configured and ready for use in route redistribution and policy enforcement. The route map entries and associated match and set clauses are applied AS specified.

What to do next

Review the route map configuration to ensure that all required match and set clauses are correctly defined. Make any necessary adjustments to optimize routing policies.

- Monitor route redistribution and verify that routes are processed according to the configured route map.

Security intelligence

Security Intelligence is a traffic filtering mechanism that

- uses collections of IP addresses, domain names, and URLs to quickly filter traffic that matches entries
- requires the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types), and
- operates through lists and feeds that are grouped into DNS, Network, and URL categories.

Security intelligence components

Security Intelligence *lists* and *feeds* are collections of IP addresses, domain names. You can use these to quickly filter traffic that matches an entry on a list or feed.

- A list is a static collection that you manage manually.
- A feed is a dynamic collection that updates on an interval over HTTP or HTTPS.

Security Intelligence lists/feeds are grouped into:

- DNS (Domain names)
- Network (IP addresses)
- URLs

System-provided feeds:

Cisco provides these feeds as Security Intelligence objects:

- Security Intelligence feeds updated regularly with the latest threat intelligence from Talos:
  - Cisco-DNS-and-URL-Intelligence-Feed (under DNS Lists and Feeds)
  - Cisco-Intelligence-Feed (for IP addresses, under Network Lists and Feeds)

  You cannot delete the system-provided feeds, but you can change the frequency of (or disable) their updates.
- Cisco-TID-Feed (under Network Lists and Feeds)

  This feed is not used in the Security Intelligence tab of the access control policy.

  Instead, you must enable and configure Secure Firewall Threat Intelligence Director to use this feed. The feed is a collection of TID observables data.

  Use this object to configure the frequency of data publication to TID elements.

  For more information, see Threat Intelligence Director, on page 2121.

Predefined global Block and Do Not Block lists:

The system includes predefined global Block lists and Do Not Block lists for domains (DNS), IP addresses (Networks), and URLs.

These lists are empty until you populate them. To build these lists, see Global and domain security intelligence lists, on page 2420.

By default, access control and DNS policies use these lists as part of Security Intelligence.

Custom feeds:

You can use third-party feeds or use a custom internal feed to easily maintain an enterprise-wide Block list in a large deployment with multiple Secure Firewall Management Center appliances.

See Custom security intelligence feeds, on page 2428.

Custom lists:

Custom lists can augment and fine-tune feeds and the global lists.

See Custom Security Intelligence lists, on page 2430.

Security Intelligence lists and feeds usage locations:

- IP address and address blocks—Use Block and Do Not Block lists in access control policies, as part of Security Intelligence.
- Domain Names—Use Block and Do Not Block lists in DNS policies, as part of Security Intelligence.
- URLs—Use Block and Do Not Block lists in access control policies, as part of Security Intelligence. You can also use URL lists in access control and QoS rules, whose analysis and traffic handling phases occur after Security Intelligence.

Modify security intelligence objects

This topic explains how to add or delete entries on a Block list, Do Not Block list, feed, or sinkhole object. It also describes the edit capabilities and redeployment requirements for each object type.

The table summarizes the editing options and redeployment requirements for various security intelligence object types.

Object Type	Edit Capabilities	Requires Redeploy After Edit?
Custom Block and Do Not Block lists	Upload new and replacement lists using the object manager.	No
Default (but custom-populated) Block lists and Do Not Block lists: Global, descendant, and domain-specific	Add entries using the context menu or delete entries using the object manager.	No
System-provided Intelligence Feeds	Disable or change update frequency using the object manager.	No
Custom feeds	Fully modify using the object manager.	No
Sinkhole	Fully modify using the object manager.	Yes

Global and domain security intelligence lists

A security intelligence list helps you manage firewall policies by

- lets you manage lists of connections to block or exempt,

- applies your policies consistently across global and domain contexts, and
- enables further threat evaluation without the need to redeploy firewall policies.

Security intelligence list reference information

The Firewall Management Center includes Global Block and Do Not Block lists, so you can use Security Intelligence to consistently block or exempt connections, allowing evaluation by other threat detection processes you configure.

Access control and DNS policies use these Global lists by default, and they apply to all security zones. If you want, you can turn these lists off for individual policies.

- Global Block list: Lets you block specified connections in all security zones.
- Do-Not-Block list: Lets you exempt specified connections from blocking so you can further evaluate threats.



Note These options apply only to Security Intelligence. Security Intelligence does not block traffic already fastpathed. Adding an item to a Security Intelligence Do Not Block list does not mean matching traffic is trusted or fastpathed. For more information, see Security intelligence, on page 1595.

Global and domain security intelligence lists example

For example, if you notice a set of routable IP addresses in intrusion events associated with exploit attempts, you can immediately block those IP addresses. Although it may take a few minutes for your changes to propagate, you do not have to redeploy.

Security intelligence lists and multitenancy

A security intelligence list is a multitenancy feature that

- enables the creation of block or do not block lists that apply to specific subdomains,
- supports descendant domain lists that aggregate the lists of a domain's descendants, and
- allows administrators at or above a domain to populate lists, while only domain-specific administrators can remove items.

Domain lists and descendant domain lists

Domain lists are block or do not block lists whose contents apply to a particular subdomain. The global lists are domain lists for the global domain. Each subdomain has its own named lists, and their contents apply only to that subdomain.

For example, a subdomain named Company A owns these lists:

- Domain Block list - Company A and Domain Do Not Block list - Company A
- Domain Block list for DNS - Company A, Domain Do Not Block list for DNS - Company A
- Domain Block list for URL - Company A, Domain Do Not Block list for URL - Company A

Any administrator at or above the current domain can populate these lists. You can use the context menu to add an item to the block or do not block list in the current and all descendant domains. However, only an administrator in the associated domain can remove an item from a domain list.

For example, a global administrator could add the same IP address to the block list in the global domain and Company A's domain, but not in Company B's domain. This action would add the same IP address to:

- Global Block list (removable only by global administrators)
- Domain Block list - Company A (removable only by Company A administrators)

A descendant domain list is a do not block list or block list that aggregates the domain lists of the current domain's descendants. Leaf domains do not have descendant domain lists.

Descendant domain lists are useful because a higher-level domain administrator can enforce general security intelligence settings, while subdomain users can add items to a block or do not block list in their own deployment.

For example, the global domain has these descendant domain lists:

- Descendant Block lists - Global, Descendant Do Not Block lists - Global
- Descendant Block lists for DNS - Global, Descendant Do Not Block lists for DNS - Global
- Descendant Block lists for URL - Global, Descendant Do Not Block lists for URL - Global



Note Descendant domain lists do not appear in the object manager because they are symbolic aggregations, not hand-populated lists. They appear where you can use them: in access control and DNS policies.

Add entries to global security intelligence lists

Add entries to global Security Intelligence lists to control access and improve threat detection by blocking or exempting specific IP addresses, domains, and URLs.

When reviewing events and dashboards, you can instantly block future traffic involving IP addresses, domains, and URLs that appear in those events by adding them to a predefined Block list.

Similarly, if Security Intelligence is blocking traffic that you want evaluated by threat detection processes subsequent to Security Intelligence blocking, you can add IP addresses, domains, and URLs from events to a predefined Do-Not-Block list.

Traffic is evaluated against entries on these lists during the Security Intelligence phase of threat detection.

For more information about these lists, see Global and domain security intelligence lists, on page 2420.

Before you begin

Because adding an entry to a Security Intelligence list affects access control, you must have one of the following user roles:

- Administrator
- Network Admin or Access Admin, plus Security Analyst and Security Approver
- A custom role with both "Modify Access Control Policy" and "Deploy Configuration to Devices" permissions

- Verify that these lists are used in the policies where you expect them to be effective.

Procedure

Step 1 Navigate to an event that includes an IP address, domain, or URL that you want to always block using Security Intelligence, or exempt from Security Intelligence blocking.

Step 2 Right-click the IP address, domain, or URL and choose the appropriate option.

Item Type	Context Menu Option
IP address	Add IP to Block List Add IP to Do-Not-Block List These options add the IP address to the respective lists for Networks.
URL	Add URL to Global Block List for URL Add URL to Global Do-Not-Block List for URL
Domain of a URL in the URL field	Add Domain to Global Block List for URL Add Domain to Global Do-Not-Block List for URL
Domain in the DNS Query field	Add Domain to Global Block List for DNS Add Domain to Global Do-Not-Block List for DNS

What to do next

You do not need to redeploy for these changes to take effect.

If you want to delete an item from a list, see Delete entries from global security intelligence lists, on page 2423.

Delete entries from global security intelligence lists

Update your security intelligence lists by removing entries that should no longer be blocked or allowed. This helps you maintain accurate and effective security intelligence lists.

Note To add entries to these lists, see Add entries to global security intelligence lists, on page 2422.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence**.

Step 2 Click the appropriate option:

- **Network Lists and Feeds** (for IP addresses)
- **DNS Lists and Feeds** (for domain names)
- **URL Lists and Feeds**

Step 3 Click the pencil beside the Global Block or Global Do-Not-Block list.

Step 4 Click the trash button beside the entry to delete.

List and feed updates for security intelligence feeds

A list and feed update is a security intelligence mechanism that performs the following functions:

- Replaces the existing list or feed file with the contents of the new file.
- Does not merge contents of existing and new files.
- If a corrupt or unrecognizable feed is downloaded, the system keeps using previous feed data. This is not true for the first download. If the system recognizes at least one entry in the feed, it uses only the entries it can recognize.

Feed update frequency and device polling

- Each feed updates the Firewall Management Center every two hours by default; you can modify this frequency.
- When the Firewall Management Center receives updates, it immediately passes them to your managed devices.
- Your managed devices poll the Firewall Management Center every 30 minutes for changes. You cannot change this polling frequency.
- For Secure Firewall 200, updates are downloaded once a day, not every 30 minutes.

To modify feed update intervals, see Change the update frequency for security intelligence feeds, on page 2424.

Change the update frequency for security intelligence feeds

Set the intervals at which Security Intelligence feeds are updated in the system. Adjusting the update frequency ensures that threat data is refreshed according to your organization's needs.

You can specify the intervals at which the Firewall Management Center updates Security Intelligence Feeds.

For details about feed updates, see List and feed updates for security intelligence feeds, on page 2424.

Before you begin

No explicit prerequisites are stated. Ensure you have access to the system interface where Security Intelligence feeds are managed.

Follow these steps to change the update frequency for Security Intelligence feeds:

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Expand the **Security Intelligence** node, then choose the feed type whose frequency you want to change.

The system-provided URL feed is combined with the domain feed under **DNS Lists and Feeds**.

Step 3 Next to the feed you want to update, click **Edit** ( ).

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 Edit the **Update Frequency**.

Step 5 Click **Save**.

The Security Intelligence feed will update at the new interval you specified. The system will retrieve threat data according to the configured frequency.

Custom security intelligence lists and feeds

This reference describes custom Security Intelligence lists and feeds.

List custom lists and feeds requirements

Each custom list or feed must be a simple text file no larger than 500 MB. List files must have the `.txt` extension. Include one entry or comment per line—for example, one IP address, one URL, or one domain name per line.

List and feed formatting

Each custom list or feed must be a simple text file no larger than 500 MB. List files must have the `.txt` extension. Include one entry or comment per line—for example, one IP address, one URL, or one domain name per line.

Tip The number of entries is limited by the maximum file size. For example, a URL list with no comments and an average URL length of 100 characters (including Unicode representations and newlines) can support more than 5.24 million entries.

- In a DNS list entry, you can use an asterisk (`*`) wildcard character for a domain label. All labels match the wildcard. Example: `www.example.*` matches `www.example.com` and `www.example.co`.
- Comment lines must start with the pound (`#`) character.
- Comments are removed during upload. Files you download contain only the entries, not the comments.

Feed requirements

- When configuring a feed, specify its location using a URL; the URL cannot be Punycode-encoded.
- For feed update intervals of 30 minutes or less, you must provide an MD5 URL to prevent frequent downloads of unchanged feeds. If your feed server does not provide an MD5 URL, use a download interval of at least 30 minutes.
- If you use an MD5 checksum, store it in a simple text file. The file should contain only the checksum. Do not add comments to the file.

List URL syntax and matching criteria for URL lists and feeds

Security Intelligence URL lists and feeds, including custom lists and feeds and entries in the global Block list and Do Not Block list, can include hostnames, URLs, slashes for exact matches, wildcards, and IP addresses, each with specific matching behavior.

- Hostnames

  For example, **`www.example.com`**.

- URLs
  - **`example.com`** matches **`example.com`** and all subdomains, including:
    - **`www.example.com`**
    - **`eu.example.com`**
    - **`example.com/abc`**
    - **`www.example.com/def`**
  - Does not match:
    - **`example.co.uk`**
    - **`examplexyz.com`**
    - **`example.com.malicious-site.com`**
  - When a feed or list includes a single entry, every URL that ends with those domains is identified and blocked
  - Example feed:

    If you add `www.netflix.com, www.amazon.*, org, edu, www.hulu.*` to the feed, these are blocked:
    - `http://www.amazon.in`
    - `http://www.rajiv.org/`
    - `http://www.edu.edu/`
    - `http://www.edu.org/`
    - `http://org.org/`

- `http://edu.edu`

- You can also include an entire URL path, such as **`https://www.cisco.com/c/en/us/products/security/firewalls/index.html`**

- Custom feeds with embedded credentials:

  You can create a custom URL, Network, and DNS feeds, including the username and password inside the URL (for example: **`https://admin:password@server.domain.com/list.txt`**).

Note If your password contains special characters (such as a colon (:) or an at sign (@)), transmission would fail. Ensure that your passwords do not contain these special characters, or use encoded passwords.

- A slash at the end of a URL to specify an exact match

  `example.com/` matches only **`example.com`**; it does not match **`www.example.com`** or any other URL.

- A wildcard (*) to represent any domain in a URL

  - An asterisk can represent a complete domain string separated by dots, but not a partial domain string, and not any part of the URL following the first slash.

    Valid examples:

    - **`*.example.com`**
    - **`www.*.com`**
    - **`example.*`**

      (This will match **`example.com`** and **`example.org`** and **`example.de`**, for example, but not **`example.co.uk`**)

    - **`*.example.*`**
    - **`example.*/`**

    Invalid examples:

    - **`example*.com`**
    - **`example.com/*`**

- IP addresses (IPv4)

  - For IPv6 addresses, or to use ranges or CIDR notation, use the Security Intelligence Network object.
  - You can include one or more wildcards representing an octet, for example 10.10.10.* or 10.10.*.*.

See also Custom Security Intelligence lists, on page 2430.

Custom security intelligence feeds

A custom security intelligence feed is a threat intelligence source that

- enables augmentation of system-provided intelligence feeds with regularly updated reputable block lists and do not block lists from the internet,
- supports configuration of internal feeds for updating multiple Secure Firewall Management Center appliances using a single source list, and
- allows use of MD5 checksums to determine if a feed requires downloading, reducing unnecessary updates for large or internal feeds.

Security intelligence feed management

Custom or third-party Security Intelligence feeds allow you to augment the system-provided intelligence feeds with other regularly updated reputable block lists and do not block lists on the internet. You can also set up an internal feed, which is useful if you want to update multiple Secure Firewall Management Center appliances in your deployment using one source list.

You can configure the system to use an MD5 checksum to determine whether to download an updated feed. If the checksum has not changed since the last download, the system does not need to re-download it. Using MD5 checksums is especially helpful for internal feeds that are large.

Note You cannot add address blocks to block or do not block lists using a `/0` netmask in a Security Intelligence feed. If you want to monitor or block all traffic targeted by a policy, use an access control rule with the **Monitor** or **Block** rule action and specify`any` for the **Source Networks** and **Destination Networks**.

Note The system does **not** perform peer SSL certificate verification when downloading custom feeds, nor does the system support the use of certificate bundles or self-signed certificates to verify the remote peer.

If you want strict control over when the system updates a feed from the internet, you can disable automatic updates for that feed. However, automatic updates ensure that the data is always current and relevant.

When you manually update Security Intelligence feeds, the system updates all feeds, including the system-provided intelligence feeds.

See complete requirements at List custom lists and feeds requirements, on page 2425.

Create custom security intelligence feeds

Configure security intelligence feeds to enhance your device's ability to detect and respond to threats by importing external or custom threat data sources.

You must have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Use this task when you need to add new threat intelligence feeds for IP, DNS, or URL data to your security device.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence** node, then choose a feed type you want to add.

Step 2 Click the option appropriate to the feed type you chose:

- **Add Network Lists and Feeds** (for IP addresses)
- **Add DNS Lists and Feeds**
- **Add URL Lists and Feeds**

Step 3 Enter a **Name** for the feed.

Step 4 Choose **Feed** from the **Type** drop-down list.

Step 5 Enter a **Feed URL**.

Step 6 Enter an **MD5 URL**.

- The MD5 URL is used to check if the feed content has changed since the last update and is required for update intervals shorter than 30 minutes.
- If your feed provider does not supply an MD5 URL, set the update interval to at least 30 minutes.

Step 7 Choose an **Update Frequency**.

Step 8 Click **Save**.
Unless you disabled feed updates, the system downloads and verifies the feed.

Update custom security intelligence feeds manually

Manually updating Security Intelligence feeds allows you to ensure that your deployment uses the most current threat intelligence data for filtering network traffic.

You must have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Before you begin

At least one device must already be added to the management center.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence**.

Step 2 Click **Update Feeds**, then confirm.

Step 3 Click **OK**.

After the Secure Firewall Management Center downloads and verifies the feed updates, it communicates any changes to its managed devices. Your deployment begins filtering traffic using the updated feeds.

Custom Security Intelligence lists

A custom Security Intelligence list is a static list that

- contains IP addresses, address blocks, URLs, or domain names that you manually upload to the system,
- enables you to augment and fine-tune feeds or global lists for the managed devices of a single Firewall Management Center, and
- is useful when you need to override or supplement existing feed behavior without removing the entire feed from a policy.

Formatting requirements for custom Security Intelligence lists

- Netmasks for address blocks must be integers from `0` to `32` for IPv4 or from `0` to `128` for IPv6.
- Encode Unicode in domain names using Punycode format. The encoding is not case sensitive.
- Characters in domain names are not case sensitive.
- Unicode in URLs must be percent-encoded.
- Characters in URL subdirectories are case sensitive.
- List entries that start with the number sign (`#`) are treated as comments.
- For more information about formatting requirements, see the List custom lists and feeds requirements, on page 2425.

Matching requirements for custom Security Intelligence lists

- If you add a higher-level domain to a URL or DNS list, any sub-level domains also match. For example, if you add `example.com` to a DNS list, `www.example.com` and `test.example.com` also match.
- DNS lookups (forward or reverse) are not performed on DNS or URL list entries. For example, if you add `http://198.51.100.2` to a URL list, the list matches only that exact address and not any domain it resolves to.

Note You cannot add address blocks to a Block or Do Not Block list using a `/0` netmask in a Security Intelligence list. To monitor or block all traffic targeted by a policy, use an access control rule with the **Monitor** or **Block** action, and set the **Source Networks** and **Destination Networks** to `any`.

Examples for customizing Security Intelligence lists

- If a global feed blocks access to a vital resource but is otherwise useful, you can upload a custom list to allow access to that resource without disabling the feed entirely.
- You can supplement an existing feed by adding URLs or domains relevant to your organization.

Upload new custom security intelligence lists to the Secure Firewall Management Center

To modify a Security Intelligence list, you must make your changes to the source file and upload a new copy. You cannot modify the file's contents using the web interface. If you do not have access to the source file, download a copy from the system.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence** node, then choose a list type.

Step 2 Click the option appropriate to the list you chose above:

- **Add Network Lists and Feeds** (for IP addresses)
- **Add DNS Lists and Feeds**
- **Add URL Lists and Feeds**

Step 3 Enter a **Name**.

Step 4 From the **Type** drop-down list, choose **List**.

Step 5 Click **Browse** to browse to the list `.txt` file, then click **Upload**.

Step 6 Click **Save**.

What to do next

You do not need to redeploy these changes to take effect. If you want to delete an entry from the list, see Delete entries from global security intelligence lists, on page 2423.

Update custom security intelligence lists

Modify, add, or remove entries from your security intelligence lists in Secure Firewall Management Center. Update your lists when new threats emerge or when you need to refine your firewall's response to known risks. Perform this task as part of routine security maintenance or to update your firewall based on new threat intelligence.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Security Intelligence** node, then choose a list type.

Step 2 Next to the list you want to update, click **Edit** ( ).

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 To edit the list, click **Download** and save the list as a text file using your browser's prompts.

Step 4 Change the list as needed.

Step 5 On the Security Intelligence pop-up window, click **Browse** to browse to the modified list, then click **Upload**.

Step 6 Click **Save**.

What to do next

These changes take effect without redeployment. If you want to delete an entry from the list, see Delete entries from global security intelligence lists, on page 2423.

Sinkhole objects

A sinkhole object is a network security object that

- represents either a DNS server that gives non-routable addresses for all domain names within the sinkhole
- can represent an IP address that does not resolve to a server, and
- requires assignment of both an IPv4 address and an IPv6 address.

Sinkhole object usage in DNS policy rules

You can reference the sinkhole object within a DNS policy rule to redirect matching traffic to the sinkhole.

Create a sinkhole object

Create a sinkhole object to redirect or block suspicious traffic for enhanced threat detection and analysis.

Use this task when you need to configure a sinkhole object for traffic redirection or blocking to maintain security.

Before you begin

Ensure you have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Procedure

Step 1 Choose **Objects** > **Object Management** > **Sinkhole**.

Step 2 Click **Add Sinkhole**.

Step 3 Enter a **Name**.

Step 4 Enter the **IPv4 Address** and **IPv6 Address** of your sinkhole.

Step 5 You have these options:

- To redirect traffic to a sinkhole server, choose **Log Connections to Sinkhole**.
- To redirect traffic to a non-resolving IP address, choose **Block and Log Connections to Sinkhole**.

Step 6 (Optional) From the **Type** drop-down list, assign an Indication of Compromise (IoC) type for the sinkhole object, if needed.

Step 7 Click **Save**.

Configure an SLA monitor

Configure an SLA monitor to define a connectivity policy to a monitored address and track the availability of a route. This helps ensure that the route is periodically checked and replaced with a backup route if it becomes unavailable.

An Internet Protocol Service Level Agreement (SLA) monitor defines a connectivity policy to a monitored address and tracks the availability of a route. The monitor periodically checks the route by sending ICMP echo requests. If requests time out, the route is removed from the routing table and replaced with a backup route. SLA monitoring jobs start immediately after deployment and continue to run unless you remove the SLA monitor from the device configuration. The SLA Monitor Object is used in the Route Tracking field of an IPv4 Static Route Policy.



Note IPv6 routes do not support SLA monitors via route tracking.

Procedure

Step 1 Select **Objects** > **Object Management** > **SLA Monitor**.

Step 2 Click **Add SLA Monitor** and enter these values:

Fields	Details
Name	Enter a name for the object.
Description	Enter a description for the object.
Frequency	Enter the frequency of ICMP echo request transmissions, in seconds. Valid values range from 1 to 604800 seconds (7 days). The default is 60 seconds. **Note** The frequency cannot be less than the timeout value; you must convert frequency to milliseconds to compare the values.
SLA Monitor ID	Enter the ID number of the SLA operation. Values range from 1 to 2147483647. You can create a maximum of 2000 SLA operations on a device. Each ID number must be unique to the policy and the device configuration.
Threshold	Enter the amount of time that must pass after an ICMP echo request before a rising threshold is declared, in milliseconds. Valid values range from 0 to 2147483647 milliseconds. The default is 5000 milliseconds. The threshold value identifies events that exceed the defined value, which you can use to evaluate the proper timeout value. However, the threshold does not serve as a direct indicator of the reachability of the monitored address. **Note** The threshold value should not exceed the timeout value.

Fields	Details
Timeout	Enter the amount of time that the SLA operation waits for a response to the ICMP echo requests, in milliseconds. Values range from 0 to 604800000 milliseconds (7 days). The default is 5000 milliseconds. If a response is not received from the monitored address within the amount of time defined in this field, the static route is removed from the routing table and replaced by the backup route. **Note** The timeout value cannot exceed the frequency value (adjust the frequency value to milliseconds to compare the numbers).
Data Size	Enter the size of the ICMP request packet payload, in bytes. Values range from 0 to 16384 bytes. The default is 28 bytes, which creates a total ICMP packet of 64 bytes. Do not set this value higher than the maximum allowed by the protocol or the Path Maximum Transmission Unit (PMTU). For purposes of reachability, you might need to increase the default data size to detect PMTU changes between the source and the target. A low PMTU can affect session performance and, if detected, might indicate that the secondary path should be used.
ToS	Enter a value for type of service (ToS) defined in the IP header of the ICMP request packet. Values range from 0 to 255. The default is 0. This field contains information such as delay, precedence, reliability, and so on. It can be used by other devices on the network for policy routing and features such as committed access rate.
Number of Packets	Enter the number of packets that are sent. Values range from 1 to 100. The default is 1 packet. **Note** Increase the default number of packets if you are concerned that packet loss might falsely cause the Secure Firewall Threat Defense device to believe that the monitored address cannot be reached.
Monitored Address	Enter the IP address that is being monitored for availability by the SLA operation.

Step 3 The **Available Zones** list displays both zones and interface groups. In the **Zones/Interfaces** list, add the zones or interface groups that contain the interfaces through which the device communicates with the management station. To specify a single interface, you need to create a zone or the interface groups for the interface; see Create security zone and interface group objects, on page 610. The host will be configured on a device only if the device includes the selected interfaces or zones.

Step 4 Click **Save**.

After completing these steps, the SLA monitor is configured and begins tracking the availability of the specified route. If the monitored address becomes unreachable, the route is removed from the routing table and replaced with a backup route.

Time ranges

A time range is a configuration object that

- defines specific time periods,
- enables use of these periods to determine when rules apply, and
- supports integration with time-based ACLs.

Time range objects allow you to specify periods for rule enforcement.

Note Time-based ACLs is supported in Snort 3 also from Firewall Management Center 7.0 onwards.

Create a time range object

Establish a time range object so policies apply only during specified periods, enabling precise control of network traffic.

If you want a policy to apply only during a specified time range, create a time range object and specify that object in the policy. This object works on Firewall Threat Defense devices only.

You can specify time range objects only in certain policy types, which are listed in this topic.

Note The timezone represents the device's local time and is used only for applying the time ranges in rules in the policies that support the time ranges. The timezone does not change the configured time of the device. To verify the configuration, in the Firewall Threat Defense CLI, use the **show time-range timezone** and **show time** commands (see the *Cisco Secure Firewall Threat Defense Command Reference* guide). In addition, the timezone of a chassis overrides the management center timezone.

Before you begin

Time ranges operate based on the time zone associated with the device that processes the traffic. By default, this is UTC. To change the time zone associated with a device, go to **Devices** > **Platform Settings**.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Time Range** from the list of object types.

Step 2 Click **Add Time Range**.

Step 3 Enter the object name and specify the desired time periods.

- If you see a red error box around the object name you have entered, mouse over the **Name** field to see naming restrictions.
- All times are in UTC, unless you specify a time zone for the device in **Devices** > **Platform Settings**.

- Enter times using a 24-hour clock; for example, enter 13:30 for 1:30 PM.
- To specify a single continuous range, such as typical weekend hours (Fridays at 5pm through Mondays at 8am, including evenings and nights), choose Range Type **Range**.
- To specify part of multiple days, such as Monday through Friday from 8am to 5pm (excluding evenings, nights, and early mornings every day), choose Range Type **Daily Interval**.
- You may specify up to 28 periods per object.
- For multiple noncontiguous times of day or different hours for different days, create multiple recurring intervals. For example, to apply a policy at all times other than standard working hours, create a single time range object with the following two recurring intervals:
  - A Daily Interval for Monday through Friday from 5pm through 8am, and
  - A Range recurring interval for Friday at 5pm through Monday at 8am.

Step 4 Click **Save**.

What to do next

Configure time ranges in any of these:

- Access control rules
- Prefilter rules
- Tunnel rules
- VPN group policy

In a VPN group policy object, specify the time range object using the **Access Hours** field. For details, see Configure a group policy object, on page 2461 and Advanced group policy option fields and values, on page 2467.

Time zones

A time zone is a configuration object that

- specifies the local time zone for a managed device
- is used only for applying time ranges in rules in policies that support time ranges, such as access control, prefilter, and VPN group policies), and
- defaults to UTC if not assigned to a device.

Device support and usage of time zones

- Time zone objects are supported only for Firewall Threat Defense devices.
- Time-based ACLs is supported in Snort 3 also from Firewall Management Center 7.0 onwards.

Tunnel zones

A tunnel zone is a network object that

- represents certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis,
- is not an interface object, and
- can be used as an interface constraint in some configurations.

For detailed information, see Using tunnel zones to apply access control at the tunnel level, on page 1970.

URLs

A URL object is a configuration element that

- defines a single URL or IP address for use within access control policies, event searches, and Security Intelligence configurations,
- can be used in multiple locations throughout the system's web interface to specify what traffic is filtered or monitored, and
- provides distinct matching behavior compared to URL group objects, which define multiple URLs or addresses.

URL object configuration guidelines



Important For best practices for using this and similar options in Security Intelligence configurations and for URL rules in access control and QoS policies, see Manual URL filtering options, on page 1668.

When creating URL objects, consider the following guidelines:

- If the URL does not include a path (no / characters), the match is based only on the server's hostname. If a path is included (one or more / characters), the entire URL string is used for a substring match.
- A URL is considered a match if:
  - the string appears at the beginning of the URL,
  - the string follows a dot,
  - the string contains a dot at the beginning,
  - or the string follows the :// characters.
- The system ignores the encryption protocol (HTTP or HTTPS). Blocking a website applies to both unless an application condition targets a specific protocol. Specify URLs without the protocol (use example.com, not http://example.com).
- To match HTTPS traffic in access control rules, use the subject common name from the public key certificate. Do not include subdomain information. The subject common name in certificates may differ

from the web site's domain (for example, youtube.com uses *.google.com). Use SSL Decryption policy to decrypt HTTPS traffic for consistent URL filtering results.

- URL objects will not match HTTPS traffic if the browser resumes a TLS session, as certificate information may not be available, which can lead to inconsistent results.
- When using URL objects as aliases in remote access VPN policies, ensure the URL is 128 characters or less.
- Do not use manual URL filtering to block or allow individual web pages or parts of sites (that is, URL strings with / characters), as servers can be reorganized and pages moved to new paths.

URL object matching examples

For example, ign.com matches ign.com or www.ign.com, but not versign.com. Use example.com rather than http://example.com when specifying a URL object.

Create a URL object

Use this task when you need to define a new URL object in the Secure Firewall Management Center for use in access control or other security policies.

Procedure

Step 1 Choose **Objects** > **Object Management** > **URL** from the list of object types.

Step 2 Choose **Add Object** from the **Add URL** drop-down list.

Step 3 Enter a **Name**.

Step 4 (Optional) Enter a **Description**.

Step 5 Enter the **URL** or IP address.

Step 6 (Optional) Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.
- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Variable sets

A variable set is a configuration group that

- collects and manages variables used in intrusion rules and policies
- allows customization of predefined and user-defined variables, and
- enables linking of variable sets to intrusion policies for flexible network security management.

Variable set management and usage

Variables represent values commonly used in intrusion rules to identify source and destination IP addresses and PORTS. You can also use variables in intrusion policies to represent IP addresses in rule suppressions, adaptive profile updates, and dynamic rule states.



Tip Preprocessor rules can trigger events regardless of the hosts defined by network variables used in intrusion rules.

You use variable sets to manage, customize, and group your variables. You can use the default variable set provided by the system or create your own custom sets. Within any set you can modify predefined default variables and add and modify user-defined variables.

Most of the shared object rules and standard text rules that the system provides use predefined default variables to define networks and port numbers. For example, the majority of the rules use the variable `$HOME_NET` to specify the protected network and the variable `$EXTERNAL_NET` to specify the unprotected (or outside) network. In addition, specialized rules often use other predefined variables. For example, rules that detect exploits against web SERVERS use the `$HTTP_SERVERS` and `$HTTP_PORTS` variables.

Rules are more effective when variables more accurately reflect your network environment. At a minimum, you should modify default variables in the default set. By ensuring that a variable such as `$HOME_NET` correctly defines your network and `$HTTP_SERVERS` includes all web SERVERS on your network, processing is optimized and all relevant systems are monitored for suspicious activity.

To use your variables, you link variable sets to intrusion policies associated with access control rules or with the default action of an access control policy. By default, the default variable set is linked to all intrusion policies used by access control policies.

Adding a variable to any set adds it to all sets; that is, each variable set is a collection of all variables currently configured on your system. Within any variable set, you can add user-defined variables and customize the value of any variable.

Initially, the system provides a single, default variable set comprised of predefined default values. Each variable in the default set is initially set to its default value, which for a predefined variable is the value set by the Talos Intelligence Group and provided in rule updates.

Although you can leave predefined default variables configured to their default values, Cisco recommends that you modify a subset of predefined variables.

You could work with variables only in the default set, but in many cases you can benefit most by adding one or more custom sets, configuring different variable values in different sets, and perhaps even adding new variables.

When using multiple sets, it is important to remember that the *current value* of any variable in the default set determines the *default value* of the variable in all other sets.

When you select **Variable Sets** on the Object Manager page, the object manager lists the default variable set and any custom sets you created.

On a freshly installed system, the default variable set is comprised only of the default variables predefined by Cisco.

Each variable set includes the default variables provided by the system and all custom variables you have added from any variable set. Note that you can edit the default set, but you cannot rename or delete the default set.



Caution Importing an access control or an intrusion policy overwrites existing default variables in the default variable set with the imported default variables. If your existing default variable set contains a custom variable not present in the imported default variable set, the unique variable is preserved.

Related Topics

Manage variables, on page 2452
Manage variable sets, on page 2451

Variable sets in intrusion policies

A variable set is a configuration group that

- links to intrusion policies used in an access control policy,
- provides variable values for enabled intrusion rules, and
- affects deployment status when modified.

Deployment status for variable sets in intrusion policies

By default, the system links the default variable set to all intrusion policies used in an access control policy. When you deploy an access control policy that uses an intrusion policy, intrusion rules that you have enabled in the intrusion policy use the variable values in the linked variable set.

When you modify a custom variable set used by an intrusion policy in an access control policy, the system reflects the status for that policy as out-of-date on the Access Control Policy page. You must re-deploy the access control policy to implement changes in your variable set. When you modify the default set, the system reflects the status of all access control policies that use intrusion policies as out-of-date, and you must re-deploy all access control policies to implement your changes.

Variables

A variable is a configuration element that

- can be provided by the system or created by users
- is categorized as default, customized, or advanced, and
- enables flexible management of network addresses and ports in rule creation.

Variable categories

Variables are grouped into three categories: default, customized, and advanced.

- **Default variables** are provided by the system. You cannot rename or delete a default variable, and you cannot change its default value. However, you can create a customized version of a default variable.
- **Customized variables** are variables you create. These variables can include:
  - *customized default variables*

    When you edit the value for a default variable, the system moves the variable from the Default Variables area to the Customized Variables area. Variable values in the default set determine the default values of variables in custom sets. If you customize a default variable in the default set, the system changes the default value of the variable in all other sets.
  - *user-defined variables*

    You can add and delete your own variables, customize their values within different variable sets, and reset customized variables to their default values. When you reset a user-defined variable, it remains in the Customized Variables area.

    User-defined variables can be one of these types:
    - *network* variables specify the IP addresses of hosts in your network traffic.
    - *port* variables specify TCP or UDP ports in network traffic, including the value `any` for either type.
- **Advanced variables** are provided by the system under specific conditions. These variables have a very limited deployment.

Variable usage examples

For example, if you create custom standard text rules, you might also want to add your own user-defined variables to more accurately reflect your traffic or as shortcuts to simplify the rule creation process. Alternatively, if you create a rule that you want to inspect traffic in the "demilitarized zone" (or DMZ) only, you can create a variable named `$DMZ` whose value lists the server IP addresses that are exposed. You can then use the `$DMZ` variable in any rule written for this zone.

List predefined default variables

By default, the system provides a single default variable set, which is comprised of predefined default variables. The Talos Intelligence Group uses rule updates to provide new and updated intrusion rules and other intrusion policy elements, including default variables. Because many intrusion rules from the system use predefined default variables, set appropriate values for these variables. You can modify the values for these default variables in any or all variable sets, depending on how you use variable sets to identify traffic on your network.



Caution Importing an access control or an intrusion policy overwrites existing default variables in the default variable set with the imported default variables. If your existing default variable set contains a custom variable not present in the imported default variable set, the unique variable is preserved.

This table describes the variables provided by the system and indicates which variables you typically would modify. For assistance determining how to tailor variables to your network, contact Professional Services or Support.

Table 155: System-Provided variables

Variable Name	Description	Modify?
`$AIM_SERVERS`	Defines known AOL Instant Messenger (AIM) SERVERS, and is used in chat-based rules and rules that look for AIM exploits.	Not required.
`$DNS_SERVERS`	Defines Domain Name Service (DNS) SERVERS. If you create a rule that affects DNS SERVERS specifically, you can use the `$DNS_SERVERS` variable as a destination or source IP address.	Not required in current r
`$EXTERNAL_NET`	Defines the network that the system views as the unprotected network, and is used in many rules to define the EXTERNAL network.	Yes, you should adequat `$HOME_NET` and then excl `$HOME_NET` as the value f `$EXTERNAL_NET`.
`$FILE_DATA_PORTS`	Defines non-encrypted ports used in intrusion rules that detect files in a network stream.	Not required.
`$FTP_PORTS`	Defines the ports of FTP SERVERS on your network, and is used for FTP server exploit rules.	Yes, if your FTP SERVE ports other than the defa (you can view the defaul the web interface).
`$GTP_PORTS`	Defines the data channel ports where the packet decoder extracts the payload inside a GTP (General Packet Radio Service [GPRS] Tunneling Protocol) PDU.	Not required.
`$HOME_NET`	Defines the network that the associated intrusion policy monitors, and is used in many rules to define the internal network.	Yes, to include the IP add your internal network.
`$HTTP_PORTS`	Defines the ports of web SERVERS on your network, and is used for web server exploit rules.	Yes, if your web SERVE ports other than the defa (you can view the defaul the web interface).
`$HTTP_SERVERS`	Defines the web SERVERS on your network. Used in web server exploit rules.	Yes, if you run HTTP SE
`$ORACLE_PORTS`	Defines Oracle database server ports on your network, and is used in rules that scan for attacks on Oracle databases.	Yes, if you run Oracle SI
`$SHELLCODE_PORTS`	Defines the ports you want the system to scan for shell code exploits, and is used in rules that detect exploits that use shell code.	Not required.
`$SIP_PORTS`	Defines the ports of SIP SERVERS on your network, and is used for SIP exploit rules.	Not required.

Variable Name	Description	Modify?
$SIP_SERVERS	Defines SIP SERVERS on your network, and is used in rules that address SIP-targeted exploits.	Yes, if you run SIP SI should adequately de $HOME_NET and then i $HOME_NET as the val $SIP_SERVERS.
$SMTP_SERVERS	Defines SMTP SERVERS on your network, and is used in rules that address exploits that target mail SERVERS.	Yes, if you run SMTI
$SNMP_SERVERS	Defines SNMP SERVERS on your network, and is used in rules that scan for attacks on SNMP SERVERS.	Yes, if you run SNM
$SNORT_BPF	Identifies a legacy advanced variable that appears only when it existed on your system in a software release before Version 5.3.0 that you subsequently upgraded to Version 5.3.0 or greater.	No, you can only view variable. You cannot recover it after deleti
$SQL_SERVERS	Defines database SERVERS on your network, and is used in rules that address database-targeted exploits.	Yes, if you run SQL S
$SSH_PORTS	Defines the ports of SSH SERVERS on your network, and is used for SSH server exploit rules.	Yes, if your SSH SEI ports other than the d (you can view the de the web interface).
$SSH_SERVERS	Defines SSH SERVERS on your network, and is used in rules that address SSH-targeted exploits.	Yes, if you run SSH S you should adequatel $HOME_NET and then i $HOME_NET as the val $SSH_SERVERS.
$TELNET_SERVERS	Defines known Telnet SERVERS on your network, and is used in rules that address Telnet server-targeted exploits.	Yes, if you run Telne
$USER_CONF	Provides a general tool that allows you to configure one or more features not otherwise available via the web interface. Conflicting or duplicate $USER_CONF configurations will halt the system.	No, only as instructed description or with th Support.

Network variables

A network variable is a configuration element that

- represents IP addresses for use in intrusion rules, intrusion policy rule suppressions, dynamic rule states, and adaptive profile updates
- differs from network objects and network object groups by being specific to intrusion policies and intrusion rules, and
- enables specification of host IP addresses in various configurations within an intrusion policy.

Network variable usage and configuration

Network variables can be used to specify the IP addresses of hosts on the network in the following configurations:

- Intrusion rules: The **Source IPs** and **Destination IPs** fields restrict packet inspection to traffic originating from or destined to specific IP addresses.
- Suppressions: The **Network** field in source or destination intrusion rule suppressions suppresses intrusion event notifications when a specific IP address or range triggers an intrusion rule or preprocessor.
- Dynamic rule states: The **Network** field in dynamic rule states identifies when too many matches for an intrusion rule or preprocessor occur within a given time period.
- adaptive profile updates: The**Networks** field identifies hosts where packet fragment and TCP stream reassembly is improved in passive deployments.

When variables are used in these fields, the variable set linked to an intrusion policy determines the variable values applied to network traffic handled by the related access control policy.

A variable can include any combination of the following network configurations:

- network variables, network objects, and network object groups selected from the available networks list,
- individual network objects added from the New or Edit Variable page, which can then be used in variables or other configurations,
- literal single IP addresses or address blocks; multiple literal IP addresses and address blocks may be included individually, supporting both IPv4 and IPv6 addresses.

  When specifying IPv6 addresses, any addressing convention defined in RFC 4291 may be used.

The default value for included networks in any variable is `any`, which indicates any IPv4 or IPv6 address. The default value for excluded networks is `none`, meaning no network. If you specify the address `::`, it means any IPv6 address when included, or no IPv6 addresses when excluded.

Adding networks to the excluded list negates those addresses and blocks; all addresses except the excluded ones can be matched.

For example, excluding `192.168.1.1` specifies any IP address other than 192.168.1.1. Excluding `2001:db8:ca2e::fa4c`specifies any IP address except 2001:db8:ca2e::fa4c.

Exclusions can be made with any combination of literal or available networks. For instance, excluding both `192.168.1.1` and `192.168.1.5` matches any IP address other than 192.168.1.1 or 192.168.1.5.

Keep these points in mind when you add or edit network variables:

- The value `any` cannot be logically excluded, as it would mean no address; for example, it is not possible to add a variable with the value `any` to the exclusion list.
- Network variables identify traffic for specific intrusion rule and intrusion policy features; preprocessor rules can trigger events regardless of the hosts defined by network variables.
- Excluded values must resolve to a subset of included values; for example, including the address block 192.168.5.0/24 and excluding 192.168.6.0/24 is not valid.

Port variables

A port variable is a network configuration element that

- represents TCP and UDP ports you can use in the **Source Port** and **Destination Port** header fields in intrusion rules,
- is specific to intrusion rules and differs from port objects and port object groups, and
- can be used to restrict packet inspection to packets originating from or destined to specific TCP or UDP ports.

Port variable configuration details

Port variables are linked to intrusion policies associated with access control rules or policies, determining the values for these variables in the network traffic where you deploy the access control policy.

When configuring a port variable, you can include:

- any combination of port variables and port objects that you select from the list of available ports (excluding port object groups, which cannot be added to variables),
- individual port objects that you add while creating or editing a variable, which can also be reused for other variables,
- and single literal port values as well as port ranges (ranges must use a dash, e.g., 80-90; colon-separated ranges are supported for backward compatibility but not for new variables).

  You can list multiple literal port values and ranges by adding each individually in any combination.

Port variable configuration has these important considerations:

- The default value for included ports in any variable is `any`, indicating all ports or port ranges. The default for excluded ports is `none`, indicating no ports.



Tip To create a variable with the value `any`, name and save the variable without adding a specific value.

- You cannot exclude the value `any` from a variable, as that would result in no ports being matched.
- Adding ports to an excluded list prevents matching on those specified ports or port ranges. The system matches any port except those excluded.
- Excluded values must be a subset of the included values. For example, if you include the port range 10-50, you cannot exclude port 60.

Advanced variables

An advanced variable is a configuration mechanism that

- enables you configure of features not available through the web interface
- includes the USER_CONF variable as your primary advanced variable, and
- allows you to enter custom instructions or lines up to the maximum character length.

User_CONF variable details

The USER_CONF variable provides a general tool that allows configuration of one or more features not otherwise available via the web interface.

Caution Do **not** use the advanced variable USER_CONF to configure an intrusion policy feature unless you are instructed to do so in the feature description or by Support. Conflicting or duplicate configurations will halt the system.

When editing USER_CONF, you can type up to 4096 characters on a single line. The line wraps automatically. You can include any number of valid instructions or lines until you reach either the 8192-character maximum length for a variable or a physical limit, such as disk space. Use the backslash (\) character as a line continuation after any complete argument in a command directive.

Resetting USER_CONF empties it.

Variable resets

A variable reset is a configuration action that

- returns a variable to its default value on the variable set new or edit variables page,
- applies different reset behaviors depending on whether the variable is in a default or custom set, and
- affects the value used in any intrusion policy where the variable set is linked.

Variable reset values

You can reset a variable to its default value on the variable set new or edit variables page. This table summarizes the basic principles of resetting variables.

Table 156: Variable reset values

Resetting this variable type...	In this set type...	Resets it to...
default	default	the rule update value
user-defined	default	`any`
default or user-defined	custom	the current default set value (modified or unmodified)

When you reset a variable in a custom set, you return it to the current value for that variable in the default set.

If you reset or change a variable in the default set, you update the default value in all custom sets. If the reset icon is unavailable, you cannot reset the variable because it has no customized value in the set. If you have not customized the variable in a custom set, changing it in the default set also updates any intrusion policy where you have linked the variable set.

Note Before you modify a variable in the default set, check how this change affects any intrusion policy that uses the variable in a linked custom set, especially if you have not customized the variable value in the custom set.

You can hover your pointer over the **Reset** icon in a variable set to see the reset value. If the customized value and the reset value match, you are in one of these situations:

- you are in the custom or default set where you added the variable with the value `any`.
- you are in the custom set where you added the variable with an explicit value and elected to use the configured value as the default value.

Variable sets

A variable set is a configuration grouping that

- allows variables to be managed collectively across multiple sets
- enables the addition of variables to all sets simultaneously, and
- provides options for using configured or default values when adding variables.

Variable set behavior

When you add a variable to a variable set, it is also added to all other sets. If you add a variable from a custom set, decide if you want to use the configured value as the customized value in the default set.

- **If you use the configured value** (for example, 192.168.0.0/16), the variable is added to the default set using the configured value as a customized value with a default value of `any`. The current value in the default set determines the default value in other sets. Therefore, the initial default value in other custom sets is the configured value (which in this example is 192.168.0.0/16).
- **If you do not use the configured value**, the variable is added to the default set using only the default value `any` and, consequently, the initial, default value in other custom sets is `any`.

Examples: Adding user-defined variables to default sets

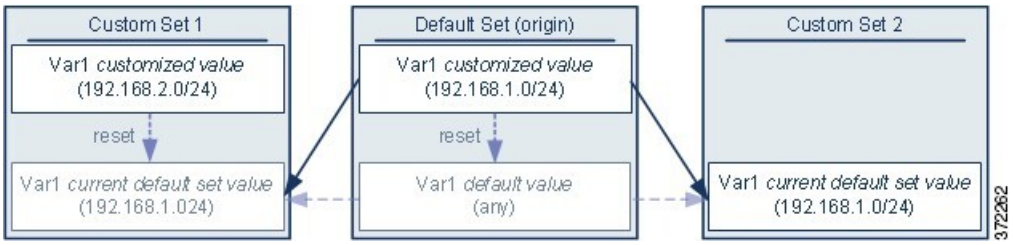
A user-defined variable addition is a configuration action that

- enables adding a variable, such as Var1, to a default set with a specific value (like 192.168.1.0/24),
- allows customization of the variable value in any set, and
- ensures that resetting the variable in the default set resets its default value to `any` across all sets.

Set interactions and variable customization

The diagram below illustrates how adding and customizing user-defined variables affects default and custom sets.

Figure 426: Set interaction diagram



Customizing the value of `Var1` in a custom set overrides the default value. For example, if `Var1` is customized in `Custom Set 1`, it takes on a new value, while in `Custom Set 2`, if `Var1` is not customized, it retains the default value (e.g., `192.168.1.0/24`). Resetting the user-defined variable in the default set updates its default value to `any` in all sets.

Further, when `Var1` in `Custom Set 2` is not updated, customizing or resetting `Var1` in the default set updates its current value in `Custom Set 2`, affecting any intrusion policy linked to the variable set.

Note While the interactions are the same for user-defined variables and default variables, resetting a default variable in the default set resets it to the value configured by Cisco in the current rule update, not `any`.

Customizing user-defined variable values

In Custom Set 1, the customized value `192.168.2.0/24` of `Var1` overrides the default value, while in Custom Set 2, `Var1` retains the default value `192.168.1.0/24` unless customized.

Resetting default variables in default sets

Although not shown in the example, note that interactions between sets are the same for user-defined variables and default variables except that resetting a default variable in the default set resets it to the value configured by Cisco in the current rule update.

Examples: User-defined variables in custom sets

A user-defined variable in a custom set is a configuration element that:

- enables you to add variables to custom sets,
- allows you to choose whether the configured value becomes the default for other sets, and
- affects how variable values and interactions propagate across sets.

Variable set interactions and default value behavior

When you add a user-defined variable to a custom set, you are prompted to decide if the configured value should be used as the default value for other sets. The examples illustrate the outcomes of each choice.

- Choosing to use the configured value as the default copies the value to the default set as a customized value, with a default value of `any`.

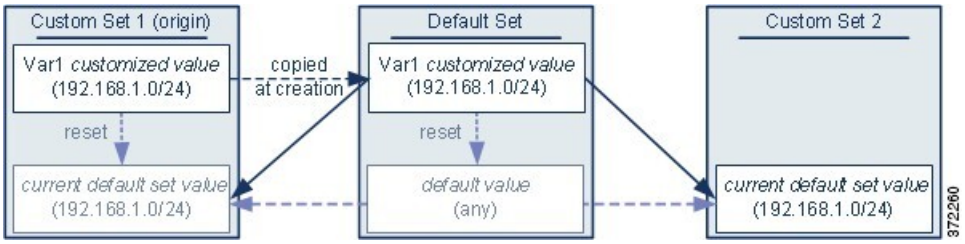
- Choosing not to use the configured value as the default adds the variable to all sets with a default value of `any`, allowing customization in any set.

Note Further customizing or resetting a variable in the default set updates the current, default value in other sets, which can affect any intrusion policy linked to the variable set.

Examples of adding user-defined variables to custom sets

The first example shows adding `Var1` with the value `192.168.1.0/24` to Custom Set 1 and electing **to use** the configured value as the default for other sets.

Figure 427: Variable set interaction when using the configured value as default

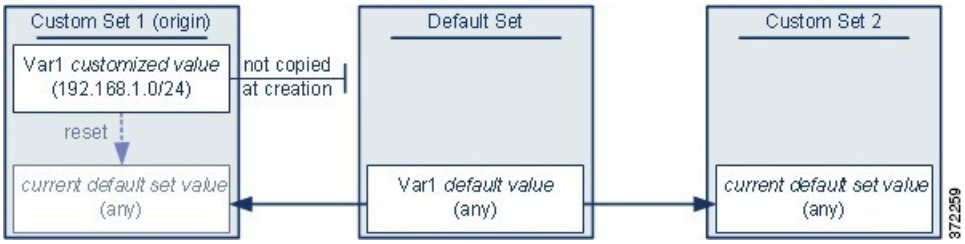


Except for the origin of `Var1` from Custom Set 1, this example is identical to adding `Var1` to the default set. Adding the customized value `192.168.1.0/24` for `Var1` to Custom Set 1 copies the value to the default set as a customized value with a default value of `any`. Thereafter, `Var1` values and interactions are the same as if you had added `Var1` to the default set. Further customizing or resetting `Var1` in the default set updates the current, default value of `Var1` in Custom Set 2, affecting any intrusion policy linked to the variable set.

Adding a variable and not using the configured value as default

The second example shows adding `Var1` with the value `192.168.1.0/24` to `Custom Set 1`, but electing **not to use** the configured value as the default in other sets.

Figure 428: Variable set interaction when not using the configured value as default



This approach adds `Var1` to all sets with a default value of `any`. After adding `Var1`, you can customize its value in any set. An advantage of this approach is that, by not initially customizing `Var1` in the default set, you decrease your risk of customizing the value in the default set and inadvertently changing the current value in a set such as Custom Set 2 where you have not customized `Var1`.

Nesting variables

A nesting variable is a configuration element that

- can include other variables as part of its definition
- does not support circular nesting, and
- does not support nested, negated variables.

Valid nested variables

In this example, SMTP_SERVERS, HTTP_SERVERS, and OTHER_SERVERS are valid nested variables.

Variable	Type	Included Networks	Excluded Networks
SMTP_SERVERS	customized default	10.1.1.1	—
HTTP_SERVERS	customized default	10.1.1.2	—
OTHER_SERVERS	user-defined	10.2.2.0/24	—
HOME_NET	customized default	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Invalid nested variable

In this example, HOME_NET is an invalid nested variable because the nesting of HOME_NET is circular; that is, the definition of OTHER_SERVERS includes HOME_NET, so you would be nesting HOME_NET in itself.

Variable	Type	Included Networks	Excluded Networks
SMTP_SERVERS	customized default	10.1.1.1	—
HTTP_SERVERS	customized default	10.1.1.2	—
OTHER_SERVERS	user-defined	10.2.2.0/24 HOME_NET	—
HOME_NET	customized default	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

Unsupported nested, negated variable

Because nested, negated variables are not supported, do not use the variable NONCORE_NET to represent IP addresses outside your protected networks.

Variable	Type	Included Networks	Excluded Networks
HOME_NET	customized default	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	customized default	—	HOME_NET
DMZ_NET	user-defined	10.4.0.0/16	—
NOT_DMZ_NET	user-defined	—	DMZ_NET
NONCORE_NET	user-defined	EXTERNAL_NET NOT_DMZ_NET	—

Alternative to unsupported nested, negated variable

As an alternative to the example above, you could represent IP addresses that are outside of your protected networks by creating the variable NONCORE_NET to represent IP addresses outside your protected networks.

Variable	Type	Included Networks	Excluded Networks
HOME_NET	customized default	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	user-defined	10.4.0.0/16	—
NONCORE_NET	user-defined	—	HOME_NET DMZ_NET

Manage variable sets

Manage variable sets to organize and control the variables used by your devices. This task helps you add, edit, delete, or filter variable sets as needed for device configuration.

Variable sets are used to efficiently manage collections of variables crucial for device configuration. To use variable sets, you must have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Procedure

Step 1 Choose **Objects** > **Object Management** > **Variable Set**.

Step 2 Manage your variable sets:

- Add — If you want to add a custom variable set, click **Add Variable Set**; see Create a variable set, on page 2452.
- Delete — If you want to delete a custom variable set, click **Delete** ( ) next to the variable set, then click **Yes**. You cannot delete the default variable set or variable sets belonging to ancestor domains.

Note Variables created in a variable set you delete are not deleted or otherwise affected in other sets.

- Edit — If you want to edit a variable set, click **Edit** ( ) next to the variable set you want to modify; see Edit objects, on page 2337.
- Filter — If you want to filter variable sets by name, begin entering a name; as you type, the page refreshes to display matching names. If you want to clear name filtering, click **Clear** ( ) in the filter field.
- Manage Variables — To manage the variables included in variable sets, see Manage variables, on page 2452.

Create a variable set

Variable sets allow you to define and group variables for use in Secure Firewall Management Center. Use this task when you need to create a new set of variables for policy configuration or reuse.

Procedure

Step 1 Choose **Objects** > **Object Management** > **Variable Set**.

Step 2 Click **Add Variable Set**.

Step 3 Enter a **Name**.

Step 4 (Optional) Enter a **Description**.

Step 5 Manage the variables in the set; see Manage variables, on page 2452.

Step 6 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Manage variables

Configure variable sets to control device policies and manage variables for Secure Firewall Management Center.

- You can display, add, delete, edit, or reset variables as required for your environment.

To manage variables in Secure Firewall Management Center, you must have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Procedure

Step 1 Choose **Objects** > **Object Management** > **Variable Set**.

Step 2 Click **Edit** ( ) next to the variable set you want to edit.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Manage your variables:

- Display — If you want to display the complete value for a variable, hover your pointer over the value in the **Value** column next to the variable.
- Add — If you want to add a variable, click **Add**; see Add variables, on page 2454.
- Delete — Click **Delete** ( ) next to the variable. If you have saved the variable set since adding the variable, click **Yes** to confirm that you want to delete the variable.

  You *cannot* delete these:

  - default variables
  - user-defined variables that are used by intrusion rules or other variables
  - variables belonging to ancestor domains

- Edit — Click **Edit** ( ) next to the variable you want to edit; see Edit variables values in a variable set, on page 2455.
- Reset — If you want to reset a modified variable to its default value, click **Reset** next to a modified variable. If reset is dimmed, one of these is true:
  - The current value is already the default value.
  - The configuration belongs to an ancestor domain.

Tip Hover your pointer over an active reset to display the default value.

Step 4 Click **Save** to save the variable set. If the variable set is in use by an access control policy, click **Yes** to confirm that you want to save your changes.

The current value in the default set determines the default value in all other sets. If you modify or reset a variable in the default set, the current value changes in other sets where you have not customized the default value.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Add variables

Add variables to a variable set so you can define reusable network or port values for use in policies.

Use variables in device policies to enable flexible, reusable configurations that simplify network management.

Before you begin

Ensure you have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

Procedure

Step 1 In the variable set editor, click **Add**.

Step 2 Enter a unique variable **Name**.

Step 3 From the **Type** drop-down list, choose either **Network** or **Port**.

Step 4 Define the values for the variable:

- To include or exclude specific networks or ports, select them and click **Include** or **Exclude**. If there is overlap, excluded addresses or ports always take precedence over included ones.
- To add literal values, enter a single IP address, address block, port, or port range. If you need to add more than one value, repeat this action.
- To remove any items from included or excluded lists, select the item and click **Delete** ( ) next to the item.
- You may use a combination of literal values, existing variables, objects, or network object groups when specifying included or excluded items for network variables.

Step 5 Save the variable.

- If adding a new variable from a custom set, choose whether to add it as a customized value in the default set or as a default value of `any` in the default and other custom sets.

Step 6 Save the variable set.

- Any access control policy linked to the variable set will display an out-of-date status until changes are deployed.

The variable is added to the variable set and is available for use in policies. Any access control policy linked to the variable set displays an out-of-date status until you deploy the changes.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

Edit variables values in a variable set

You must have the IPS license (for Firewall Threat Defense devices) or the Protection license (all other device types).

You can edit both custom and default variables.

You cannot change the **Name** or **Type** values in an existing variable.

Procedure

Step 1 In the variable set editor, click **Edit** ( ) next to the variable you want to modify.

If **View** ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 2 Modify the variable:

- If you want to move items from the list of available networks or ports to the list of included or excluded items, you can select one or more items and then drag and drop, or click **Include** or **Exclude**.

Tip If addresses or ports overlap between the included and excluded lists for a network or port variable, the excluded addresses or ports take precedence.

- Enter a single literal value, then click **Add**. For network variables, you can enter a single IP address or address block. For port variables, you can add a single port or port range, separating the upper and lower values with a hyphen (-). Repeat this step as needed to enter multiple literal values.
- If you want to remove an item from the included or excluded lists, click **Delete** ( ) next to the item.

Note The list of items to include or exclude can be comprised of any combination of literal strings and existing variables, objects, and network object groups in the case of network variables.

Step 3 Click **Save** to save the variable.

Step 4 Click **Save** to save the variable set. If the variable set is in use by an access control policy, click **Yes** to confirm that you want to save your changes. Your changes are saved, and any access control policy the variable set is linked to displays an out-of-date status.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

VLAN tags

A VLAN tag is a network identifier that

- represents a single VLAN or a range of VLAN tags,
- can be grouped with other VLAN tag objects to create tag groups, and

VLAN tag usage

You can use VLAN tag objects and groups in various places in the system's web interface, such as rules and event searches. For example, you could write an access control rule that applies only to a specific VLAN.

Create a VLAN tag object

Use this task when you need to add or manage VLAN tag objects in your Secure Firewall Management Center. VLAN tag objects are referenced in access control and other policies to match specific VLAN tags or ranges.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VLAN Tag**.

Step 2 Choose **Add Object** from the **Add VLAN Tag** drop-down list.

Step 3 Enter a **Name**.

Step 4 Enter a **Description**.

Step 5 Enter a value in the **VLAN Tag** field. Use a hyphen to specify a range of VLAN tags.

Step 6 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see Allow object overrides, on page 2344.
- If you want to add override values to this object, expand the Override section and click **Add**; see Add object overrides, on page 2344.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes; see Deploy configuration changes, on page 135.

VPN

You can use the following VPN objects on Firewall Threat Defense devices. To use these objects, you must have Admin privileges, and your Smart License account must satisfy export controls. You can configure these objects in leaf domains only.

Certificate map objects

A certificate map object is a configuration element that

- contains a named set of certificate matching rules,
- associates a received certificate with a remote access VPN connection profile, and
- matches rules in priority order, ending when the first rule results in a match.

Certificate map object reference information

Remote access VPN policies use certificate map objects to map certificates to connection profiles. If a received certificate matches the rules in a certificate map, the system associates the connection with the specified profile.

Both certificate map objects and connection profiles are components of a remote access VPN policy.

- The rules are matched in the order shown in the UI.
- Matching ends when the first rule within the certificate map object results in a match.

Navigation path for certificate map objects:

- **Objects** > **Object Management** > **VPN** > **Certificate Map**

Fields in certificate map objects:

- **Name**: Identifies this object so it can be referred to from other configurations, such as remote access VPN.
- **Mapping criteria**: Specifies the contents of the certificate to evaluate. If the certificate satisfies these rules, the user is mapped to the connection profile containing this object.
  - **Field**: Select the field for the matching rule according to the subject or issuer of the client certificate.

    If you set the **Field** to *Alternative Subject* or *Extended Key Usage*, the component remains fixed as *Whole Field*.
  - **Component**: Select the component of the client certificate to use for the matching rule.

Note **SER (Serial Number) component**: Ensure you specify the serial number for the subject field. The certificate map only matches with a serial number attribute in the subject name.

  - **Operator**: Select the operator for the matching rule:
    - Equals: The certificate component must match the entered value. If they do not match exactly, the connection is denied.
    - Contains: The certificate component must contain the entered value. If the component does not contain the value, the connection is denied.

- Does not equal: The certificate component cannot equal the entered value. For example, for a selected certificate component of country and an entered value of US, if the client country value equals US, then the connection is denied.
- Does not contain: The certificate component cannot contain the entered value. For example, for a selected certificate component of country and an entered value of US, if the client country value contains US, the connection is denied.

- **Value**: The value of the matching rule. The value entered is associated with the selected component and operator.

Related Topics

Configure Certificate Maps, on page 1460

Secure Client custom attributes objects

Custom attributes objects enable Secure Client (formerly AnyConnect) to configure features such as Per App VPN, allow or defer upgrade, and dynamic split tunneling. You define the attribute type, then assign one or more named values for this type. In Secure Firewall Management Center, you create custom attributes objects, add them to a group policy, and associate the policy with a remote access VPN to enable features for VPN clients.

Supported features using custom attributes objects

Firewall Threat Defense supports these features using custom attribute objects:

- **Per App VPN**—You can specify which applications may use the VPN tunnel. The system identifies these apps and tunnels only the allowed applications.
- **Allow or defer upgrade**—You can delay downloading Secure Client updates. When a client update becomes available, you can prompt users to upgrade or defer the update.
- **Dynamic Split Tunneling**—You can configure policies to selectively include or exclude IP addresses or networks from the VPN tunnel. Create a custom attribute and add it to a group policy to achieve this.

For step-by-step instructions to configure Secure Client custom attributes, see Configure custom attributes for Secure Client, on page 2458.

For details about the specific custom attributes to configure for a feature, see the *Cisco Secure Client (including AnyConnect) Administrator Guide* for the Secure Client release you are using.

Configure custom attributes for Secure Client

Use this task when you need to configure custom attributes for Secure Client clients, such as Per App VPN, update deferment, or dynamic split tunneling, in Secure Firewall Management Center.

This is relevant for environments where device management and application-specific VPN rules are required, and when deploying secure client features that depend on custom attribute objects.

Applicable when integrating MDM-enrolled devices and advanced VPN features.

Before you begin

Ensure that you have done these steps before adding a custom attribute object for Per App VPN:

- Per App VPN must be properly configured via MDM and each device must be enrolled to the MDM server.
- Create a base64 encoded string for each app using the Cisco Secure Client Enterprise Application Selector Tool.
  1. Download the Cisco Secure Client Enterprise Application Selector Tool from here.
  2. Open the Application Selection Tool and select the mobile platform from the drop-down menu located on the upper left.
  3. Add rule by entering friendly name and App ID; the other fields are optional.
  4. On the menu bar, click **Policy**. The encoded base64 rule appears.
  5. Select and copy the policy string, and save it to use later when you create the Secure Client Custom Attributes object.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **Custom Attribute**.

Step 2 Click **Secure Client Custom Attribute**.

Step 3 Enter a **Name** and optionally a **Description** for the attribute.

Step 4 Select an attribute from the **Secure Client Attribute** drop-down list:

- **Per App VPN**—Select this option and specify the base64 encoded string in the **Attribute Value** box.
- **Allow Defer Update**—Select one of these options and specify the required information to allow or defer Secure Client update:
  - **Show the prompt until user takes action**—Display the prompt to the VPN user until the user chooses to allow or defer the VPN client update.
  - **Show the prompt until times out**—Choose this option to display the prompt for a specified duration and specify the duration in the **Timeout** box.
  - **Do not show the prompt and take automatic action**—Choose this option to automatically allow or defer the VPN update.
  - **Default Action**—Select the default action to be taken when the user does not respond, or when you want to configure an automatic action without the user's intervention. You can choose to update the Secure Client or postpone the update.
  - **Minimum Version**—Specify the minimum Secure Client version to be present on the client system to allow or defer the update.
- **Dynamic Split Tunneling**—Select this option to include or exclude IP addresses or networks from the VPN tunnel.
  - **Include domains**—Specify domain names that will be included in the remote access VPN tunnel.
  - **Exclude domains**—Specify domain names that will be excluded from the remote access VPN tunnel.

Step 5 Select the **Allow Overrides** check box to enable object overrides.

Step 6 Click **Save**.
The custom attributes object is added to the list.

What to do next

Associate the custom attributes with a group policy. See Add custom attributes to your group policy, on page 2460.

Add custom attributes to your group policy

Add custom attributes to a group policy to enable their use with remote access VPN connections. You can assign advanced VPN features to users based on their group policy membership.

To use Secure Client custom attributes with remote access VPN connections, you must associate them with the appropriate group policy. This enables you to offer advanced VPN customization to users based on their group policy membership.

Procedure

Step 1 Select **Objects** > **Object Management** > **VPN** > **Group Policy**.

Step 2 Add a new group policy or edit an existing group policy.

Step 3 Click **Secure Client** > **Custom Attributes**.

Step 4 Click **Add**.

Step 5 Select the **Secure Client Attribute**: Per App VPN, Allow Defer Update, or Dynamic Split Tunneling.

Step 6 Select a **Custom Attribute Object** from the list.

Note Click Add (+) to create a new custom attribute object for the selected Secure Client attribute. You can also create a custom attribute object at **Objects** > **Object Management** > **VPN** > **Custom Attribute**. See Configure custom attributes for Secure Client, on page 2458.

Step 7 Click **Add** to save the attributes to the group policy, and then click **Save** to save the changes to the group policy.

Related Topics

Group policy options for Secure Client, on page 2464

Firewall Threat Defense group policy objects

A group policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. For example, in the group policy object, you configure general attributes such as addresses, protocols, and connection settings.

Group policy object assignment and licensing

The group policy applied to a user is determined when the VPN tunnel is established. The RADIUS authorization server assigns the group policy, or it is obtained from the current connection profile.

Note There is no group policy attribute inheritance on the Firewall Threat Defense. A group policy object is used, in its entirety, for a user. The group policy object identified by the AAA server upon login is used, or, if that is not specified, the default group policy configured for the VPN connection is used. The provided default group policy can be set to your default values, but will only be used if it is assigned to a connection profile and no other group policy has been identified for the user.

To use group objects, you must have one of these Secure Client licenses associated with your Smart License account with Export-Controlled Features enabled:

- Secure Client VPN Only
- Secure Client Advantage
- Secure Client Premier

Configure a group policy object

Group policy objects are used to manage and enforce security and access policies for remote access VPN connections.

See Firewall Threat Defense group policy objects, on page 2460.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **Group Policy**.

Previously configured policies are listed including the system default. Depending on your level of access, you may edit, view, or delete a group policy.

Step 2 Click **Add Group Policy** or choose a current policy to edit.

Step 3 Enter a **Name** and optionally a **Description** for this policy.

The name can be up to 64 characters. Spaces are allowed. The description can be up to 1,024 characters.

Step 4 Specify the **General** parameters for this Group Policy as described in Group policy general options, on page 2462.

Step 5 Specify the **Secure Client** parameters for this Group Policy as described in Group policy options for Secure Client, on page 2464.

Step 6 Specify the **Advanced** parameters for this Group Policy as described in Advanced group policy option fields and values, on page 2467.

Step 7 Click **Save**.
The new Group Policy is added to the list.

What to do next

Add the group policy object to a remote access VPN connection profile.

Group policy general options

This topic describes the general options available when configuring a group policy, including navigation, VPN protocol selection, IP address pool assignment, banner configuration, DNS/WINS settings and split tunneling options.

Navigation path

Objects > **Object Management** > **VPN** > **Group Policy**, click **Add Group Policy** or choose an existing policy to edit, then select the **General** tab.

VPN protocols fields

Specify the types of Remote Access VPN tunnels (**SSL** or **IPsec IKEv2**) you want to apply for this group policy.

IP address pools

- Specifies the IPv4 address assignment based on address pools designated for user groups in Remote Access VPN.
- You can assign IP addresses from specific pools for identified user groups using RADIUS/ISE for authorization.
- You can enforce policy for users or user groups in non-identity-aware systems by configuring the Group Policy as the RADIUS Authorization attribute (GroupPolicy/Class).

Example: Select a specific address pool for contractors and enforce policy for restricted access to the internal network using those addresses.

The Firewall Threat Defense device assigns IPv4 address pools to the clients in this order:

1. RADIUS attribute for IPv4Address Pool
2. RADIUS attribute for Group Policy
3. Address Pool in Group Policy mapped to a Connection Profile
4. IPv4Address Pool in Connection Profile

Limitations:

- IPv6 address pool is not supported.
- A maximum of six IPv4 address pools can be configured in a Group Policy.
- Deployment failures may occur when address pools in use are modified. Before making any changes to the address pools, you must log off all users.
- If you rename address pools or configure overlapping address pools, deployment may fail. To address this, first remove the old address pool, then deploy the changed address pool.

  Troubleshooting commands :

- `show ip local pool <address-pool-name>`
- `show vpn-sessiondb detail anyconnect`
- `vpn-sessiondb loggoff all noconfirm`

Banner fields

Specifies the banner text to present to users at login. You can enter up to 491 characters in the banner. By default, no value is configured. The IPsec VPN client supports full HTML for the banner, however, the Secure Client supports only partial HTML. To ensure that the banner displays properly to remote users, use the /n tag for IPsec clients and the <BR> tag for SSL clients.

DNS/WINS fields

Domain Naming System (DNS) and Windows Internet Naming System (WINS) servers. Used for Secure Client name resolution.

- **Primary DNS Server** and **Secondary DNS Server**—Choose or create a Network Object which defines the IPv4 or IPv6 addresses of the DNS servers you want this group to use.
- **Primary WINS Server** and **Secondary WINS Server**—Choose or create a Network Object containing the IP addresses of the WINS servers you want this group to use.
- **DHCP Network Scope**—Choose or create a Network Object containing a routable IPv4 address on the same SUBNET as the desired pool, but not within the pool. The DHCP server determines which SUBNET this IP address belongs to and assigns an IP address from that pool. If not set properly, deployment of the VPN policy fails.

  If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same SUBNET identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server for this specific group.

  If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address.

  We recommend using the IP address of an interface whenever possible for routing purposes. For example, if the pool is 10.100.10.2-10.100.10.254, and the interface address is 10.100.10.1/24, use 10.100.10.1 as the DHCP scope. Do not use the network number. Use DHCP only for IPv4 addressing. If the address you choose is not an interface address, you might need to create a static route for the scope address.

  LINK-SELECTION (RFC 3527) and SUBNET-SELECTION (RFC 3011) are currently not supported.
- **Default Domain**—Name of the default domain. Specify a top-level domain, for example, example.com.

Split tunneling fields

Split tunneling directs some network traffic through the VPN tunnel (encrypted) and the remaining network traffic outside the VPN tunnel (unencrypted or “in the clear”).

- **IPv4 Split Tunneling / IPv6 Split Tunneling**—By default, split tunneling is not enabled. For both IPv4 and IPv6 it is set to **Allow all traffic over tunnel**. Left as is, all traffic from the endpoint goes over the VPN connection.

To configure split tunneling, choose the **Tunnel networks specified below** or **Exclude networks specified below** policy, and then configure an access control list for that policy.

- **Split Tunnel Network List Type**—Choose the type of Access List you are using. Then choose or create a **Standard Access List** or **Extended Access List**. See Access lists, on page 2351 for details.

Note From Version 7.4, the **Standard Access List** option is disabled by default. Use the **Extended Access List** option to add an access list.

- **DNS Request Split Tunneling**—Also known as Split DNS. Configure the DNS behavior expected in your environment.

  By default, split DNS is not enabled and set to **Send DNS request as per split tunnel policy**. Choosing **Always send DNS request over tunnel** forces all DNS requests to be sent over the tunnel to the private network.

  To configure split DNS, choose **Send only specified domains over tunnel**, and enter the list of domain names in the **Domain List** field. These requests are resolved through the split tunnel to the private network. All other names are resolved using the public DNS server. Enter up to 10 entries in the list of domains, separated by commas. The entire string can be no longer than 491 characters.

Related Topics

Configure a group policy object, on page 2461

Group policy options for Secure Client

This topic lists and describes the specifications and configuration fields for group policy Secure Client VPN operation. This includes navigation steps, profile fields, management profile settings, client modules, SSL settings, connection options, and custom attributes.

These specifications apply to the operation of the Secure Client VPN.

Navigation

Objects > **Object Management** > **VPN** > **Group Policy**. Click **Add Group Policy** or choose a current policy to edit., and then select the **Secure Client** tab.

Profile fields

Profile—Choose or create a file object containing the Secure Client Profile. See File objects, on page 2474 for object creation details.

The Secure Client Profile is a group of configuration parameters stored in an XML file. The Secure Client software uses it to configure the connection entries that appear in the client's user interface. These parameters (XML tags) also configure settings to enable more Secure Client features.

Use the GUI-based Secure Client Profile Editor, an independent configuration tool, to create the Secure Client Profile. See the *Secure Client Profile Editor* chapter in the appropriate release of the Cisco Secure Client (including AnyConnect) Administrator Guide for details.

Management profile fields

Management VPN Tunnel—Provides always-on connectivity to the corporate network when the endpoint is powered up, regardless of the user's VPN connection status.

Management VPN Profile—The Management Profile file contains settings for enabling and establishing Management VPN Tunnel on endpoint.

The Standalone Management VPN Tunnel profile editor can be used to create a new profile file or modify an existing file. You can download the profile editor from Cisco Software Download Center.

For more information about adding a profile file, see File objects, on page 2474.

Client modules fields

Cisco Secure Client VPN Only offers enhanced security through various built-in modules. These modules provide services such as web security, network visibility into endpoint flows, and off-network roaming protection. Each module includes a custom client profile.

The following Secure Client modules are optional and you can configure these modules to be downloaded when a VPN user downloads Secure Client:

- **AMP Enabler**—Deploys advanced malware protection (AMP) for endpoints.
- **DART**—Captures a snapshot of system logs and other diagnostic information, which can be sent to the Cisco TAC for troubleshooting.
- **ISE Posture**—Uses the OPSWAT library to perform posture checks to assess an endpoint's compliance.
- **Network Access Manager**—Provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks.
- **Network Visibility**—Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics.
- **Start Before Login**—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting Secure Client before the Windows login dialog box appears.
- **Umbrella Roaming Security**—Provides DNS-layer security when no VPN is active.
- **Web Security**—Enforces web security policies and blocks malicious content.

Click **Add** and select the following for each client module:

- **Client Module**—Select the Secure Client module from the list.
- **Profile to download**—Choose or create a file object containing the Secure Client Profile. See File objects, on page 2474 for object creation details.
- **Enable module download**—Select to enable endpoints to download the client module along with the profile. If not selected, the endpoints can download only the client profile.

Use the GUI-based Secure Client Profile Editor, an independent configuration tool to create a client profile for each module. Download the Secure Client Profile Editor from Cisco Software Download Center. See the *Secure Client Profile Editor* chapter in the appropriate release of the Cisco Secure Client (including AnyConnect) for details.

SSL settings fields

- **SSL Compression**—Determines if data compression is enabled, and specifies the method to use (Deflate or LZS). SSL Compression is disabled by default.

  Data compression speeds up transmission rates, but also increases the memory requirement and CPU usage for each user session. Thereby, decreasing the overall throughput of the security appliance.

- **DTLS Compression**—Specifies whether to compress Datagram Transport Layer Security (DTLS) connections for this group using LZS. DTLS Compression is disabled by default.

- **MTU Size**—TSpecifies the maximum transmission unit (MTU) size for SSL VPN connections established by Cisco Secure Client VPN Only. The default is 1406 bytes; the valid range is 576 to 1462 bytes.

  - **Ignore DF Bit**—Whether to ignore the Don't Fragment (DF) bit in packets that need fragmentation. Allows the forced fragmentation of packets that have the DF bit set, allowing them to pass through the tunnel.

Connection settings fields

- **Enable Keepalive Messages between Secure Client and VPN gateway** and its **Interval** setting.—Determines whether peers exchange keepalive messages to demonstrate availability for sending and receiving data in the tunnel. By default, this feature is enabled. Keepalive messages are transmitted at set intervals. If enabled, enter the time interval (in seconds) that the remote client waits between sending IKE keepalive packets. The default interval is 20 seconds, the valid range is 15 to 600 seconds.

- **Enable Dead Peer Detection** and its **Interval** settings.—Dead Peer Detection (DPD) ensures that the VPN secure gateway or client quickly detects when the peer is no longer responding and the connection has failed. Default is enabled for both the gateway and the client. DPD messages transmit at set intervals. If enabled, enter the time interval (in seconds) that the remote client waits between sending DPD messages. The default interval is 30 seconds, the valid range is 5 to 3600 seconds.

- **Enable Client Bypass Protocol**—Allows you to configure how the secure gateway manages IPv4 traffic (when it is expecting only IPv6 traffic), or how it manages IPv6 traffic (when it is expecting only IPv4 traffic).

  After the Secure Clientconnects to the headend, the headend assigns the VPN connection an IPv4 address, an IPv6 address, or both. If the headend assigns only one type of address, you can configure the Client Bypass Protocol to either drop network traffic for which an IP address was not assigned (default, disabled, not checked), or allow that traffic to bypass the headend and be sent from the client unencrypted (“in the clear”; enabled, checked).

  For example, if the secure gateway assigns only an IPv4 address to the Secure Client connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

- **SSL rekey**—Enables the client to rekey the connection, renegotiating the crypto keys and initialization vectors, increasing the security of the connection. This is disabled by default. When enabled, the renegotiation can be done at a specified interval and rekey the existing tunnel or create a new tunnel by setting the following fields:

  - **Method**—Available when SSL rekey is enabled. Create a **New Tunnel** (default), or renegotiate, the **Existing Tunnel**'s specifications.

- **Interval**—Available when SSL rekey is enabled. Set to a default of 4 minutes with a range of 4-10080 minutes (1 week).

- **Client Firewall Rules**—Use the Client Firewall Rules to configure firewall settings for the VPN client's platform. Rules are based on criteria such as source address, destination address, and protocol. Extended Access Control List building block objects are used to define the traffic filter criteria. Choose or create an Extended ACL for this group policy. Define a **Private Network Rule** to control data flowing to the private network, a **Public Network Rule** to control data flowing "in the clear", outside of the established VPN tunnel, or both.



Note Ensure that the ACL contains only TCP/UDP/ICMP/IP ports and source network as any, any-ipv4 or any-ipv6.

Only VPN clients running Microsoft Windows can use these firewall settings.

Custom attributes fields

Custom attributes are used by the Secure Client to configure features such as Per App VPN, Allow or defer upgrade, and Dynamic split tunneling. Click **Add** to add custom attributes to the group policy.

1. Select the **Secure Client Attrinute**: Per App VPN, Allow Defer Update, or Dynamic Split Tunneling.
2. Select a **Custom Attribute Object** from the list.



Note Click Add (+) to create a new custom attribute object for the selected Secure Client attribute. You can also create a custom attribute object at **Objects** > **Object Management** > **VPN** > **Custom Attribute**. See Configure custom attributes for Secure Client, on page 2458.

3. Click **Add** to save the attributes to the group policy, and then click **Save** to save the changes to the group policy.

Related Topics

Configure a group policy object, on page 2461

Advanced group policy option fields and values

The advanced group policy includes options and attributes for configuring VPN access and session behavior. This reference describes where to locate advanced settings, outlines attributes related to traffic filtering, and summarizes session control fields and their allowed values.

Navigation path

Objects > **Object Management** > **VPN** > **Group Policy**. Click **Add Group Policy** or choose a current policy to edit. Then select the **Advanced** tab.

Traffic filter fields

- **Access List Filter**—Filters consist of rules that determine whether to allow or block tunneled data packets coming through the VPN connection. You set rules using criteria such as source address, destination address, and protocol.

  The VPN filter applies only to initial connections. It does not control secondary connections, such as a SIP media connection, that are opened during application inspection.

  Use Extended Access Control List building block objects to define traffic filter criteria. Choose or create an Extended ACL for this group policy.

- **Restrict VPN to VLAN**—Also called "VLAN mapping," this parameter specifies the egress VLAN interface for sessions to which this group policy applies. The ASA forwards all group traffic to the VLAN you select.

  Use this attribute to assign a VLAN to the group policy to simplify access control. You can assign a value to this attribute instead of using ACLs to filter session traffic. The drop-down list shows only the VLANs that are configured in this ASA. Allowed values range from 1 to 4094. The default value is Unrestricted.

Session settings fields

- **Access Hours**—Choose or create a time range object. This object specifies the range of time this group policy is available to be applied to a remote access user. See Time ranges, on page 2435 for details.
- **Simultaneous Logins Per User**—Specifies the maximum number of simultaneous logins allowed for a user. The default value is 3. If the minimum value is set to 0, logins are disabled and users cannot access the VPN. If you allow several simultaneous connections, security may be compromised and performance reduced.
- **Maximum Connection Time / Alert Interval**—Specifies the maximum user connection time in minutes. At the end of this time, the system disconnects the user. The minimum is 1 minute). The Alert interval lets you display a message to the user before the maximum connection time is reached.
- **Idle Timeout / Alert Interval**—Specifies this user's idle timeout period in minutes. If there is no communication activity on the user connection in this period, the system stops the connection. The minimum time is 1 minute. The default is 30 minutes. The Alert interval lets you display a message to the user before the idle time is reached.

Related Topics

Configure a group policy object, on page 2461

Firewall Threat Defense IPsec proposals

IPsec Proposals (or Transform Sets) are used when configuring VPN topologies. During the IPsec security association negotiation with ISAKMP, both peers must agree on the same proposal to protect the data flow.

IPsec proposal types and negotiation

IPsec proposals are categorized based on the IKE version: IKEv1 or IKEv2.

- For an IKEv1 IPsec proposal (Transform Set), select the mode for IPsec operation and define the required encryption and authentication types. Select only one option for each algorithm. To support multiple combinations in a VPN, create multiple IKEv1 IPsec proposal objects.

- For an IKEv2 IPsec proposal, select all encryption and hash algorithms allowed in the VPN. During IKEv2 negotiations, the peers negotiate and use the most appropriate options supported by both devices.

Both IKEv1 and IKEv2 IPsec proposals use the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and antireplay services. ESP uses IP protocol type 50.

Note We recommend that you use both encryption and authentication on IPsec tunnels.

Configure an IKEv1 IPsec proposal object

Use this task when you need to create or modify IKEv1 IPsec proposal objects in Secure Firewall Management Center. Proposal objects define the cryptographic parameters for VPN connections and are required for establishing secure tunnels between firewalls or security gateways.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **IKEv1 IPsec Proposal** and then **VPN** > **IPsec IKev1 Proposal** from the table of contents.

Previously configured Proposals are listed including system defined defaults. Depending on your level of access, you may **Edit** ( ), **View** ( ), or **Delete** ( ) a Proposal.

Step 2 Choose **Add IPsec IKEv1 Proposal** to create a new Proposal.

Step 3 Enter a **Name** for this proposal.

The name of the policy object can be up to 128 characters.

Step 4 Enter a **Description** for this Proposal.

Provide a description of the policy object that is up to 1024 characters.

Step 5 Choose the **ESP Encryption** method. The Encapsulating Security Protocol (ESP) encryption algorithm for this Proposal.

For IKEv1, select one of the options. When deciding which encryption and Hash Algorithms to use for the IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN. For a full explanation of the options, see Decide encryption algorithms for VPN policies, on page 1334.

Step 6 Select an option for **ESP Hash**.

For a full explanation of the options, see Decide which hash algorithms to use, on page 1335.

Step 7 Click **Save**
The new Proposal is added to the list.

Configure an IKEv2 IPsec proposal object

Use this task when you need to define or update the cryptographic settings for IKEv2 IPsec VPN tunnels on your Secure Firewall Management Center. This is relevant when setting up new VPNs or adjusting security policies to meet organizational requirements.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **IKEv2 IPsec Proposal** from the table of contents.

Previously configured proposals are listed including system defined defaults. Depending on your level of access, you may **Edit** ( ), **View** ( ), or **Delete** ( ) a Proposal.

Step 2 Choose **Add IKEv2 IPsec Proposal** to create a new proposal.

Step 3 Enter a **Name** for this proposal.

The policy object name can be up to 128 characters.

Step 4 Enter a **Description** for this proposal.

The policy object description can contain up to 1,024 characters.

Step 5 Click **ESP Hash**, the hash or integrity algorithm to use in the proposal for authentication.

Note Firewall Threat Defense does not support IPSec tunnels with NULL encryption. Make sure that you do not choose NULL encryption for IPSec IKEv2 proposal.

For IKEv2, select all the options you want to support for **ESP Hash**. For a full explanation of the options, see Decide which hash algorithms to use, on page 1335.

Step 6 Click **ESP Encryption** . Select the Encapsulating Security Protocol (ESP) encryption algorithm for this proposal.

For IKEv2, click Select to open a dialog box where you can select all of the options you want to support. When deciding which encryption and hash algorithms to use for the IPsec proposal, choose only algorithms supported by the devices in the VPN. For a full explanation of the options, see Decide encryption algorithms for VPN policies, on page 1334.

Step 7 Click **Save**.
The new proposal is added to the list.

IKE policies

A IKE policy is a key management policy that

- defines security parameters and algorithms used to authenticate IPsec peers,
- negotiates and distributes IPsec encryption keys, and

- establishes secure communications by negotiating security associations in IPsec VPNs.
- The Internet Key Exchange (IKE) protocol manages authentication, key negotiation, and automatic establishment of IPsec security associations (SAs).
- IKE negotiation occurs in two phases:
  - Phase 1 negotiates a security association between two IKE peers, enabling secure communication in Phase 2.
  - Phase 2 establishes SAs for applications, such as IPsec.
- Both phases use proposals to negotiate connections. An IKE proposal is a set of algorithms that two peers use to secure negotiation.
- IKE negotiation starts with peers agreeing on a shared IKE policy, which defines the security parameters to protect future negotiations.
- For IKEv1, proposals include a single set of algorithms and a modulus group; multiple, prioritized policies can be created to match remote peers.
- For IKEv2, you can select multiple algorithms and modulus groups in one policy.
- Peers choose proposals during Phase 1 negotiation, enabling creation of a single IKE proposal but consideration of multiple prioritized options.
- For IKEv2, the policy object does not specify authentication; other policies must define authentication requirements.
- An IKE policy is required when you configure a site-to-site IPsec VPN. .

Configure an IKEv1 policy object

Use the IKEv1 Policy page to create, edit, or delete IKEv1 policy objects. These policy objects specify settings such as encryption, authentication, priority, and other parameters necessary for establishing secure VPN tunnels.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **IKEv1 Policy** from the table of contents.

Previously configured policies are listed including system-defined defaults. Depending on your level of access, you may **Edit** ( ), **View** ( ), or **Delete** ( ) a proposal.

Step 2 (Optional) Click **Add IKEv1 Policy** to create a new policy object. Then, enter a **Name** for this policy. The policy object name can be up to 128 characters. Optionally, you can enter the description. The policy object description can contain up to 1,024 characters.

Step 3 Enter the **Priority** value of the IKE policy.

The priority value determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, it tries to use the parameters defined in the next lowest priority. Valid values range from 1 to 65,535. The lower the number, the higher the priority. If you leave this field blank,

Management Center assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Step 4 Select the **Encryption** method.

When deciding which encryption and Hash Algorithms to use for the IKEv1 policy, your choice is limited to algorithms supported by the peer devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. For IKEv1, select one of the options. For a full explanation of the options, see Decide encryption algorithms for VPN policies, on page 1334.

Step 5 Select the **Hash** Algorithm that creates a Message Digest, which is used to ensure message integrity.

When deciding which encryption and Hash Algorithms to use for the IKEv1 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. For a full explanation of the options, see Decide which hash algorithms to use, on page 1335.

Step 6 Select the **Diffie-Hellman Group**.

The Diffie-Hellman group to use for encryption. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select the group that you want to allow in the VPN. For a full explanation of the options, see Decide which Diffie-Hellman modulus group to use, on page 1336.

Step 7 Enter the **Lifetime** of the security association (SA), in seconds. You can specify a value from 120 to 2,147,483,647 seconds. The default is 86400.

When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, the shorter the lifetime (up to a point), the more secure your IKE negotiations. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.

Step 8 Select the **Authentication Method** to use between the two peers.

- **Preshared Key**—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If one of the participating peers is not configured with the same preshared key, the IKE SA cannot be established.
- **Certificate**—When you use Certificates as the authentication method for VPN connections, peers obtain digital certificates from a CA server in your PKI infrastructure, and trade them to authenticate each other.

Note In a VPN topology that supports IKEv1, the **Authentication Method** specified in the chosen IKEv1 Policy object becomes the default in the IKEv1 **Authentication Type** setting. These values must match, otherwise, your configuration will error.

Step 9 Click **Save**
The new IKEv1 policy is added to the list.

Configure an IKEv2 policy object

Use the IKEv2 policy dialog box to create, delete, and edit an IKEv2 policy object. These policy objects contain the parameters required for IKEv2 policies.

Procedure

Step 1 Choose **Objects** > **Object Management** > **VPN** > **IKEv2 Policy** from the table of contents.

Previously configured policies are listed including system defined defaults. Depending on your level of access, you may **Edit** ( ), **View** ( ), or **Delete** ( ) a policy.

Step 2 Click **Add IKEv2 Policy** to create a new policy. Then, enter a **Name** for this policy. The policy object name can be up to 128 characters. Optionally, enter the description. The description can be up to 1024 characters.

Step 3 Enter the **Priority**.

The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, it tries to use the parameters defined in the next lowest priority policy. Valid values range from 1 to 65535. The lower the number, the higher the priority. If you leave this field blank, Management Center assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Step 4 Enter the **Lifetime** of the security association (SA), in seconds. You can specify a value from 120 to 2,147,483,647 seconds. The default is 86400.

When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, the shorter the lifetime (up to a point), the more secure your IKE negotiations. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.

Step 5 Select algorithms for these methods:

a. Click **Integrity Algorithms** portion of the Hash Algorithm used in the IKE policy. The Hash Algorithm creates a Message Digest, which is used to ensure message integrity.

When deciding which encryption and Hash Algorithms to use for the IKEv2 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. Select all the algorithms that you want to allow in the VPN.For a full explanation of the options, see Decide which hash algorithms to use, on page 1335.

b. Click **Encryption Algorithm** used to establish the Phase 1 SA for protecting Phase 2 negotiations.

When deciding which encryption and Hash Algorithms to use for the IKEv2 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. Select all the algorithms that you want to allow in the VPN. For a full explanation of the options, see Decide encryption algorithms for VPN policies, on page 1334.

c. Click **PRF Algorithm**.

The pseudorandom function (PRF) portion of the Hash Algorithm used in the IKE policy. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all of the algorithms that you want to allow in the VPN. For a full explanation of the options, see Decide which hash algorithms to use, on page 1335.

d. Click **Diffie-Hellman Group** for encryption.

A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select the groups that you want to allow in the VPN. For a full explanation of the options, see Decide which Diffie-Hellman modulus group to use, on page 1336.

Step 6 Click **Save**.
If a valid combination of choices has been selected the new IKEv2 policy is added to the list. If not, errors are displayed and you must make changes accordingly to successfully save this policy.

Secure client customizations

A Secure Client customization is a configuration object that

- represents files used to customize Secure Client,
- enables deployment of customizations to the VPN headend, and
- allows threat defense to distribute customizations to endpoints when users connect from Secure Client.

Supported secure client customizations

Secure Client customization objects represent files used to modify Secure Client. Secure Client supports these types of customizations:

- GUI text and messages
- Icons and images
- Scripts
- Binaries
- Custom installer transforms
- Localized installer transforms

For more information about configuring Secure Client customizations, see Customize Cisco Secure Client, on page 1472.

File objects

File objects are configuration element that

- represent files used in configurations, typically for remote access VPN policies
- can contain Secure Client Profile and Secure Client Image files, and
- are created, edited, and managed through the Add and Edit File Object dialog boxes.

File object management and usage

File objects are used to manage files for remote access VPN policies and are associated with profiles and images for deployment to endpoints.

File objects can be created and edited using the Add and Edit File Object dialog boxes. They are used in configurations for remote access VPN policies and can contain Secure Client Profile and Secure Client Image files.

Create profiles for each AnyConnect module and Secure Client Management VPN using independent profile editors. Deploy these profiles to meet administrator-defined end user requirements and authentication policies on endpoints Secure Client only. This makes preconfigured network profiles available to end users

When you create a file object, the Firewall Management Center makes a copy of the file in its repository. When you back up the database, these files are included. If you restore the database, the files are restored as well. To use a file in a file object, upload it through the management center interface, not directly to the file repository.

When you deploy configurations that specify a file object, the associated file is downloaded to the device in the appropriate directory.

You can take these actions for each file object:

- **Download**: Download the Secure Client file.
- **Edit**: Modify the file object details.
- **Delete**: Delete the Secure Client file object. When you delete a file object, the associated file is not deleted from the file repository, only the object is deleted.

Navigation path

Objects > **Object Management** > **VPN** > **Secure Client File**.

Fields

- **Name**: Enter the name of the file to identify the file object; you can add up to 128 characters.
- **File Name**: Click **Browse** to select the file. The file name and full path of the file are added when you select the file.
- **File Type**: Choose the file type corresponding to the file you have selected. These file types are available:

File Types	Details
Secure Client Image	Select when you add the Secure Client image you have downloaded from the Cisco Software Download Center. You can associate any new or additional Secure Client images to the remote access VPN policy. You can also remove unsupported or end-of-life client packages that are no longer required.
Secure Client VPN Profile	Choose for the Secure Client VPN profile file. The profile file is created using the GUI-based Secure Client Profile Editor, an independent configuration tool. See the *Secure Client Profile Editor* chapter in the appropriate release of the Cisco Secure Client (including AnyConnect) User Guide for details.

File Types	Details
Secure Client Management VPN Profile	Select when you add a profile file for the Secure Client management VPN tunnel. Download the Secure Client **VPN Management Tunnel Standalone Profile Editor** from Cisco Software Download Center if you have not done already and create a profile with required settings for the Secure Client management VPN tunnel.
AMP Enabler Service Profile	The profile is used for the Secure Client The AMP Enabler and this profile are deployed to endpoints from Firewall Threat Defense when a user connects to the VPN using remote access.
Feedback Profile	You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and use.
ISE Posture Profile	Choose if you are adding a profile file for the Secure Client ISE Posture module.
NAM Service Profile	Configure and add the NAM profile file using the Network Access Manager profile editor.
Network Visibility Service Profile	Profile file for Secure Client Network Visibility module. You can create the profile using the NVM profile editor.
Umbrella Roaming Security Profile	You must select this file type if you are deploying the Umbrella Roaming Security module using the .json file created using the profile editor.
Web Security Service Profile	Select this option when you add a profile file for the Web security module.
HostScan Posture Package	Select when you add a Secure Firewall Posture Package file. This file is used while configuring a Dynamic Access Policy (DAP) to collect information about the operating system, anti-virus, anti-spyware, and firewall software installed on the endpoints.
Secure Client External Browser Package	For selecting an external browser package file for SAML single sign-on web authentication. You can add the package file when a new version of the external package file is available. For more information, see Configure AAA Settings for Remote Access VPN, on page 1439.
Description	Add an optional description.

Related Topics

Cisco Secure Client Image, on page 1457
Group policy options for Secure Client, on page 2464

History for object management

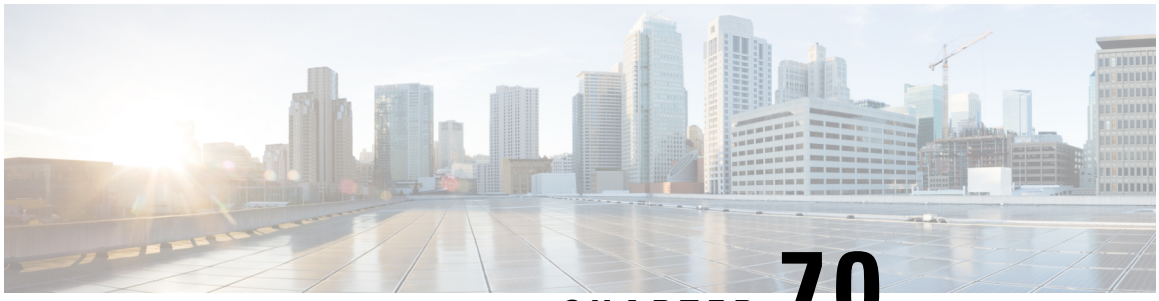
This reference provides a history of object management features, enhancements, and changes across releases, including details and supported platforms for each feature.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged ACL and AV ACL	7.4.1	Any	New/modified screens: **Objects** > > **Object Management** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Merge Downloadable ACL with Cisco AV Pair ACL** New CLI commands: • **sh run AAA-server AAA-server ISE-Server protocol RADIUS merge-dacl after-avpair** • **sh run AAA-server AAA-server ISE-Server protocol RADIUS merge-dacl before-avpair**
Secure Client Customization	Any	7.4	You can now customize Secure Client and deploy these customizations to the VPN headend. The threat defense distributes these customizations to the endpoint when an end user connects from the Secure Client.
IPv6 support for CRL and OCSP urls	Any	7.4	You can now configure IPv6 OCSP and CRL URLs.
Loopback and Management type interface group objects	Any	7.4	You can now create interface group objects that include only management-only interfaces or only loopback interfaces. You can then use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are supported for any feature that supports loopback interfaces. Note that DNS does not support management interfaces. New/Modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group**
Loopback interface support for AAA	Any	7.4	You can use a loopback interface group for configuring a RADIUS server. New/Modified screens: **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group**
Clone network and port objects	Any	7.4	You can now clone network and port objects. In the object manager (**Objects** > **Object Management**), click the new **Clone** icon next to a port or network object. You can then change the new object's properties and save it using a new name.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
DHCP IPv6 Pool	Any	7.3	The Firewall Threat Defense now supports a light DHCPv6 stateless server when using the DHCPv6 Prefix Delegation client. The Firewall Threat Defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to the Firewall Threat Defense. The Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. New/Modified screens: • **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **DHCP** • **Objects** > **Object Management** > **DHCP IPv6 Pool** New/Modified commands: **show ipv6 DHCP**
BFD Template	Any	7.3	In the previous releases, BFD was configurable on threat defense only through FlexConfig. FlexConfig no longer supports BFD configuration. You can now configure BFD policies for threat defense in the management center UI. Hence, the BFD Template object was introduced. New/modified screens: • **Devices** > **Device Management** > **Routing** > **BFD**. • **Objects** > **Object Management** > **BFD Template**
New Applications tab for policy based routing	Any	7.1	A new tab for selecting the applications for configuring direct internet access policy (policy based routing) was introduced in the extended access list object. New/Modified Screens: New option to select applications when configuring **Object** > **Object Management** > **Access List** > **Extended** page. Supported platforms: Secure Firewall Management Center
New Extended Community List object and	Any	7.1	Extended community list object was introduced to be used in policy list and route map objects. The extended community list object is applicable only for importing or exporting routes in BGP route leaking support for virtual routers. New/Modified Screens: New object for configuring policy list and route maps **Object** > **Object Management** > **Community list** > **Extended Community** page. Supported platforms: Secure Firewall Management Center

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Enhancements to Policy List object and Route Map object	Any	7.1	Options to select the newly introduced Extended Community List objects in policy list and route maps. New/Modified Screens: New options for configuring policy list and route maps **Object** > **Object Management** > **Policy List** > **Community rule** tab, and **Object** > **Object Management** > **Route Map** > **BGP** > **Community List** tab. Supported platforms: Secure Firewall Management Center
Time-based ACL support for Snort 3	Any	7.0	Time-based rules in access control and prefilter policies are supported in Snort 3 as well. Supported platforms: Firewall Threat Defense
EST for certificate enrollment	Any	7.0	Support for Enrollment over Secure Transport for certificate enrollment was provided. New/Modified Screens: New enrollment options when configuring **Objects** > **PKI** > **Cert Enrollment** > **CA Information** tab. Supported platforms: Secure Firewall Management Center
Support for EdDSA certificate type	Any	7.0	A new certificate key type- EdDSA was added with a key size of 256. New/Modified Screens: New certificate key options when configuring **Objects** > **PKI** > **Cert Enrollmet** > **Key** tab. Supported platforms: Secure Firewall Management Center
Restrictions on ciphers and key sizes	Any	7.0	Certificates having SHA-1 with RSA Encryption signature algorithm, and RSA key sizes smaller than 2048 bits are not supported. To override these restrictions on existing certificates, you can enable the weak-crypto option on Firewall Threat Defense. However, you cannot generate RSA keys with sizes smaller than 2048 bits. New/Modified Screens: New toggle button when configuring **Devices** > **Certificates**. Supported platforms: Secure Firewall Management Center
Security Intelligence feed options	Any	6.7	New update frequency options (5 and 15 minutes) for custom Security Intelligence feeds. Update frequencies of less than 30 minutes require an MD5 URL, to prevent unnecessary downloads if the feed has not changed. New/Modified Screens: New frequency choices when configuring **Security Intelligence** > **Network Lists and Feeds**. Supported platforms: Secure Firewall Management Center

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Bulk upload of objects using a comma-separated-values (csv) file	Any	6.7	Objects can be imported from a comma-separated-values file. Up to 1000 objects can be imported in one attempt. New/Modified Screens: The following object types have a new **Import Object** option in the **Add [Object Type]** drop-down list. • **Distinguished Name** > **Individual Objects** • **Network Object** • **Port** • **URL** • **VLAN Tag** Supported platforms: Secure Firewall Management Center
See the policies in which interface objects are used	Any	6.6	See the policies in which interface objects are used. New/Modified Screens: The **Interface** object page in **Object** > **Object management** has a new **Find** button. Supported platforms: Secure Firewall Management Center
Time zone objects introduced	Any	6.6	You can assign time zones to Firewall Threat Defense devices, for use when applying time-based policies. New/Modified Screens: New **Time Zone Object** in **Object** > **Object management**. Supported platforms: Secure Firewall Management Center
Time-based objects can now be used in access control and prefilter policies	Any	6.6	Use time range objects in conjunction with new time zone objects for applying time-based rules in access control and prefilter policies. You can specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic.
View Object Details from prefilter rule page	Any	6.6	Feature introduced: Option to view details for an object or object group when viewing prefilter rules. New options: Right-clicking a value in any of the following columns in the prefilter rule list offers options to view object details: Source Networks, Destination Networks, Source Port, Destination Port, and VLAN Tag. Supported platforms: Secure Firewall Management Center



CHAPTER 70

Certificates

- Requirements and prerequisites for certificates, on page 2481
- Secure Firewall Threat Defense VPN certificate guidelines and limitations, on page 2481
- Manage Firewall Threat Defense certificates, on page 2483
- Install a certificate using self-signed enrollment, on page 2486
- Install a certificate using EST enrollment, on page 2487
- Install a certificate using SCEP enrollment, on page 2487
- Install a certificate using manual enrollment, on page 2488
- Install a certificate using a PKCS12 file, on page 2489
- Troubleshoot Threat Defense certificates, on page 2490
- History for certificates, on page 2491

Requirements and prerequisites for certificates

This topic outlines the domain and role-based access requirements for certificate management.

Requirement	Supported values
Supported domains	Any
User roles	• Admin • Network Admin

Secure Firewall Threat Defense VPN certificate guidelines and limitations

Certificate enrollment guidelines

When a PKI enrollment object is associated with and then installed on a device, the certificate enrollment process starts immediately. The process is automatic for self-signed and SCEP enrollment types; it does not require any additional administrator's action. Manual certificate enrollment requires administrator's action.

- When a PKI enrollment object is associated with and then installed on a device, the certificate enrollment process starts immediately. The process is automatic for self-signed and SCEP enrollment types; it does not require any additional administrator's action. Manual certificate enrollment requires administrator's action.
- When importing identity certificates into Firewall Threat Defense devices, the expiration date of the certificate must not exceed February 6, 2106. Ensure that all certificates used within devices have expiration dates earlier to February 6, 2106 to avoid issues during certificate import or renewal.
- When the certificate enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your VPN Authentication Method.
- Firewall Threat Defense devices support certificate enrollment using Microsoft Certificate Authority(CA) Service, and CA Services provided on Cisco Adaptive Security Appliances(ASA) and Cisco IOS Router.
- Firewall Threat Defense devices cannot be configured as a certificate authority (CA).
- Ensure that only valid and properly functioning certificates are assigned to VPN or Remote Access VPN policies to prevent blocking deployments or causing validation errors. If a certificate is marked as failed but not referenced by any VPN policy, deployments will proceed with a warning rather than a failure. This practice helps maintain smooth deployment operations and avoids interruptions caused by certificate issues.

Guidelines for certificates and multitenancy

Firewall Threat Defense devices support certificate enrollment using Microsoft CA Service, as well as CA services provided by Cisco Adaptive Security Appliances and Cisco IOS Routers.

Supported certificate enrollment services:

Certificate enrollment domains

- Certificate enrollment can be done in a **child domain** or a **parent domain**.
- When enrollment is done from a **parent domain**, the certificate enrollment object must also be in the same domain.
- If the trustpoint on a device is overridden in the child domain, the overridden value will be deployed on the device.

Enrollment visibility and behavior in leaf domains

- When certificate enrollment is done on a device in a **leaf domain**, the enrollment will be visible to the parent domain or another child domain.
- Adding additional certificates in a leaf domain is possible.

Certificate enrollment restrictions and permissions

- Once a device has certificates enrolled in one domain, it will be allowed to be enrolled in any other domain. The certificates can be added in the other domain.

Device movement between domains

- When you move a device from one domain to another, the certificates also get moved accordingly. You will receive an alert to delete the enrollments on these devices.

Manage Firewall Threat Defense certificates

This task enables you to manage certificates on devices including viewing certificate status, enrolling new certificates, and performing certificate operations such as export and re-enrollment.

See PKI infrastructure and digital certificates, on page 1337 for an introduction to Digital Certificates.

See Certificate enrollment objects, on page 2400 for a description of the objects used to enroll and obtain certificates on managed devices.

Procedure

Step 1 Select **Devices** > **Certificates**.

You can see the following columns for each device listed on this screen:

- **Name**—Lists the devices that already have trustpoints associated with them. Expand the device to see the list of associated trustpoints.
- **Domain**—Displays the certificates that are enrolled in a specific domain.
- **Enrollment Type**—Displays the type of enrollment used for a trustpoint.
- **Status**—Provides the status of the **CA Certificate** and **Identity Certificate**. You can view the certificate contents, when `Available`, by clicking the magnifying glass.

  When you view the CA certificate information, you can view the hierarchy of all the certifying authorities, which issued your CA certificate. If the enrollment fails, click status to view the failure message.
- Click **Enable weak-crypto** on the right to enable weak cipher usage in certificates. When you click the toggle button, you get a warning to confirm before enabling weak ciphers. Click **Yes** to enable weak ciphers.

Note When a certificate enrollment fails due to weak cipher usage, you get a prompt to enable the weak cipher. You can choose to enable weak cipher when you need to use weak encryption.

- The additional column lists icons to perform the following tasks:
  - **Export Certificate**—Click to export and download a copy of the certificate. You can choose to export the PKCS12 (Complete Certificate Chain) or the PEM (Identity Certificate Only) format.

    You must provide a pass phrase to export a PKCS12 certificate format to import the file later.
  - **Re-enroll certificate**—Re-enroll an existing certificate.
  - **Refresh certificate status**—Refresh a certificate to synchronize the device certificate status to the Firewall Management Center.
  - **Delete certificate**—Delete all the associated certificates for a trustpoint.

Step 2 Choose **(+) Add** to associate and install an enrollment object on a device.

When a certificate enrollment object is associated with and then installed on a device, the process of certificate enrollment starts immediately. The process is automatic for self-signed and SCEP enrollment types, meaning it does not require any additional administrator action. Manual certificate enrollment requires extra administrator action.

Note The certificate enrollment on a device does not block the user interface and the enrollment process gets executed in the background, enabling the user to perform certificate enrollment on other devices in parallel. The progress of these parallel operations can be monitored on the same user interface. The respective icons display the certificate enrollment status.

Related Topics

Install a certificate using self-signed enrollment, on page 2486
Install a certificate using SCEP enrollment, on page 2487
Install a certificate using manual enrollment, on page 2488
Install a certificate using a PKCS12 file, on page 2489

Automatically update CA bundles

You can set the management center to automatically update the CA certificates through CLI commands. By default, the CA certificates are automatically updated when you install or upgrade to version 7.0.5.

Note In an IPv6-only deployment, the automatic update of CA certificates may fail, because, some of the Cisco servers do not support IPv6. In such cases, force update the CA certificates using the **configure cert-update run-now force** command.

Procedure

Step 1 Log into the FMC CLI using SSH, or, if virtual, open the VM console.

Step 2 You can verify whether the CA certificates in the local system are the latest or not:

configure cert-update test

This command compares the CA bundle on the local system with the latest CA bundle (from the Cisco server). If the CA bundle is up to date, no connection check is executed and the test result is displayed as the one below:

Example:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

If the CA bundle is out of date, the connection check is executed on the downloaded CA bundle and the test result is displayed.

Example:

When the connection check fails:

```
> configure cert-update test
Test failed, not able to fully connect.
```

Example:

When the connection check succeeds, or the CA bundle is already up to date:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Step 3 (Optional) To instantly update the CA bundles:

configure cert-update run-now

Example:

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

When you execute this command, the CA certificates (from the Cisco server) are verified for SSL connectivity. If the SSL connectivity check fails for even one of the Cisco servers, the process is terminated.

Example:

```
> configure cert-update run-now
Certs failed some connection checks.
```

To proceed with the update despite connection failures, use the **force** keyword.

Example:

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Step 4 If you do not want the CA bundles to be automatically updated, disable the configuration:

configure cert-update auto-update disable

Example:

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

Step 5 To re-enable the automatic update of CA bundles:

configure cert-update auto-update enable

Example:

```
> configure cert-update auto-update enable
```

```
Autoupdate is enabled and set for every day at 12:18 UTC
```

When you enable the automatic update on the CA certificates, the update process is executed daily at a system-defined time.

Step 6 (Optional) View the status of automatic update of CA certificates:

show cert-update

Example:

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

Install a certificate using self-signed enrollment

Install a self-signed certificate to establish secure VPN connections by creating an identity certificate directly on the managed device.

Procedure

Step 1 On the **Devices** > **Certificates** screen, choose **Add** to open the **Add New Certificate** dialog.

Step 2 Choose a device from the **Device** drop-down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the type Self-Signed from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Add certificate enrollment objects, on page 2402.

Step 4 Press **Add** to start the Self Signed, automatic, enrollment process.

For self signed enrollment type trustpoints, the **CA Certificate** status will always be displayed, since the managed device is acting as its own CA and does not need a CA certificate to generate its own Identity Certificate.

The **Identity Certificate** will go from InProgress to Available as the device creates its own self signed identity certificate.

Step 5 Click the magnifying glass to view the self-signed Identity Certificate created for this device.

What to do next

When enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your Site to Site and Remote Access VPN Authentication Method.

Install a certificate using EST enrollment

Use EST enrollment to automatically obtain and install identity certificates on devices from a Certificate Authority (CA).

Before you begin

Note Using EST enrollment establishes a direct connection between the managed device and the CA server. So be sure your device is connected to the CA server before beginning the enrollment process.

Note EST's ability to auto-enroll a device when its certificate expires is not supported.

Follow these steps to install a certificate using EST enrollment:

Procedure

Step 1 On the **Devices** > **Certificates** screen, click **Add** to open the **Add New Certificate** dialog.

Step 2 Choose a device from the **Device** drop-down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose the EST certificate enrollment object from the **Cert Enrollment** drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Add certificate enrollment objects, on page 2402.

Step 4 Click **Add** to enroll the certificate on the device.

The **Identity Certificate** will go from `InProgress` to `Available` as the device obtains its identity certificate using EST from the specified CA. Sometimes, a manual refresh might be required to obtain the identity certificate.

Step 5 Click the magnifying glass to view the Identity Certificate created and installed on this device.

Install a certificate using SCEP enrollment

Install a certificate using SCEP enrollment to enable secure authentication for VPN connections and other security features on your device.

Before you begin

Note Using SCEP enrollment establishes a direct connection between the managed device and the CA server. So be sure your device is connected to the CA server before beginning the enrollment process.

Follow these steps to install a certificate using SCEP enrollment:

Procedure

Step 1 On the **Devices** > **Certificates** screen, choose **Add** to open the **Add New Certificate** dialog.

Step 2 Choose a device from the **Device** drop-down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the type SCEP from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Add certificate enrollment objects, on page 2402.

Step 4 Press **Add**, to start the automatic enrollment process.

For SCEP enrollment type trustpoints, the **CA Certificate** status will transition from InProgress to Available as the CA Certificate is obtained from the CA server and installed on the device.

The **Identity Certificate** will go from `InProgress` to `Available` as the device obtains its identity certificate using SCEP from the specified CA. Sometimes, a manual refresh might be required to obtain the identity certificate.

Step 5 Click the magnifying glass to view the Identity Certificate created and installed on this device.

What to do next

When enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your Site to Site and Remote Access VPN Authentication Method.

Install a certificate using manual enrollment

Manual enrollment allows you to obtain and install an identity certificate on a managed device by generating a certificate signing request (CSR) and working with your PKI CA server to obtain the corresponding identity certificate.

Procedure

Step 1 On the **Devices** > **Certificates** screen, choose **Add** to open the **Add New Certificate** dialog.

Step 2 Choose a device from the **Device** drop-down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the type Manual from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Add certificate enrollment objects, on page 2402.

Step 4 Press **Add** to start the enrollment process.

Step 5 Execute the appropriate activity with your PKI CA Server to obtain an identity certificate.

a) Click **Identity Certificate** warning to view and copy the CSR.

b) Execute the appropriate activity with your PKI CA Server to obtain an identity certificate using this CSR.

This activity is completely independent of the Secure Firewall Management Center or the managed device. When complete, you will have an Identity Certificate for the managed device. You can place it in a file.

c) To finish the manual process, install the obtained identity certificate onto the managed device.

Return to the Secure Firewall Management Center dialog and select **Browse Identity Certificate** to choose the identity certificate file.

Note Ensure not to choose a binary certificate (PKCS12, DER, and alike) file because Firewall Threat Defense does not support them.

Step 6 Select **Import** to import the Identity Certificate.

The Identity Certificate status will be `Available` when the import complete.

Step 7 Click the magnifying glass to view the **Identity Certificate** for this device.

What to do next

When enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your Site to Site and Remote Access VPN Authentication Method.

Install a certificate using a PKCS12 file

Install a certificate using a PKCS12 file to enable secure authentication and encrypted communications on managed devices.

Procedure

Step 1 Go to **Devices** > **Certificates** screen, choose **Add** to open the **Add New Certificate** dialog.

Step 2 Choose a pre-configured managed device from the **Device** drop down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the PKCS type from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Add certificate enrollment objects, on page 2402.

Step 4 Press **Add**.

The CA Certificate and Identity Certificate status will go from `In Progress` to `Available` as it installs the PKCS12 file on the device.

Note When you upload the PKCS12 file for the first time, the file is stored in Firewall Management Center as part of the CertEnrollment object. For any failed enrollments due to a wrong passphrase or failed deployment, retry enrolling the PKCS12 certificate without uploading the file again. Also, whenever you modify the certificate enrollment object to permit overrides, you must update the **Passphrase** for the certificate for a sucessful enrollment. A PKCS12 file size should not be larger than 24K.

Step 5 Once `Available`, click the magnifying glass to view the Identity Certificate for this device.

What to do next

The certificate (trustpoint) on the managed device is named the same as the PKCS#12 file. Use this certificate in your VPN authentication configuration.

Troubleshoot Threat Defense certificates

See Secure Firewall Threat Defense VPN certificate guidelines and limitations, on page 2481 to determine if variations in your certificate enrollment environment may be causing a problem.

Certificate expiration monitoring
CA server connectivity

Ensure there is a route to the CA Server from the device. If the CA Server's host name is given in the Enrollment Object, use Flex Config to configure DNS appropriately to reach the server. Alternatively, use the IP Address of the CA Server.

Microsoft 2012 CA server template configuration

If you are using a Microsoft 2012 CA Server, the default IPsec Template is not accepted by the managed device and must be changed.

To configure a working template, follow these steps as you use MS CA documentation as a reference.

1. Duplicate the IPsec (Offline Request) template.
2. In **Extensions** > **Application policies**, select *IP security end system*, instead of the *IP security IKE intermediate*.
3. Set the permissions and the template name.
4. Add the new template and change the registry settings to reflect the new template name.

Default keyring certificate regeneration

On the Firewall Management Center, you might receive this health alert related to the Firewall Threat Defense device:

`Code - F0853; Description - default Keyring's certificate is invalid, reason: expired`

Solution: In such cases, use the following command to regenerate the default certificate in CLISH CLI:

```
> system support regenerate-security-keyring default
```

CA certificate configuration errors

A red cross appears in the CA certificate status with this error:

Error: `Fail to configure CA certificate`

Solution: See Troubleshoot Certificate Error on FMC.

Certificate verification in .pfx files

To check the list of the certificates in a .pfx file, use tools such as `certutil` or `openssl`. You can see the whole chain with ID certificate, SubCA certificate, and CA certificate (if any).

- `certutil -dump cert.pfx`
- `openssl pkcs12 -info -in cert.pfx`

Identity certificate import errors

Error: `Identity certificate import required`

Solution: See Troubleshoot Certificate Error "Identity certificate import required" on FMC.

Self-signed certificates hostname behavior in Threat Defense high-availability environments

In a Threat Defense HA configuration, the secondary unit adopts the primary unit's hostname. When you break the HA pair, you must perform these actions:

- Manually update the hostname on the secondary unit to its unique identifier
- Perform a certificate re-enrollment to ensure that the certificate accurately reflects the unit's identity.

History for certificates

This table lists the certificate feature history and enhancements introduced in different software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Support for OCSP and CRL IPv6 URL	7.4	Any	You can now add IPv6 OCSP and CRL URLs for certificate authentication (revocation checking). The IPv6 addresses must be enclosed in square brackets.
Enhancements to Manual Enrollment	6.7	Any	You can now create only a CA certificate without an identity certificate. You can also generate a CSR without a CA certificate and obtain an identity certificate from the CA.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
PKCS CA Chain	6.7	Any	You can view and manage the chain of certifying authorities (CAs) issuing your certificates. You can also export a copy of the certificates.