

Cisco Secure Firewall Management Center 设备配置指南，10.x

上次修改日期: 2026 年 6 月 24 日

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

本手册中有关产品的规格和信息如有更改，恕不另行通知。我们相信本手册中的所有声明、信息和建议均准确可靠，但不为其提供任何明示或暗示的担保。用户必须为使用任何产品负全部责任。

随附产品的软件许可证和有限保证在随产品一起提供的信息包中阐明，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 信头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

不管本文其他地方列出了何种保证，这些供应商的所有文档和软件均“按现状”提供并可能带有各种缺陷。Cisco 和上述供应商拒绝作任何明示或暗示的保证，包括（但不限于）适销性、特定目的适用性、非侵权或出于交易、使用或买卖而产生的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科或其供应商概不负责，即使思科或其供应商已获知此类损坏的可能性也不例外。

本文档中使用的所有 Internet 协议 (IP) 地址和电话号码都是虚构的。此文档中的所有示例、命令显示输出、网络拓扑图和其它图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

本文档的所有打印副本和复制的电子副本均视为非受控副本。有关最新版本，请参阅当前在线版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址和电话号码。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。 要查看思科商标的列表，请访问此 URL：https://www.cisco.com/c/en/us/about/legal/trademarks.html。 文中提及的第三方商标均属于其各自所有者。 “合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。 (1721R)

© 2025 – 2026 Cisco Systems, Inc. 保留所有权利。



目录

第 I 部分： 设备配置入门 87

第 1 章 设备注册 1

关于设备注册 1

管理中心概述 1

关于防火墙管理中心和设备管理 2

Secure Firewall Management Center可以管理哪些内容？ 2

关于管理连接 3

除策略和事件以外的其他功能 3

关于设备管理接口 4

Firewall Threat Defense上的管理和事件接口 4

使用Firewall Threat Defense数据接口进行管理 4

每个设备型号的管理接口支持 6

设备管理接口上的网络路由 7

NAT 环境 7

管理和事件流量通道示例 9

设备注册前提条件 11

登录到设备的命令行界面 12

为手动注册完成Firewall Threat Defense初始配置 14

使用防火墙设备管理器完成Firewall Threat Defense初始配置 15

使用 CLI 完成Firewall Threat Defense初始配置 21

配置事件接口 27

管理设备注册 29

关于设备管理页面 29

添加设备组 32
向管理中心注册 32
注册密钥方法 32
序列号方法（零接触调配） 39
添加机箱 52
向新的管理中心注册 55
解决序列号（零接触调配）注册问题 56
从 防火墙管理中心 取消注册设备 63
关闭或重新启动设备 64
下载托管设备列表 65
迁移 Firewall Threat Defense 设备 65
支持进行迁移的设备 66
迁移许可证 67
迁移的前提条件 67
向导可以迁移哪些配置？ 68
迁移准则和限制 70
迁移安全 Firewall Threat Defense 71
威胁防御 设备迁移最佳实践 74
交换机管理器 74
从 防火墙设备管理器切换到 防火墙管理中心 74
从 防火墙管理中心 切换到 防火墙设备管理器 79
设备注册的历史记录 80

第 2 章 使用设备模板进行设备注册 87
关于使用设备模板进行设备注册 87
使用模板注册设备的方法 88
变量和网络对象覆盖 88
型号映射 88
模板和高可用性 88
模板和域 89
在设备上应用模板前后验证模板配置 90

使用设备模板进行设备注册的先决条件 91
使用设备模板进行设备注册的许可证 91
使用设备模板进行设备注册的准则 92
使用设备模板进行设备管理的工作流程 95
配置设备模板 95
添加设备模板 95
创建新设备模板 95
从现有设备生成新设备模板 96
导入设备模板 96
在模板中配置设备设置 97
添加物理接口 97
添加逻辑接口 98
编辑接口 98
配置其他设备设置 99
配置模板设置 100
编辑常规设置 100
编辑许可证 101
编辑应用的策略 101
编辑高级设置 101
编辑部署设置 102
模板模板参数 103
添加模型映射 106
在设备模板中配置站点间 VPN 连接 108
具有站点间 VPN 连接的设备模板工作流程 108
配置 SD-WAN VPN 连接 108
配置基于路由的站点间 VPN 连接 109
配置基于策略的站点间 VPN 连接 110
使用设备模板注册设备并将其添加到基于路由的 VPN 拓扑中 112
在双 ISP 部署中为 SD-WAN 拓扑添加设备 112
为使用数据接口管理的 Firewall Threat Defense 设备配置模板 113
将模板与设备一起使用 115

使用设备模板向管理中心添加设备 115
将模板应用于现有设备 116
应用模板 116
重新应用模板 117
监控设备模板 117
查看关联设备 117
生成模板应用报告 118
审核日志 119
设备模板故障排除 119
使用设备模板进行设备管理的历史记录 121

第 3 章 透明或路由防火墙模式 123
关于防火墙模式 123
关于路由防火墙模式 123
关于透明防火墙模式 124
在网络中使用透明防火墙 124
允许路由模式功能通过流量 124
关于网桥组 125
网桥虚拟接口 (BVI) 125
透明防火墙模式下的网桥组 125
路由防火墙模式下的网桥组 126
允许第 3 层流量 127
允许的 MAC 地址 127
BPDU 处理 127
MAC 地址与路由查找 128
透明模式下网桥组不支持的功能 130
路由模式下网桥组不支持的功能 130
默认设置 131
防火墙模式准则 131
设置防火墙模式 132

第 4 章 CLI 用户 135
关于 CLI 用户 135
内部和外部用户 135
CLI 访问 135
CLI 用户角色 136
CLI 用户准则 136
在 CLI 中添加内部用户 137
配置 FTD 的外部身份验证 139
关于Firewall Threat Defense外部身份验证 139
关于 LDAP 140
关于 RADIUS 140
为 Firewall Threat Defense 添加 LDAP 外部身份验证对象 140
为 Firewall Threat Defense 添加 RADIUS 外部身份验证对象 146
为 FTD 设备上的用户启用外部身份验证 151
LDAP 身份验证连接故障排除 151
CLI 用户的历史记录 153

第 5 章 变更管理 155
关于变更管理 155
如何在变更管理工作流程中配置设备 155
创建独立的审批人和配置角色 156
支持变更管理的策略和对象 157
变更管理的要求和前提条件 159
变更管理的准则和限制 160
启用或禁用更改管理 160
管理工单 161
创建变更管理工单 162
为配置更改开单 163
预览工单 163
提交工单 164

丢弃工单 164
批准或拒绝工单 165
接管或重新分配工单 165
变更管理的历史记录 166

第 6 章 配置部署 167
关于配置部署 167
需要部署的配置更改 167
部署预览 168
选择性策略部署 169
系统用户名 171
自动启用应用检测器 172
网络发现策略更改带来的资产重新发现 172
Snort 重新启动场景 172
设备的重启警告 172
在策略应用期间检测流量 173
Snort 重启流量行为 174
部署或激活时重启 Snort 进程的配置 176
会立即重新启动 Snort 进程的更改 177
策略管理的要求和前提条件 178
部署配置更改的最佳实践 178
部署配置 179
部署配置更改 180
将现有配置重新部署到设备 186
管理部署 187
查看部署状态 187
查看部署历史记录 187
设置配置版本数 192
回滚部署 192
执行回滚 194
查看部署回滚脚本 196

下载多个设备的策略更改报告 196
比较策略 197
生成当前策略报告 198
配置部署的历史记录 199

第 II 部分： 高可用性和可扩展性 203

第 7 章 多实例模式 205
关于多实例模式 205
多实例模式与应用模式 205
机箱管理接口 206
实例接口 206
接口类型 206
机箱接口与实例接口 207
共享接口可扩展性 209
共享接口最佳实践 209
机箱如何将数据包分类 211
分类示例 212
级联实例 215
典型多实例部署 216
实例接口的自动 MAC 地址 217
多实例功能的性能扩展因素 218
实例与高可用性 218
实例的许可证 218
实例的要求和前提条件 218
实例的准则和限制 220
配置实例 222
将设备转换为多实例模式 223
配置机箱接口 226
配置物理接口 226
配置 EtherChannel 229

配置子接口 233
添加实例 235
自定义系统配置 241
配置 SNMP 242
导入或导出机箱配置 243
配置机箱平台设置 245
创建机箱平台设置策略 245
配置 DNS 246
配置 SSH 和 SSH 访问列表 247
配置系统日志 252
配置时间同步 257
配置时区 259
管理多实例模式 260
在 CLI 启用多实例模式 260
更改分配给实例的接口 263
在 FXOS CLI 中更改机箱管理设置 265
监控多实例模式 267
监控多实例设置 267
监控实例接口 268
多实例模式的历史记录 270

第 8 章 **Firepower 4100/9300 上的逻辑设备 273**
关于接口 273
机箱管理接口 273
接口类型 274
FXOS 接口与应用接口 276
共享接口可扩展性 278
共享接口最佳实践 278
共享接口使用示例 280
查看共享接口资源 290
防火墙威胁防御 支持的内联集链路状态传播 290

关于逻辑设备 291
独立和集群逻辑设备 291
逻辑设备应用实例：容器和本地 291
容器实例接口 292
机箱如何将数据包分类 292
分类示例 292
级联容器实例 296
典型多实例部署 297
容器实例接口的自动 MAC 地址 298
容器实例资源管理 299
多实例功能的性能扩展因素 299
容器实例与高可用性 299
容器实例和集群 299
容器实例的许可证 299
逻辑设备的要求和前提条件 300
硬件和软件组合的要求与前提条件 300
容器实例的要求和前提条件 302
高可用性的要求和前提条件 303
集群要求和前提条件 303
逻辑设备的准则和限制 307
接口的准则和限制 307
一般准则和限制 309
配置接口 310
启用或禁用接口 310
配置物理接口 310
添加 EtherChannel（端口通道） 311
为容器实例添加 VLAN 子接口 313
配置逻辑设备 315
为容器实例添加资源配置文件 315
为 防火墙管理中心 316
添加高可用性对 321

更改Firewall Threat Defense逻辑设备上的接口 322
连接到应用控制台 324
逻辑设备的历史记录 326

第 9 章 设备的高可用性 333
Cisco Secure Firewall Threat Defense 高可用性 333
系统要求 334
硬件要求 334
软件要求 335
高可用性对中 Firewall Threat Defense 设备的许可证要求 335
故障转移和状态故障转移链路 336
故障切换链路 336
状态故障转移链路 338
避免故障转移和数据链路中断 339
中的 MAC 地址和 IP 地址 340
状态故障转移 342
支持的功能 342
不支持的功能 344
高可用性的网桥组要求 345
故障转移运行状态监控 345
设备运行状况监控 345
心跳模块冗余 346
接口监控 347
故障转移触发器和检测计时 349
主用/备用故障转移 350
主/辅角色与主/备状态 350
启动时的主用设备确定 351
故障转移事件 351
Config-sync 优化 352
高可用性的要求和先决条件 353
准则 354

添加高可用性对 356
配置可选高可用性参数 359
配置备用 IP 地址和接口监控 359
编辑高可用性故障切换条件 360
配置虚拟 MAC 地址 360
管理 361
在 Firewall Threat Defense 高可用性对中切换主用对等体 361
刷新单个 Firewall Threat Defense 高可用性对的节点状态 362
暂停和恢复高可用性 362
更换 Firewall Threat Defense 高可用性对中的设备 363
将主 Firewall Threat Defense 高可用性设备替换为无备份 363
将辅助 Firewall Threat Defense HA 单元更换为无备份 364
中断高可用性对 365
取消注册高可用性对和注册新 防火墙管理中心 367
监控 368
查看故障切换历史记录 368
查看状态故障切换统计信息 368
配置同步失败故障排除 369
高可用性历史记录 369

第 10 章 群集技术：Cisco Secure Firewall 3100/4200/6100 373
关于 Cisco Secure Firewall 3100/4200/6100 的集群 373
集群如何融入网络中 373
控制和数据节点角色 374
集群接口 374
集群控制链路 374
配置复制 374
管理网络 374
集群的许可证 375
集群要求和前提条件 375
面向集群的指导原则 376

配置集群 380
关于集群接口 380
集群控制链路 380
跨网络 EtherChannel（推荐） 383
独立接口（仅适用于路由防火墙模式） 385
连接电缆并将设备添加到防火墙管理中心 387
创建集群 388
配置接口 396
配置跨区以太网通道 396
配置独立接口 397
配置集群运行状况监控设置 399
配置分布式站点间 VPN 404
关于分布式站点间 VPN 404
分布式站点间 VPN 的许可 406
分布式站点间 VPN 的前提条件 406
分布式站点间 VPN 准则 407
启用分布式站点间 VPN 407
重新分发分布式站点间 VPN 会话 408
管理集群节点 410
添加新的集群节点 410
中断节点 412
中断集群 413
禁用集群 414
重新加入集群 414
更改控制节点 415
编辑集群配置 416
调整集群节点 417
取消注册集群或节点并注册到新防火墙管理中心 419
监控集群 420
集群运行状况监控器控制面板 422
查看集群运行状况 423

集群指标 424
监控分布式站点间 VPN 425
对集群进行故障排除 425
在集群控制链路上执行 Ping 426
分布式站点间 VPN 故障排除 427
集群示例 428
单臂防火墙 429
流量分隔 430
集群参考 430
Firewall Threat Defense功能和集群 430
集群不支持的功能 430
集群集中化功能 431
连接设置和集群 432
FTP 和集群 432
独立接口模式下的组播路由 432
独立接口模式下的组播路由 432
NAT 和集群 432
动态路由 434
独立接口模式下的动态路由 435
SIP 检测和集群 436
SNMP 和集群 436
系统日志和集群 436
思科 TrustSec 和集群 436
VPN 和集群 436
性能换算系数 436
控制节点选择 437
集群中的高可用性 437
节点运行状况监控 437
接口监控 437
发生故障后的状态 438
重新加入集群 438

数据路径连接状态复制 439
集群管理连接的方式 439
连接角色 439
新连接所有权 441
TCP 的数据流示例 441
ICMP 和 UDP 的数据流示例 442
集群的历史记录 443

第 11 章 群集技术：私有云 447
关于群集技术：私有云 447
集群如何融入网络中 447
控制和数据节点角色 448
独立接口 448
策略型路由 449
同等成本的多路径路由 449
集群控制链路 450
集群控制链路流量概述 450
配置复制 451
管理网络 451
群集技术许可证：私有云 451
集群的先决条件：私有云 451
集群的准则：私有云 453
配置群集技术：私有云 454
向管理中心添加节点 454
创建集群 454
配置接口 462
配置集群运行状况监控设置 463
管理集群节点 468
添加新的集群节点 468
中断节点 470
中断集群 471

禁用集群 472
重新加入集群 473
更改控制节点 473
编辑集群配置 474
调整集群节点 476
删除（注销）集群或节点并注册到新集群 防火墙管理中心 477
监控集群：私有云 478
集群运行状况监控器控制面板 481
查看集群运行状况 481
集群指标 483
群集技术故障排除：私有云 484
在集群控制链路上执行 Ping 484
群集技术参考：私有云 486
威胁防御功能和集群 486
不支持的功能和集群 486
集群集中化功能 487
连接设置和集群 488
动态路由和集群 488
FTP 和集群 489
NAT 和集群 489
SIP 检测和集群 490
SNMP 和集群 490
系统日志和集群 490
思科 TrustSec 和集群 491
VPN 和集群 491
性能换算系数 491
控制节点选择 491
集群中的高可用性 492
节点运行状况监控 492
接口监控 492
发生故障后的状态 492

重新加入集群 492
数据路径连接状态复制 493
集群管理连接的方式 493
连接角色 494
新连接所有权 495
TCP 的数据流示例 495
ICMP 和 UDP 的数据流示例 496
集群的准则：私有云 497

第 12 章 群集技术：公共云 501
关于公共云中的 Threat Defense Virtual 群集 502
集群如何融入网络中 502
独立接口 502
控制和数据节点角色 503
集群控制链路 503
集群控制链路流量概述 503
配置复制 504
管理网络 504
Threat Defense Virtual 集群的许可证 504
Threat Defense Virtual 集群的要求和前提条件 504
Threat Defense Virtual 集群的准则 506
在 AWS 中部署集群 508
AWS 网关负载均衡器和 Geneve 单臂代理 508
拓扑示例 508
AWS 网关负载均衡器和 Geneve 双臂代理 510
在 AWS 上部署 Threat Defense Virtual 集群的端到端流程 511
模板 513
使用 CloudFormation 模板在 AWS 中部署堆栈 513
管理中心双臂部署的 NAT 配置 527
自动扩展参数配置 530
通过更新堆叠在 Firewall Threat Defense Virtual 集群中配置所需的 IMDSv2 模式 530

在 AWS 中手动部署集群 531
创建 AWS 的 Day0 配置 531
部署集群节点 534
在 AWS 中使用 GWLB 配置 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移 535
在 AWS 中启用 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移 536
在 Azure 中部署集群 537
基于 GWLB 的集群部署的拓扑示例 538
Azure 网关负载均衡器和配对代理 539
使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程 539
模板 541
前提条件 541
使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程 542
基于 NLB 的集群部署拓扑示例 545
使用 NLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程 545
模板 547
前提条件 547
使用 Azure 资源管理器模板通过 NLB 在 Azure 上部署集群 548
在 Azure 中手动部署集群 549
创建 Azure 的 Day0 配置 550
手动部署集群节点 - 基于 GWLB 的部署 551
手动部署集群节点 - 基于 NLB 的部署 553
Azure 中的集群部署故障排除 554
Azure 中的 Firewall Threat Defense Virtual 集群 Autoscale 解决方案 555
拓扑示例 555
前提条件 557
Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑 558
GitHub 上的部署和基础设施模板 559
输入参数 560
Firewall Threat Defense Virtual 具有自动扩展部署过程和资源的集群 568
使用自动扩展解决方案部署 Firewall Threat Defense Virtual 集群 568

部署 Azure Functions 应用 575
更新 Azure 逻辑应用 575
在 GCP 中部署集群 578
GCP 集群 Autoscale 解决方案的拓扑示例 579
在 GCP 中部署 Threat Defense Virtual 集群的端到端流程 579
模板 581
使用实例模板在 GCP 中部署实例组 581
在 GCP 中手动部署集群 583
为 GCP 创建 Day0 配置 583
手动部署集群节点 585
允许对 GCP 网络负载均衡器进行运行状况检查 585
GCP 中的 Threat Defense Virtual 集群 Autoscale 解决方案 587
GCP 集群 Autoscale 解决方案的拓扑示例 588
要求和前提条件 588
模板 589
在 GCP 上部署带有 Autoscale 的 Threat Defense Virtual 集群解决方案 589
基础设施部署参数 590
在 GCP 上使用 Terraform 部署基础设施 590
集群部署参数： 592
使用 Terraform on GCP 部署集群 596
集群部署后的部署配置 597
在 GCP 中手动部署集群 598
允许对 GCP 网络负载均衡器进行运行状况检查 599
通过 Autoscale 对 GCP 集群进行故障排除 600
将集群添加到管理中心（手动部署） 600
配置集群运行状况监控设置 608
管理集群节点 612
禁用集群 612
重新加入集群 613
调整集群节点 613
取消注册集群或节点并注册到新防火墙管理中心 614

监控集群 615
集群运行状况监控器控制面板 618
查看集群运行状况 618
集群指标 620
对集群进行故障排除 621
在集群控制链路上执行 Ping 621
升级集群 623
集群参考 624
威胁防御功能和集群 624
不支持的功能和集群 624
集群集中化功能 625
思科 TrustSec 和集群 626
连接设置和集群 626
动态路由和集群 626
FTP 和集群 627
NAT 和集群 627
SIP 检测和集群 628
SNMP 和集群 628
系统日志和集群 628
性能换算系数 629
控制节点选择 629
集群中的高可用性 629
节点运行状况监控 629
接口监控 630
发生故障后的状态 630
重新加入集群 630
数据路径连接状态复制 630
集群管理连接的方式 631
连接角色 631
新连接所有权 632
TCP 的数据流示例 632

ICMP 和 UDP 的数据流示例 633
关于公共云中的 Threat Defense Virtual 集群的历史记录 635

第 13 章 集群：Firepower 4100/9300 637
关于 Firepower 4100/9300 机箱上的集群 637
引导程序配置 638
集群成员 638
集群控制链路 638
确定集群控制链路规格 639
集群控制链路冗余 639
机箱间集群的集群控制链路可靠性 639
集群控制链路网络 640
管理网络 640
管理接口 640
集群接口 640
跨网络 EtherChannel 640
连接到冗余交换机系统 641
配置复制 641
集群许可证 641
集群要求和前提条件 642
集群准则和限制 645
配置集群 649
FXOS： 添加 防火墙威胁防御 群集 649
创建 防火墙威胁防御 集群 649
添加更多集群节点 660
防火墙管理中心：添加集群 663
防火墙管理中心：配置集群、数据 接口 669
防火墙管理中心：配置集群运行状况监控设置 671
FXOS：删除集群设备 675
FMC：管理群集成员 677
添加新的集群成员 677

替换集群成员 677
停用成员 678
重新加入集群 679
注销 数据节点 680
变更控制单元 681
调整集群成员 682
防火墙管理中心：监控集群 682
集群运行状况监控器控制面板 684
查看集群运行状况 685
集群指标 686
防火墙管理中心：对集群进行故障排除 687
在集群控制链路上执行 Ping 688
集群示例 689
单臂防火墙 690
流量分隔 691
集群参考 691
Firewall Threat Defense功能和集群 691
集群不支持的功能 691
集群集中化功能 692
连接设置 693
动态路由和集群 693
FTP 和集群 694
组播路由和集群 694
NAT 和集群 694
SIP 检测和集群 695
SNMP 和集群 695
系统日志和集群 695
TLS / SSL 连接和群集 696
思科 TrustSec 和集群 696
VPN 和集群 696
性能换算系数 696

控制设备选择 696
集群中的高可用性 697
机箱应用监控 697
设备运行状况监控 697
接口监控 697
修饰符应用监控 698
发生故障后的状态 698
重新加入集群 698
数据路径连接状态复制 699
集群管理连接的方式 699
连接角色 699
新连接所有权 701
TCP 的数据流示例 701
ICMP 和 UDP 的数据流示例 702
集群的历史记录 703

第 III 部分： 接口和设备设置 709

第 14 章 接口概述 711
管理接口 711
管理接口 711
诊断接口 712
接口模式和类型 712
安全区域和接口组 713
Auto-MDI/MDIX 功能 714
冗余接口（已弃用） 714
接口默认设置 714
创建安全区域和接口组对象 715
启用物理接口并配置以太网参数 716
配置 EtherChannel 接口 719
关于 EtherChannels 719

关于 EtherChannel 719
EtherChannel 的准则 722
配置 EtherChannel 724
与 防火墙管理中心同步接口更改 727
管理 Cisco Secure Firewall 3100/4200/6100的网络模块 728
配置分支端口 729
增加网络模块 732
热插拔网络模块 735
将网络模块更换为其他类型 737
拆卸网络模块 740
合并管理和诊断接口 743
取消合并管理接口 749
接口的历史记录 750

第 15 章 常规防火墙接口 753
常规防火墙接口的要求和前提条件 753
配置交换机端口 754
关于交换机端口 754
了解交换机端口和接口 754
Auto-MDI/MDIX 功能 755
交换机端口的前提条件 755
交换机端口准则和限制 755
配置交换机端口和以太网供电 757
启用或禁用交换机端口模式 757
配置 VLAN 接口 757
将交换机端口配置为接入端口 759
将交换机端口配置为中继端口 761
配置以太网供电 764
配置环回接口 765
关于环回接口 765
环回接口的准则和限制 766

配置环回接口 766
对流向环回接口的流量进行速率限制 766
配置 VLAN 子接口和 802.1Q 中继 770
VLAN 子接口准则 770
各设备型号的最大 VLAN 子接口数量 771
添加子接口 772
配置 VXLAN 接口 774
关于 VXLAN 接口 774
封装 774
VXLAN 隧道端点 774
VTEP 源接口 775
VNI 接口 775
VXLAN 数据包处理 775
对等体 VTEP 776
VXLAN 使用案例 777
VXLAN 接口的要求和前提条件 782
VXLAN 接口准则 782
配置 VXLAN 或 Geneve 接口 783
配置 VXLAN 接口 783
配置 Geneve 接口 786
允许网关负载均衡器运行状况检查 788
配置路由和透明模式接口 789
关于路由和透明模式接口 789
双 IP 堆栈（IPv4 和 IPv6） 789
31 位子网掩码 789
路由和透明模式接口准则和限制 790
配置路由模式接口 792
配置网桥组接口 797
配置常规网桥组成员接口参数 797
配置网桥虚拟接口 (BVI) 799
配置 IPv6 寻址 801

关于 IPv6 801
配置 IPv6 前缀代理客户端 802
配置全局 IPv6 地址 805
配置 IPv6 邻居发现 810
配置高级接口设置 814
关于高级接口配置 814
关于 MAC 地址 814
关于 MTU 816
关于 TCP MSS 816
网桥组流量的 ARP 检测 817
MAC 地址表 818
默认设置 818
ARP 检测和 MAC 地址表准则 819
配置 MTU 819
配置 MAC 地址 820
添加静态 ARP 条目 821
添加静态 MAC 地址并为网桥组禁用 MAC 学习 821
设置安全配置参数 822
常规防火墙接口的历史记录 824

第 16 章 内联集和被动接口 833
关于 IPS 接口 833
内联集 833
多个内联对和异步路由 834
被动接口 835
关于内联集的硬件旁路 835
硬件旁路触发器 835
硬件旁路切换 836
Snort 故障开启与硬件旁路 836
硬件旁路 状态 836
内联集的要求和前提条件 836

内联集和被动接口的准则 838
配置被动接口 840
配置内联集 841
内联集和被动接口的历史记录 844

第 17 章 设备设置 847
编辑常规设置 847
生成故障排除文件 849
查看 CLI 输出 852
将配置复制到另一台设备 855
导出和导入设备配置 856
编辑许可证设置 861
查看系统信息 862
查看设备资产 863
查看检测引擎 863
编辑运行状况设置 864
带外配置检测 864
带外配置准则 865
访问诊断 CLI 中的恢复配置模式 868
确认带外配置 871
编辑管理设置 874
配置冗余管理器访问数据接口 874
更改管理器访问接口设置 879
更改设备 IP 地址 879
更改 防火墙管理中心 IP 地址 892
更改防火墙管理中心和威胁防御 IP 地址 893
更改管理器访问接口 897
管理连接故障排除 909
如果防火墙管理中心断开连接，则手动回滚配置 909
排除数据接口上的管理连接故障 910
查看清单详细信息 915

编辑应用的策略 916
编辑高级设置 917
配置自动应用旁路 918
配置对象组搜索 919
配置接口对象优化 920
编辑部署设置 921
编辑集群运行状况监控设置 923
热插拔 SSD 928
禁用 USB 端口 930
禁用设备上的 USB 端口。 931
在多实例模式下禁用 USB 端口 932
为 FXOS 配置 SNMP 933
为 FXOS 启用 SNMP 934
为 FXOS 创建 SNMP 陷阱 935
为 FXOS 创建 SNMP 用户 937
配置 ISA 3000 的报警 937
关于告警 938
报警输入接口 938
告警输出接口 938
系统日志报警 939
SNMP 报警 939
报警默认值 939
报警先决条件 940
配置 ISA 3000 的报警 940
配置报警输入触点 940
配置电源报警 943
配置温度报警 946
关闭外部告警 948
监控告警 948
监控报警状态 948
监控报警系统日志消息 949

设备设置历史记录 950

第 18 章

DHCP 和 DDNS 955

关于 DHCP 和 DDNS 服务 955

关于 DHCPv4 服务器 955

DHCP 选项 955

关于 DHCPv6 无状态服务器 956

关于 DHCP 中继代理 956

DHCP 和 DDNS 的要求和前提条件 956

DHCP 和 DDNS 服务准则 957

配置 DHCPv4 服务器 958

配置 DHCPv6 无状态服务器 960

创建 DHCP IPv6 池 960

启用 DHCPv6 无状态服务器 963

配置 DHCP 中继代理 964

配置动态 DNS 965

DHCP 和 DDNS 的历史记录 971

第 19 章

平台设置 973

平台设置简介 974

平台设置策略的要求和前提条件 974

管理平台设置策略 974

机箱平台设置 975

ARP 检测 975

横幅 977

DNS 977

外部身份验证 980

为平台的外部身份验证启用虚拟路由器感知接口 985

片段设置 986

HTTP 访问 987

ICMP 访问 988

NetFlow 990
在 NetFlow 中添加收集器 990
将流量类添加到 NetFlow 991
SSH 访问 991
SMTP 服务器 993
SNMP 994
关于 SNMP 995
SNMP 术语 995
MIB 和陷阱 996
MIB 中支持的表格和对象 997
添加 SNMPv3 用户 1000
添加 SNMP 主机 1003
配置 SNMP 陷阱 1005
配置 SSL 设置 1007
关于 SSL 设置 1007
系统日志 1011
关于系统日志 1011
严重性级别 1012
系统日志消息过滤 1013
系统日志消息类 1013
日志记录准则 1016
配置 Firewall Threat Defense 设备的系统日志日志记录 1018
适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置 1019
启用日志记录并配置基本设置 1019
启用日志记录目标 1021
将系统日志消息发送给邮件消息 1022
创建自定义事件列表 1023
限制系统日志消息生成速率 1024
配置系统日志设置 1025
配置系统日志服务器 1026
超时 1028

时间同步 1030
时区 1031
UCAPL/CC 合规性 1032
性能配置文件 1033
平台设置的历史记录 1034

第 20 章

FlexConfig 策略 1041
FlexConfig 策略概述 1041
FlexConfig 策略的建议用法 1042
FlexConfig 对象中的 CLI 命令 1042
确定 ASA 软件版本和当前 CLI 配置 1042
禁止的 CLI 命令 1043
模板脚本 1045
FlexConfig 变量 1045
如何处理变量 1046
如何查看将为设备返回什么变量 1049
FlexConfig 策略对象变量 1050
FlexConfig 系统变量 1051
预定义的 FlexConfig 对象 1052
预定义文本对象 1056
FlexConfig 策略的要求和先决条件 1060
FlexConfig 的准则与限制 1060
使用 FlexConfig 策略自定义设备配置 1061
配置 FlexConfig 对象 1063
将策略对象变量添加到 FlexConfig 对象 1065
配置密钥 1066
配置 FlexConfig 文本对象 1067
配置 FlexConfig 策略 1068
为 FlexConfig 策略设置目标设备 1069
预览 FlexConfig 策略 1070
验证部署的配置 1071

删除使用 FlexConfig 配置的功能 1072
从 FlexConfig 转换为管理功能 1074
FlexConfig 示例 1074
如何配置精确时间协议 (ISA 3000) 1074
如何对电源故障配置自动硬件旁路 (ISA 3000) 1078
迁移 FlexConfig 策略 1080
FlexConfig 的历史记录 1082

第 IV 部分： 路由 1085

第 21 章 静态和默认路由 1087
关于静态路由和默认路由 1087
默认路由 1087
静态路由 1088
使用到 null0 接口的路由丢弃不必要的流量 1088
路由优先级 1088
透明防火墙模式和网桥组路由 1088
静态路由跟踪 1089
静态路由的要求和前提条件 1089
静态和默认路由准则 1090
添加静态路由 1090
路由参考 1091
确定路径 1092
支持的路由类型 1092
静态与动态 1092
单路径与多路径 1092
平面与分层 1093
链路状态与距离矢量 1093
支持的互联网路由协议 1093
路由表 1094
路由表的填充方式 1094

如何制定转发决策 1096
动态路由和 1096
集群下的动态路由 1096
独立接口模式下的动态路由 1097
管理流量的路由表 1098
等价多路径 (ECMP) 路由 1099
路由 GRE 流量 1100
关于路由映射 1100
Permit 和 Deny 子句 1100
Match 和 Set 子句值 1100

第 22 章 虚拟路由器 1103
关于虚拟路由器和虚拟路由与转发 (VRF) 1103
关于虚拟路由器和动态 VTI 1104
如何使用动态 VTI 配置虚拟路由器 1104
虚拟路由器的应用 1104
全局和用户定义的虚拟路由器 1105
配置策略以感知虚拟路由器 1106
互联虚拟路由器 1106
重叠 IP 地址 1108
在用户定义的虚拟路由器上配置 SNMP 1109
按设备型号划分的最大虚拟路由器数量 1109
虚拟路由器的要求和前提条件 1111
虚拟路由器的准则和限制 1111
防火墙管理中心 Web 界面 - 路由页面修改 1113
管理虚拟路由器 1114
创建虚拟路由器 1114
配置虚拟路由器 1114
修改虚拟路由器 1116
删除虚拟路由器 1117
监控虚拟路由器 1117

虚拟路由器的配置示例 1118
如何通过虚拟路由器路由到远程服务器 1118
如何提供包含重叠地址空间的互联网访问权限 1122
如何允许对虚拟路由中的内部网络进行 RA VPN 访问 1129
如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量 1132
如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量 1136
如何在虚拟路由中的两个重叠网络主机之间路由流量 1138
如何使用 BVI 接口在路由防火墙模式下管理重叠网段 1141
如何使用重叠网络来配置用户身份验证 1144
如何使用 BGP 来互连虚拟路由器 1150
虚拟路由器的历史记录 1156

第 23 章 ECMP 1159
ECMP 路由方法 1159
ECMP 的准则和限制 1160
管理虚拟路由器的 ECMP 区域 1161
创建 ECMP 区域 1161
配置等价静态路由 1162
修改 ECMP 区域 1163
删除 ECMP 区域 1164
配置 ECMP 1165
Cisco Secure Firewall Threat Defense 中按时间顺序排列的 ECMP 发展历史记录 1168

第 24 章 双向转发检测路由 1169
BFD 路由协议 1169
BFD 路由准则 1169
配置 BFD 1171
配置 BFD 策略 1171
配置单跳 BFD 策略 1172
配置多跳 BFD 策略 1173
BFD 路由的历史记录 1174

第 25 章 OSPF 1175

OSPF 1175

关于 OSPF 1175

快速呼叫数据包 OSPF 支持 1176

OSPF 支持快速呼叫数据包的前提条件 1177

OSPF 呼叫间隔和停顿间隔 1177

OSPF 快速呼叫数据包 1177

OSPF 快速呼叫数据包的优势 1177

OSPFv2 与 OSPFv3 之间的实施差异 1177

OSPF 的要求和前提条件 1178

OSPF 准则 1178

配置 OSPFv2 1180

配置 OSPF 区域、范围和虚拟链路 1181

配置 OSPF 重新分发 1183

配置 OSPF 区域间过滤 1185

配置 OSPF 过滤规则 1186

配置 OSPF 汇总地址 1187

配置 OSPF 接口和邻居 1188

配置 OSPF 高级属性 1190

配置 OSPFv3 1192

配置 OSPFv3 区域、路由摘要和虚拟链路 1192

配置 OSPFv3 重新分发 1195

配置 OSPFv3 摘要前缀 1196

配置 OSPFv3 接口、身份验证和邻居 1197

配置 OSPFv3 高级属性 1199

OSPF 的历史记录 1202

第 26 章 EIGRP 1203

关于 EIGRP 路由 1203

EIGRP 的要求和前提条件 1204

EIGRP 路由的准则和限制 1204
配置 EIGRP 1206
配置 EIGRP 设置 1206
配置 EIGRP 邻居设置 1207
配置 EIGRP 过滤器规则设置 1207
配置 EIGRP 重新分发设置 1208
配置 EIGRP 摘要地址设置 1209
配置 EIGRP 接口设置 1209
配置 EIGRP 高级设置 1210
EIGRP 的历史记录 1212

第 27 章 BGP 1213
关于 BGP 1213
路由表更改 1213
何时使用 BGP 1214
BGP 路径选择 1215
BGP 多路径 1215
BGP 的要求和前提条件 1216
BGP 准则 1217
配置 BGP 1217
配置 BGP 基本设置 1218
配置 BGP 常规设置 1220
配置 BGP 邻居设置 1221
配置 BGP 汇聚地址设置 1225
配置 BGPv4 过滤设置 1226
配置 BGP 网络设置 1227
配置 BGP 重新分发设置 1227
配置 BGP 路由注入设置 1228
配置 BGP 路由导入/导出设置 1229
BGP 的历史记录 1231

第 28 章 RIP 1233
关于 RIP 1233
路由更新过程 1233
RIP 路由指标 1234
RIP 稳定性功能 1234
RIP 计时器 1234
RIP 的要求和前提条件 1235
RIP 准则 1235
配置 RIP 1236

第 29 章 组播 1239
关于组播路由 1239
IGMP 协议 1239
末节组播路由 1240
PIM 组播路由 1240
PIM 稀疏模式 1241
PIM 源特定组播支持 1241
组播双向 PIM 1241
PIM 自举路由器 (BSR) 1242
PIM 引导程序路由器 (BSR) 术语 1242
组播组概念 1243
组播地址 1243
集群 1243
组播路由的先决条件 1243
组播路由准则 1244
配置 IGMP 功能 1245
启用组播路由 1245
配置 IGMP 协议 1246
配置 IGMP 访问组 1247
配置 IGMP 静态组 1248

配置 IGMP 加入组 1248
配置 PIM 功能 1249
配置 PIM 协议 1250
配置 PIM 邻居过滤器 1251
配置 PIM 双向邻居过滤器 1251
配置 PIM 交汇点 1252
配置 PIM 路由树 1253
配置 PIM 请求过滤器 1254
将 Cisco Secure Firewall Threat Defense设备配置为候选自举路由器 1254
配置组播路由 1255
配置组播边界过滤器 1256

第 30 章 策略型路由 1259
策略型路由 1259
策略型路由的许可证 1261
策略型路由的最佳实践 1261
用于确定最佳路径路由的路径监控指标 1263
配置路径监控设置 1265
添加路径监控控制面板 1266
配置策略型路由策略 1266
为 PBR 创建自定义应用检测器 1269
配置带有自定义应用检测器的 PBR（基本） 1269
配置策略型路由 1276
配置具有路径监控的 PBR 1281
用于监控 PBR 的有用 CLI 1283
对PBR进行故障排除 1286
策略型路由的历史记录 1288

第 V 部分： 网络策略 1291

第 31 章 网络地址转换 1293

为何使用 NAT? 1293
NAT 基础知识 1294
NAT 术语 1294
NAT 类型 1294
路由和透明防火墙模式下的 NAT 1295
路由模式下的 NAT 1295
透明模式下的 NAT 或网桥组内的 NAT 1296
自动 NAT 和手动 NAT 1297
自动 NAT 1297
手动 NAT 1297
比较自动 NAT 和手动 NAT 1297
NAT 规则顺序 1298
NAT 接口 1300
NAT 免除 1301
为 NAT 配置路由 1301
地址与映射接口在相同的网络中 1301
唯一网络上的地址 1302
与实际地址相同的地址（身份 NAT） 1302
NAT 策略的要求和先决条件 1302
NAT 准则 1303
NAT 防火墙模式准则 1303
IPv6 NAT 准则 1303
IPv6 NAT 最佳实践 1304
对检测到的协议的 NAT 支持 1304
FQDN 目标准则 1306
NAT 的其他准则 1306
管理 NAT 策略 1309
创建 NAT 策略 1309
配置 NAT 策略目标 1310
配置用于威胁防御的 NAT 1310
为多个设备自定义 NAT 规则 1312

搜索和过滤 NAT 规则表 1314
启用、禁用或删除多个规则 1315
动态 NAT 1316
关于动态 NAT 1316
动态 NAT 的不足与优势 1317
配置动态自动 NAT 1318
配置动态手动 NAT 1319
动态 PAT 1321
关于动态 PAT 1321
动态 PAT 的优缺点 1322
PAT 池对象准则 1322
配置动态自动 PAT 1323
配置动态手动 PAT 1325
使用端口块分配配置 PAT 1328
静态 NAT 1331
关于静态 NAT 1331
配置静态自动 NAT 1335
配置静态手动 NAT 1336
身份 NAT 1339
配置身份自动 NAT 1339
配置身份手动 NAT 1341
Firewall Threat Defense 的 NAT 规则属性 1343
接口对象 NAT 属性 1344
自动 NAT 的转换属性 1344
手动 NAT 的转换属性 1345
PAT 池 NAT 属性 1346
高级 NAT 属性 1347
转换 IPv6 网络 1348
NAT64/46：将 IPv6 地址转换为 IPv4 地址 1349
NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网 1349
NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络 1352

NAT66：将 IPv6 地址转换为其他 IPv6 地址 1355
NAT66 示例，网络之间的静态转换 1355
NAT66 示例：简单 IPv6 接口 PAT 1358
监控 NAT 1361
NAT 示例 1362
提供对内部 Web 服务器的访问权限（静态自动 NAT） 1362
面向内部主机的动态自动 NAT 和面向外部 Web 服务器的静态 NAT 1365
具有多个映射地址的内部负载均衡器（静态自动 NAT，一对多） 1369
FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT） 1372
转换因目标而异（动态手动 PAT） 1378
转换因目标地址和端口而异（动态手动 PAT） 1384
NAT 和站点间 VPN 1390
使用 NAT 重写 DNS 查询和响应 1395
DNS64 回复修改 1396
DNS 应答修改，外部接口上的 DNS 服务器 1404
DNS 应答修改，主机网络上的 DNS 服务器 1407
Firewall Threat Defense NAT 的历史记录 1411

第 32 章 服务质量 1413
QoS 简介 1413
关于 QoS 策略 1413
QoS 的要求和前提条件 1414
QoS 策略准则和限制 1414
使用 QoS 策略的速率限制 1415
创建 QoS 策略 1416
为 QoS 策略设置目标设备 1416
按设备过滤 QoS 规则 1417
配置 QoS 规则 1417
QoS 规则组成部分 1418
QoS 规则条件 1419
接口规则条件 1419

网络规则条件 1420
用户规则条件 1420
应用规则条件 1420
端口规则条件 1421
URL 规则条件 1423
自定义 SGT 规则条件 1423
ISE SGT 与自定义 SGT 规则条件 1423
从自定义 SGT 自动过渡到 ISE SGT 1423
QoS 的历史记录 1424

第 VI 部分： 安全连接 1425

第 33 章 安全连接概览 1427
VPN 类型 1427
VPN 基础知识 1428
互联网密钥交换 (IKE) 1429
IPSec 1430
VPN 数据包流 1431
IPsec 流分流 1431
VPN 许可 1432
VPN 加密与性能 1432
符合安全认证要求 1432
为 VPN 策略决定加密算法 1432
决定使用哪些散列算法 1433
决定要使用的 Diffie-Hellman 模数组 1434
决定 VPN 身份验证方法 1434
预共享密钥 1435
PKI 基础设施与数字证书 1435
已弃用的哈希算法、加密算法和 Diffie-Hellman 模数组 1437
VPN 拓扑 1438
点对点 VPN 拓扑 1438

中心辐射型 VPN 拓扑 1438
全网状 VPN 拓扑 1439
隐式拓扑 1440

第 34 章 站点间 VPN 1443
关于站点间 VPN 1443
Cisco Secure Firewall Threat Defense站点间 VPN 准则和限制 1444
站点间 VPN 拓扑的类型 1446
站点间 VPN 的许可证要求 1446
站点间 VPN 的要求和前提条件 1447
管理站点间 VPN 1447
配置策略型站点间 VPN 1449
Firewall Threat Defense VPN 终端选项 1450
Firewall Threat Defense VPN IKE 选项 1454
Firewall Threat Defense VPN IPSec 选项 1456
Firewall Threat Defense高级站点间 VPN 部署选项 1458
Firewall Threat Defense VPN 高级 IKE 选项 1459
Firewall Threat Defense VPN高级 IPsec 选项 1460
Firewall Threat Defense 高级站点间 VPN 隧道选项 1460
配置 Virtual Tunnel Interfaces 1462
关于 Virtual Tunnel Interface 1462
静态 VTI 1463
动态 VTI 1464
Virtual Tunnel Interfaces 准则和限制 1466
添加 VTI 接口 1470
创建基于路由的站点间 VPN 1471
为点对点拓扑配置终端 1472
为中心辐射型拓扑配置终端 1475
在基于路由的 VPN 中配置多个集线器 1478
通过备用 VTI 隧道路由流量 1482
为路由型站点间 VPN 配置动态 VTI 1484

如何使用动态 VTI 配置虚拟路由器 1485
为 VTI 配置路由和 AC 策略 1485
查看虚拟隧道信息 1488
在 Umbrella 上部署 SASE 隧道 1488
为 Umbrella 配置 SASE 隧道的准则和限制 1489
如何在 Umbrella 上部署 SASE 隧道 1490
配置 Umbrella SASE 隧道的前提条件 1490
映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥 1491
为 Umbrella 配置 SASE 隧道 1493
监控站点间拓扑 1495
使用站点间 VPN 摘要页面监控站点间 VPN 1495
使用站点间 VPN 控制面板监控站点间 VPN 1495
站点间 VPN 连接事件监控 1502
查看站点间 VPN 连接事件 1502
站点间 VPN 的历史记录 1503

第 35 章 SD-WAN 1507
SD-WAN 功能 1507
功能 1508
使用 SD-WAN 向导进行安全分支机构网络部署 1510
使用 SD-WAN 向导的准则和限制 1510
配置 SD-WAN 拓扑的许可证要求 1512
使用 SD-WAN 向导的前提条件。 1512
使用 SD-WAN 向导配置 SD-WAN 拓扑 1512
向中心添加动态虚拟隧道接口 1517
使用 SD-WAN 向导部署双 ISP 的配置示例 1517
双 ISP 部署：同一区域中的两个中心和四个分支 1517
双 ISP 部署：不同区域中的两个中心和四个分支 1519
验证 SD-WAN 拓扑的隧道状态 1522
SD-WAN 功能的使用案例 1525
监控 SD-WAN 拓扑 1525

Cisco SD-WAN 摘要控制面板 1525
使用 SD-WAN 摘要控制面板的前提条件 1526
使用 SD-WAN 摘要控制面板监控 WAN 设备和接口 1529
使用 SD-WAN 摘要控制面板监控 WAN 接口的应用性能指标 1530

第 36 章 远程访问 VPN 1531
远程接入 VPN 概述 1531
远程访问 VPN 功能 1532
安全客户端 组件 1534
远程访问 VPN 身份验证 1534
了解权限和属性的策略实施 1536
了解 AAA 服务器连接 1536
远程接入 VPN 的许可证要求 1537
远程接入 VPN 的要求和前提条件 1537
远程访问 VPN 准则和限制 1538
配置新的远程访问 VPN 连接 1541
配置远程访问 VPN 的前提条件 1541
创建新的远程访问 VPN 策略 1542
在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略 1545
（可选）配置 NAT 豁免 1546
配置 DNS 1547
添加 安全客户端配置文件 XML 文件 1547
（可选）配置分割隧道 1548
（可选）配置动态分割隧道 1549
验证动态分割隧道配置 1550
检验配置 1550
创建现有远程接入 VPN 策略的副本 1551
设置远程访问 VPN 策略的目标设备 1551
将本地领域与远程接入 VPN 策略相关联 1552
其他远程访问 VPN 配置 1552
配置连接配置文件设置 1552

配置 VPN 客户端的 IP 地址 1553
配置远程访问 VPN 的 AAA 设置 1555
创建或更新连接配置文件的别名 1570
配置远程访问 VPN 的访问接口 1571
配置远程访问 VPN 的高级选项 1573
思科 安全客户端 映像 1573
远程访问 VPN 地址分配策略 1575
配置连接配置文件映射证书 1576
配置组策略 1577
配置 LDAP 属性映射 1578
配置 VPN 负载均衡 1579
配置 IPsec 设置 1582
自定义 Cisco Secure Client 1588
配置 安全客户端 管理 VPN 隧道 1599
安全客户端 管理 VPN 隧道的要求和前提条件 1599
安全客户端 管理 VPN 隧道的限制 1600
在 Firewall Threat Defense 上配置 安全客户端 管理 VPN 隧道 1600
多证书身份验证 1602
多重证书身份验证的准则和限制 1602
配置多证书身份验证 1602
基于地理位置管理远程用户的 VPN 访问 1604
基于地理位置管理远程用户 VPN 访问的工作流程 1604
基于地理位置管理远程接入 VPN 用户的准则和限制 1604
监控服务访问策略并进行故障排除 1605
自定义远程接入 VPN AAA 设置 1608
通过客户端证书对 VPN 用户进行身份验证 1608
通过客户端证书和 AAA 服务器配置 VPN 用户身份验证 1609
通过 VPN 会话管理密码更改 1611
向 RADIUS 服务器发送记账记录 1612
将组策略选择委派给授权服务器 1612
授权服务器覆盖组策略或其他属性的选择 1613

拒绝用户组的 VPN 访问 1614
限制用户组的连接配置文件选择 1615
更新远程接入 VPN 客户端的 Secure Client 配置文件 1616
RADIUS 动态授权 1616
配置 RADIUS 动态授权 1617
双因素身份验证 1618
配置 RSA 双因素身份验证 1618
配置 Duo 双因素身份验证 1619
辅助身份验证 1621
配置远程访问 VPN 辅助身份验证 1621
使用 SAML 2.0 的单点登录身份验证 1623
SAML 2.0 的准则和限制 1624
配置 SAML 单点登录身份验证 1625
配置 SAML 授权 1626
高级 Secure Client 配置 1628
在 Firewall Threat Defense上配置 Secure Client 模块 1628
Secure Client 模块类型 1628
配置 Secure Client 模块的前提条件 1630
配置 Secure Client 模块的准则 1630
使用 Firewall Threat Defense安装 Secure Client 模块 1631
使用 Secure Client 模块配置远程接入 VPN 组策略 1632
验证 Secure Client 模块配置 1633
在移动设备上配置基于应用的（Per App VPN）远程访问 VPN 1633
配置 Per App VPN 隧道的前提条件和许可 1634
确定移动应用的应用 ID 1634
配置基于应用的 VPN 隧道 1635
验证每个应用配置 1636
远程访问 VPN 示例 1637
如何限制每个用户的 安全客户端 带宽 1637
如何对基于用户 ID 的访问控制规则使用 VPN 身份 1637
配置Firewall Threat Defense多证书身份验证 1638

监控远程访问 VPN 1642
远程访问 VPN 控制面板 1642
VPN 会话和用户信息 1643
查看远程接入 VPN 活动会话 1643
查看远程接入 VPN 用户活动 1644
远程接入 VPN 的功能历史记录 1644

第 37 章 动态访问策略 1649
Firewall Threat Defense 动态访问策略 1649
Firewall Threat Defense 设备中权限和属性的策略实施层次结构 1650
动态访问策略的先决条件 1651
动态访问策略的准则与限制 1651
配置动态访问策略 (DAP) 1652
创建动态访问策略 1652
创建动态访问策略记录 1652
配置终端安全评估条件 1653
为 DAP 记录配置 AAA 条件设置 1654
Configure Endpoint Attribute Selection Criteria in DAP 1655
Add an Anti-Malware Endpoint Attribute to a DAP 1656
Add a Device Endpoint Attribute to a DAP 1656
Add Secure Client Endpoint Attributes to a DAP 1657
Add NAC Endpoint Attributes to a DAP 1657
Add an Application Attribute to a DAP 1658
Add a Personal Firewall Endpoint Attribute to a DAP 1658
Add an Operating System Endpoint Attribute to a DAP 1659
Add a Process Endpoint Attribute to a DAP 1659
Add a Registry Endpoint Attribute to a DAP 1659
Add a File Endpoint Attribute to a DAP 1660
Add Certificate Authentication Attributes to a DAP 1661
配置 DAP 高级设置 1661
将动态访问策略与远程访问 VPN 关联 1662
动态访问策略历史记录 1662

第 VII 部分： 零信任网络访问 1665

第 38 章 零信任网络访问 1667

关于无客户端和通用 Zero Trust 网络访问 1667

无客户端 Cisco Zero Trust 访问 1668

威胁防御如何与 Zero Trust 访问配合使用 1669

为何使用 Zero Trust 网络访问？ 1669

无客户端 Cisco Zero Trust 访问 配置的组件 1670

无客户端 Cisco Zero Trust 访问 工作流程 1671

无客户端 Cisco Zero Trust 访问 的限制 1672

Zero Trust 应用策略的前提条件 1673

管理 Zero Trust 应用策略 1673

创建 Zero Trust 应用策略 1673

创建应用组 1675

创建应用 1676

为目标设备设置 Zero Trust 访问策略 1678

编辑 Zero Trust 应用策略 1679

监控 Zero Trust 会话 1681

通用零信任网络访问 1683

威胁防御如何与 通用 ZTNA 配合使用 1684

通用零信任网络访问 的前提条件 1684

通用零信任网络访问 的限制 1686

将防火墙管理中心与安全云控制集成 1686

安全云控制设置 1689

配置安全设备 1690

Zero Trust 网络访问历史记录 1696

第 VIII 部分： 访问控制策略基础 1699

第 39 章 访问控制策略 1701

关于访问控制策略 1701
访问控制策略组件 1702
访问控制策略默认操作 1703
访问控制策略继承 1704
规则和其他策略警告 1705
访问控制策略的要求和前提条件 1706
管理访问控制策略 1707
创建基本访问控制策略 1708
编辑访问控制策略 1709
锁定访问控制策略 1711
并发编辑和合并更改 1712
设置访问控制默认操作 1714
管理访问控制策略继承 1715
选择基本访问控制策略 1715
锁定后代访问控制策略中的设置 1716
继承基本策略的访问控制策略设置 1716
在域中要求访问控制策略 1717
将设备分配给访问控制策略 1717
访问控制策略的日志记录设置 1718
将其他策略与访问控制相关联 1719
使用策略分析器和优化器识别和修复异常 1720
查看规则命中计数 1721
分析规则冲突和警告 1723
搜索规则 1725
访问控制策略的历史记录 1726

第 40 章 安全智能 1729
关于安全智能 1729
安全智能许可证要求 1730
安全智能的要求和前提条件 1730
安全智能的最佳实践 1730

安全情报准则和限制 1731
安全智能来源 1731
配置安全智能 1732
安全智能选项 1734
安全智能类别 1736
阻止列表图标 1737
配置示例：安全智能阻止 1737
安全智能监控 1738
覆盖安全智能阻止 1739
安全智能故障排除 1740
可用选项列表中缺少安全智能类别 1740
安全智能阻止列表的历史记录 1741

第 41 章 访问控制规则 1743
关于访问控制规则 1743
访问控制规则管理 1745
访问控制规则组成部分 1745
访问控制规则顺序 1747
访问控制规则操作 1748
访问控制规则监控操作 1748
访问控制规则信任操作 1748
访问控制规则阻止操作 1749
访问控制规则交互式阻止操作 1749
访问控制规则允许操作 1750
使用文件和入侵策略的深度检测 1750
文件和入侵检查顺序 1751
使用入侵和文件策略的访问控制流量处理 1752
访问控制规则的要求和先决条件 1754
访问控制规则的准则与限制 1754
应用控制的最佳实践 1755
应用控制的建议 1755

在应用匹配和端口匹配之间进行选择 1757
特定于应用的说明和限制 1758
访问控制规则的最佳实践 1758
访问控制最佳实践 1758
规则排序的最佳实践 1759
应用程序规则顺序 1760
规则抢占 1760
规则操作和规则顺序 1761
简化和集中规则的最佳实践 1762
访问控制规则和入侵策略的最大数量 1762
管理访问控制规则 1763
添加访问控制规则类别 1763
创建和编辑访问控制规则 1764
访问控制规则条件 1766
启用和禁用访问控制规则 1773
从一项访问控制策略复制访问控制规则 1773
将访问控制规则移至预过滤策略 1774
定位访问控制规则 1776
将注释添加到访问控制规则 1777
访问控制规则的示例 1777
如何使用安全区域来控制访问 1777
如何控制应用的使用 1777
如何阻止威胁 1779
访问控制规则的历史记录 1781

第 42 章 **URL 过滤规则** 1785
URL 过滤概述 1785
关于使用类别和信誉进行 URL 过滤 1786
URL 类别和信誉说明 1787
来自思科云的 URL 过滤数据 1787
URL 过滤的最佳实践 1787

过滤 HTTPS 流量 1791
在 URL 过滤中使用类别 1792
QUIC 指纹识别 1792
URL 过滤的许可证要求 1793
URL 过滤的要求和前提条件 1793
如何使用类别和信誉配置 URL 过滤 1793
使用类别和信誉启用 URL 过滤 1794
URL 过滤选项 1795
配置 URL 条件 1796
具有 URL 条件的规则 1798
URL 规则顺序 1798
DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别 1798
启用 DNS 过滤以在域查找期间识别 URL 1798
DNS 过滤限制 1799
DNS 过滤和事件 1799
手动 URL 过滤 1799
手动 URL 过滤选项 1800
补充或选择性覆盖基于类别和信誉的 URL 过滤 1801
配置 HTTP 响应页面 1801
对 HTTP 响应页面的限制 1802
HTTP 响应页面的要求和前提条件 1802
选择 HTTP 响应页面 1803
配置对 HTTP 响应页面的交互式阻止 1803
配置交互式阻止 1804
为受阻网站设置用户绕过超时 1804
配置 URL 过滤运行状况监控器 1805
争议 URL 类别和信誉 1805
如果 URL 类别集发生更改，请执行操作 1806
URL 类别和信誉变更：对事件的影响 1807
URL 过滤故障排除 1807
URL 过滤的历史记录 1810

第 43 章 入侵防御 1813
关于入侵防御 1813
Snort 检测引擎 1814
关于 Snort 3 1815
Snort 3 多进程支持 1816
禁用 Snort 3 多进程支持 1817
网络分析和入侵策略的准则和限制 1817
策略如何检查流量是否存在入侵 1818
解码、规范化和预处理：网络分析策略 1819
访问控制规则：入侵策略选择 1820
入侵检查：入侵策略、规则和变量集 1821
入侵事件生成 1822
Snort 中的不对称流检查 1823
系统提供的与自定义的网络分析和入侵策略 1824
系统提供的网络分析和入侵策略 1824
自定义网络分析和入侵策略的优势 1825
自定义网络分析策略的优势 1826
自定义入侵策略的优势 1827
自定义策略的限制 1827
网络分析和入侵策略的必备条件 1829

第 IX 部分： 访问控制的解密策略和加密可视性 1831

第 44 章 流量解密概述 1833
流量解密已说明 1833
TLS/SSL 握手处理 1835
ClientHello 消息的处理 1835
ServerHello 和服务器证书消息处理 1838
解密 规则和策略基础知识 1840
解密案例 1841

何时解密流量以及何时不解密 1841
哪种类型的解密策略适合我？ 1843
解密和重新签名（传出流量） 1844
传入流量解密 1844
其他 解密规则 操作 1845
解密规则 组件 1845
解密规则基于规则的解密规则 顺序评估 1846
多规则示例 1847
TLS 加密加速 1849
TLS 加密加速准则和限制 1850
查看 TLS 加密加速的状态 1851
DTLS 加密加速 1851
DTLS 加密加速的先决条件 1852
监控 DTLS 加密加速 1852
的历史记录解密策略 1855

第 45 章 标准解密 策略 1861
关于标准解密策略 1861
哪种类型的解密策略适合我？ 1861
10.0.0 之前版本的标准解密策略部署问题 1862
创建新的 标准解密 策略 1863
创建具有入站保护的 标准解密 策略 1863
安全区 1864
内部服务器详细信息（入站解密） 1866
创建具有入站保护的 标准解密 策略 1867
安全区 1868
解密网络和用户 1869
内部证书颁发机构 1871
解密时绕过流量 1873
阻止连接 1878
标准解密 策略高级选项 1879

添加受信任 CA 证书 1881
解密策略操作 1882
将 标准解密 策略转换为 基于规则的解密 策略 1882
复制解密策略 1883
生成解密策略报告 1883

第 46 章 基于规则的解密 策略 1885
关于基于规则的解密策略 1885
哪种类型的解密策略适合我？ 1885
创建一个 基于规则的解密策略 1887
创建具有出站连接保护的 基于规则的解密策略 1887
创建具有入站连接保护的 基于规则的解密策略 1889
基于规则的解密策略 阻止连接 1891
基于规则的解密策略 排除项 1892
为出站保护生成内部 CA 1895
为出站保护上传内部 CA 1896
为入站保护上传内部证书 1897
在客户端计算机上安装内部 CA 1897
创建一个带有其他规则操作的 基于规则的解密策略 1898
基于规则的解密策略默认操作 1899
无法解密流量的默认处理选项 1900
设置无法解密的流量的默认处理 1901
基于规则的解密策略高级选项 1902
TLS 1.3 解密最佳实践 1904

第 47 章 基于规则的解密 规则 1907
关于基于规则的解密 1907
基于规则的解密规则 的要求和先决条件 1907
基于规则的解密规则准则和限制 1908
使用TLS/SSL解密的准则 1908
基于规则的解密规则 不支持的功能 1909

TLS/SSL 不解密准则 1910
TLS/SSL 传入流量解密准则 1911
TLS/SSL 解密 - 重新签名准则 1912
TLS/SSL 阻止准则 1914
TLS/SSL证书固定准则 1914
TLS/SSL 心跳准则 1915
TLS/SSL 匿名密码套件限制 1915
TLS/SSL 标准化程序准则 1915
其他 解密规则基于规则的解密规则 准则 1915
解密规则基于规则的解密规则 流量处理 1916
加密流量检查配置 1918
解密规则基于规则的解密规则 顺序评估 1919
解密规则基于规则的解密规则 条件 1920
安全区域规则条件 1921
安全区域条件和多租户 1921
网络规则条件 1921
VLAN 标记规则条件 1922
用户规则条件 1922
客户端威胁规则条件 1923
应用规则条件 1923
端口规则条件 1924
类别规则条件 1925
基于服务器证书的规则条件 1925
证书规则条件 1926
可分辨名称 (DN) 规则条件 1926
信任外部证书颁发机构 1930
证书状态 解密规则 条件 1932
密码套件规则条件 1934
加密协议版本规则条件 1937
解密规则基于规则的解密规则 操作 1937
基于规则的解密 规则监控操作 1937

基于规则的解密 规则 不解密操作 1938
基于规则的解密 规则阻止操作 1939
基于规则的解密 规则解密操作 1939
传入流量解密操作 1940
解密 - 重新签名规则操作 1942
选择内部证书对象 1943
监控 TLS/SSL 硬件加速 1943
信息计数器 1943
警报计数器 1944
错误计数器 1944
严重错误计数器 1945
对基于规则的解密规则进行故障排除 1945
关于 TLS/SSL 超订用 1945
对 TLS/SSL 超订用进行故障排除 1946
关于 TLS 心跳 1947
对 TLS 心跳进行故障排除 1948
关于 TLS/SSL 锁定 1949
对 TLS/SSL 锁定进行故障排除 1950
对未知或错误的证书或证书颁发机构进行故障排除 1952
验证 TLS/SSL 密码套件 1953
使用加密归档进行故障排除 1954

第 48 章 加密可视性引擎 1957
加密可视性引擎概述 1957
EVE 工作原理 1958
危害事件表现 1959
EVE 中的 QUIC 指纹识别 1959
配置 EVE 1959
查看 加密可视性引擎事件 1960
查看 EVE 控制面板 1961
配置 EVE 例外规则 1962

从统一事件添加例外规则 1964
升级 EVE 例外规则 1964
事件扩充 1965
EVE 示例 1965
关于加密可视性引擎 1965
优势 1966
示例业务情景 1966
前提条件 1966
高级工作流程 1966
在 EVE 中配置阻止阈值 1966
查看 EVE 事件 1970
其他参考资料 1971

第 X 部分： 访问控制的身份策略 1973

第 49 章 身份概述 1975
关于用户身份 1975
身份术语 1976
关于用户身份源 1976
用户身份的最佳实践 1978
身份部署 1980
如何设置身份策略 1982
用户活动数据库 1985
用户数据库 1985
主机和用户限制 1986
主机限制 1986
Microsoft Active Directory 的用户限制 1988
多实例设备中的最大用户映射数 1990
身份领域限制 1991
Microsoft Azure Active Directory 领域的用户限制 1991

第 50 章 领域 1993

领域的许可证要求 1993

领域的要求和先决条件 1993

创建Microsoft Azure AD (SAML)领域 1994

如何为被动身份验证创建 Microsoft Azure AD (SAML) 1995

关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE 1996

关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE 1996

如何为 Microsoft Azure AD (SAML) 配置Cisco ISE 1997

为被动身份验证配置 Microsoft Entra ID 1997

配置 Entra ID 基本设置 1999

获取 Microsoft Azure AD (SAML) 领域所需的信息 2000

为被动身份验证创建Microsoft Azure AD (SAML)领域 2002

如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户） 2005

配置 Entra ID 基本设置 2008

在 Entra ID 中创建单点登录 (SSO) 应用 2009

创建具有“解密-重新签名”操作的解密规则 2010

获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证） 2011

创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户） 2014

创建 LDAP 领域或 Active Directory 领域和领域目录 2019

关于领域和领域序列 2022

领域和受信任的域 2023

领域支持的服务器 2027

支持的服务器对象类和属性名称 2028

Kerberos 身份验证的必备条件 2029

领域字段 2029

领域目录和同步字段 2032

安全地连接到 Active Directory 或 LDAP 2035

查找 Active Directory 服务器名称 2035

导出 Active Directory 服务器的根证书 2036

同步用户和组 2037

创建领域序列 2039
将防火墙管理中心配置为跨域信任：设置 2040
为Secure Firewall Management Center配置跨域信任 步骤 1：配置领域和目录 2041
为Secure Firewall Management Center配置跨域信任 步骤 2：同步用户和组 2046
为跨域信任配置Secure Firewall Management Center 步骤 3：解决问题 2047
管理领域 2048
比较领域 2049
领域和用户下载故障排除 2049
检测领域或用户不匹配 2053
排除跨域信任故障 2054
领域的历史记录 2057

第 51 章 身份源：强制网络门户 2059
强制网络门户身份源 2059
关于主机名重定向 2060
强制门户的许可证要求 2060
强制网络门户的要求和先决条件 2060
强制网络门户准则和限制 2060
如何为用户控制配置强制网络门户 2063
创建网络对象 2064
创建身份策略和主动身份验证规则 2066
更新自定义身份验证表单 2068
创建 TCP 端口访问控制规则 2068
创建用户访问控制规则 2069
创建带有出站规则的解密策略 2070
将身份策略和解密策略与访问控制策略相关联 2072
强制网络门户字段 2073
排除强制网络门户中的应用 2074
强制网络门户身份源故障排除 2075
强制网络门户历史记录 2077

第 52 章 身份源：ISE/ISE-PIC 2079

The ISE/ISE-PIC 身份源 2079

源和目标安全组标记 (SGT) 匹配 2080

ISE/ISE-PIC 的许可证要求 2081

ISE/ISE-PIC 的要求和先决条件 2081

ISE/ISE-PIC 准则和限制 2081

如何为用户控制配置 ISE/ISE-PIC 2084

如何在不使用领域的情况下配置 ISE/ISE-PIC 2084

如何为无领域的用户控制配置 ISE/ISE-PIC 2085

配置 ISE/ISE-PIC 2086

在 ISE 中配置安全组和 SXP 发布 2086

从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center中使用 2089

导出系统证书 2090

生成自签名证书 2090

导入 ISE/ISE-PIC 证书 2091

配置思科身份服务引擎 (Cisco ISE)身份源的方法 2092

关于Cisco ISE快速配置 2092

Cisco ISE快速配置的前提条件 2093

快速配置 2094

思科身份服务引擎 (Cisco ISE)快速配置结果 2095

Cisco ISE 高级配置 2098

ISE/ISE-PIC 配置字段 2100

排除 Cisco ISE/ISE-PIC 或思科 TrustSec 问题 2101

ISE/ISE-PIC 的历史记录 2103

第 53 章 身份源：被动身份代理 2107

被动身份代理身份源 2107

部署 被动身份代理 2109

简单 被动身份代理 部署 2110

单 被动身份代理 监控多个域控制器 2110

多个 被动身份代理 监控多个域控制器 2111
被动身份代理 主/辅助代理部署 2113
如何创建 被动身份代理 身份源 2114
配置 被动身份代理 2116
启用 dynamic attributes connector 2116
创建 Microsoft Active Directory 领域 2116
创建被动身份代理身份源 2117
创建独立被动身份代理身份源 2118
创建主身份源或辅助被动身份代理身份源 2120
关于被动身份代理角色 2122
为被动身份代理创建Secure Firewall Management Center用户 2123
关于被动身份代理安装 2124
安装 被动身份代理 的先决条件 2125
安装 被动身份代理 软件 2129
卸载被动身份代理软件 2132
升级被动身份代理软件 2133
监控 被动身份代理 2133
管理被动身份代理 2134
编辑 被动身份代理 2135
删除独立 被动身份代理 2135
删除主和辅助 被动身份代理 2135
被动身份代理 故障排除 2136
被动身份代理 的安全要求 2137
被动身份代理的互联网接入要求 2138
被动身份代理 的历史记录 2139

第 54 章 **身份源：pxGrid Cloud 身份（ISE 3.3 及更低版本） 2141**
关于 pxGrid 云身份源 2141
pxGrid 云身份源 的限制 2142
pxGrid 云身份源 工作原理 2142
如何配置 pxGrid 云身份源 2143

如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本） 2143
在 Cisco ISE 中启用 pxGrid Cloud 服务 2146
使用 Catalyst 云门户 注册 Cisco ISE 2146
向 Cisco ISE 注册 pxGrid 云 连接 2149
创建一个 pxGrid 云身份源 2150
创建应用实例 2151
创建身份源 2152
激活应用实例 2153
激活 pxGrid 云身份源 2156
测试 pxGrid 云身份源 2158
创建动态属性过滤器 2164
使用动态属性过滤器来创建访问控制规则或 DNS 规则 2165
pxGrid 云身份源 故障排除 2167
无法处理主设备 2167
停用并删除 pxGrid 云身份源 2168
停用 pxGrid 云 应用实例 2168
删除 pxGrid 云身份源 2171

第 55 章 **身份源：pxGrid Cloud 身份（ISE 3.4 及更高版本）** 2173
关于 pxGrid 云身份源 2173
pxGrid 云身份源 的限制 2174
pxGrid 云身份源 工作原理 2174
如何配置 pxGrid 云身份源 2175
如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本） 2175
在 Cisco ISE 中启用 pxGrid 云 服务 2177
在 Catalyst 云门户 中验证 Cisco ISE 注册 2179
创建应用实例 2180
创建身份源 2181
激活应用实例 2182
激活 pxGrid 云身份源 2185
测试 pxGrid 云身份源 2187

pxGrid 云身份源 故障排除 2193
无法处理主设备 2193
创建动态属性过滤器 2194
使用动态属性过滤器来创建访问控制规则或 DNS 规则 2196
停用并删除 pxGrid 云身份源 2197
停用 pxGrid 云 应用实例 2197
删除 pxGrid 云身份源 2200

第 56 章 身份源：远程访问 VPN 2203
远程访问 VPN 身份源 2203
配置用户控制 RA VPN 2204
远程访问 VPN 身份源的故障排除准则 2205
未观察到 VPN 统计信息的正确设置 2205
远程接入 VPN 的历史记录 2206

第 57 章 身份源：TS 代理 2207
终端服务 (TS) 代理身份源 2207
TS 代理准则 2208
身份源：TS 代理 2208
TS 代理身份源故障排除 2208
TS 代理的历史记录 2209

第 58 章 身份策略 2211
关于身份策略 2211
身份策略的许可证要求 2212
身份策略的要求和先决条件 2212
创建身份策略 2213
创建身份映射过滤器 2214
身份规则条件 2215
安全区域规则条件 2215
安全区域条件和多租户 2216

网络规则条件 2216
重定向到主机名的网络规则条件 2216
VLAN 标记规则条件 2217
端口规则条件 2217
端口、协议和 ICMP 代码规则条件 2218
领域和设置规则条件 2219
创建身份规则 2221
身份规则字段 2222
示例身份策略和规则 2223
创建带有被动身份验证规则的身份策略 2224
使用主动身份验证规则创建示例身份策略 2226
使用领域进行主动身份验证 2228
使用领域序列的主动身份验证 2229
管理身份策略 2230
管理身份规则 2230
用户控制故障排除 2231

第 XI 部分： 访问控制的高级策略和设置 2233

第 59 章 预过滤器策略 2235
关于预过滤器策略 2235
默认预过滤策略 2236
预过滤策略规则顺序 2236
隧道与预过滤器规则 2237
系统如何处理明文隧道 2237
使用隧道区域在隧道级别应用访问控制 2238
大型流量分流 2238
流量卸载限制 2240
预过滤器与访问控制策略 2242
预过滤策略 的要求和先决条件 2243
预过滤策略 的准则和限制 2244

封装流量处理的准则和限制 2244
快速路径预过滤器的最佳实践 2245
配置预过滤策略 2246
配置默认操作 2248
配置预过滤规则 2248
VLAN 标记规则条件 2250
预过滤规则的端口规则条件 2250
配置隧道规则 2251
创建隧道区域 2253
将预过滤器规则移至访问控制策略 2254
预过滤器策略示例 2255
如何为重定区域隧道进行自定义检测 2255
如何卸载大型流量 2257
预过滤策略的历史记录 2259

第 60 章 安全情报 DNS 策略 2261
DNS 策略概述 2261
Cisco Umbrella DNS 策略 2262
DNS 策略组件 2262
DNS 策略许可证要求 2263
DNS 策略的要求和前提条件 2263
管理 DNS 和 Umbrella DNS 策略 2264
创建基本 DNS 策略 2264
编辑 DNS 策略 2265
DNS 规则 2266
创建和编辑 DNS 规则 2266
DNS 规则管理 2267
启用和禁用 DNS 规则 2267
DNS 规则顺序评估 2268
DNS 规则操作 2268
DNS 规则条件 2269

安全区域规则条件 2270
网络规则条件 2270
VLAN 标记规则条件 2270
DNS 策略规则条件 2271
动态属性规则条件 2271
如何创建 DNS 规则 2271
根据 DNS 和安全区域控制流量 2272
根据 DNS 和网络控制流量 2272
根据 DNS 和 VLAN 控制流量 2273
根据 DNS 列表或源来控制流量 2274
根据安全组标记或动态属性控制流量 2274
使用 DNS Sinkhole 执行内容限制 2275
DNS 策略部署 2276
Cisco Umbrella DNS 策略 2276
如何将 DNS 请求重定向到 Cisco Umbrella 2277
配置 Umbrella DNS 连接器的前提条件 2277
配置 Cisco Umbrella 连接设置 2279
创建 Umbrella DNS 策略 2280
编辑 Cisco Umbrella DNS 策略和规则 2280
将 Umbrella DNS 策略与访问控制策略相关联 2281

第 61 章 网络恶意软件防护的文件策略 2283
关于网络恶意软件防护和文件策略 2283
文件策略 2284
文件策略的要求和前提条件 2284
文件和恶意软件策略许可证要求 2285
文件策略和恶意软件检测的最佳实践 2285
文件规则最佳实践 2285
文件检测最佳实践 2286
文件阻止最佳实践 2286
文件策略最佳实践 2287

如何配置恶意软件防护 2288
规划和准备恶意软件防护 2289
配置文件策略 2290
将文件策略添加到访问控制配置 2290
配置访问控制规则以执行恶意软件保护 2291
设置恶意软件防护的维护和监控 2292
恶意软件防护的云连接 2293
AMP 云连接配置 2294
AMP 云连接的要求和最佳实践 2294
选择 AMP 云 2295
思科 AMP 私有云 2295
管理与 AMP 云的连接（公共或私有） 2297
更改 AMP 选项 2298
动态分析连接 2298
动态分析的要求 2298
查看默认动态分析连接 2298
动态分析本地设备 (Cisco Secure Secure Malware Analytics) 2299
启用对公共云中动态分析结果的访问权限 2300
维护您的系统：符合动态分析条件的文件类型 2301
文件策略和文件规则 2302
创建或编辑策略 2302
高级和存档文件检查选项 2303
管理文件策略 2306
文件规则 2307
文件规则组成部分 2307
文件规则操作 2308
创建文件规则 2315
用于恶意软件防护的访问控制规则日志记录 2316
追溯处置情况更改 2316
文件和恶意软件检测性能和存储选项 2317
调整文件和恶意软件检测性能和存储 2318

（可选）Secure Endpoint 的恶意软件防护 2319
恶意软件防护比较：Firepower 与Secure Endpoint 2319
关于将 Firepower 与Secure Endpoint 进行集成 2320
集成 Firepower 和Secure Endpoint 的优势 2320
Secure Endpoint 和 AMP 私有云 2321
集成 Firepower 和 Secure Endpoint 2321
网络恶意软件保护和文件策略的历史记录 2323

第 62 章 **Dynamic Attributes Connector** 2325
关于 dynamic attributes connector 2325
运作方式 2325
网络下载模式 2327
dynamic attributes connector 的历史记录 2329
Dynamic Attributes Connector 的系统要求 2330
启用 dynamic attributes connector 2330
为 Docker 容器配置网络和子网 2331
关于控制面板 2333
未配置系统的控制面板 2334
已配置系统的控制面板 2335
添加、编辑或删除连接器 2337
添加、编辑或删除动态属性过滤器 2338
创建连接器 2340
Amazon Web Services 连接器 — 关于用户权限和导入的数据 2341
为 dynamic attributes connector 创建具有最小权限的 AWS 用户 2341
创建 AWS 连接器 2343
Amazon Web 服务安全组连接器 - 关于用户权限 2344
为 dynamic attributes connector 创建具有最小权限的 AWS 用户 2344
创建 AWS 安全组连接器 2345
创建 AWS 服务标签连接器 2346
Azure 连接器 - 关于用户权限和导入的数据 2347
创建对 dynamic attributes connector 具有最小权限的 Azure 用户 2348

创建 Azure 连接器 2350
创建 Azure 服务标签连接器 2351
思科 APIC 连接器 2352
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象 2353
与 思科 APIC 集成的系统要求 2354
获取集成所需的信息 2354
创建连接器思科 APIC 2358
手动获取证书颁发机构 (CA) 链 2359
创建 Cisco Cyber Vision 连接器 2362
创建通用文本连接器 2364
创建 GitHub 连接器 2365
Google 云连接器 - 关于用户权限和导入的数据 2366
创建对 dynamic attributes connector 具有最小权限的 Google 云用户 2366
创建 Google Cloud 连接器 2367
创建 Office 365 连接器 2368
vCenter 连接器 - 关于用户权限和导入的数据 2369
创建对 dynamic attributes connector 具有最小权限的 vCenter 用户 2370
创建 vCenter 连接器 2371
创建 Webex 连接器 2373
创建 Zoom 连接器 2374
创建动态属性过滤器 2375
动态属性过滤器示例 2376
手动获取证书颁发机构 (CA) 链 2378
在访问控制策略或 DNS 策略中使用动态对象 2381
关于访问控制规则或 DNS 规则中的动态对象 2381
创建动态属性过滤器 2381
动态属性规则条件 2383
在 Secure Firewall Management Center 中查看动态对象 2383
使用动态属性过滤器来创建访问控制规则或 DNS 规则 2385
在 DNS 策略中使用动态对象 2386

动态防火墙 2386
关于 动态防火墙 2387
如何配置 动态防火墙 2387
启用 dynamic attributes connector 2390
获取所需的 身份情报 信息 2390
为 动态防火墙 创建身份源和领域 2392
创建 动态防火墙 实例 2392
将身份源与 身份情报 相关联 2393
配置 身份情报 2395
查看系统定义的过滤器 2396
查看系统定义的访问控制规则 2397
编辑用户排除列表 2399
查看和编辑系统创建的访问控制策略 2400
创建动态属性过滤器 2401
禁用 dynamic attributes connector 2403
使用 Secure Firewall Management Center 进行故障排除 2403
手动获取证书颁发机构 (CA) 链 2403
安全要求 2406
互联网接入要求 2407
dynamic attributes connector 的历史记录 2408

第 63 章 威胁情报导向器 2411
Cisco Secure Firewall 威胁智能导向器 概述 2411
威胁智能导向器和安全智能 2413
威胁情报导向器的性能影响 2413
威胁情报导向器要求和前提条件 2414
平台、元素和许可证要求 2414
源要求 2415
源内容限制 2416
如何设置威胁智能导向器 2416
配置策略以支持威胁智能导向器 2417

采集数据源的选项 2418
获取要用作源的 TAXII 源 2419
从 URL 获取源 2420
上传本地文件以用作源 2421
处理重复指示器 2422
为 威胁智能导向器 源配置 TLS/SSL 设置 2423
具有 威胁智能导向器 访问权限的用户角色 2424
关于备份和恢复 威胁智能导向器 数据 2424
分析 威胁智能导向器 事件和观察数据 2425
观察和事故生成 2425
查看和管理事故 2427
事故摘要信息 2428
事件详细信息 2428
查看 威胁智能导向器 观察的事件 2432
Secure Firewall Management Center事件中的 威胁智能导向器 观察对象 2432
影响所执行操作的因素 2433
威胁智能导向器-防火墙管理中心 操作优先级 2433
查看和更改威胁智能导向器 配置 2437
查看元素（托管设备）的 威胁智能导向器 状态 2437
查看和管理源 2437
源摘要信息 2438
源状态详细信息 2439
查看和管理指示器 2440
指示器摘要信息 2441
指标详细信息 2442
查看和管理可观察对象 2443
可观察对象摘要信息 2444
过滤表视图中的 威胁智能导向器 数据 2444
威胁智能导向器 配置中的继承 2445
继承多个父级的 TID 设置 2445
关于覆盖继承的 TID 设置 2446

在源、指示器或可观察对象级别编辑 威胁智能导向器操作 2447
关于暂停发布 2447
暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据 2448
在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 2449
修改可观察对象的发布频率 2449
关于将 威胁智能导向器 可观察对象添加到“不阻止”列表 2450
将 威胁智能导向器 可观察对象添加到不阻止列表 2450
查看 STIX 源文件 2451
对威胁智能导向器进行故障排除 2451
的历史记录威胁智能导向器 2453

第 64 章 访问控制的高级设置 2455
高级设置的要求与前提条件 2455
为访问控制策略配置高级设置 2456
常规设置 2458
TLS 服务器身份发现 2459
智能应用绕行 2461
配置智能应用旁路 2462
IAB 日志记录和分析 2463
传输/网络层预处理器设置 2466
检测增强设置 2467
自适应配置文件更新 2468
自适应配置文件更新和建议的规则 2468
性能设置 2468
基于延迟的性能设置 2470
访问控制策略的高级设置历史记录 2471

第 65 章 服务策略 2473
关于威胁防御服务策略 2473
服务策略如何关联 FlexConfig 和其他功能 2474
什么是连接设置？ 2474

服务策略的要求和先决条件 2475
服务策略准则和限制 2475
配置威胁防御服务策略 2476
配置服务策略规则 2476
绕过非对称路由的 TCP 状态检查（TCP 状态绕行） 2479
非对称路由问题 2479
有关 TCP 状态绕行的准则和限制 2480
配置 TCP 状态绕行 2481
禁用 TCP 序列随机化 2483
监控服务策略 2484
服务策略规则示例 2484
保护服务器免受 SYN 洪水 DoS 攻击（TCP 拦截） 2485
使 Firewall Threat Defense 设备显示在跟踪路由上 2487
威胁防御服务策略的历史记录 2489

第 66 章 威胁检测 2491
端口扫描检测和预防 2491
端口扫描检测的预定义敏感度级别 2491
在低敏感度级别检测 2493
威胁检测的要求和先决条件 2493
威胁检测准则和限制 2494
端口扫描防护最佳实践 2494
配置端口扫描检测和预防 2495
监控威胁检测 2497
查看端口扫描警报 2497
在防火墙上监控端口扫描 2498
取消阻止主机 2498
威胁检测的历史记录 2499

第 67 章 大象流检测 2501
关于大象流检测和补救 2501

从智能应用绕行升级大象流 2501
配置大象流检测 2502
大象流检测示例 2505
关于大象流 2505
关于大象流检测和补救的优势 2505
大象流工作流程 2505
示例业务情景 2506
前提条件 2506
配置大象流参数 2506
查看大象流的事件 2509
配置大象流补救豁免 2511
查看大象流补救豁免事件 2513
其他参考资料 2514

第 XII 部分： 网络发现 2515

第 68 章 网络发现概述 2517
主机、应用和用户数据的检测 2517
主机和应用检测基础知识 2518
操作系统和主机数据被动检测 2518
操作系统和主机数据主动检测 2519
应用和操作系统的当前身份 2519
当前用户身份 2521
应用和操作系统的身份冲突 2521
NetFlow 数据 2522
使用 NetFlow 数据的要求（原则） 2523
NetFlow 与受管设备数据之间的差异 2523

第 69 章 主机身份源 2527
概述：主机数据收集 2527
主机身份源的要求和前提条件 2528

确定系统可以检测的主机操作系统 2528
识别主机操作系统 2528
自定义指纹 2529
管理指纹 2530
激活和停用指纹 2530
编辑活动指纹 2531
编辑非活动指纹 2531
为客户端创建自定义指纹 2532
为服务器创建自定义指纹 2534
主机输入数据 2536
第三方数据使用要求 2537
第三方产品映射 2537
映射第三方产品 2538
映射第三方产品修补程序 2539
映射第三方漏洞 2540
自定义产品映射 2541
创建自定义产品映射 2541
编辑自定义产品映射列表 2542
激活和停用自定义产品映射 2543
配置主机输入客户端 2543
Nmap 扫描 2544
Nmap 补救选项 2545
Nmap 扫描准则 2549
示例：使用 Nmap 解析未知操作系统 2550
示例：使用 Nmap 响应新主机 2551
管理 Nmap 扫描 2552
添加 Nmap 扫描实例 2553
编辑 Nmap 扫描实例 2554
添加 Nmap 扫描目标 2554
编辑 Nmap 扫描目标 2555
创建 Nmap 补救 2556

编辑 Nmap 补救 2558
运行按需 Nmap 扫描 2558
Nmap 扫描结果 2559
查看 Nmap 扫描结果 2559
Nmap 扫描结果字段 2560
导入 Nmap 扫描结果 2561
主机身份源的历史记录 2562

第 70 章 应用检测 2563
概述：应用检测 2563
应用检测器基础知识 2564
在 Web 界面中识别应用协议 2565
通过客户端检测进行隐含应用协议检测 2566
主机限制和发现事件日志记录 2566
应用检测的特殊注意事项 2567
Snort 3 中的应用检测 2568
应用检测的要求和前提条件 2569
自定义应用检测器 2569
自定义应用检测器和用户定义的应用字段 2569
配置自定义应用检测器 2572
创建用户定义的应用。 2573
指定基本检测器中的检测模式 2574
指定高级检测器中的检测条件 2575
指定 EVE 进程分配 2576
测试自定义应用协议检测器 2577
查看或下载检测器详细信息 2577
检测器列表排序 2578
过滤检测器列表 2578
检测器列表的过滤器组 2579
导航至其他检测器页面 2580
激活和停用检测器 2580

编辑自定义应用检测器 2581
删除检测器 2582

第 71 章 网络发现策略 2583
概述：网络发现策略 2583
网络发现策略的要求和前提条件 2584
网络发现自定义 2584
配置网络发现策略 2585
网络发现规则 2585
配置网络发现规则 2585
操作和发现的资产 2586
受监控网络 2587
端口排除 2589
网络发现规则中的区域 2591
基于流量的检测身份源 2592
配置高级网络发现选项 2594
网络发现常规设置 2595
配置网络发现常规设置 2595
网络发现身份冲突设置 2596
配置网络发现身份冲突解决方法 2596
网络发现漏洞影响评估选项 2597
启用网络发现漏洞影响评估 2597
危害表现 2598
启用危害表现规则 2598
将 NetFlow 导出器添加到网络发现策略 2599
网络发现数据存储设置 2599
配置网络发现数据存储 2601
配置网络发现事件日志记录 2601
添加网络发现操作系统和服务器身份源 2601
对网络发现策略进行故障排除 2602

第 XIII 部分： 对象和证书 2605

第 72 章 对象管理 2607

对象简介 2608

对象管理器 2610

导入对象 2610

编辑对象 2613

查看对象及其使用情况 2614

过滤对象或对象组 2615

对象组 2615

对可重用对象进行分组 2616

对象覆盖 2617

管理对象覆盖 2618

允许对象覆盖 2618

添加对象覆盖 2619

编辑对象覆盖 2619

AAA 服务器 2620

添加 RADIUS 服务器组 2620

RADIUS 服务器组选项 2620

RADIUS 服务器选项 2622

添加单点登录服务器 2623

访问列表 2625

配置扩展 ACL 对象 2625

配置服务访问对象 2628

配置标准 ACL 对象 2629

地址池 2630

应用过滤器 2631

AS 路径 2632

BFD 模板 2632

密码套件列表 2634

创建密码套件列表 2634
社区列表 2634
扩展社区 2635
DHCP IPv6 池 2637
可分辨名称 2637
创建可分辨名称对象 2639
DNS 服务器组 2640
创建 DNS 服务器组对象 2640
加密可视性引擎例外列表 2640
外部属性 2642
动态对象 2642
首次创建动态对象 2642
使用嵌入式 Dynamic Attributes Connector创建动态对象 2644
使用 Security Cloud Control创建动态对象 2645
在本地创建动态对象 Dynamic Attributes Connector 2646
处理动态对象 2647
动态对象映射 2647
关于 API 创建的动态对象 2647
安全组标记 2649
创建安全组标记对象 2649
文件列表 2650
文件列表的源文件 2650
将单个 SHA-256 值添加到文件列表 2651
将单个文件上传到文件列表 2652
将源文件上传到文件列表 2652
编辑文件列表中的 SHA-256 值 2653
从文件列表下载源文件 2654
FlexConfig 2654
地理定位 2655
创建地理位置对象 2655
接口 2655

密钥链 2656
创建密钥链对象 2656
网络 2658
网络通配符掩码 2659
创建网络对象 2660
导入网络对象 2661
PKI 2661
内部证书颁发机构对象 2662
CA 证书和私钥导入 2662
导入 CA 证书和私钥 2663
生成新的 CA 证书和私钥 2663
新签名证书 2664
创建未签名的 CA 证书和 CSR 2664
上传为响应 CSR 而颁发的签名证书 2664
CA 证书和私钥下载 2665
下载 CA 证书和私钥 2665
受信任证书颁发机构对象 2666
受信任的 CA 对象 2666
添加受信任 CA 对象 2666
受信任 CA 对象中的证书撤销列表 2667
向受信任 CA 对象添加证书撤销列表 2667
外部证书对象 2668
添加外部证书对象 2668
内部证书对象 2668
添加内部证书对象 2669
证书注册对象 2669
添加证书注册对象 2671
添加证书注册 2673
证书注册对象 EST选项 2673
证书注册对象 SCEP 选项 2674
证书注册对象 ACME 选项 2675

证书注册对象 证书参数 2677
证书注册对象 密钥选项 2678
证书注册对象 撤销选项 2680
策略列表 2680
端口 2682
创建端口对象 2683
导入端口对象 2683
前缀列表 2683
配置 IPv6 前缀列表 2684
配置 IPv4 前缀列表 2684
路由映射 2685
安全智能 2689
如何修改安全智能对象 2690
全局和域安全智能列表 2690
安全智能列表和多租户 2691
将条目添加到全局安全智能列表 2692
从全局安全智能列表中删除条目 2693
安全智能的列表和源更新 2693
更改安全智能源的更新频率 2694
自定义安全智能列表和源 2694
自定义列表和源：要求 2694
URL 列表和源：URL 语法和匹配条件 2695
自定义安全智能源 2696
自定义安全智能列表 2698
Sinkhole 2700
创建 Sinkhole 对象 2700
SLA 监控器 2700
时间范围 2702
创建时间范围对象 2702
时区 2703
隧道区域 2704

URL 2704
创建 URL 对象 2705
变量集 2705
入侵策略中的变量集 2706
变量 2707
预定义默认变量 2707
网络变量 2709
端口变量 2711
高级变量 2712
变量重置 2712
将变量添加到变量集 2713
嵌套变量 2714
管理变量集 2716
创建变量集 2716
管理变量 2717
添加变量 2718
编辑变量 2719
VLAN 标记 2720
创建 VLAN 标记对象 2720
VPN 2720
证书映射对象 2721
Secure Client 自定义属性对象 2722
添加 Secure Client 自定义属性对象 2722
向组策略中添加自定义属性 2723
Firewall Threat Defense组策略对象 2724
配置组策略对象 2724
组策略常规选项 2725
组策略 Secure Client 选项 2727
组策略高级选项 2730
Firewall Threat Defense IPSec 提议 2731
配置 IKEv1 IPsec 方案对象 2732

配置 IKEv2 IPsec 方案对象 2732
IKE 策略 2733
配置 IKEv1 策略对象 2733
配置 IKEv2 策略对象 2735
Secure Client 自定义 2736
文件对象 2737
对象管理的历史记录 2739

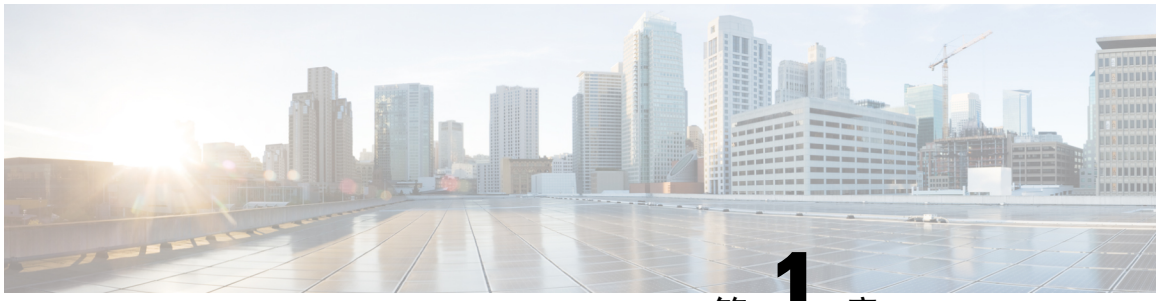
第 73 章 证书 2743
证书的要求和前提条件 2743
Cisco Secure Firewall Threat Defense VPN 证书准则和限制 2743
管理 Firewall Threat Defense 证书 2744
自动更新 CA 捆绑包 2745
使用自签注册安装证书 2747
使用 EST 注册安装证书 2748
使用 SCEP 注册安装证书 2749
使用手动注册安装证书 2750
使用 PKCS12 文件安装证书 2751
使用 ACME 注册安装证书 2751
排除 Firewall Threat Defense 证书问题 2752
证书的历史记录 2753



第 部分

设备配置入门

- 设备注册， 第 1 页
- 使用设备模板进行设备注册， 第 87 页
- 透明或路由防火墙模式， 第 123 页
- CLI 用户， 第 135 页
- 变更管理， 第 155 页
- 配置部署， 第 167 页



第 1 章

设备注册

您可以在 Secure Firewall Management Center 中添加和管理设备。

- 关于设备注册， 第 1 页
- 设备注册前提条件， 第 11 页
- 登录到设备的命令行界面， 第 12 页
- 为手动注册完成Firewall Threat Defense初始配置， 第 14 页
- 管理设备注册， 第 29 页
- 交换机管理器， 第 74 页
- 设备注册的历史记录， 第 80 页

关于设备注册

将设备注册到 防火墙管理中心。

管理中心概述

本指南适用于作为主要管理器或仅作为分析管理器的本地设备 防火墙管理中心。在将 Security Cloud Control 云交付的防火墙管理中心 用作主管理器时，您只能使用本地部署 防火墙管理中心 进行分析。请勿将本指南用于 云交付的防火墙管理中心；请参阅思科安全云控制：用于 *Cisco Secure Firewall Threat Defense* 的云交付防火墙管理中心。

防火墙管理中心是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。如果您需要多设备管理器，并且您需要 Firewall Threat Defense上的所有功能，则应使用 防火墙管理中心 。防火墙管理中心 还提供强大的流量和事件的分析与监控功能。

注释 如果您有 Security Cloud Control 托管设备，并且仅将本地部署防火墙管理中心用于分析，则本地部署防火墙管理中心不支持策略配置或升级。本指南中的某些相关章节和程序可能不适用于主要管理器为 Security Cloud Control的设备。

用作主用管理器的 防火墙管理中心： 防火墙管理中心 与其他管理器不兼容，因为 防火墙管理中心 拥有 Firewall Threat Defense 配置，不允许绕过 防火墙管理中心直接配置 Firewall Threat Defense 。

关于防火墙管理中心和设备管理

在防火墙管理中心管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。防火墙管理中心使用此信道向设备发送有关要如何分析和管理流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到防火墙管理中心。

通过使用防火墙管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向托管设备推送运行状况策略并从防火墙管理中心监控其运行状态



注释 如果您有 Security Cloud Control 托管设备，并且仅将本地部署防火墙管理中心用于分析，则本地部署防火墙管理中心不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为 Security Cloud Control 的设备。

防火墙管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用防火墙管理中心来管理设备行为的几乎每个方面。



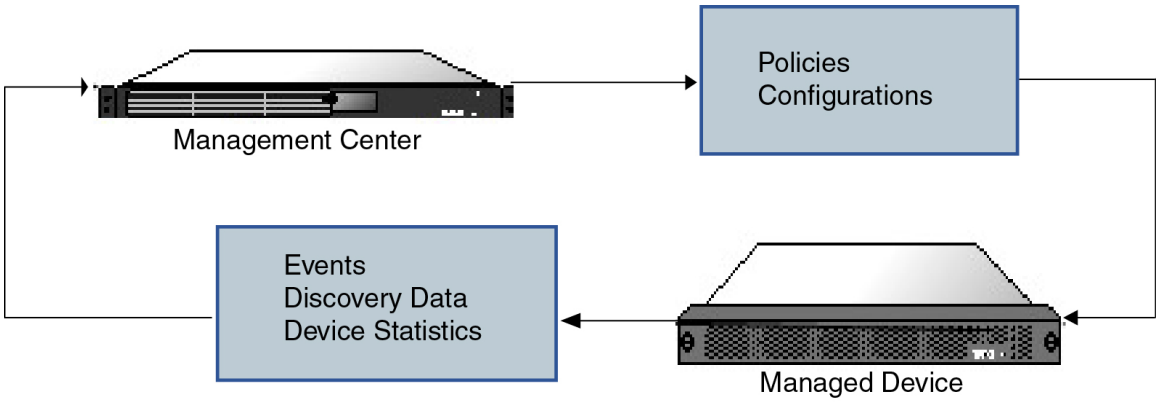
注释 尽管防火墙管理中心可以按照 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 中提供的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本Firewall Threat Defense软件的新功能不适用于这些以前发布的设备。某些防火墙管理中心功能可能适用于早期版本。

Secure Firewall Management Center可以管理哪些内容？

您可以将 Secure Firewall Management Center 用作集中管理点来管理Firewall Threat Defense设备。

管理设备时，信息通过 TLS-1.3-加密的安全隧道在防火墙管理中心和该设备之间传输。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

下图列出了在防火墙管理中心及其托管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



关于管理连接

使用防火墙管理中心信息配置设备并将设备添加到防火墙管理中心后，设备或防火墙管理中心可以建立管理连接。根据初始设置：

- 设备或防火墙管理中心都可以启动。
- 只有设备可以启动。
- 只有防火墙管理中心可以发起。

启动始终使用防火墙管理中心上的 eth0 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。 防火墙管理中心上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。默认情况下，管理连接使用 TCP 端口 8305（此端口可配置）。如果您在设备和防火墙管理中心之间放置另一个Firewall Threat Defense，为了防止潜在的管理中断，请务必通过为其应用预过滤器策略来豁免管理流量执行深度检查。

注释 管理连接是信道自身与设备之间的 TLS-1.3 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

除策略和事件以外的其他功能

除将策略部署到设备和从其接收事件以外，还可以在防火墙管理中心上执行其他设备相关任务。

备份设备

您无法从 FTD CLI 备份物理托管设备。要备份配置数据和（可选的）统一文件，请使用管理设备的防火墙管理中心来执行设备备份。

要备份事件数据，请对管理设备的防火墙管理中心执行备份。

更新设备

思科会不定期发布 Firepower 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库 (VDB) 更新
- 地理位置更新
- 软件补丁和更新

可以使用防火墙管理中心在其管理的设备上安装更新。

关于设备管理接口

每个设备都包含一个用于与 防火墙管理中心通信的管理接口。您可以选择将设备配置为使用数据接口进行管理，而不是专用的管理接口。

您可以在管理接口或控制台端口上执行初始设置。

管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

Firewall Threat Defense上的管理和事件接口

设置设备时，指定要连接到的防火墙管理中心 IP 地址或主机名称（如已知）。如果设备启动了连接，管理和事件流量都在初始注册时转到此地址。如果防火墙管理中心未知，则防火墙管理中心建立初始连接。在这种情况下，它最初可能从与Firewall Threat Defense上指定的不同的防火墙管理中心管理接口连接。后续连接应使用具有指定 IP 地址的防火墙管理中心管理接口。

单独的仅事件接口

您可以在防火墙管理中心和托管设备上配置单独的事件专用接口，以隔离事件流量。此设置通过将事件数据与管理操作分离来增强性能和安全性。

- 在托管设备上配置单独的仅事件接口之前，请始终在防火墙管理中心上启用事件接口。如果防火墙管理中心具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到防火墙管理中心仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。
- 如果事件网络关闭，则事件流量将恢复到防火墙管理中心和/或托管设备上的常规管理接口。如果设备管理接口关闭，系统将使用事件接口建立管理连接，即使您为其禁用管理流量也是如此。
- 请确保防火墙管理中心和托管设备在管理和事件接口方面具有一致的配置，以避免出现通信问题。

使用Firewall Threat Defense数据接口进行管理

您可以使用专用的管理接口或常规数据接口与防火墙管理中心通信。如果想要从外部接口远程管理 Firewall Threat Defense，或者您没有单独的管理网络，则在数据接口上进行管理器访问非常有用。此外，使用数据接口可以配置冗余辅助接口，以便在主接口发生故障时接管管理功能。

管理器访问要求

从数据接口进行管理器访问遵循以下要求。

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel，也不能在管理器访问接口上创建子接口。您还可以使用 防火墙管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 Firewall Threat Defense 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 防火墙管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 Firewall Threat Defense Virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。

高可用性要求

将数据接口与设备高可用性配合使用时，请参阅以下要求。

- 在两台设备上使用相同的数据接口进行管理器访问。
- 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。



注释 如果您使用 零接触调配 注册设备，则当您使用外部接口进行管理器访问时，它会默认使用 DHCP。在启用高可用性之前，需要将 IP 地址更改为静态地址。请参阅更改设备 IP 地址，第 879 页。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

- 在同一子网中有不同的静态 IP 地址。
- 使用相同的管理器配置（**configure manager add** 命令）确保连接相同。
- 不能将数据接口用作故障切换链路或状态链路。

每个设备型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。



注释 对于 Firepower 4100/9300，MGMT 接口用于机箱管理，而不是用于Firewall Threat Defense逻辑设备管理。必须将单独的接口配置为 mgmt（和/或 firepower-eventing）类型，然后将其分配给 Firewall Threat Defense 逻辑设备。

对于具有管理接口和事件接口的设备，如果一个接口关闭，则另一个接口将用作管理或事件的备份，即使您为接口禁用该功能也是如此。

有关每个托管设备型号上支持的管理接口，请参阅下表。

表 *1:* 托管设备上的管理接口支持

型号	管理界面	可选的事件接口
Secure Firewall 200	management0 **注释** management0 是管理 1/1 接口的内部名称。	不支持
Firepower 1000	management0 **注释** management0 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall 1200	management0 **注释** management0 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall 3100	management0 **注释** management0 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall 4200	management0 **注释** management0 是管理 1/1 接口的内部名称。	management1 **注释** management1 是管理 1/2 接口的内部名称。

型号	管理界面	可选的事件接口
Cisco Secure Firewall 6100	management0 注释 management0 是管理 1/1 接口的内部名称。	management1 注释 management1 是管理 1/2 接口的内部名称。
Firepower 4100 和 9300	management0 注释 management0 是此接口的内部名称，与物理接口 ID 无关。	management1 注释 management1 是此接口的内部名称，与物理接口 ID 无关。
ISA 3000	br1 注释 br1 是管理 1/1 接口的内部名称。	不支持
Secure Firewall Threat Defense Virtual	eth0	不支持

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。

注释 用于管理接口的路由完全独立于您为数据接口配置的路由。如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

在某些平台上，可以配置多个管理接口（一个管理接口和一个仅事件接口）。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到 Firewall Threat Defense的路由问题。

注释 用于管理连接的接口不由路由表决定。始终首先使用编号最低的接口来进行连接。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发防火墙管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共

IP 地址和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

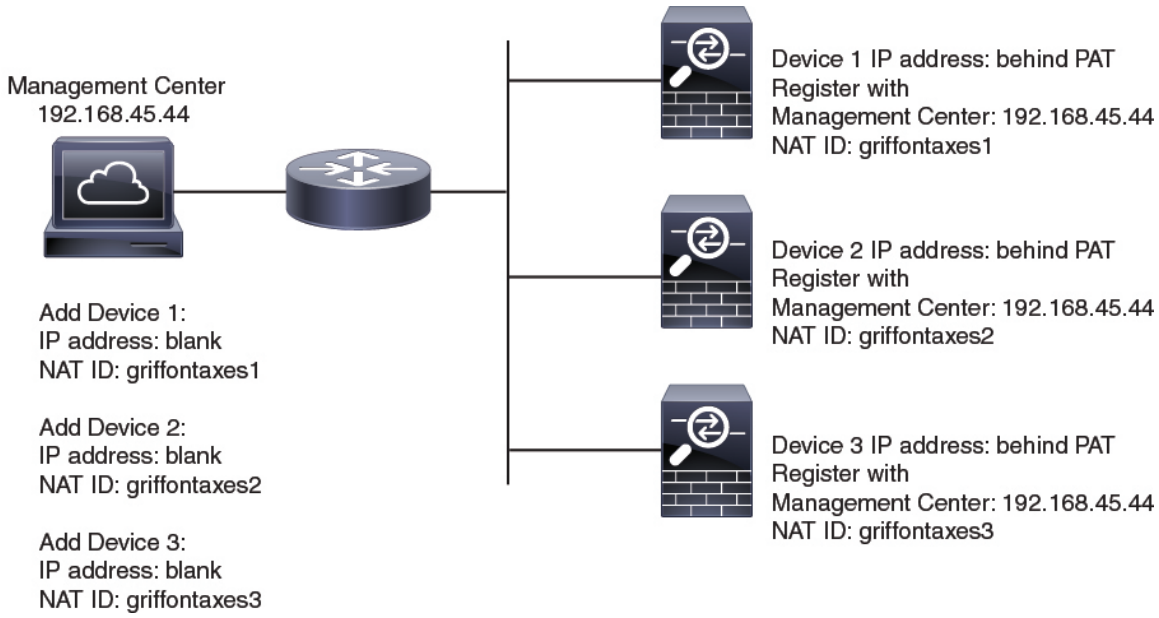
通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同一个注册密钥）：防火墙管理中心当添加一个设备时，指定设备 IP 地址，设备指定 防火墙管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。防火墙管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

例如，您将设备添加到 防火墙管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在 防火墙管理中心 上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定 防火墙管理中心 IP 地址、相同的 NAT ID 和相同的注册密钥。设备将注册到 防火墙管理中心的 IP 地址。此时，防火墙管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向 防火墙管理中心添加多个设备的过程。在 防火墙管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定 防火墙管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

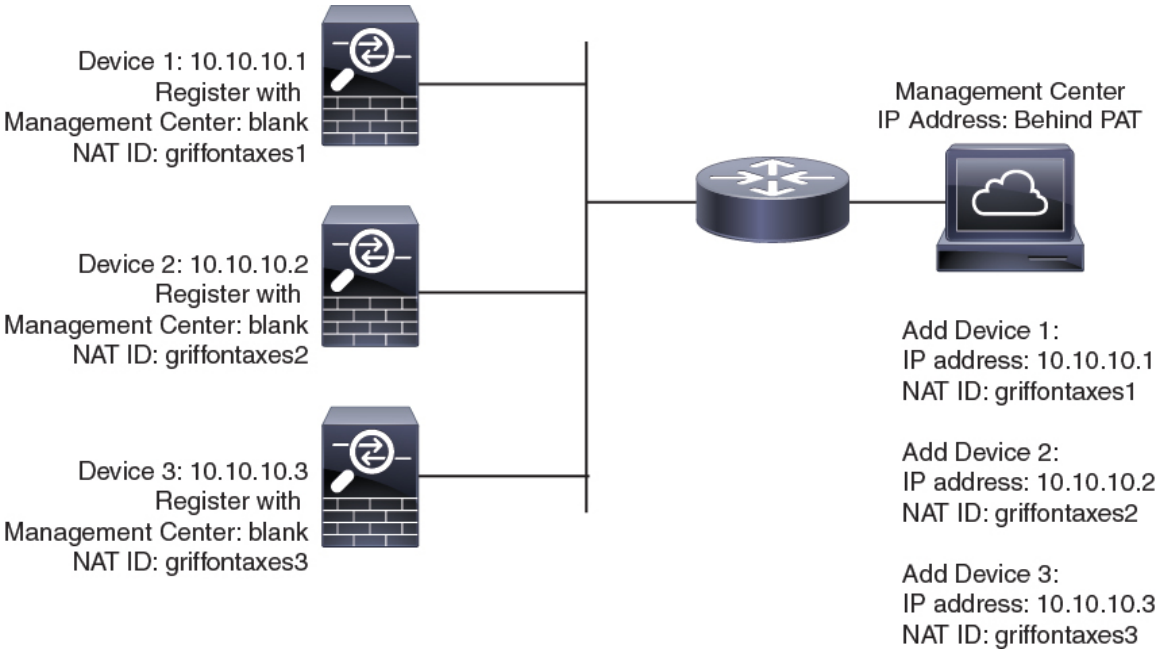
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在 防火墙管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定 防火墙管理中心 IP 地址。

图 *1: PAT* 后的托管设备 *NAT ID*



以下示例为 PAT IP 地址后的 防火墙管理中心。在这种情况下，在防火墙管理中心和这些设备上为每个设备指定一个唯一的 NAT ID，并在防火墙管理中心上指定设备 IP 地址。

图 *2: PAT* 后的 *FMC NAT ID*



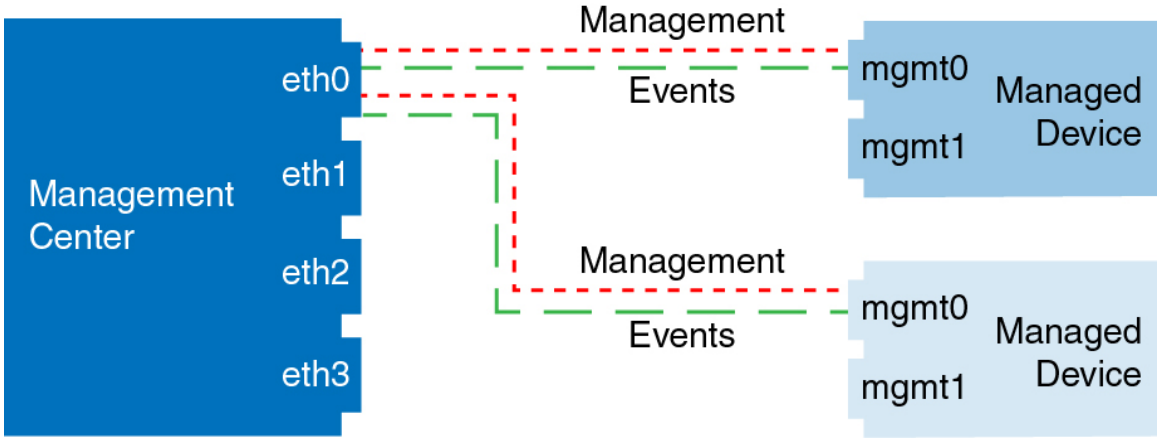
管理和事件流量通道示例

注释

- 在 防火墙管理中心 和托管设备上配置单独的专用事件接口，以将事件流量与管理流量隔离开来。这种分离通过隔离事件数据流来提高性能和安全性。
- 如果 防火墙管理中心 对管理和事件流量使用单个接口，则托管设备必须在该同一接口上发送事件流量。如果 防火墙管理中心 具有专用事件接口，则托管设备也必须配置专用事件接口。
- 在 防火墙管理中心 上混合使用和事件通道，而托管设备使用单独的事件接口，可能会导致连接或事件传送问题。确保 防火墙管理中心 与托管设备之间的接口配对一致。
- 如果在Firewall Threat Defense上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

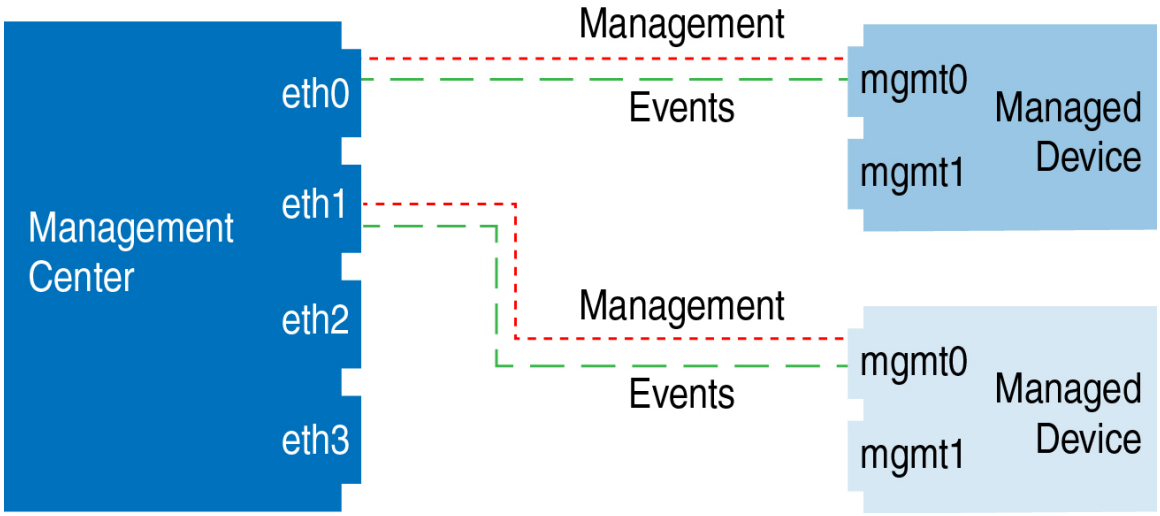
以下示例显示仅使用默认管理接口的防火墙管理中心和托管设备。

图 *3: Secure Firewall Management Center*上的单个管理接口



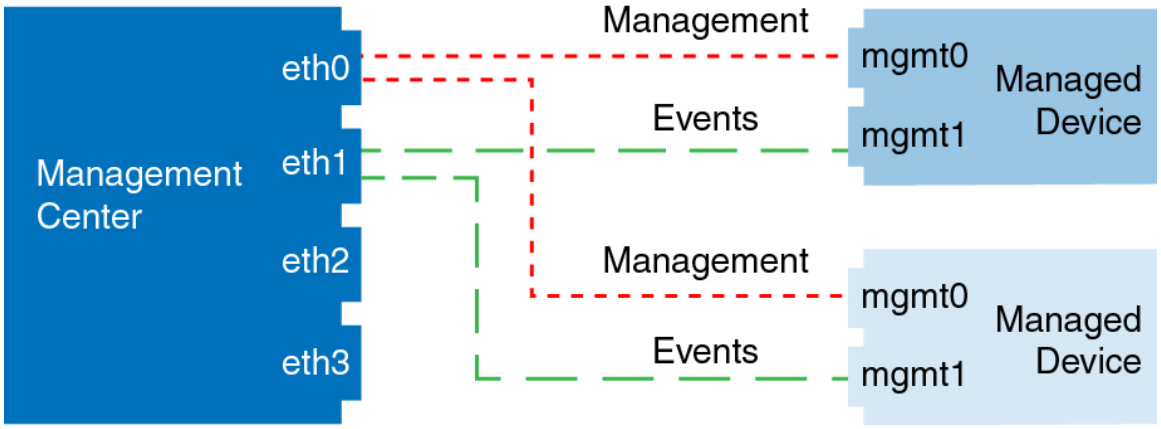
以下示例显示为设备使用单独管理接口的防火墙管理中心；每台托管设备均使用 1 管理接口。

图 *4: Secure Firewall Management Center*上的多个管理接口



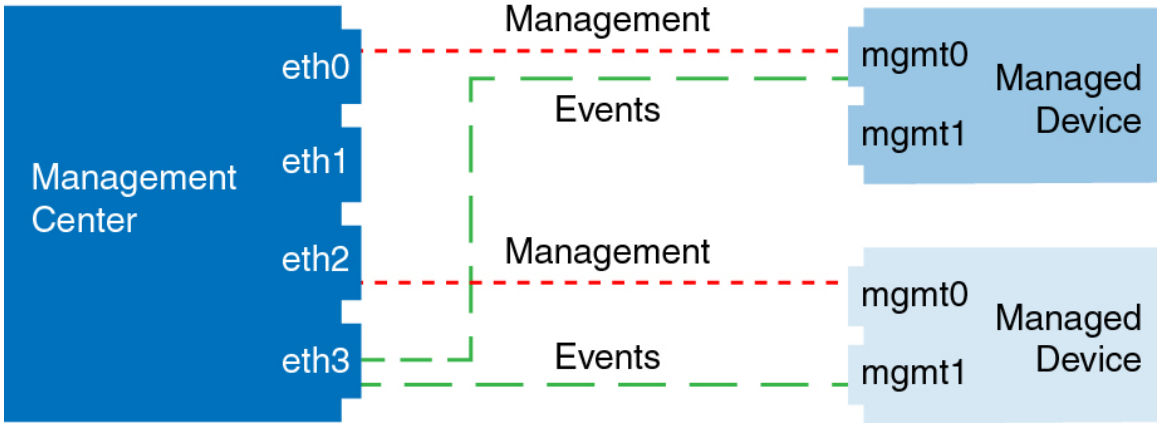
以下示例显示使用单独事件接口的防火墙管理中心和托管设备。

图 *5: Secure Firewall Management Center*和托管设备上的单独事件接口



以下示例显示防火墙管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的托管设备的混合。

图 *6:* 混合管理和事件接口用法



设备注册前提条件

支持的域

设备所在的域。

用户角色

- 管理员
- 网络管理员

管理连接

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

零接触调配 要求

零接触调配 不支持集群或多实例模式。

仅当使用管理接口时才支持高可用性，因为 零接触调配 使用 DHCP，数据接口和高可用性不支持 DHCP。

以下运行 7.4 或更高版本的型号支持零接触调配：

- Cisco Secure Firewall 200
- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（在支持的设备版本上）
- Cisco Secure Firewall 3100

登录到设备的命令行界面

您可以在Firewall Threat Defense设备上直接登录命令行界面。如果这是您第一次登录，请使用默认**管理员**用户完成初始设置过程；请参阅使用 CLI 完成Firewall Threat Defense初始配置 ，第 21 页。

对于零接触调配，如果您必须访问Firewall Threat Defense CLI 并运行设置脚本，请在系统出现以下提示时回答：**n**`是否要配置 IPv4? (y/n) [y]:` 和`是否要配置 IPv6? (y/n) [y]:`。您还必须接受默认本地管理器：`本地管理设备? (yes/no) [yes]:`。这些设置将保留零接触调配功能。

对于 Cisco Secure Firewall 200，设备最多仅支持三个并发 CLI 会话。例如，可以设置一个控制台会话，设置两个连接管理接口的 SSH 会话（该限制独立于连接数据接口的 SSH）。如果您已经有三个活动 SSH 会话，然后连接到控制台，则系统会允许控制台连接，因为控制台访问永远不会被阻止。

注释 当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

- 创建可以使用 **configure user add** 命令登录 CLI 的其他用户账号。
- 如果在连接到控制台端口时出现无法识别的字符，请验证端口设置。如果正确，请使用相同设置的另一台设备尝试使用该电缆。如果电缆正常，您可能需要更换控制台端口的硬件。另请考虑尝试其他工作站以进行连接。

过程

步骤 1 通过控制台端口或使用 SSH连接至 Firewall Threat Defense CLI。

可以通过 SSH 连接到Firewall Threat Defense设备的管理接口。如果您为 SSH 连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。请参阅 SSH 访问，第 991 页，以允许与特定数据接口建立 SSH 连接。

对于物理设备，您可以直接连接到设备上的控制台端口。有关控制台电缆的详细信息，请参阅设备的硬件指南。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

控制台端口上的 CLI 是 FXOS（ISA 3000 除外，它是常规 Firewall Threat Defense CLI）。使用 Firewall Threat Defense CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

对于多实例模式下的机箱，您可以通过控制台端口连接到 FXOS，也可以根据配置 SSH 和 SSH 访问列表，第 247 页在管理接口上为 FXOS 启用 SSH。默认情况下禁用 SSH。

步骤 2 使用**管理员**用户名和密码登录。

示例：

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

firepower#
```

步骤 3 如果您使用的是控制台端口，请访问 Firewall Threat Defense CLI。

connect ftd

多实例模式：

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

注释
此步骤不适用于 ISA 3000。

示例：

```
firepower# connect ftd
>
```

步骤 4 在 CLI 提示符 (>) 处，使用命令行访问级别所允许的任何命令。

要返回到控制台端口上的 FXOS，请输入 **exit**。

步骤 5 （可选） 如果您使用 SSH，则可以连接到 FXOS。

connect fxos

要返回到 Firewall Threat Defense CLI，请输入 **exit**。

步骤 6 （可选）访问诊断 CLI：

system support diagnostic-cli

使用此 CLI 可进行高级故障排除。此CLI包括额外 **show** 和其他命令。

此 CLI 有子模式：用户 EXEC、特权 EXEC 模式和恢复配置模式。相比用户 EXEC 模式，在特权 EXEC 模式中，有更多命令可用。要进入特权 EXEC 模式，请输入 **enable** 命令；在收到提示时按 Enter 键，无需输入密码。

示例：

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

要使用恢复配置模式，请参阅访问诊断 CLI 中的恢复配置模式。

要返回到常规 CLI，请键入 **Ctrl+a**, **d**。

为手动注册完成Firewall Threat Defense初始配置

您可以使用 CLI 完成Firewall Threat Defense初始配置，也可以为除 Firepower 4100/9300 之外的所有防火墙设备管理器型号完成初始配置。对于 Firepower 4100/9300，部署逻辑设备时，完成所有初始配置。请参阅Firepower 4100/9300 上的逻辑设备， 第 273 页。

对于零接触调配（序列号注册），您不应登录设备或执行初始设置。请参阅使用序列号添加设备（零接触调配） - 基本配置， 第 39 页。

注释 仅用于分析目的而注册到防火墙管理中心 (FMC) 的设备会计入 FMC 平台设备容量限制。随着设备数量的增加，对事件处理的要求也会增加。在规划仅分析部署时，请适当调整虚拟 FMC (vFMC) 层级的大小。

使用防火墙设备管理器完成Firewall Threat Defense初始配置

当您使用防火墙设备管理器进行初始设置时，除管理接口和管理器访问设置外，还会预配置以下接口：

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 1010/1210/1220/200，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的DHCP服务器、访问控制策略或安全区域等其他设置均未配置。

如果在向防火墙管理中心注册之前在防火墙设备管理器中执行其他特定于接口的配置，则会保留该配置。

使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

- Cisco Secure Firewall 4200/6100 不支持 防火墙设备管理器。您需要使用 CLI 程序：使用 CLI 完成Firewall Threat Defense初始配置，第 21 页
- 此程序不适用于仅将本地 防火墙管理中心 部署用于分析的 *Security Cloud Control*托管设备。防火墙设备管理器 配置是为了用于配置主管理器。有关配置设备以便进行分析的详细信息，请参阅使用 CLI 完成Firewall Threat Defense初始配置，第 21 页。
- 此程序适用于除 Firepower 4100/9300 和 ISA 3000 以外的所有 其他 设备。您可以使用 防火墙设备管理器将这些设备载入防火墙管理中心，但由于它们的默认配置不同于其他平台，所以此程序中的详细信息可能会不适用于这些平台。

过程

步骤 1 登录防火墙设备管理器。

a) 在浏览器中输入以下 URL。

- 内部 - **https://192.168.95.1**。
- 管理 - **https://***management_ip*。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。在此过程中，您必须将管理IP地址设置为静态地址，因此我们建议您使用内部接口，以免连接被断开。

b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。

c) 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

步骤 2 首次登录防火墙设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的 **跳过设备设置 (Skip device setup)** 来跳过安装向导。

完成设置向导后，除了内部接口的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到 防火墙管理中心 管理接口时进行维护。

a) 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

1. **外部接口地址 (Outside Interface Address)** - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

   如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

   配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置IPv4地址。您无法使用安装向导配置PPPoE。如果接口连接到DSL、电缆调制解调器或ISP的其他连接，并且ISP使用PPPoE来提供IP地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

   配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

2. **管理接口**

   如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。

   即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

   DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

   防火墙主机名 (Firewall Hostname) - 系统管理地址的主机名。

b) 配置**时间设置 (NTP) (Time Setting [NTP])** 并点击**下一步 (Next)**。

1. **时区** - 选择系统时区。
2. **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择**启动 90 日评估期而不注册**。

不要向智能软件管理器注册Firewall Threat Defense；所有许可均在防火墙管理中心上执行。

d) 点击**完成**。

e) 系统将提示您选择**云管理 (Cloud Management)** 或**独立 (Standalone)**。对于 防火墙管理中心 管理，请选择**独立 (Standalone)**，然后选择**知道了 (Got It)**。

步骤 3 （可能需要）配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用 防火墙设备管理器 连接的管理接口，则必须重新连接到 防火墙设备管理器 。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网

络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。

- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

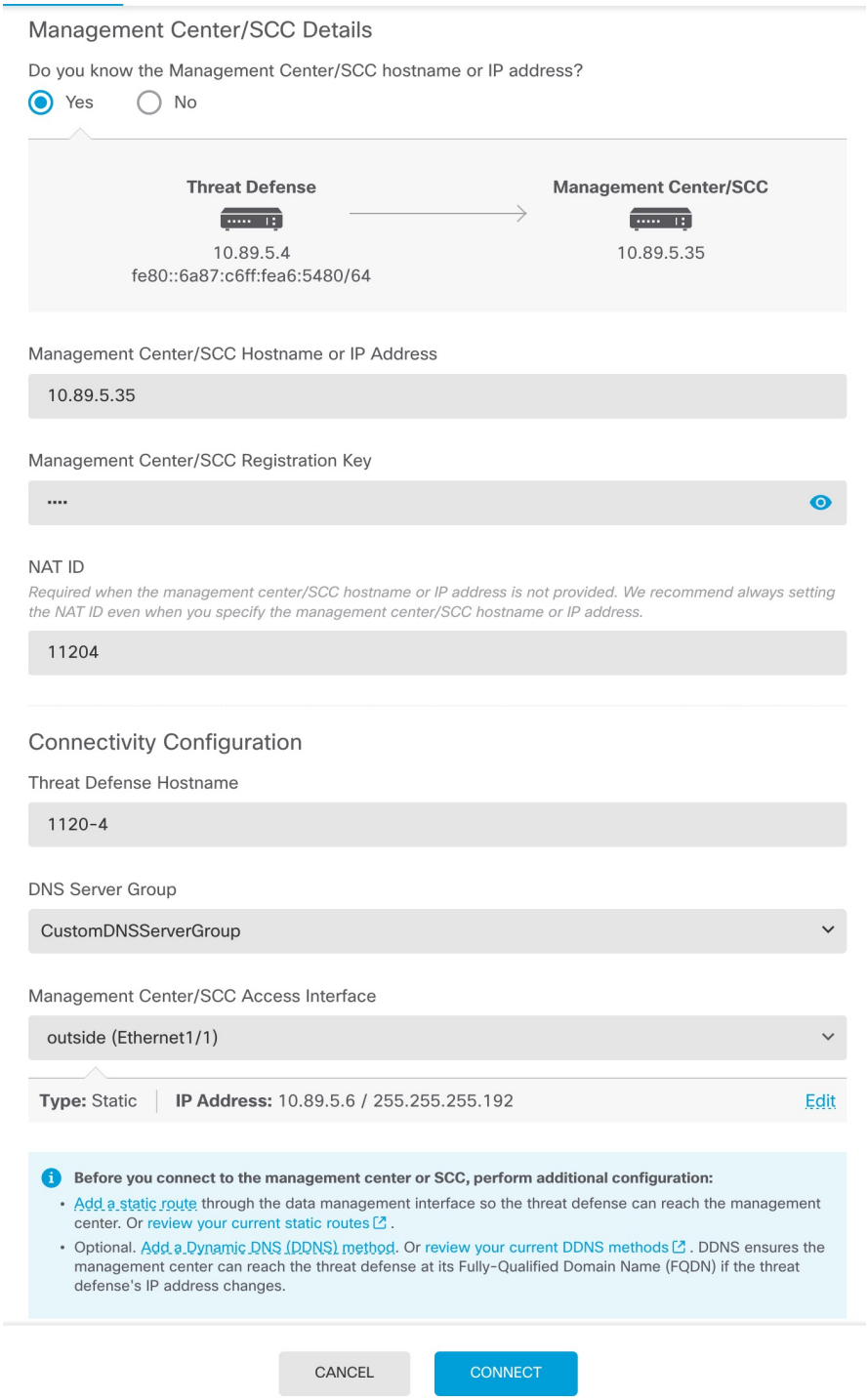
步骤 4 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

在向 防火墙管理中心 注册设备时，不会保留其他 防火墙设备管理器 配置。

步骤 5 选择**设备** > **系统设置** > **集中管理**，然后点击**继续**以设置 防火墙管理中心 管理。

步骤 6 配置**管理中心/SCC 详细信息**。

图 *7:* 管理中心/*SCC* 详细信息



a) 对于**是否知道管理中心/SCC 主机名或 IP 地址？**，如果您可以使用 IP 地址或主机名访问 防火墙管理中心，请点击**是**，如果 防火墙管理中心Security Cloud Control 位于 NAT 之后或没有公共 IP 地址或主机名，请点击**否**。

必须至少有一个设备（ 防火墙管理中心 或 Firewall Threat Defense 设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

b) 如果您选择**是 (Yes)**，则输入**管理中心/SCC 主机名或 IP 地址**。

c) 指定**管理中心/SCC 注册密钥**。

此密钥是您选择的一次性注册密钥，注册Firewall Threat Defense设备时也要在 防火墙管理中心上指定它。注册密钥必须为 2 到 36 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 可用于将多台设备注册到 防火墙管理中心。

a) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 防火墙管理中心上指定它。NAT ID 必须介于 2 到 36 个字符之间。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能 用于将任何其他设备注册到 防火墙管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：

- 您将 防火墙管理中心 IP 地址设置为 **DONTRESOLVE**。
- 在 防火墙管理中心上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
- 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
- 防火墙管理中心 使用多个管理接口。

步骤 7 配置**连接配置**。

a) 指定 **FTD 主机名**。

如果您使用数据接口进行**管理中心/SCC 访问接口**访问，则此 FQDN 将用于此接口。

b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为**管理中心/SCC访问接口**选择数据接口，则此设置会设置数据接口DNS服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在 防火墙管理中心上，数据接口 DNS 服务器在您分配给此 Firewall Threat Defense 的平台设置策略中配置。当您将Firewall Threat Defense设备添加到防火墙管理中心时，本地设置将保留，并且 DNS 服务器 不会 添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 Firewall Threat Defense 设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 防火墙管理中心 和 Firewall Threat Defense 设备同步。

此外，仅当在初始注册时发现 DNS 服务器， 防火墙管理中心 才会保留本地 DNS 服务器。

如果要为 管理中心/ **访问接口FMC**访问接口选择管理接口，则此设置会配置管理 DNS 服务器。

c) 对于**管理中心/SCC访问接口**，请选择任何已配置的接口。

将Firewall Threat Defense设备注册到防火墙管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 8 （可选） 如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到 防火墙管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 9 （可选） 如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保 防火墙管理中心 可接通完全限定域名 (FQDN) 的 Firewall Threat Defense 设备。参阅**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。

如果您在将Firewall Threat Defense设备添加到防火墙管理中心之前配置 DDNS，则Firewall Threat Defense设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便Firewall Threat Defense设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。 Firewall Threat Defense支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (https://help.dyn.com/remote-access-api/)。

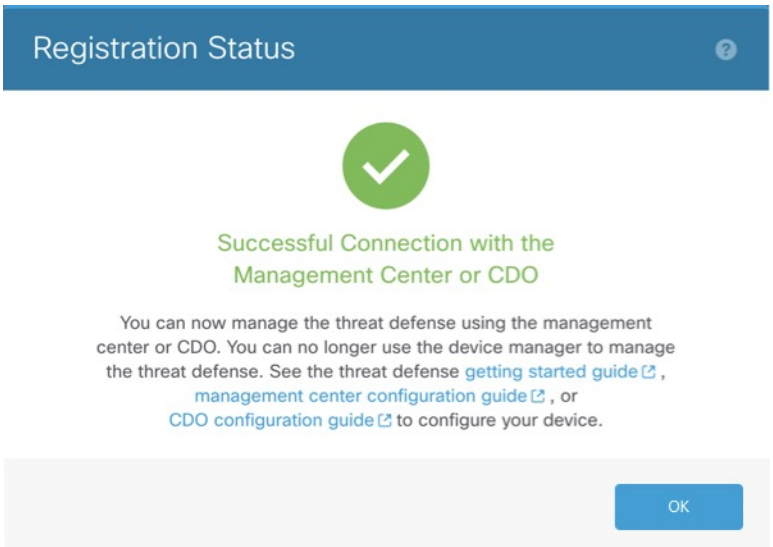
使用管理接口访问管理器时，不支持 DDNS。

步骤 10 点击**连接 (Connect)**。**注册状态** 对话框显示切换到防火墙管理中心的当前状态。在**保存管理中心/SCC 注册设置**步骤后，转到 防火墙管理中心，并添加防火墙。

如果要取消切换到 防火墙管理中心，请点击 **取消注册**。否则，请在**保存管理中心/SCC 注册设置**步骤之后关闭防火墙设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到防火墙设备管理器时才会恢复。

如果您在**保存管理中心/SCC 注册设置**步骤后保持连接到 防火墙设备管理器，您最终将看到**与管理中心/SCC** 成功连接对话框。您将断开与 防火墙设备管理器 的连接。

图 *8:* 成功连接



使用 CLI 完成Firewall Threat Defense初始配置

连接到 Firewall Threat Defense CLI 以执行初始设置，包括使用设置向导设置管理 IP 地址、网关和其他基本网络设置。专用管理接口是一种具有自己的网络设置的特殊接口。如果您不想使用管理接口访问管理器，可以使用 CLI 配置数据接口。您还将配置 防火墙管理中心 通信设置。当您使用 防火墙设备管理器 执行初始设置时，如果您切换到 防火墙管理中心 进行管理，除管理接口和管理器访问接口设置外，在 防火墙设备管理器 中完成的所有 接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

此过程适用于除 Firepower 4100/9300之外的所有模式。要在 Firepower 4100/9300上部署逻辑设备并完成初始配置，请参阅 Firepower 4100/9300 上的逻辑设备, on page 273。

Procedure

步骤 1 从控制台端口连接到 Firewall Threat Defense CLI，或使用管理接口连接至 SSH，默认情况下其从 DHCP 获取 IP 地址。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

控制台端口连接到 FXOS CLI。SSH 会话直接连接到 Firewall Threat Defense CLI。但 ISA 3000 除外，它的控制台连接到 Firewall Threat Defense CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

对于控制台端口，连接到 FXOS CLI。第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的Firewall Threat Defense登录。

Note
如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。

对于 Firepower 和 Cisco Secure Firewal l硬件，请参阅《Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 带威胁防御的 Cisco FXOS 故障排除指南》中的重新映像过程。

请参阅《Cisco Secure Firewall ASA 和威胁防御重新映像指南》。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

步骤 3 如果您在控制台端口已连接到 FXOS， 则需要连接到Firewall Threat Defense CLI。

connect ftd

Example:

```
firepower# connect ftd
>
```

步骤 4 第一次登录 Firewall Threat Defense 时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接，则会提示您更改 admin 密码。然后，系统将显示 CLI 设置脚本。

Note
除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 威胁防御命令参考。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

Note
即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

请参阅以下准则：

- **是否要配置 IPv4**？ 和/或 **是否要配置 IPv6**？-为至少一种地址类型输入 **y** 。
- **输入管理接口的 IPv4 默认网关** 和/或 **输入管理接口的 IPv6 默认网关**-如果要使用数据接口而不是使用管理接口来进行管理器访问，请选择 **手动**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- **输入管理接口的 IPv4 默认网关** 和/或 **通过 DHCP、路由器或手动方式来配置 IPv6**？ - 如果想要使用数据接口而非管理接口进行管理器访问，请将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。如果要使用管理接口进行管理器访问，应在管理 1/1 网络上设置网关 IP 地址。
- **如果您的网络信息已更改，需要重新连接** - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **本地管理设备**？ - 输入 **否** 以使用 防火墙管理中心。回答**是**意味着您将改为使用 Cisco Secure Firewall 设备管理器。
- **配置防火墙模式**？ - 建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。请注意，只有路由防火墙模式支持数据接口管理器访问。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
```

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:


System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.89.5.1
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

步骤 5 确定将管理此Firewall Threat Defense的防火墙管理中心 。

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

Note
如果您使用 Security Cloud Control 进行管理，请在此步骤中使用 Security Cloud Control生成的 **configure manager add** 命令。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} - 指定 防火墙管理中心 的 FQDN 或 IP 地址。如果 防火墙管理中心 不能直接寻址，请使用 **DONTRESOLVE** 并指定 *nat_id*。必须至少有一个设备（防火墙管理中心 或 Firewall Threat Defense）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则 Firewall Threat Defense 必须有可访问的 IP 地址或主机名。
- *reg_key* - 指定您选择的一次性注册密钥，注册Firewall Threat Defense时也要在防火墙管理中心上指定它。注册密钥必须为 2 到 36 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。
- *nat_id* - 指定了您选择的唯一一次性字符串，您还需要在注册 Firewall Threat Defense 时在 防火墙管理中心 上指定它。NAT ID 必须介于 2 到 36 个字符之间。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用NAT ID，即使它是可选的，但在以下情况下必须使用：
  - 您将 防火墙管理中心 IP 地址设置为 **DONTRESOLVE**。
  - 在 防火墙管理中心上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
  - 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
  - 防火墙管理中心 使用多个管理接口。
- *display_name* - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 Security Cloud Control 标识为仅用于分析的主用管理器和本地部署 防火墙管理中心 ，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：
  - *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字）
  - **manager-***timestamp*

Example:

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

Example:

如果防火墙管理中心位于 NAT 设备之后，请输入唯一的 NAT ID 以及注册密钥，并指定 DONTRESOLVE 而非主机名，例如：

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

Example:

如果 Firewall Threat Defense 位于 NAT 设备之后，请输入唯一的 NAT ID 以及 防火墙管理中心 IP 地址或主机名，例如：

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

步骤 6 如果您使用 Security Cloud Control 作为主要管理器，并希望仅将本地部署防火墙管理中心用于分析，请确定本地部署防火墙管理中心。

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

Example:

以下示例对具有 Security Cloud Control 生成的显示名称的 Security Cloud Control使用生成的命令，然后仅使用“分析-FMC”显示名称指定用于分析的本地 防火墙管理中心。

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

步骤 7 (Optional) 配置用于管理器访问的数据接口。

configure network management-data-interface

按下 **Enter** 键后，系统会提示您为数据接口配置基本网络设置。

Note
使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

请参阅以下有关使用此命令的详细信息。另请参阅使用Firewall Threat Defense数据接口进行管理, on page 4。

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令立即设置它。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您将 Firewall Threat Defense 添加到 防火墙管理中心时， 防火墙管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。在 防火墙管理中心中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止 Firewall Threat Defense 或 防火墙管理中心 重新建立管理连接。如果管理连接中断， Firewall Threat Defense 将包含 **configure policy rollback** 命令以恢复以前的部署。
- 如果 IP 地址发生变化，DDNS 可确保 防火墙管理中心 访问完全限定域名 (FQDN) 内的 Firewall Threat Defense。如果配置 DDNS 服务器更新 URL，则 Firewall Threat Defense 会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便 Firewall Threat Defense 可以验证用于

HTTPS 连接的 DDNS 服务器证书。Firewall Threat Defense 支持使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。

- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

  在 防火墙管理中心 上，数据接口 DNS 服务器在您分配给此 Firewall Threat Defense 的平台设置策略中配置。当您将 Firewall Threat Defense 添加到 防火墙管理中心 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 Firewall Threat Defense，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 防火墙管理中心 和 Firewall Threat Defense 同步。

  此外，仅当在初始注册时发现 DNS 服务器， 防火墙管理中心 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 防火墙管理中心中手动配置所有这些设置（包括 DNS 服务器），以便与 FTD 配置匹配。

- 将 Firewall Threat Defense 注册到 防火墙管理中心 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
```

```
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network,
if you wish to change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 8 (Optional) 限制在特定网络上通过数据接口访问管理器。

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

默认情况下，允许所有网络。

What to do next

将设备注册到 防火墙管理中心。

配置事件接口

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，例如，Firepower 4100/9300 和 Cisco Secure Firewall 4200/6100，则可以为仅事件流量启用该接口。

您可以在防火墙管理中心和托管设备上配置单独的事件专用接口，以隔离事件流量。此设置通过将事件数据与管理操作分离来增强性能和安全性。

如果无法访问事件接口，事件流量将回退到管理接口。

开始之前

在托管设备上配置单独的仅事件接口之前，请确保已在防火墙管理中心上启用事件接口。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南。

如果使用数据接口对被管理设备进行管理，则不能配置单独的管理接口和事件接口。

过程

步骤 1 启用第二个管理接口作为仅事件的接口。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即

使您禁用了事件通道，设备也会通过管理接口发送事件。同样，如果管理接口关闭，仅事件接口将作为备份用于管理。

无法同时禁用接口上的事件通道和管理通道。

示例：

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

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

>
```

步骤 2 配置事件接口的 IP 地址。

事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。

a) 配置 IPv4 地址：

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

请注意，此命令中的 *gateway_ip* 用于为设备创建默认路由，因此，您应该输入已经为 management0 接口设置的值。它不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您为仅事件接口创建静态路由。

示例：

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

>
```

b) 配置 IPv6 地址：

- 无状态自动配置：

  configure network ipv6 router management1

  示例：

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

  >
  ```

- 手动配置：

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

  示例：

  ```
  > configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
  ```

```
Setting IPv6 network configuration.
Network settings changed.

>
```

步骤 3 如果 防火墙管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

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

对于 默认 路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 步骤 2，第 28 页）。

示例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

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

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

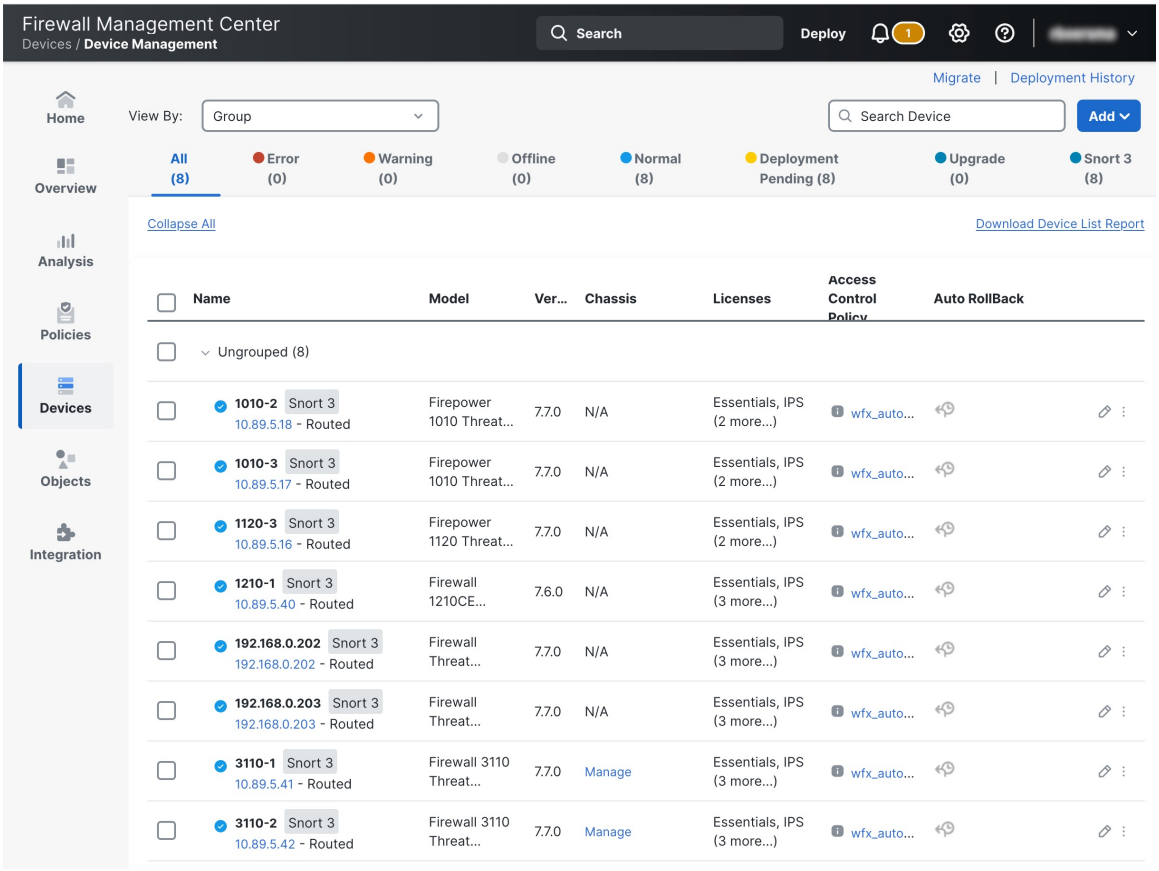
管理设备注册

向 防火墙管理中心 注册和取消注册设备。

关于设备管理页面

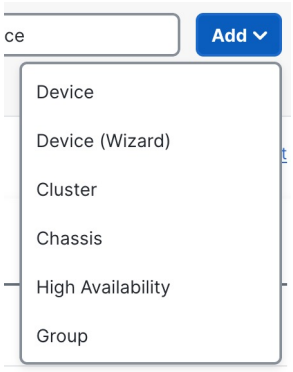
设备 > **设备管理**页面为您提供一系列信息和选项：

图 *9:* 设备管理页面



- **查看方式 (View By)** - 根据组、许可证、型号、版本或访问控制策略查看设备。
- **设备状态 (Device State)** - 根据状态（**错误**、**警告**等）查看设备。您可以点击状态图标查看属于它的设备。括号内为各状态所对应的的设备数量。
- **搜索设备 (Search Device)** - 按设备名称、主机名或 IP 地址搜索设备。
- **添加 (Add)** - 添加设备和其他可管理组件。

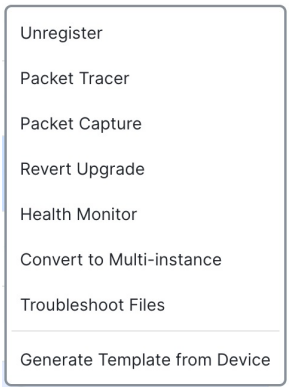
图 *10:* 添加菜单



- 列 - 点击列标题可按该列进行排序。
  - **名称**
  - **型号**
  - **版本**
  - **机箱 (Chassis)** - 对于支持的型号，点击**管理 (Manage)** 以显示集成机箱管理器。对于 Firepower 4100/9300，该链路会交叉启动 防火墙机箱管理器。
  - **许可证**
  - **访问控制策略 (Access Control Policy)** - 点击访问控制策略列中的链接以查看部署到设备的策略。
  - **自动回滚 (Auto-Rollback)** - 显示在部署导致管理连接中断时，配置的自动回滚是启用 ( ) 还是禁用 (）。请参阅编辑部署设置，第 921 页。
- **编辑 (Edit)** - 对于每个设备，使用 **编辑** ( ) 图标编辑设备设置。

  您也可以点击设备名称或 IP 地址。
- **更多 (More)** - 对于每个设备，点击 **更多** ( ) 图标以执行其他操作：

  图 *11:* 更多菜单



  - **取消注册**-取消注册设备。
  - **数据包跟踪器 (Packet Tracer)** - 导航至数据包跟踪器页面，以便通过将模型数据包注入系统来检查设备上的策略配置。
  - **数据包捕获 (Packet Capture)** - 导航至数据包捕获页面，您可以在其中查看系统在处理数据包时所采取的判定和操作。
  - **恢复升级 (Revert Upgrade)** - 恢复上次升级后所做的升级和配置更改。此操作会将设备恢复到升级前的版本。
  - **运行状况监控器 (Health Monitor)** - 导航至设备的运行状况监控页面。
  - **转换为多实例 (Convert to Multi-instance)** - 对于支持的型号，将机箱转换为多实例模式。

- **故障排除文件 (Troubleshooting Files)** - 生成故障排除文件，您可以在其中选择要在报告中包含的数据类型。
- **从设备生成模板 (Generate Template from Device)** - 从已注册的设备生成新的设备模板。新模板的配置与生成模板的设备相同。您可以从独立设备和 HA 设备生成新的设备模板。但是，如果从 HA 设备生成模板，新模板将不包含故障转移配置。

添加设备组

防火墙管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

如果将高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果取消高可用性，则两台设备均会保留在该组中。

在多域环境中不支持组。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

要编辑现有的组，请点击要编辑的组的 **编辑** ()。

步骤 3 输入 **Name**。

步骤 4 在**可用设备 (Available Devices)** 下，选择一台或多台要添加到设备组的设备。点击的同时使用 Ctrl 或 Shift 选择多台设备。

步骤 5 点击**添加 (Add)** 将所选设备包含在设备组中。

步骤 6 或者，要将设备从设备组中删除，请点击要删除的设备旁边的 **删除** ()。

步骤 7 点击**确定 (OK)** 以添加组。

向管理中心注册

防火墙管理中心 提供多种设备注册方法。

注册密钥方法

使用您在防火墙管理中心和设备初始配置中指定的注册密钥来添加设备。

使用注册密钥添加设备 - 基本配置

开始之前

- 将设备设置为由 防火墙管理中心管理。请参阅：
  - 为手动注册完成Firewall Threat Defense初始配置， 第 14 页
  - 《适用于您的型号的入门指南》
- 防火墙管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须删除并重新注册该设备。

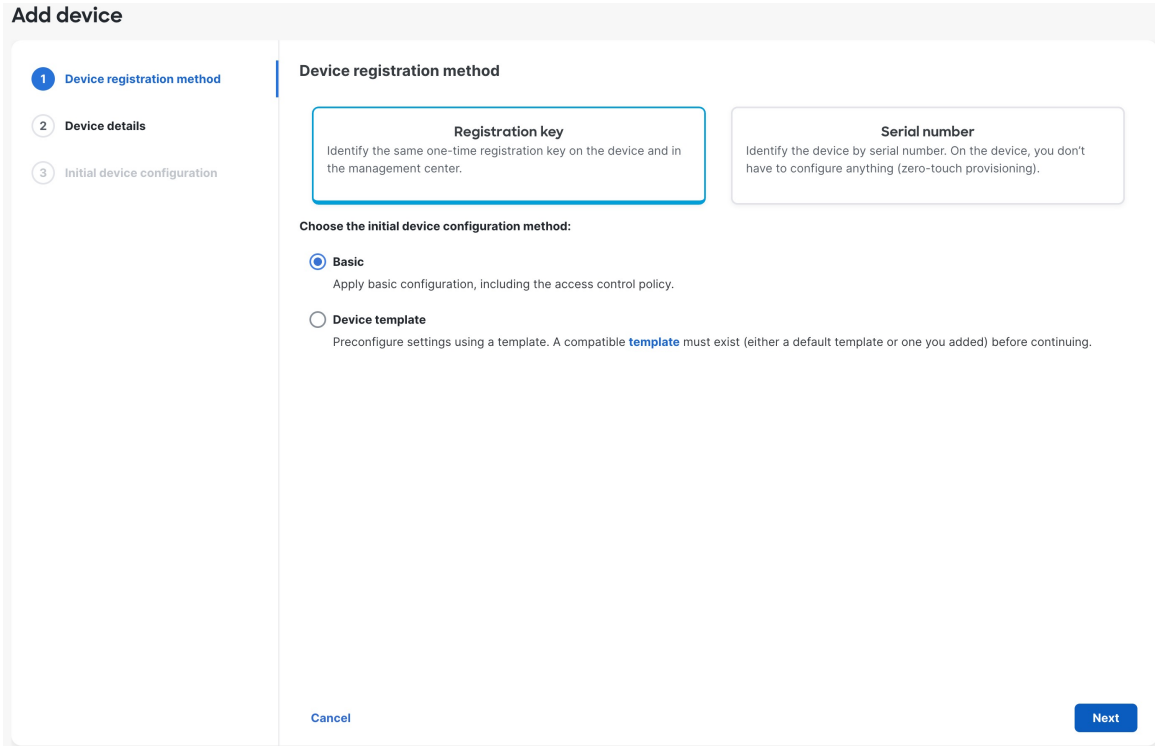
过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加**下拉菜单中，选择**设备**。

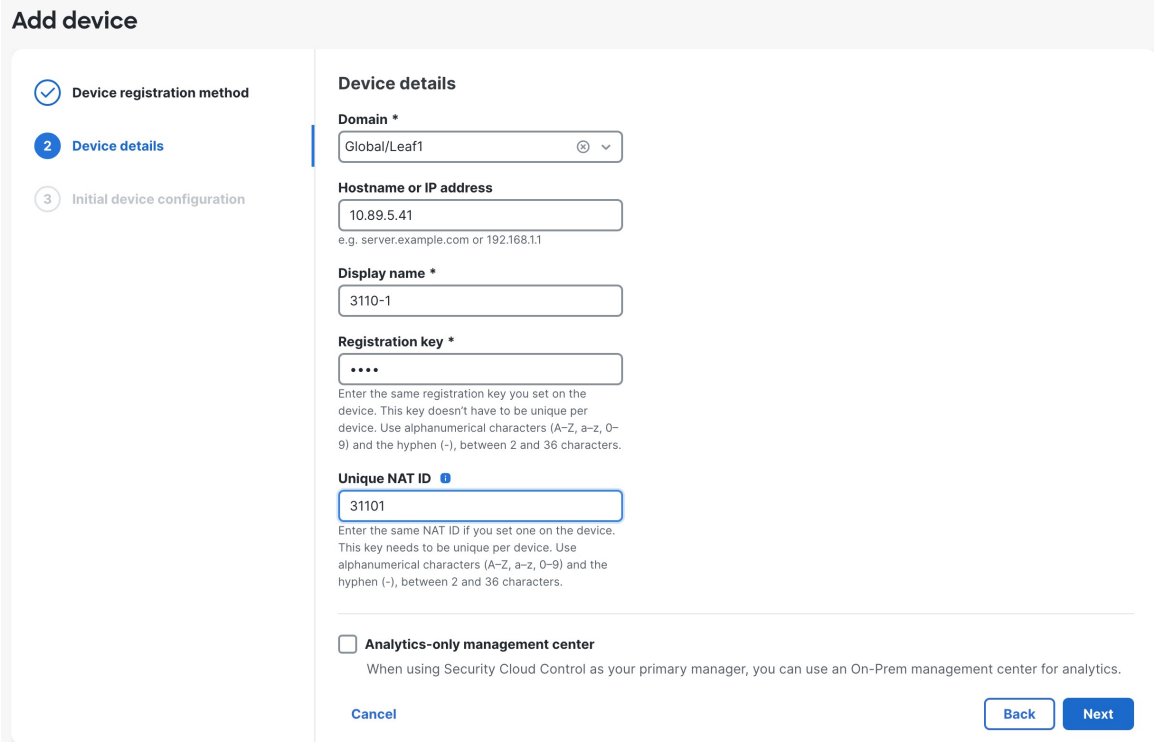
步骤 3 依次点击**注册密钥**、**基本**和**下一步**。

图 *12:* 设备注册方法



步骤 4 配置设备详细信息并点击**下一步**。

图 *13:* 设备详细信息



- **域 (Domain)**- 在多域环境中，选择分叶域。
- **设备组**- 在单域环境中，将设备添加到 **设备组**。
- **主机名或 IP 地址** - 对于主机，输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。

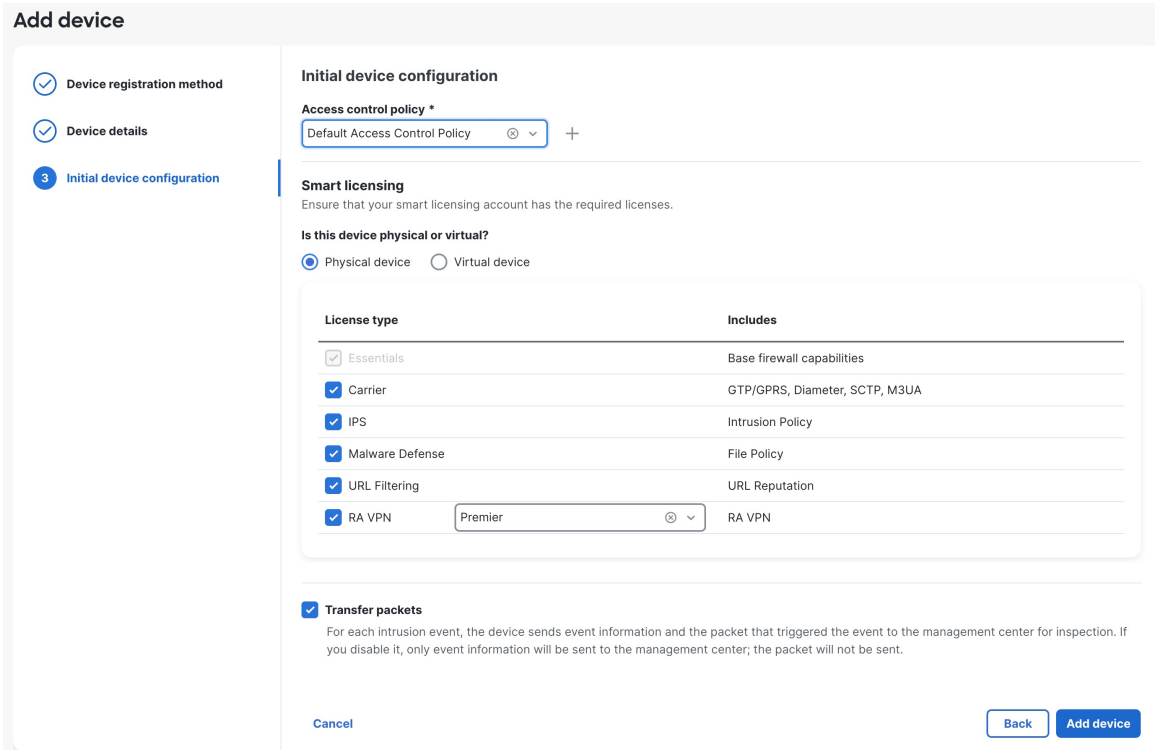
  如果您将此字段留空，则设备上的初始配置需要包括可访问的防火墙管理中心IP地址或主机名以及 NAT ID。有关详细信息，请参阅NAT 环境，第 7 页。
- **显示名称** - 输入要在 防火墙管理中心 中显示的设备名称。之后将无法更改该名称。
- **注册密钥** - 输入初始配置中相同的注册密钥。注册密钥是一个一次性的共享密钥。密钥最多37个字符，包括字母数字（A－Z、a－z、0－9）和连字符 (-)。不需要每台设备的注册密钥都是唯一的。
- **唯一 NAT ID** - 输入初始配置中相同的 ID。

  唯一 NAT ID 指定您选择的唯一的一次性字符串，您也可以在初始设置时在设备上指定该字符串。当一端未指定可访问的IP地址或主机名时（例如，如果您将**主机 (Host)** 字段留空），则需要填写。虽然在技术上是可选的，但我们建议始终指定 NAT ID，因为它在某些情况下是必需的，即使您知道两端的 IP 地址也是如此。ID 最多37个字符，包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。
- **仅分析管理中心** - 除非您知道设备由云交付的防火墙管理中心管理，否则不要选中此选项。

  对于仅分析模式，现在便已完成。点击**添加设备**。

步骤 5 配置初始设备配置。

图 *14:* 初始设备配置



- **访问控制策略** - 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。
- **智能许可**- 选择您的许可证。
  - **此设备是物理设备还是虚拟设备？** - 选择 **物理设备** 或虚拟设备。对于 Firewall Threat Defense Virtual，您还必须选择**性能层**。选择与您帐户中的许可证相匹配的级别很重要。在选择级别之前，您的设备默认为 FTDv50。
  - **许可证类型**- 选中要分配给设备的每个许可证类型。

  在添加设备后，您可以从**管理** > **许可证** > **智能许可证** 页面应用许可证。
- **传输数据包** - 启用此选项，以便对于每个入侵事件，设备会将数据包传输到 防火墙管理中心 进行检查。

  对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到防火墙管理中心进行检查。如果禁用此选项，则只会向 防火墙管理中心 发送事件信息，而不会发送数据包。

步骤 6 点击**添加设备**。

防火墙管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果设备注册失败，请检查以下项：

- Ping - 访问设备 CLI，然后使用以下命令 ping 防火墙管理中心 IP 地址：

ping system *ip_address*

如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改设备 IP 地址，使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令。

- 注册密钥、NAT ID 和 防火墙管理中心IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在设备上使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 https://cisco.com/go/fmc-reg-error。

使用注册密钥添加设备-设备模板

您可以使用模板添加设备，向 防火墙管理中心 注册设备，并使用所给模板配置来调出设备。

开始之前

按照使用设备模板进行设备注册 ， 第 87 页创建设备模板。您必须为每个设备指定所需的变量和网络对象覆盖，并确保为目标设备模型进行了模型映射。

建议您创建核对表，以确保在设备上应用模板之前已正确输入模板中的所有配置。

核对表示例如下所示。

- 检查版本、型号、操作模式。
- 检查变量和覆盖列表。
- 检查变量和覆盖值的健全性。
- 检查是否存在所需的模型映射。
- 检查并行设备模板操作是否正在进行。

注释 如果要添加将由数据接口管理的设备，请确保配置的模板与设备的连接参数兼容。有关详细信息，请参阅为通过数据接口管理的威胁防御设备配置模板。

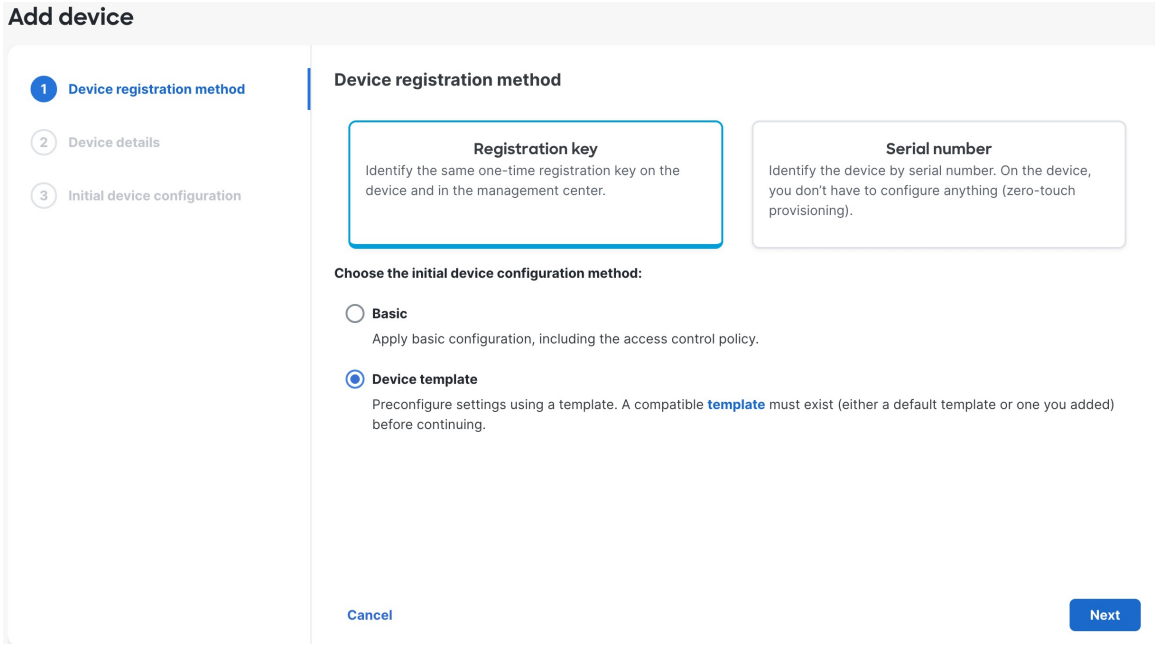
过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加**下拉菜单中，选择**设备**。

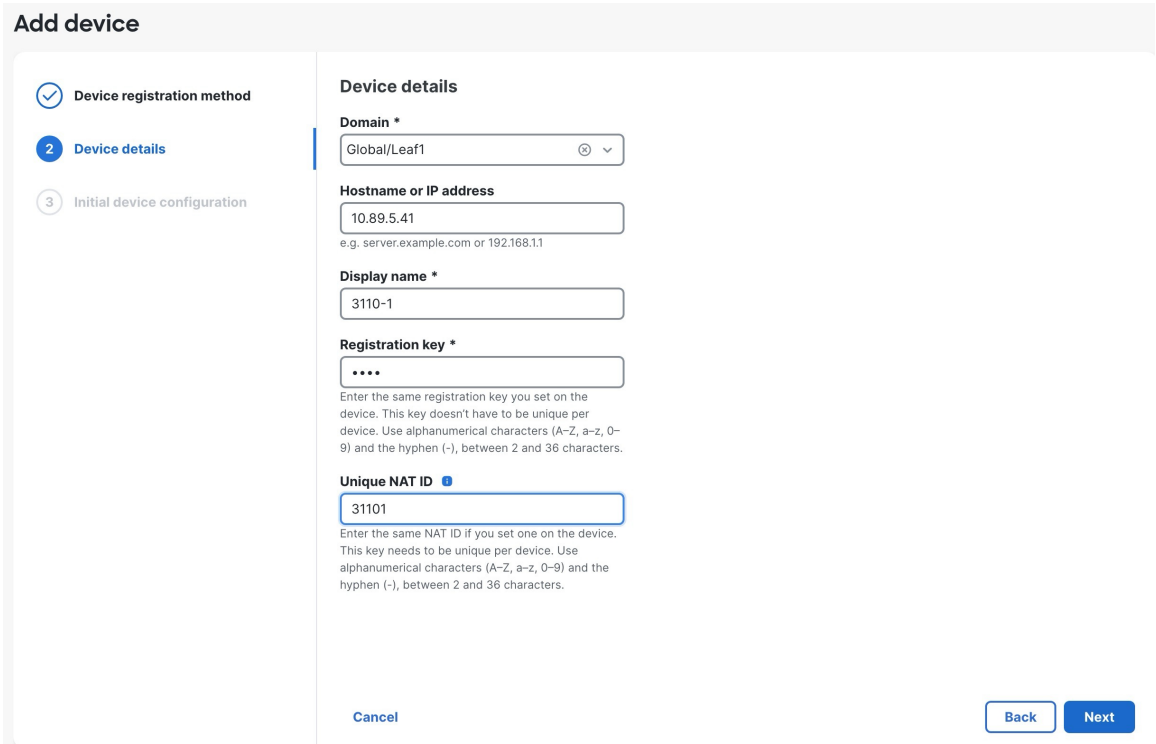
步骤 3 依次点击**注册密钥**、**设备模板**和**下一步**

图 *15:* 设备注册方法



步骤 4 配置设备详细信息并点击**下一步**。

图 *16:* 设备详细信息



- **设备组** - 将设备添加到**设备组**。

- **主机名或 IP 地址** - 对于主机，输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。

  如果您将此字段留空，则设备上的初始配置需要包括可访问的防火墙管理中心IP地址或主机名以及 NAT ID。有关详细信息，请参阅NAT 环境。

- **显示名称** - 输入要在 防火墙管理中心 中显示的设备名称。之后将无法更改该名称。

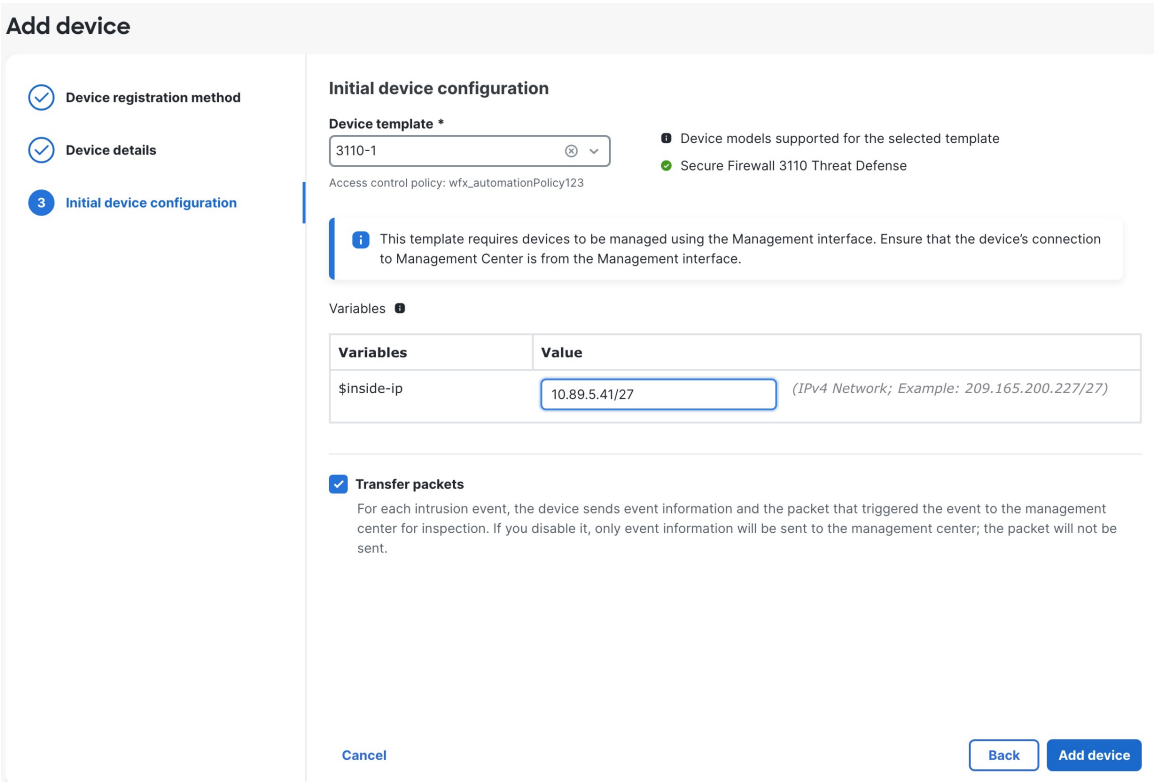
- **注册密钥** - 输入初始配置中相同的注册密钥。注册密钥是一个一次性的共享密钥。密钥最多37个字符，包括字母数字（A－Z、a－z、0－9）和连字符 (-)。不需要每台设备的注册密钥都是唯一的。

- **唯一 NAT ID** - 输入初始配置中相同的 ID。

  唯一 NAT ID 指定您选择的唯一的一次性字符串，您也可以在初始设置时在设备上指定该字符串。当一端未指定可访问的 IP 地址或主机名时（例如，如果您将**主机 (Host)** 字段留空），则需要填写。虽然在技术上是可选的，但我们建议始终指定 NAT ID，因为它在某些情况下是必需的，即使您知道两端的 IP 地址也是如此。ID 最多37个字符，包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。

步骤 5 配置初始设备配置设置。

图 *17*: 初始设备配置



- **设备模板**- 从 **设备模板 (Device template)** 下拉列表中选择对您的型号、机箱配置和管理器访问接口有效的模板。

- **变量** - 输入**变量**和**网络对象覆盖**的值。
- **传输数据包** - 启用此选项，以便对于每个入侵事件，设备会将数据包传输到 防火墙管理中心 进行检查。

  对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到防火墙管理中心进行检查。如果禁用此选项，则只会向 防火墙管理中心 发送事件信息，而不会发送数据包。

步骤 6 点击**添加设备 (Add Device)** 以启动设备注册。向 防火墙管理中心 成功注册设备后，系统将应用模板配置。

防火墙管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果设备注册失败，请检查以下项：

- Ping - 访问设备 CLI，然后使用以下命令 ping 防火墙管理中心 IP 地址：

  ping system *ip_address*

  如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改设备 IP 地址，使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令。

- 注册密钥、NAT ID 和 防火墙管理中心IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在设备上使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 https://cisco.com/go/fmc-reg-error。

序列号方法（零接触调配）

通过零接触调配，您可以按序列号将设备注册到 防火墙管理中心，而无需在设备上执行任何初始设置。

使用序列号添加设备（零接触调配）- 基本配置

通过零接触调配，您可以按序列号将设备注册到 防火墙管理中心，而无需在设备上执行任何初始设置。Security Cloud Control 集成以实现此功能。

按照此程序使用基本配置将单个设备添加到 防火墙管理中心。要使用模板添加一个或多个设备，请参阅使用序列号来添加设备（零接触调配）- 设备模板 ， 第 46 页。

注册后的默认配置

使用 零接触调配时，系统会预配置以下接口：请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 200/ 1010/ 1210// 1220，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

要求

零接触调配 不支持集群或多实例模式。

当您使用外部接口进行管理器访问时，它会默认使用 DHCP。在启用高可用性之前，需要将 IP 地址更改为静态地址。请参阅更改设备 IP 地址，第 879 页。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

零接触调配 仅在以下运行 7.2 和 7.4 或更高版本的型号上受支持；在 7.2.4 之前的版本中， 防火墙管理中心 必须可公开访问。

- Cisco Secure Firewall 200
- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（在支持的设备版本上）
- Cisco Secure Firewall 3100

开始之前

- 确保设备已取消配置或全新安装。零接触调配仅适用于新设备。预配置可以禁用 零接触调配，具体取决于您配置设备的方式。
- 连接外部接口或管理接口，使其能够访问互联网。如果您使用外部接口进行零接触调配，请勿同时连接管理接口；如果管理接口从 DHCP 获取 IP 地址，则外部接口的路由将不正确。
- 如果设备没有公共 IP 地址或 FQDN，或者您使用管理接口，请为 防火墙管理中心 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅**管理 > 配置 > 管理器远程访问**。
- 为管理或以太网 1/1 提供 IP 地址和默认网关的 DHCP 服务器。
- 通过网络访问 OpenDNS 公共 DNS 服务器。IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35。系统从不使用从 DHCP 获取的 DNS 服务器。

  需要解析以下名称：

  表 *2: FQDN* 的零接触调配

FQDNs
*.cisco.com（多个 FQDN）
defenseorchestrator.com
*.defenseorchestrator.eu（供欧盟地区使用，许多 FQDN）
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, 3.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa

FQDNs
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

- 防火墙管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须取消注册并该设备。

过程

步骤 1 首次使用序列号添加设备时，请将 防火墙管理中心 与Security Cloud Control集成。

注释
对于 防火墙管理中心 高可用性对，您还需要将辅助 防火墙管理中心 与Security Cloud Control集成。

a) 选择**集成** > **安全云控制**。
b) 点击**启用安全云控制**打开单独的浏览器选项卡，让您登录Security Cloud Control帐户并确认显示的代码。

确保此页面未被弹出窗口阻止程序阻止。如果您还没有Security Cloud Control 帐户，您可以在程序期间添加一个。

有关此集成的详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的“系统配置”一章。

Security Cloud Control 会在您将 防火墙管理中心 与Security Cloud Control集成后载入本地 防火墙管理中心。Security Cloud Control 需要其清单中的 防火墙管理中心，以便 零接触调配 运行。但是，您不需要直接使用 Security Cloud Control。如果您使用 Security Cloud Control，其 防火墙管理中心 支持仅限于设备载入、查看其托管设备、查看与 防火墙管理中心 关联的对象，以及交叉启动 防火墙管理中心。

c) 确保选中**启用零接触调配 (Enable Zero-Touch Provisioning)** 。
d) 点击**保存**。

步骤 2 获取设备的序列号。

设备包含两个序列号：机箱序列号和 PCB（电路板）序列号。任一序列号均可使用。

- 如果您有装运箱，则可以在标签上看到机箱序列号。
- 机箱序列号位于设备底部、背面的合规标签上，或前面的抽拉式标签上。
- PCB 序列号位于机箱上名为“S/N”的标签上。

- 您可以使用以下 CLI 命令查看序列号：
  - FXOS CLI - **show chassis detail**显示两个序列号。
  - Firewall Threat Defense - **show inventory**显示机箱序列号。**show serial-number**显示 PCB 序列号。

步骤 3 检查 LED，确保防火墙已准备好注册。

1000

表 *3:* 零接触调配：系统 *(S) LED* 行为

S LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁（错误情况）	设备无法连接到思科云。	15:00 - 30:00

200、1200、3100

表 *4:* 零接触调配：受管 *(M) LED* 行为

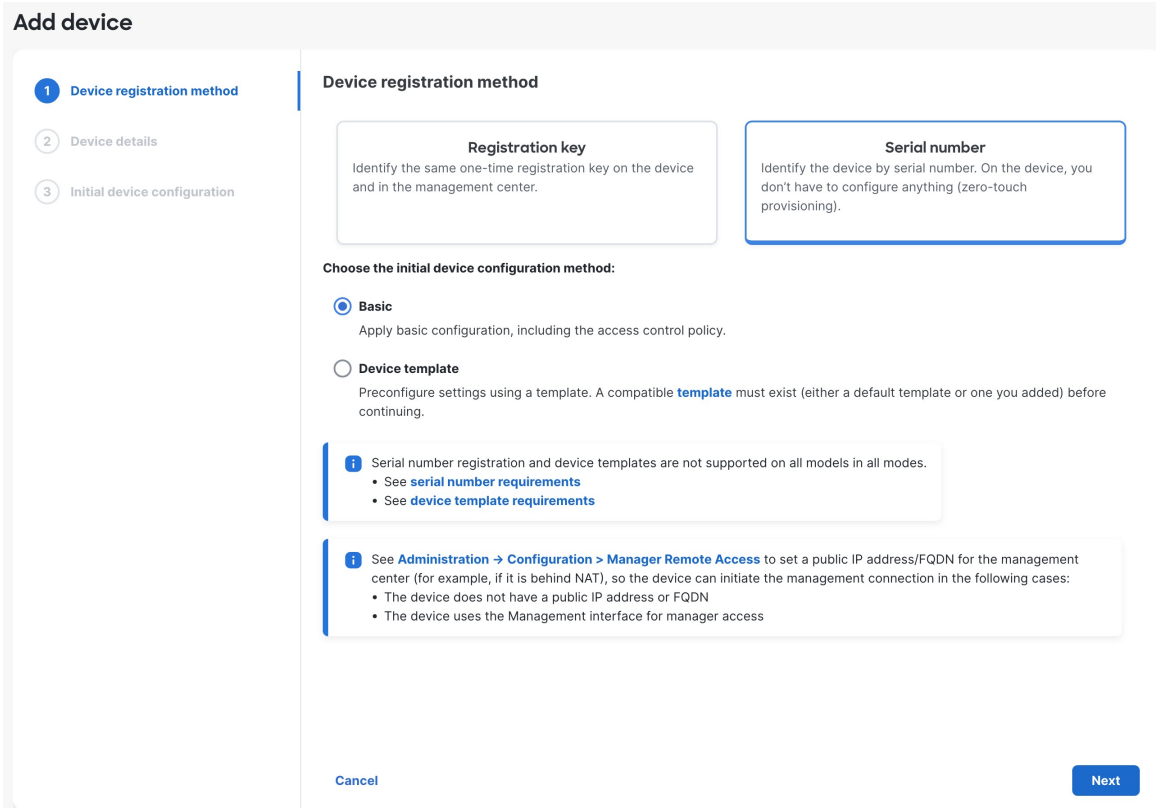
M LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁（错误情况）	设备无法连接到思科云。	15:00 - 30:00
绿灯常亮	已自行激活	20:00 - 45:00

步骤 4 选择**设备** > **设备管理**。

步骤 5 从**添加**下拉菜单中，选择**设备**。

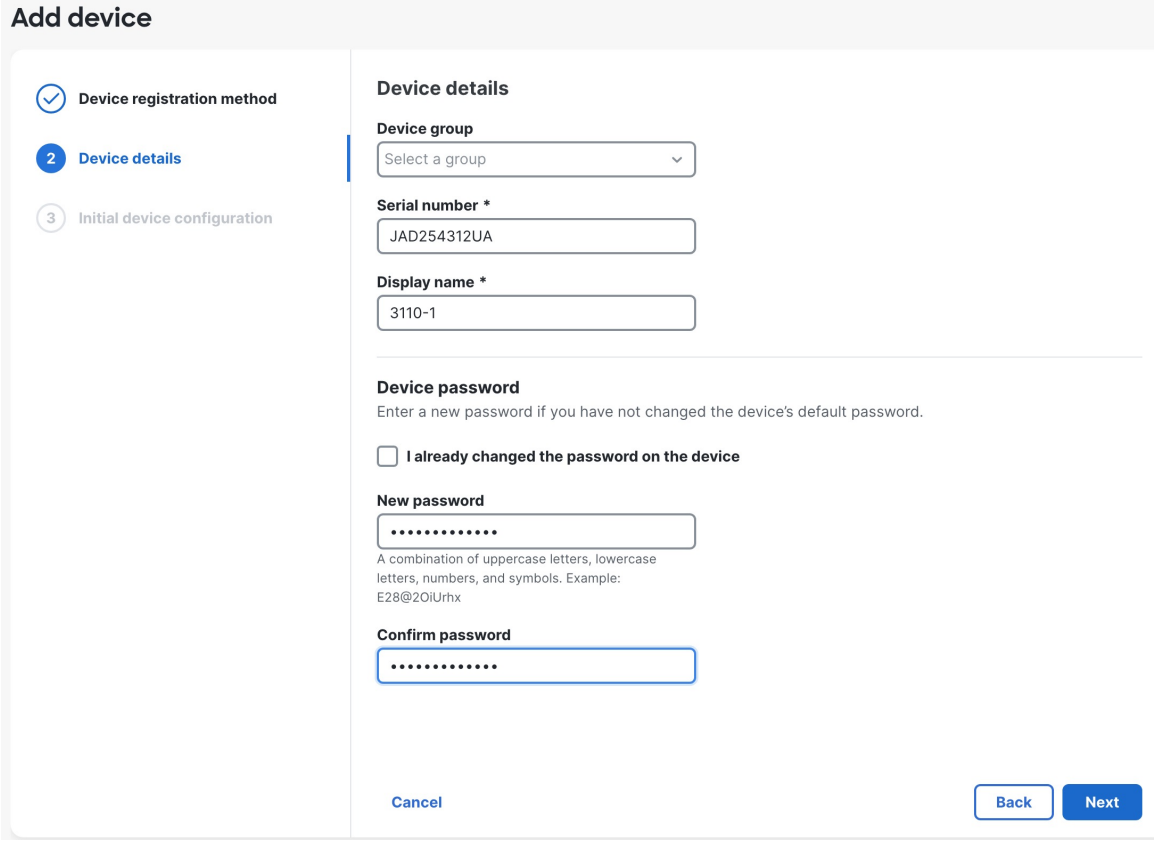
步骤 6 依次点击**序列号**、**基本**和**下一步**。

图 *18:* 设备注册方法



步骤 7 配置设备详细信息并点击**下一步**。

图 *19:* 设备详细信息

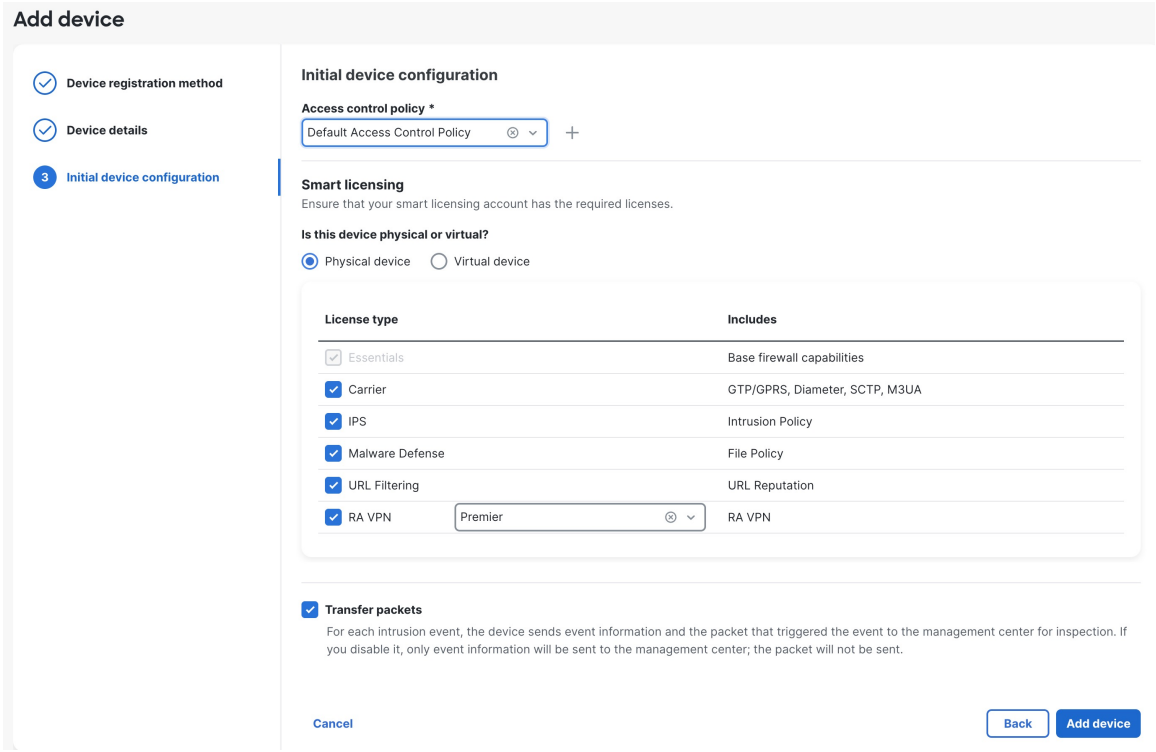


- **域 (Domain)**- 在多域环境中，选择分叶域。
- **设备组**- 在单域环境中，将设备添加到 **设备组**。
- **序列号** - 输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。
- **显示名称** - 输入要在 防火墙管理中心 中显示的设备名称。之后将无法更改该名称。
- **设备密码** - 如果此设备未配置或全新安装，则需要设置**新密码**并进行确认。

  仅当您已登录并更改 **密码时，才可检查我已在设备上** 更改密码。否则，注册将失败。

步骤 8 配置初始设备配置。

图 *20:* 初始设备配置



- **访问控制策略** - 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。
- **智能许可**- 选择您的许可证。
  - **此设备是物理设备还是虚拟设备？** - 选择 **物理设备** 或虚拟设备。对于 Firewall Threat Defense Virtual，您还必须选择**性能层**。选择与您帐户中的许可证相匹配的级别很重要。在选择级别之前，您的设备默认为 FTDv50。
  - **许可证类型**- 选中要分配给设备的每个许可证类型。

  在添加设备后，您可以从**管理** > **许可证** > **智能许可证** 页面应用许可证。
- **传输数据包** - 启用此选项，以便对于每个入侵事件，设备会将数据包传输到 防火墙管理中心 进行检查。

  对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到防火墙管理中心进行检查。如果禁用此选项，则只会向 防火墙管理中心 发送事件信息，而不会发送数据包。

步骤 9 点击**添加设备**。

防火墙管理中心可能需要长达两分钟来验证设备的心跳并建立通信。

在外部接口上使用零接触调配时，Security Cloud Control 会充当 DDNS 提供商并执行以下操作：

- 使用**仅限 FMC (FMC Only)** 方法在外部启用 DDNS。此方法仅支持零接触调配设备。
- 使用以下主机名映射外部 IP 地址： *serial-number*.**local**。

- 提供到 防火墙管理中心 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
- 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 防火墙管理中心 发送通知。

如果在管理接口上使用零接触调配，则不支持 DDNS。 防火墙管理中心 必须可公开访问，以便设备能够发起管理连接。

您可以继续使用 Security Cloud Control 作为 DDNS 提供商，也可以稍后将 防火墙管理中心 中的 DDNS 配置更改为其他方法。有关详细信息，请参阅配置动态 DNS，第 965 页。

如果设备注册失败，请参阅解决序列号（零接触调配）注册问题，第 56 页。

使用序列号来添加设备（零接触调配）- 设备模板

通过零接触调配，您可以按序列号将设备注册到 防火墙管理中心，而无需在设备上执行任何初始设置。Security Cloud Control 集成以实现此功能。

您可以使用模板添加设备，向 防火墙管理中心 注册设备，并使用模板配置来调出设备。

使用此程序可使用序列号和设备模板将设备添加到 防火墙管理中心。要添加设备而不使用模板，请参阅使用序列号添加设备（零接触调配） - 基本配置，第 39 页。

要求

零接触调配 不支持集群或多实例模式。

当您使用外部接口进行管理器访问时，它会默认使用 DHCP。在启用高可用性之前，需要将 IP 地址更改为静态地址。请参阅更改设备 IP 地址。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

零接触调配以下使用 7.4 或更高版本的型号支持使用模板：

- Cisco Secure Firewall 200
- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（在支持的设备版本上）
- Cisco Secure Firewall 3100

开始之前

- 确保设备已取消配置或全新安装。零接触调配仅适用于新设备。预配置可以禁用 零接触调配，具体取决于您配置设备的方式。
- 连接外部接口或管理接口，使其能够访问互联网。如果您使用外部接口进行零接触调配，请勿同时连接管理接口；如果管理接口从 DHCP 获取 IP 地址，则外部接口的路由将不正确。

- 如果设备没有公共 IP 地址或 FQDN，或者您使用管理接口，请为 防火墙管理中心 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅**管理** > **配置** > **管理器远程访问**。
- 为管理或以太网 1/1 提供 IP 地址和默认网关的 DHCP 服务器。
- 通过网络访问 OpenDNS 公共 DNS 服务器。IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35。系统从不使用从 DHCP 获取的 DNS 服务器。

  需要解析以下名称：

  表 *5: FQDN* 的零接触调配

FQDNs
*.cisco.com（多个 FQDN）
defenseorchestrator.com
*.defenseorchestrator.eu（供欧盟地区使用，许多 FQDN）
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, 3.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

- 防火墙管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须取消注册并该设备。
- 按照使用设备模板进行设备注册，第 87 页创建设备模板。您必须为每个设备指定所需的变量和网络-对象覆盖，并确保为目标设备模型进行了模型映射。

  建议您创建核对表，以确保在设备上应用模板之前已正确输入模板中的所有配置。

  核对表示例如下所示。

  - 检查版本、型号、操作模式。
  - 检查变量和覆盖列表。
  - 检查变量和覆盖值的健全性。
  - 检查是否存在所需的模型映射。
  - 检查并行设备模板操作是否正在进行。

注释 如果要添加将由数据接口管理的设备，请确保配置的模板与设备的连接参数兼容。有关详细信息，请参阅为通过数据接口管理的威胁防御设备配置模板。

过程

步骤 1 首次使用序列号添加设备时，请将 防火墙管理中心 与Security Cloud Control集成。

注释
对于 防火墙管理中心 高可用性对，您还需要将辅助 防火墙管理中心 与Security Cloud Control集成。

a) 选择**集成** > **安全云控制**。
b) 点击**启用安全云控制**打开单独的浏览器选项卡，让您登录Security Cloud Control帐户并确认显示的代码。

确保此页面未被弹出窗口阻止程序阻止。如果您还没有Security Cloud Control 帐户，您可以在程序期间添加一个。

有关此集成的详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的“系统配置”一章。

Security Cloud Control 会在您将 防火墙管理中心 与Security Cloud Control集成后载入本地 防火墙管理中心。Security Cloud Control 需要其清单中的 防火墙管理中心，以便 零接触调配 运行。但是，您不需要直接使用 Security Cloud Control。如果您使用 Security Cloud Control，其 防火墙管理中心 支持仅限于设备载入、查看其托管设备、查看与 防火墙管理中心 关联的对象，以及交叉启动 防火墙管理中心。

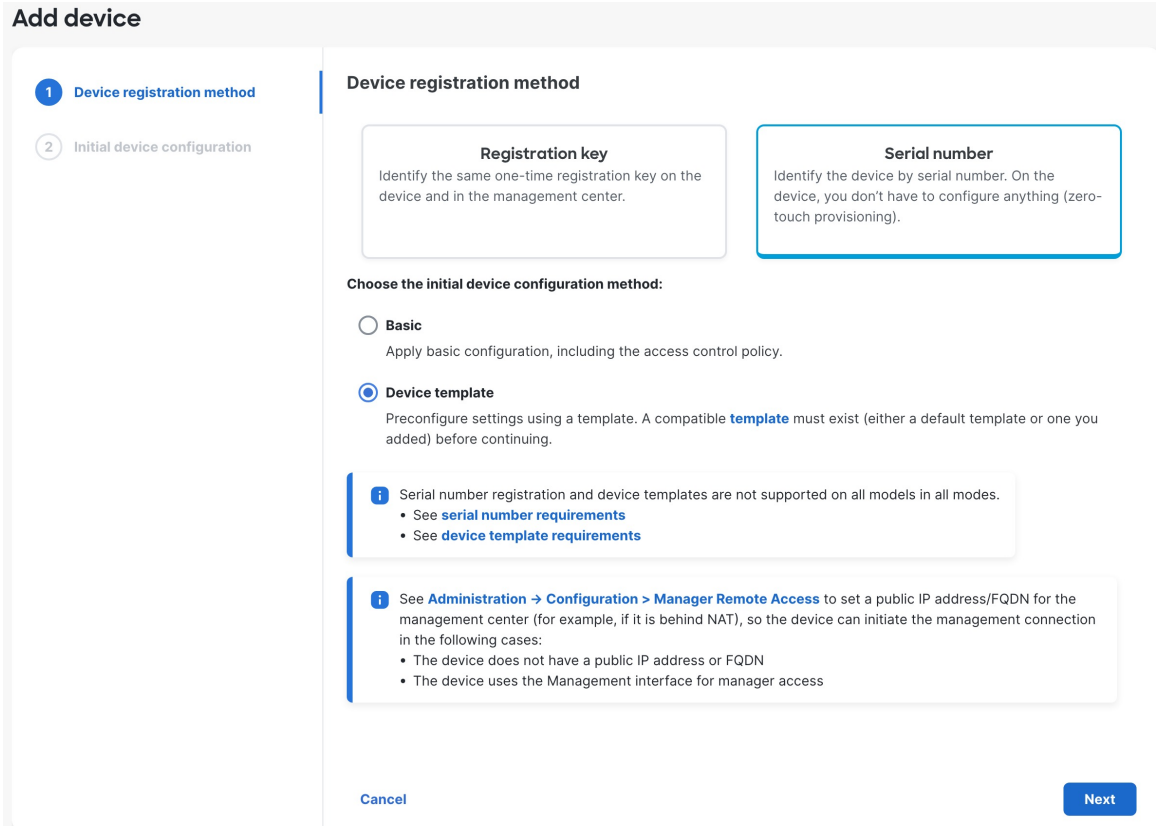
c) 确保选中**启用零接触调配 (Enable Zero-Touch Provisioning)** 。
d) 点击**保存**。

步骤 2 选择**设备** > **设备管理**。

步骤 3 从**添加**下拉菜单中，选择**设备**。

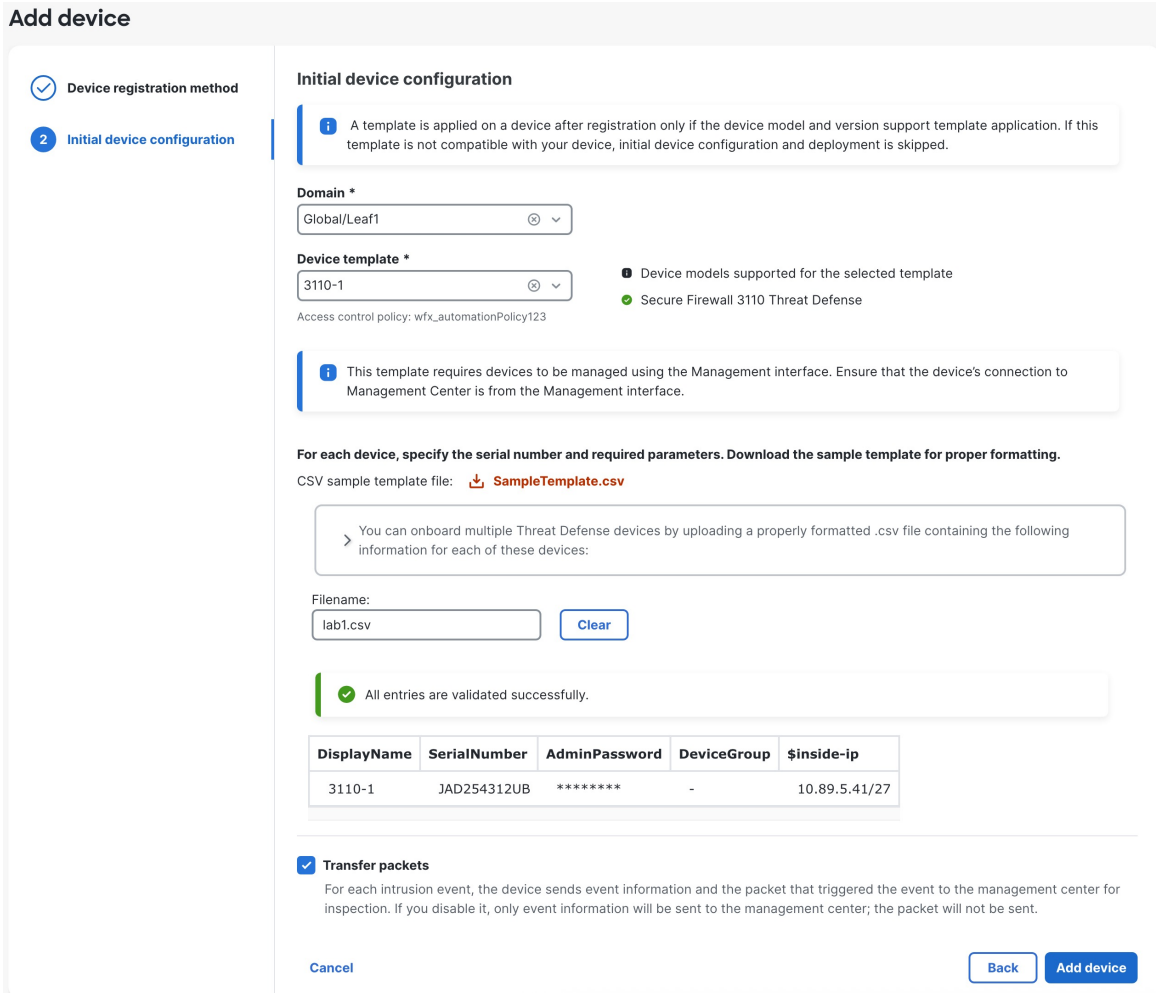
步骤 4 点击**序列号**，点击**设备模板**，然后点击**下一步**。

图 *21:* 设备注册方法



步骤 5 配置初始设备配置。

图 *22*: 初始设备配置



- **域 (Domain)**- 在多域环境中，选择分叶域。
- **设备组**- 在单域环境中，将设备添加到 **设备组**。
- 从**设备模板 (Device template)** 下拉列表中，选择模板。
- **SampleTemplate.csv**- 点击进行下载。此文件包含您需要为每台设备定义的值的所有必需报头。有关 CSV 模板文件字段的详细信息，请参阅 CSV 模板文件。
- **点击或拖动 CSV 文件到此区域以上传**- 拖放 CSV 模板文件，或点击 以浏览到要上传的 CSV 模板文件。系统会在上传文件后进行验证检查。

  CSV 模板文件上传成功后，CSV 模板文件的内容将以表格格式显示。

步骤 6 点击**添加设备**以注册设备。

在外部接口上使用零接触调配时，Security Cloud Control 会充当 DDNS 提供商并执行以下操作：

- 使用 "fmcOnly" 方法在外部启用 DDNS。此方法仅支持零接触调配设备。

- 使用以下主机名映射外部 IP 地址： *serial-number*.**local**。
- 提供到 防火墙管理中心 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
- 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 防火墙管理中心 发送通知。

如果在管理接口上使用零接触调配，则不支持 DDNS。 防火墙管理中心 必须可公开访问，以便设备能够发起管理连接。

您可以继续使用 Security Cloud Control 作为 DDNS 提供商，也可以稍后将 防火墙管理中心 中的 DDNS 配置更改为其他方法。有关详细信息，请参阅配置动态 DNS ， 第 965 页。

如果设备注册失败，请参阅解决序列号（零接触调配）注册问题 ， 第 56 页。

使用设备模板注册序列号的 *CSV* 模板文件

CSV 模板文件的大小必须小于 2 MB。文件名必须满足以下条件：

- 最多可包含 64 个字符。
- 只允许使用字母数字字符和特殊字符，如破折号 (-)、句点 (.) 和下划线 (_)。
- 不得包含任何空格。

包含两个设备配置的 CSV 模板文件示例如下。

```
DisplayName,SerialNumber,AdminPassword,$WANLinkIP,Host:gateway
Branch A FTD,JADX345410AB,C15c05n0rt#,10.20.30.1/24,10.2.3.1
Branch B FTD,JADX345670CE,Admin123!,10.20.30.5/24,10.2.3.1
```

格式正确的 CSV 文件包含以下字段。

必填字段

- **DisplayName**— 设备的名称。类型：字符串。示例：test1
- **SerialNumber** - 设备的序列号。类型：字符串，示例：JADX345670EG
- **AdminPassword** - 用于管理员访问的密码，类型：字符串，示例： E28@2OiUrhx 如果此设备未配置或全新安装，则需要设置 **AdminPassword**。如果您已登录并更改了密码，请将此字段留空。

可选字段

- **DeviceGroup** - 设备组的名称，类型：字符串，示例：testgroup

变量

使用以下格式：**$***varName*。

变量示例：**$LAN-Devices-IPv4Address** - LAN 设备的 IPv4 地址。类型：字符串。示例：10.2.3.4/24。

网络对象覆盖

使用以下格式：*objType*:*objName*。

网络对象覆盖示例：**Network:LAN-Devices-Network**- LAN 设备网络的 IP 地址。类型：字符串。示例：10.2.3.0/24

FQDNs

对于序列号注册，会自动启用 DDNS。如果要为 **仅 FMC** 类型 DDNS 设置与默认值不同的值，则可以在模板中配置设置。在此情况下，为 hostaname 提供 CSV 值时，请务必将其指定为 *serialnumber*.**local**。

添加机箱

您可以将 Firepower 4100/9300 添加到防火墙管理中心。管理中心和机箱使用机箱 MGMT 接口共享单独的管理连接。防火墙管理中心提供机箱级运行状况警报。对于配置，您仍需要使用 Cisco Secure Firewall 机箱管理器 或 FXOS CLI。

注释 对于其他支持多实例的模型， 机箱会作为多实例模式的一部分被添加到 防火墙管理中心 ，的过程中完成 。请参阅将设备转换为多实例模式 ， 第 223 页。 但是，如果您使用 CLI 转换为多实例模式(在 CLI 启用多实例模式 ， 第 260 页)，请跳至此程序的 步骤 3 ， 第 53 页 以便将机箱添加到管理中心。

过程

步骤 1 通过控制台端口或使用 SSH连接至机箱 FXOS CLI。

步骤 2 配置防火墙管理中心。

create device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

系统将提示您输入注册密钥。

您可以从任何范围输入此命令。无需使用 **commit-buffer**即可立即接受此命令。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the 防火墙管理中心。必须至少有一个设备（防火墙管理中心或机箱）具有可访问的IP地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果未在此命令中指定 **hostname** ，则机箱必须具有可访问的 IP 地址或主机名，并且必须指定 **nat-id**。
- **nat-id** *nat_id*- 指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 防火墙管理中心 机箱上指定它。如果您不指定 **hostname**，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。NAT ID 不得超过 37 个字符。

有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。

- **Registration Key:** *reg_key*- 系统将提示您输入选择的一次性注册密钥，注册机箱时也要在 防火墙管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

示例：

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

步骤 3 在 防火墙管理中心中，使用机箱管理 IP 地址或主机名添加机箱。

a) 选择 **设备** > **设备管理**，然后从 “**添加**”下拉列表中选择**机箱**。

图 ***23:*** 添加机箱

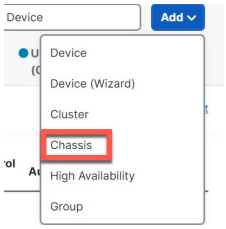
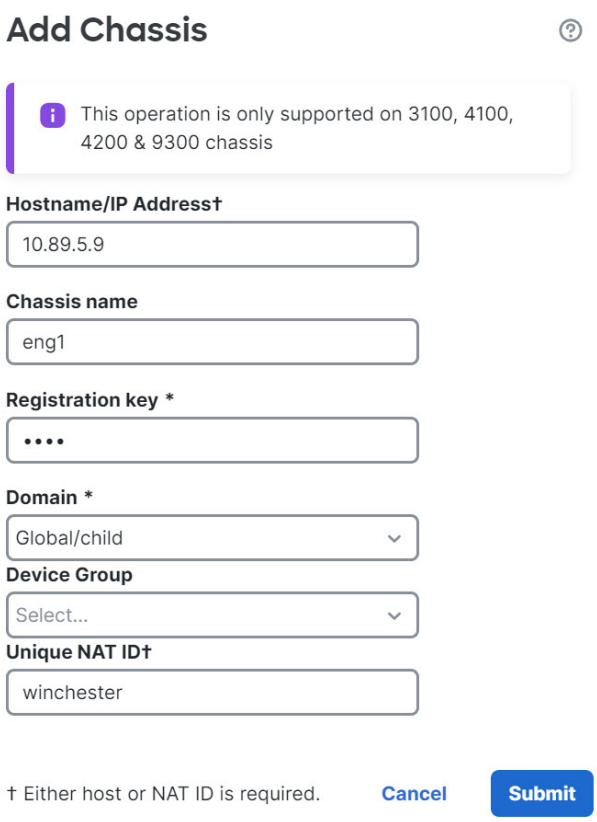


图 *24:* 添加机箱



b) 在 **主机/IP 地址**字段中，输入要添加的设备的 IP 地址或主机名。

如果您不知道主机名或 IP 地址，可以将此字段留空，指定**唯一 NAT ID**。

c) 在**机箱名称**字段中，输入要在 防火墙管理中心中显示的设备名称。

d) 在**注册密钥**字段中，输入将机箱配置为由 防火墙管理中心管理时所使用的同一注册密钥。

注册密钥是一个一次性的共享密钥。密钥可以包含字母数字字符和连字符（-）。

e) 在多域部署中，无论当前的域是什么，都将该机箱分配给叶**域**。

如果当前域是叶域，机箱会自动添加到当前域。如果当前域不是叶域，则注册后必须切换到叶域才能配置机箱。一个机箱只能属于一个域。

f) （可选）将机箱添加到 **设备组**。

g) 如果在机箱安装过程中使用了 NAT ID，请展开并在 **唯一 NAT ID** 字段中输入相同的 NAT ID。

NAT ID 可以包含字母数字字符和连字符（-）。

h) 点击 **Submit**。

机箱会被添加到**设备** > **设备管理**页面。

向新的管理中心注册

此程序显示如何使用新的 防火墙管理中心 进行注册。即使新的 防火墙管理中心 使用旧的 防火墙管理中心 的 IP 地址，也应执行这些步骤。

过程

步骤 1 在旧 防火墙管理中心 上，如果存在，请取消注册托管设备。请参阅从 防火墙管理中心 取消注册设备，第 63 页。

如果您有与 防火墙管理中心的活动连接，则无法更改 防火墙管理中心 IP 地址。

步骤 2 连接到设备 CLI，例如使用 SSH。

步骤 3 配置新的 防火墙管理中心。

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

- {hostname | IPv4_address | IPv6_address}-设置主机名，IPv4地址或IPv6地址。防火墙管理中心
- **DONTRESOLVE**-如果 防火墙管理中心 不可直接寻址，请使用 **DONTRESOLVE** 而不是主机名或 IP 地址。如果使用 **DONTRESOLVE** ，则需要使用 *nat_id* 。当您将此设备添加到 防火墙管理中心时，请确保同时指定设备 IP 地址和 *nat_id*；连接的一端需要指定 IP 地址，两端需要指定相同的唯一 NAT ID。
- *regkey*-输入注册期间要在 防火墙管理中心 和设备之间共享的注册密钥。可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加Firewall Threat Defense时，需要在防火墙管理中心上输入相同的密钥。
- *nat _id*-当一方未指定 IP 地址时，在 防火墙管理中心 与设备之间的注册流程中使用的字母数字字符串，介于 1 至 37 个字符。此 NAT ID 是仅在注册期间使用的一次性密码。确保 NAT ID 是唯一的，不会被等待注册的任何其他设备使用。添加 Firewall Threat Defense 时，在 防火墙管理中心 上指定相同的 NAT ID。
- *display_name* - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 Security Cloud Control 标识为仅用于分析的主用管理器和本地部署 防火墙管理中心 ，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：
  - *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字）
  - **manager-***timestamp*

示例：

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

>
```

步骤 4 将此设备添加到 防火墙管理中心。

解决序列号（零接触调配）注册问题

如果在 2-3 分钟后设备使用序列号注册失败，请参阅以下失败的常见原因。如果您可以物理访问设备， 请使用这些工具进行初始故障排除：

- 请检查 LED 指示灯状态。 ，第 57 页
- 在 CLI 中检查零接触调配状态 ，第 57 页

如果要绕过任何序列号故障排除，您可以随时 注册密钥方法 ，第 32 页。

有关序列号注册的其他要求，请参阅使用序列号添加设备（零接触调配） - 基本配置 ，第 39 页。

正在等待设备上线 防火墙管理中心

- **原因**：您在 CLI 中执行了初始配置并禁用了 零接触调配。

  解决方法：请参阅在 CLI 中删除已配置的管理器以重新启用零接触调配 ，第 60 页

- **原因**：您在 防火墙设备管理器 中执行了初始配置，并禁用了 零接触调配。

  解决方法：请参阅使用防火墙设备管理器重新启动零接触调配 ，第 61 页。

- **原因**： 零接触调配 已禁用，您无权访问 CLI。

  解决方法：请参阅重置设备 ，第 62 页。

- **原因**：您的设备无法访问互联网。

  解决方法：在 CLI 中检查零接触调配状态 ，第 57 页针对明确故障 。问题可能与 DHCP 相关，或者您可能无法访问默认 DNS 服务器，这需要网络管理员的支持。

”序列号为 的设备<serial-number>中已存在 防火墙管理中心中的Security Cloud Control 租户错误”。

原因：序列号已被您租户中的其他管理器申领。

解决方法：如果您已取消注册设备，或者不确定是哪个 防火墙管理中心 申领了设备，请参阅 检查安全云控制中的更改 ，第 61 页。如果 防火墙管理中心 离线且您需要删除其申领，请参阅 在 CLI 中删除序列号申领 ，第 59 页。

注释 如果存在活动的 防火墙管理中心 管理连接，您无法从当前管理器中删除申领。

”序列号为 的设备 <serial-number>防火墙管理中心中已存在于另一个 Security Cloud Control 租户中时出错”。

原因：序列号已被另一租户中的其他管理器申领。

解决方法：请参阅在 CLI 中删除序列号申领 ，第 59 页。

注释 如果存在活动的 防火墙管理中心 管理连接，您无法从当前管理器中删除申领。

请检查 LED 指示灯状态。

LED 状态会告知您零接触调配的就绪情况。

Firepower 1010、1100

表 *6:* 零接触调配：系统 *(S) LED* 行为

S LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁（错误情况）	设备无法连接到思科云。	15:00 - 30:00

Cisco Secure Firewall 200、1200、3100

表 *7:* 零接触调配：受管 *(M) LED* 行为

M LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁（错误情况）	设备无法连接到思科云。	15:00 - 30:00
绿灯常亮	已自行激活	20:00 - 45:00

在 CLI 中检查零接触调配状态

如果需要对注册进行故障排除，请检查Firewall Threat Defense CLI 上的零接触调配状态。有关详细信息，请参阅登录到设备的命令行界面 ，第 12 页。

注释 如果您是首次访问 CLI 并且必须运行设置脚本，请在系统出现以下提示时回答 **n**：`是否要配置 IPv4？(y/n) [y]:` 和`是否要配置 IPv6？(y/n) [y]:`。您还必须接受默认本地管理器：`本地管理设备？(yes/no) [yes]:`。这些设置将保留零接触调配功能。

show ztp-troubleshoot-status

```
> show ztp-troubleshoot-status
Overall Status: SUCCESS
```

```
Stage: Cloud Connector
  Status: SUCCESS

Stage: Connectivity
  Status: SUCCESS
  Detailed Status:
    IP: 10.12.414.54
    Dns Servers:
     - 208.67.222.222
     - 208.67.222.220
    Is Connected: true

Stage: Cloud Status
  Status: SUCCESS
  SubStages:
  Stage: Token Generation
    Status: SUCCESS
  Stage: Cloud Enrollment
    Status: SUCCESS
  Stage: Tenant Info
    Status: SUCCESS
    Detailed Status:
      Tenant Info:
        Registered Tenant Info:
          Company Id: 039290342
          Company Name: Default
          Domain Name: ltp.cisco.com
          Id: d874e871-5844-47ed-9120-3ec3844b52ac
          Sp Id: LTP
          Sub Domain Name: ltp.cisco.com
        Tenant Info:
          Company Id: 039290342
          Company Name: Default
          Domain Name: ltp.cisco.com
          Id: d874e871-5844-47ed-9120-3ec3844b52ac
          Sp Id: LTP
          Sub Domain Name: ltp.cisco.com
```

连接故障实例

如果设备从不注册，您将在连接阶段的命令输出中看到失败。在防火墙管理中心上，您将看到**等待设备上线的**消息。

```
> show ztp-troubleshoot-status
Overall Status: FAILED
Stage: Cloud Connector
  Status: SUCCESS
Stage: Connectivity
  Status: FAILED
  Detailed Status:
    IP: 10.12.414.54
    Dns Servers:
      - 208.67.222.222
      - 208.67.222.220
Is Connected: false
```

1. 使用 ping 检查网络连接，例如与 Google DNS 服务器的连接。

   ```
   > ping 8.8.8.8
   PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
   64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=10.7 ms
   64 bytes from 8.8.8.8: icmp_seq=2 ttl=107 time=10.3 ms
   ```

```
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 10.254/10.483/11.270/0.323 ms
```

2. 由于 ping 操作成功，请检查 DNS 解析：

```
> ping cisco.com
Please use 'CTRL+C' to cancel/abort...
 ping cisco.com
      ^
ERROR: % Invalid Hostname
```

您的设备无法访问 DNS 服务器（208.67.222.222、208.67.222.220）。请向网络管理员咨询通过 DHCP 提供的服务器信息。

在 CLI 中删除序列号申领

如果设备以前已申领，但管理连接未处于活动状态，可以清除申领。在防火墙管理中心，您会看到序列号为 的**设备 <serial-number>中已存在Security Cloud Control 租户错误**。

注释 如果存在活动的 防火墙管理中心 管理连接，您无法从当前管理器中删除申领。

过程

步骤 1 使用 SSH 或控制台端口连接到 FXOS CLI。有关详细信息，请参阅登录到设备的命令行界面，第 12 页。

如果使用 SSH，则连接到 Firewall Threat Defense CLI。在这种情况下，请输入 **connect fxos**。

注释
如果您是首次访问Firewall Threat Defense CLI 并且必须运行设置脚本，请在系统出现以下提示时回答 **n**：`是否要配置 IPv4? (y/n) [y]:` 和`是否要配置 IPv6? (y/n) [y]:`。您还必须接受默认本地管理器：`本地管理设备? (yes/no) [yes]:`。这些设置将保留零接触调配功能。

如果使用控制台端口，则直接连接到 FXOS。

如果这是您第一次使用 SSH 或控制台连接到 CLI，系统会提示您更改密码。对于零接触调配，当您载入设备时，请务必为**密码重置**区域选择**否...**，因为您已设置密码。

```
> connect fxos
firepower#
```

步骤 2 进入本地管理模式。

connect local-mgmt

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

步骤 3 从思科云取消注册设备。

cloud deregister

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

在 CLI 中删除已配置的管理器以重新启用零接触调配

如果执行了初始 CLI 设置并将设备设置为远程管理，则可以通过删除管理器并重新添加本地管理器来重新启用零接触调配。此设置并不意味着您打算使用本地管理器；您可以将其添加到管理器。它只是恢复 零接触调配所需的功能。即使您将管理器设置为本地，如果您登录 防火墙设备管理器 并完成了初始设置，则可能已禁用 零接触调配。删除并重新添加本地管理器将恢复 零接触调配。

注释 仅当没有当前的 防火墙管理中心 管理连接时，才能删除管理器。

开始之前

登录到设备的命令行界面，第 12 页。

过程

步骤 1 检查状态。

show managers

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

在这种情况下，您选择了远程管理，但未配置 防火墙管理中心。您需要将管理器设置为本地。

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

此输出显示您已在运行本地管理器。即使在这种情况下，删除管理器也会恢复 零接触调配的必要服务。

步骤 2 删除管理器。

configure manager delete

步骤 3 添加本地管理器。

configure manager local

使用防火墙设备管理器重新启动零接触调配

如果登录 防火墙设备管理器，并在 防火墙设备管理器中完成初始设置，则可能会在无意中禁用低接触调配。在这种情况下，您可以在防火墙设备管理器中重新启动零接触调配。如果您有权访问 CLI，也可以 在 CLI 中删除已配置的管理器以重新启用零接触调配，第 60 页。

过程

步骤 1 在 防火墙设备管理器 中，点击**设备 (Device)**，然后点击**系统设置 (System Settings)** > **云服务 (Cloud Services)**。

步骤 2 选中**自动注册** Security Cloud Control **或 Cisco Secure Firewall Management Center**。

步骤 3 点击**注册 (Register)**。

检查安全云控制中的更改

如果从 防火墙管理中心注销设备，则该序列号的申领应会自动删除。不过，在极少数情况下，如果申领仍处于活动状态，您可以强制 Security Cloud Control 从您的库存中移除设备。

过程

步骤 1 在 Security Cloud Control 登录到 https://security.cisco.com。

步骤 2 依次选择 **安全设备 (Security Devices)**，然后搜索序列号。

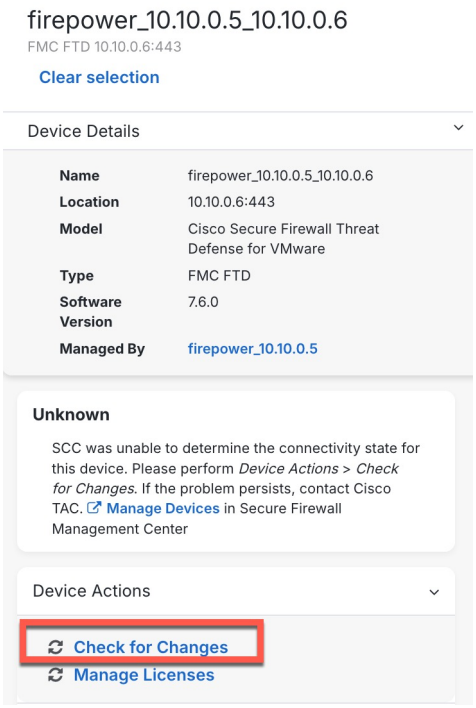
图 *25:* 按序列号搜索



如果设备未显示在搜索结果中，则它可能已注册到其他租户。在此情况下，请参阅在 CLI 中删除序列号申领，第 59 页。

步骤 3 选择设备，然后点击右边的**检查更改**。

图 *26*: 检查更改



如果设备已注销，它将从列表中消失，并且设备将再次尝试连接到云。

如果设备没有消失，则意味着它已注册到租户中的另一个管理器。设备的名称包括其注册到的管理器，例如 **firepower_10.89.5.36**_1010-1。如果您仍希望将设备注册到其他管理器，而且您无法访问防火墙管理中心 取消注册设备，您可以 在 CLI 中删除序列号申领，第 59 页 或 。

重置设备

如果您无权访问 CLI，并希望确保您的设备已取消配置并为 零接触调配做好准备，请按住凹进的小重置按钮五秒钟以上，将设备重置为默认状态。

过程

步骤 1 按住小型嵌入式重置按钮超过五秒钟。

有关详细信息，请参阅硬件安装指南。重置后，首次启动 Firewall Threat Defense 可能需要很长时间。

步骤 2 请检查 LED 指示灯状态。，第 57 页 以监控设备何时处于 零接触调配就绪。

从 防火墙管理中心 取消注册设备

如果不希望再管理设备，可以将其从防火墙管理中心中取消注册。

要取消注册集群、集群节点或高可用性对，请参阅这些部署的章节。

取消注册设备：

- 会切断 防火墙管理中心和该设备之间的所有通信。
- 从**设备管理 (Device Management)** 页面删除设备。
- 如果设备的平台设置策略配置为使用 NTP 从防火墙管理中心接收时间，则将设备返回本地时间管理。
- 保持配置不变，以便设备继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将设备再次注册到相同或不同的防火墙管理中心会导致配置被删除，因此设备将在该点停止处理流量。

在取消注册设备之前，请务必导出配置或创建模板，以便在重新注册设备时可以重新应用设备级配置（接口、路由等）。如果您没有已保存的配置或模板，则必须重新配置设备设置。

重新添加设备并导入已保存的配置、使用模板或重新配置设置后，您需要先部署配置，然后才能再次开始传递流量。

开始之前

要重新应用设备级配置（如果您将其重新添加到 防火墙管理中心），请执行以下操作之一：

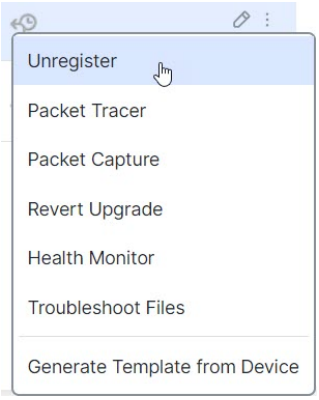
- 导出设备配置。请参阅导出和导入设备配置。
- 创建用于设备的模板。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要取消注册的设备旁边点击 **更多** (⋮)，然后点击**取消注册 (Unregister)**。

图 *27:* 取消注册



步骤 3 确认您要取消注册设备。

步骤 4 您现在可以更改管理器。

- 将设备重新注册到此 防火墙管理中心 - 如果您知道注册密钥和 NAT ID，请参阅注册密钥方法，第 32 页。如果您需要重置它们，则可以像新配置一样重新配置管理器。请参阅 向新的管理中心注册，第 55 页。
- 注册到新的 防火墙管理中心 - 向新的管理中心注册，第 55 页。
- 更改为 防火墙设备管理器 - 从 防火墙管理中心 切换到 防火墙设备管理器，第 79 页。
- 删除管理器而不指定新管理器 - 要在不识别新管理器的情况下切断 Firewall Threat Defense 上的管理连接（无管理器模式），请在 Firewall Threat Defense CLI 中使用 **configure manager delete** 命令。

关闭或重新启动设备

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

请参阅以下任务以正确关闭或重启系统。

注释 重新启动设备后，您可能会看到无法重新建立管理连接的错误。在某些情况下，在设备上的管理接口准备就绪之前尝试连接。系统将自动重试连接，并应在 15 分钟内建立连接。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要重新启动的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 要重启设备：

a) 请点击 **重启设备** ()。

b) 出现提示时，确认是否要重启设备。

步骤 5 要关闭设备：

a) 在**系统 (System)** 部分中点击 **关闭设备** ()。

b) 出现提示时，确认是否要关闭设备。

c) 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

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

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

对于 ISA 3000，完成关闭后，系统 LED 将熄灭。至少等待 10 秒，然后再断开电源。

下载托管设备列表

您可以下载所有托管设备的报告。

开始之前

要执行以下任务，您必须是管理员用户。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **下载设备列表报告** 链接。

步骤 3 您可以下载 CSV 或 PDF 格式的设备列表。选择 **下载 CSV** 或 **下载 PDF** 以下载报告。

迁移 Firewall Threat Defense 设备

Cisco Secure Firewall Threat Defense 模型迁移向导使您能够将配置从旧 Firewall Threat Defense 模型迁移到新模型。迁移后，源 Firewall Threat Defense 设备的所有路由和接口配置都将在目标 Firewall Threat Defense 中可用。

该向导支持多个型号作为源设备和目标设备，有关详细信息，请参阅支持进行迁移的设备，第 66 页。

在 7.6.1 版本中，Firewall Threat Defense 型号迁移向导具有更广泛的设备支持，以及一个用户友好的界面，旨在简化您的型号迁移。有关详细信息，请参阅《Cisco Secure Firewall Threat Defense 型号迁移指南，7.6.1 版本》。

当您将 Firepower 4100 和 9300 系列设备迁移到受支持的型号时，现在可以根据您的要求配置接口属性。您可以将源设备接口映射到目标设备接口。迁移会锁定源设备和目标设备。

支持进行迁移的设备

支持的数据迁移路径

下表列出了可从源 Firewall Threat Defense 型号迁移到的受支持目标 Firewall Threat Defense 型号。

源设备	源设备版本	目标设备	目标设备版本
Cisco Firepower 1010 系列：1010、1010E	7.3.x 及更高版本	Cisco Secure Firewall 1200 系列：1210CE、1210CP、1210CX	7.6 及更高版本
Cisco Firepower 1010 系列：1010、1010E	7.3.x 及更高版本	Cisco Firewall 200 系列：220	10.0 及更高版本
Cisco Firepower 1100 系列：1120、1140、1150	7.3.x 及更高版本	Cisco Secure Firewall 3100 系统：3105、3110、3120、3130、3140	7.4.1 及更高版本
Cisco Firepower 2100 系列：2110、2120、2130、2140	7.3.x 及更高版本	Cisco Secure Firewall 3100 系统：3105、3110、3120、3130、3140	7.4.1 及更高版本
Cisco Firepower 4100 系列：4110、4112、4115、4120、4125、4140、4145、4150	7.3.x 及更高版本	Cisco Secure Firewall 3100 系统：3105、3110、3120、3130、3140	7.4.1 及更高版本
		Cisco Secure Firewall 4200 系列：4215、4225、4245	7.4.1 及更高版本
		Cisco Secure Firewall 6100 系列：6160、6170	10.0 及更高版本

源设备	源设备版本	目标设备	目标设备版本
Cisco Firepower 9300 系列：SM-40、SM-48、SM-56	7.3.x 及更高版本	Cisco Secure Firewall 3100 系统：3105、3110、3120、3130、3140	7.4.1 及更高版本
		Cisco Secure Firewall 4200 系列：4215、4225、4245	7.4.1 及更高版本
		Cisco Secure Firewall 6100 系列：6160、6170	10.0 及更高版本

迁移许可证

- 您的智能许可帐户必须具有目标设备的许可证授权。
- 您必须使用智能许可账户注册并注册设备。迁移会将源设备许可证复制到目标设备。

迁移的前提条件

- **一般设备前提条件**
  - 将源设备和目标设备注册到 防火墙管理中心。
  - 确保目标设备是新注册的设备，且无任何配置。
  - 源设备和目标设备必须处于相同状态和模式：
    - 域
    - 防火墙模式：路由或透明
    - 合规模式（CC 或 UCAPL）
    - 管理状态

      设备必须具有相同类型的管理器访问接口（管理接口或数据接口）。
    - 多实例模式或设备模式
  - 确保您具有设备修改权限。
  - 确保源设备上的配置有效且无错误。
  - 迁移期间，两台设备上均不得运行部署、导入或导出任务。源设备可以有待处理的部署。
- **变更管理的前提条件**
  - 确保源设备和目标设备未被变更管理故障单锁定。
  - 确保分配给源设备的共享策略未被变更管理故障单锁定。

- **HA 设备的前提条件**
  - 仅从主用 防火墙管理中心 迁移设备。
- **多实例模式设备前提条件**
  - 确保源设备和目标设备处于多实例模式。
  - 手动迁移机箱配置。在将实例配置迁移到目标实例之前，先创建实例。目标设备必须具有兼容的接口。例如，在目标设备上，必须创建 EtherChannel 接口，并为这些接口创建已标记、未标记、专用或共享接口。
- **带外配置设备的前提条件**
  - 确保确认带外更改，并在防火墙管理中心内匹配配置。您无法迁移具有这些配置的设备。要查看带外配置，请执行以下操作：

    1. 选择**设备** > **设备管理**。
    2. 点击设备旁边的编辑图标，然后点击**接口**选项卡。

    或

    1. 点击设备旁边的编辑图标，然后点击**设备**选项卡。
    2. 在**运行状况**磁贴中验证**带外配置状态**。
- **具有管理器访问接口的设备的前提条件**

  确保设备未处于“数据传输”或“管理传输”状态。如果设备处于这些状态，则无法迁移。
  - 数据传输状态：管理器访问接口从数据接口更改为管理接口，但未在设备上部署变更时的设备状态。
  - 管理传输状态：管理器访问接口从管理接口更改为数据接口，但未在设备上部署变更时的设备状态。
- **带有合并管理和诊断接口的设备的前提条件**

  确保目标设备始终处于合并模式。

向导可以迁移哪些配置？

迁移向导会将以下配置从源设备复制到目标设备：

- 许可证
- 接口配置
- 内联集配置
- 路由配置

- DHCP 和 DDNS 配置
- Policies
- 关联的对象和对象覆盖
- 平台设置
- 远程分支机构部署配置

迁移向导会将以下策略配置从源设备复制到目标设备：

- 运行状况策略
- NAT 策略
- QoS 策略
- 远程访问 VPN 策略
- FlexConfig 策略
- 访问控制策略
- 预过滤器策略
- IPS 策略
- DNS 策略
- SSL 策略
- 恶意软件和文件策略
- 身份策略
- 共享策略

迁移向导会将以下路由配置从源设备复制到目标设备：

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- 策略型路由
- Static Route
- 组播路由

- 虚拟路由器

迁移向导会将以下接口从源设备复制到目标设备：

- 物理接口
- 子接口
- Etherchannel 接口
  - 在独立设备上，向导会将 EtherChannel 从源设备复制到目标设备。
  - 对于多实例模式下的设备，必须在机箱上创建 EtherChannel 并将其分配给实例。
- 网桥组接口
- VTI 接口
- VNI 接口
- 环回接口
- VXLAN 隧道端点 (VTEP) 接口

迁移向导会保留目标设备的设备组。

迁移准则和限制

准则

- **对于多实例模式下的设备：**

  迁移期间，请确保按照下表映射接口：

源设备	目标设备
物理接口	物理接口
EtherChannel 接口	EtherChannel 接口
超级管理员配置的子接口	超级管理员配置的子接口
已标记的接口	已标记的接口
未标记的接口	未标记的接口
共享接口	共享和专用接口
专用接口	专用接口

  不能将超级管理员配置的子接口映射到实例创建的子接口。

- **对于 HA 设备**，您可以迁移：

- 源 HA 设备到目标 HA 设备。
- 源 HA 设备到目标独立设备。

- **对于远程分支部署中的设备：**
  - 将源管理器访问接口映射到目标管理器访问接口。
  - 确保源和目标防火墙管理中心的管理器访问接口属于相同的IP地址类型（静态或DHCP）。
  - 两个管理器访问接口都必须具有 IPv4 或 IPv6 地址。
  - 如果管理器访问接口具有静态 IP 地址，请确保它们位于同一子网中。

- **对于 Snort：**

  默认情况下，迁移后目标设备将使用 Snort 3，即使源设备使用 Snort 2。

- **对于使用诊断接口的设备：**

  迁移后，目标设备上仅提供合并的管理接口。

限制

- 迁移向导不迁移以下内容：
  - 站点间 VPN 策略
- 一次只能执行一个迁移。
- 迁移后，远程访问 VPN 信任点证书不会注册。
- 对于 HA 设备：
  - 目标设备：不能将独立设备迁移为 HA 设备。
- 不支持群集。
- 对于远程分支部署中的设备：
  - 该向导不支持将单个 WAN 管理器访问数据接口迁移为双 WAN 管理器访问数据接口。

迁移安全 Firewall Threat Defense

开始之前

确保您查看 迁移的前提条件，第 67 页 和 迁移准则和限制，第 70 页。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击页面右上角的**迁移**。

步骤 3 在**选择源设备和目标设备中**：

a) 从**源设备**下拉列表中，选择一个设备。

b) 从**目标设备**下拉列表中，选择一个设备。

源设备和目标设备可以具有以下标记：

- 路由式：处于路由防火墙模式的设备。
- 透明式：处于透明防火墙模式的设备。
- 容器：处于多实例模式的设备。
- 高可用性：处于高可用性模式的设备。
- 仅分析：由 Security Cloud Control 管理的设备，且 防火墙管理中心 仅接收和显示事件（仅分析防火墙管理中心）。

如果该设备是 HA 对的一部分，则仅显示 HA 对名称。

步骤 4 点击**下一步 (Next)**。

步骤 5 （仅适用于设备模式下的 Firepower 4100 和 9300 系列设备）在**机箱管理器详细信息**中：

a) 如有需要，选中**跳过机箱管理器**复选框。

b) 在**机箱主机名或 IP 地址**字段中，输入值。

注释

- 验证 防火墙管理中心 可以访问 Cisco Secure Firewall 机箱管理器。
- 确保您为源设备选择了正确的机箱管理器，因为 防火墙管理中心 不会验证您的选择。

c) 点击**验证证书**，以验证机箱管理器的证书。

d) 在**用户名**和**密码**字段中，输入机箱管理器的凭据。

步骤 6 点击**下一步 (Next)**。

步骤 7 在**配置接口**中：

默认情况下，源接口和目标接口使用接口硬件名称进行映射。您必须映射命名接口、逻辑接口以及属于其他接口的接口。所有其他接口的映射不是必需的。向导会根据您提供的接口映射创建逻辑接口。

您不能映射属于 HA 故障转移配置的接口。这些接口会在向导中被禁用。

设备模式下的 Firepower 4100 和 9300 系列设备：

对于这些设备，防火墙管理中心 会从机箱管理器获取接口属性，如速度、双工模式和自动协商。

a) 点击以下选项之一，在目标设备上配置这些接口属性：

- **保留目标设备值**：（默认）保留在目标设备上配置的接口属性。
- **从源设备复制**：从源设备复制接口属性。

  只有当 防火墙管理中心 成功连接到机箱管理器时，此选项才会启用。建议您使用此选项。如果物理接口的速度、双工模式和自动协商值在目标设备中不兼容，则会将其设置为默认值。
- **自定义设备值** - 允许您在目标设备上配置所需接口属性的值。

b) 要从默认映射更改接口映射，请从**映射的接口**下拉列表中选择一个接口。

c) 对于 EtherChannel，您可以配置接口属性，并点击**添加成员接口**以添加成员接口。

EtherChannel 的接口属性根据第一个成员接口的接口属性进行配置。您最多可以添加 16 个成员接口。

Firepower 1100 和 2100 系列设备，以及多实例模式下的 Firepower 4100 和 9300 系列设备：

对于这些设备，您必须将源设备接口映射到目标设备接口。

对于多实例模式下的 Firepower 4100 和 9300 系列设备，您只能执行接口映射，无法配置接口属性（如速度、双工模式、自动协商和 FEC 模式）。

如果要从默认映射更改接口映射，请从**映射的接口**下拉列表中选择接口。

点击**重置**，以配置默认接口映射。例如，向导会将源设备中的 Ethernet1/1 映射到目标设备中的 Ethernet1/1。

接口可以具有以下标记：

- 已标记：机箱上的物理接口。
- 未标记：机箱上具有子接口的物理接口。
- 专用：分配给特定实例且不在多个实例间共享的接口。
- 共享：由多个实例共享的接口。
- 管理器访问：数据接口是管理器访问接口。

如有需要，选中**忽略警告**复选框。

步骤 8 点击**下一步 (Next)**。

步骤 9 点击**提交 (Submit)** 开始迁移。

步骤 10 要查看迁移状态，请单击 **通知** （消息中心），然后单击 **任务** 选项卡。

迁移完成后，会生成**设备型号迁移**报告。您可以在**通知 > 任务**页面中看到此报告的链接。

下一步做什么

迁移成功后，您必须完成以下任务：

- 查看 威胁防御 设备迁移最佳实践，第 74 页 中的建议。
- 验证配置。
- 在设备上部署配置。

如果迁移失败，目标设备会回滚到初始状态。

威胁防御 设备迁移最佳实践

成功迁移后，我们建议您在部署之前执行以下操作：

- 接口的 IP 地址会从源设备复制到目标设备。如果源设备处于运行状态，请更改目标设备接口的 IP 地址。
- 确保使用修改后的 IP 地址来更新 NAT 策略。
- 如果在迁移后将接口速度设置为默认值，请配置接口速度。
- 在目标设备上重新注册设备证书（如有）。
- （可选）配置远程分支机构部署配置。

  如果源或目标设备具有通过数据接口的管理器访问权限，则在迁移后，管理器访问权限将丢失。更新目标设备上的管理器访问配置。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南 或联机帮助中的将管理器访问接口从“管理”更改为“数据 ”主题。
- 如需配置站点间 VPN，请进行相应配置。这些配置不会从源设备迁移。
- 在部署之前查看部署预览。从 **部署 (Deploy)** 下拉菜单中，点击 **高级部署 (Advanced Deploy)**，然后点击设备的 **预览** () 图标。
- 在运行状况监控器中监控设备运行状况（选择 > **运行状况** > **监控器故障排除** ）。迁移后，源设备的运行状况策略会成为目标设备的运行状况策略。您还可以为设备配置新的运行状况策略。

  迁移后，由于设备迁移前后的 UUID 不同，设备监控仪表板可能会暂时显示冗余的彩色线条。这种冗余仅在迁移期间出现。迁移一小时后，仪表板的每个指标将仅显示一行。

交换机管理器

如果需要，您可以切换管理器。

从 防火墙设备管理器切换到 防火墙管理中心

当您从 防火墙设备管理器 切换到 防火墙管理中心时，除管理接口和管理器访问设置外，所有接口配置会被保留。请注意，不会保留其他配置设置，例如访问控制策略或安全区。

切换到 防火墙管理中心后，您将无法再使用 防火墙设备管理器 管理 Firewall Threat Defense 设备。

开始之前

如果防火墙已配置为高可用性，您必须首先使用 防火墙设备管理器 （如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 在 防火墙设备管理器中，从思科智能软件管理器中取消注册设备。

步骤 2 （可能需要）配置管理接口。

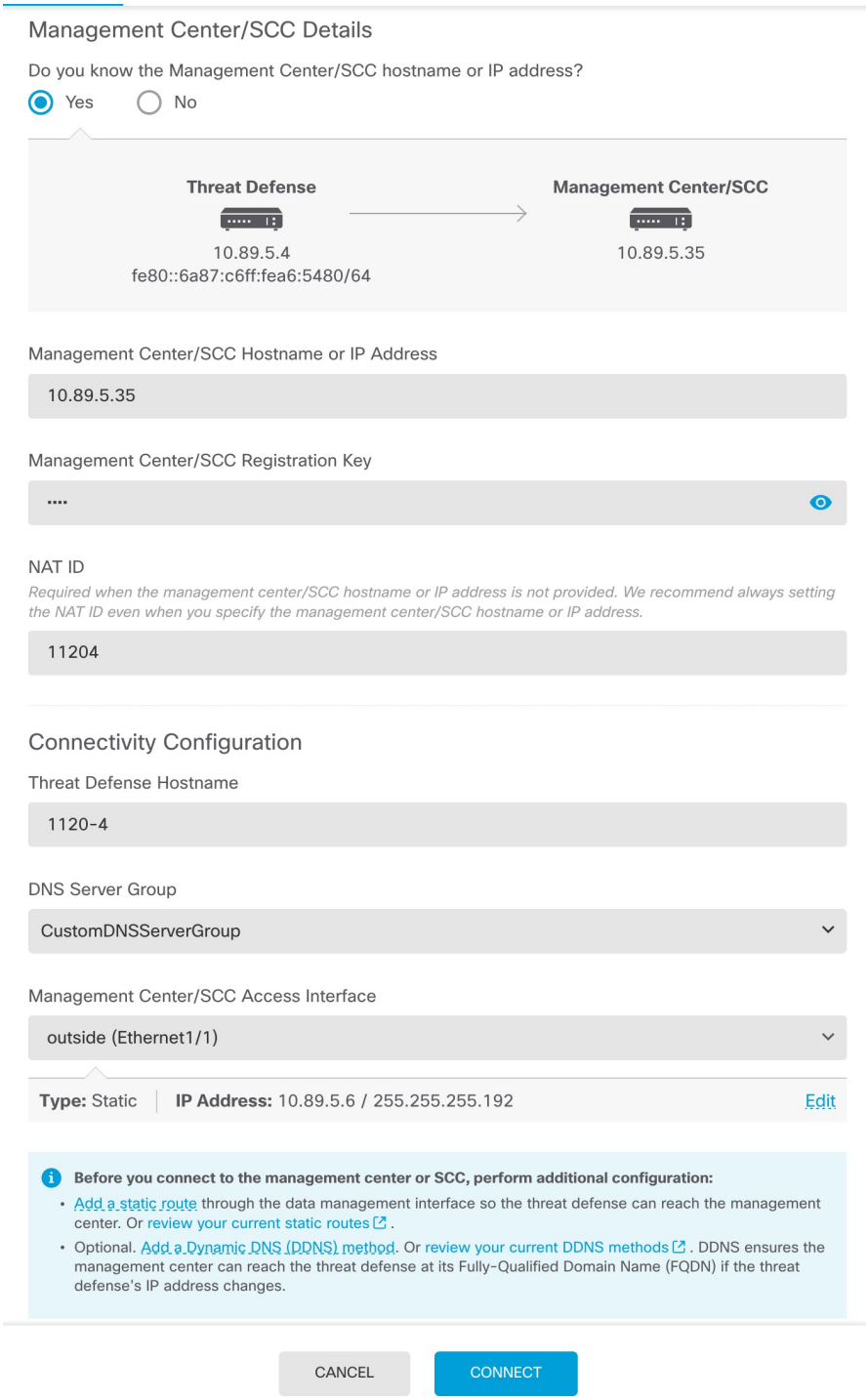
您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用 防火墙设备管理器 连接的管理接口，则必须重新连接到 防火墙设备管理器 。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 3 选择**设备** > **系统设置** > **集中管理**，然后点击**继续**以设置 防火墙管理中心 管理。

步骤 4 配置**管理中心/SCC 详细信息**。

图 *28:* 管理中心*/SCC* 详细信息



a) 对于**是否知道管理中心/SCC 主机名或 IP 地址？**，如果您可以使用 IP 地址或主机名访问 防火墙管理中心，请点击**是**，如果 防火墙管理中心Security Cloud Control 位于 NAT 之后或没有公共 IP 地址或主机名，请点击**否**。

必须至少有一个设备（ 防火墙管理中心 或 Firewall Threat Defense 设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

b) 如果您选择**是 (Yes)**，则输入**管理中心/SCC 主机名或 IP 地址**。

c) 指定**管理中心/SCC 注册密钥**。

此密钥是您选择的一次性注册密钥，注册Firewall Threat Defense设备时也要在 防火墙管理中心上指定它。注册密钥必须为 2 到 36 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 可用于将多台设备注册到 防火墙管理中心。

a) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 防火墙管理中心上指定它。NAT ID 必须介于 2 到 36 个字符之间。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能 用于将任何其他设备注册到 防火墙管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：

- 您将 防火墙管理中心 IP 地址设置为 **DONTRESOLVE**。
- 在 防火墙管理中心上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
- 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
- 防火墙管理中心 使用多个管理接口。

步骤 5 配置**连接配置**。

a) 指定 **FTD 主机名**。

如果您使用数据接口进行**管理中心/SCC 访问接口**访问，则此 FQDN 将用于此接口。

b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为**管理中心/SCC访问接口**选择数据接口，则此设置会设置数据接口DNS服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在 防火墙管理中心上，数据接口 DNS 服务器在您分配给此 Firewall Threat Defense 的平台设置策略中配置。当您将Firewall Threat Defense设备添加到防火墙管理中心时，本地设置将保留，并且 DNS 服务器 不会 添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 Firewall Threat Defense 设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 防火墙管理中心 和 Firewall Threat Defense 设备同步。

此外，仅当在初始注册时发现 DNS 服务器， 防火墙管理中心 才会保留本地 DNS 服务器。

如果要为 管理中心/ **访问接口FMC**访问接口选择管理接口，则此设置会配置管理 DNS 服务器。

c) 对于**管理中心/SCC访问接口**，请选择任何已配置的接口。

将Firewall Threat Defense设备注册到防火墙管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 6 （可选） 如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到 防火墙管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 7 （可选） 如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保 防火墙管理中心 可接通完全限定域名 (FQDN) 的 Firewall Threat Defense 设备。参阅**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。

如果您在将Firewall Threat Defense设备添加到防火墙管理中心之前配置 DDNS，则Firewall Threat Defense设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便Firewall Threat Defense设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。 Firewall Threat Defense支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (https://help.dyn.com/remote-access-api/)。

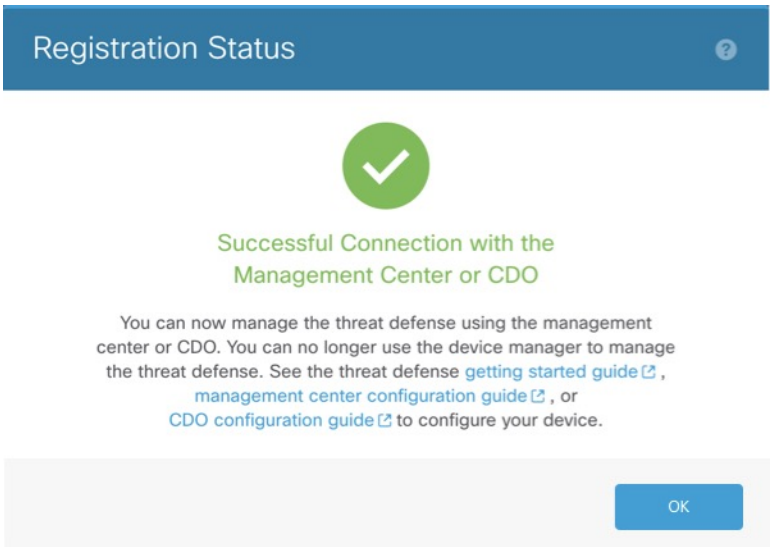
使用管理接口访问管理器时，不支持 DDNS。

步骤 8 点击**连接 (Connect)**。**注册状态**对话框显示切换到防火墙管理中心的当前状态。在**保存管理中心/SCC 注册设置**步骤后，转到 防火墙管理中心，并添加防火墙。

如果要取消切换到 防火墙管理中心，请点击 **取消注册**。否则，请在**保存管理中心/SCC 注册设置**步骤之后关闭防火墙设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到防火墙设备管理器时才会恢复。

如果您在**保存管理中心/SCC 注册设置**步骤后保持连接到 防火墙设备管理器，您最终将看到**与管理中心/SCC** 成功连接对话框。您将断开与 防火墙设备管理器 的连接。

图 *29:* 成功连接



从 防火墙管理中心 切换到 防火墙设备管理器

您可以将当前由本地部署或云交付的防火墙管理中心管理的Firewall Threat Defense设备配置为使用防火墙设备管理器设备。

您可以从防火墙管理中心切换到防火墙设备管理器，而无需重新安装软件。在从防火墙管理中心切换到防火墙设备管理器之前，请确认防火墙设备管理器满足您的所有配置要求。如果要从防火墙设备管理器 切换到 防火墙管理中心，请参阅从 防火墙设备管理器切换到 防火墙管理中心，第 74 页。

注意 切换到 防火墙设备管理器 会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

过程

步骤 1 在 防火墙管理中心 中，从**设备 (Devices)** > **设备管理 (Device Management)** 页面取消注册防火墙。

步骤 2 使用 SSH 或控制台端口连接到 Firewall Threat Defense CLI。如果使用 SSH，请打开与 **管理 IP 地址** 的连接，并使用 **admin** 用户名（或具有管理员权限的任何其他用户）登录 Firewall Threat Defense CLI。

控制台端口默认为 FXOS CLI。使用 **connect ftd** 命令连接到 Firewall Threat Defense CLI。SSH 会话直接连接到 Firewall Threat Defense CLI。

如果无法连接到管理 IP 地址，请执行以下操作之一：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。使用 **configure network ipv4/ipv6 manual** 命令。

步骤 3 验证您当前处于远程管理模式之下。

show managers

示例：

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

步骤 4 删除远程管理器，进入无管理器模式。

configure manager delete *uuid*

无法直接从远程管理转至本地管理。 如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

示例：

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

>
> show managers
No managers configured.
```

步骤 5 配置本地管理器。

configure manager local

现在，您可以使用 Web 浏览器在 **https://***management-IP-address* 位置打开本地管理器。

示例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

设备注册的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
设备（**向导**）已重命名为**设备**，并进行了精简以优化流程	10.0.0	任意	**添加** > **设备**（**向导**）菜单项已重命名为**添加** > **设备**。已移除旧版**添加** > **设备**对话框。**添加** > **设备**页面也进行了精简以优化流程。 新增/修改的屏幕：**设备** > **设备管理**，然后选择**添加设备**。
使用添加到设备（向导）的基本初始配置，通过注册密钥添加设备	7.6.1 7.7.0	任意	现在，您可以使用设备（向导）使用注册密钥添加设备，并进行基本的初始配置。此功能仍然存在于**添加 (Add)** > **设备 (Device)** 屏幕上。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备（向导）(Device [Wizard])**

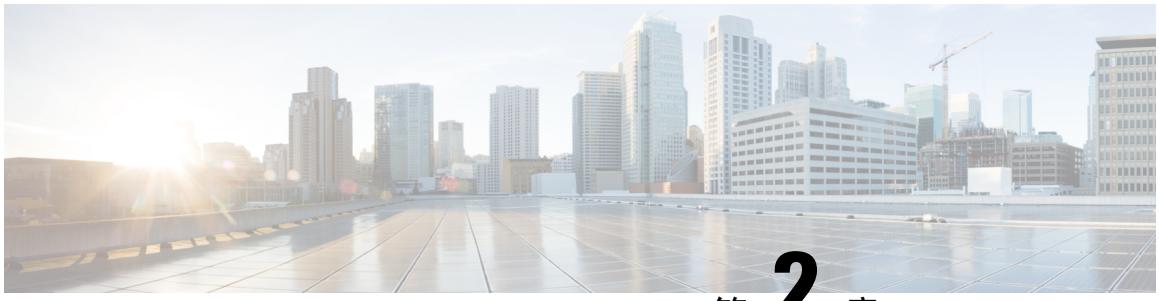
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持从本地防火墙管理中心注册序列号 (零接触调配)。	7.6.0	管理中心必须可公开访问：7.2.0 已删除限制：7.2.4/7.4.0	现在，您可以在本地防火墙管理中心内使用设备的序列号注册设备。使用模板（需要设备上的Firewall Threat Defense 7.4.1+），您可以一次注册多个设备。此功能以前称为低接触调配。 需要 思科安全云。对于升级后的Security Cloud Control，现有的 防火墙管理中心 集成将继续有效，直到您启用思科安全云为止。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备（向导）(Device [Wizard])** 支持的平台：Firepower 1000/2100、Cisco Secure Firewall 1200/3100。请注意 Firepower 2100 仅支持Firewall Threat Defense 7.4.1 – 7.4.x；这些设备无法运行版本 7.6.0。
删除 (Delete) 菜单项被重命名为**取消注册 (Unregister)**	7.6.0	任意	**删除**菜单选项已重命名为**取消注册**，以便更好地指示正在从防火墙管理中心取消注册设备、高可用性对或集群，而不是从高可用性对或集群中删除或清除其配置。设备、高可用性对或集群继续传递流量，直到重新注册为止。 新增/修改的屏幕：**设备** > **设备管理** > **更多**
使用模板添加设备	7.6.0	7.4	**设备 (Devices)** > **设备管理 (Device Management)** > **添加设备（向导）(Add** > **Device [Wizard])** 屏幕让您可使用模板来添加设备。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备（向导）(Device [Wizard])**
禁用 Firepower 1000 和 Cisco Secure Firewall 3100/4200 上的前面板 USB-A 端口。	7.6.0	7.6.0	现在可以禁用 Firepower 1000 和 Cisco Secure Firewall 3100/4200 上的前面板 USB-A 端口。默认情况下，端口处于启用状态。 新增/修改的 Firewall Threat Defense CLI 命令：**system support usb show**、**system support usb port disable**、**system support usb port enable** 多实例模式下 Cisco Secure Firewall 3100/4200 的新增/修改的 FXOS CLI 命令： **show usb-port**、**disable USB port**、**enable usb-port** 请参阅：*Cisco Secure Firewall Threat Defense 命令参考* 和 *Cisco Firepower 4100/9300 FXOS 命令参考*

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 4100/9300 的机箱级运行状况警报。	7.4.1	7.4.1	现在，只要将机箱作为只读设备注册到防火墙管理中心，您就可以查看 Firepower 4100/9300 的机箱级运行状况警报。您还必须启用防火墙威胁防御平台故障运行状况模块并应用运行状况策略。警报会出现在信息中心、运行状况监控器（在左窗格的“设备”(Devices) 下选择机箱）和运行状况事件视图中。 您还可以在多实例模式下为 Cisco Secure Firewall 3100 添加机箱（并查看运行状况警报）。对于这些设备，您可以使用防火墙管理中心来管理机箱。但对于 Firepower 4100/9300 机箱，您仍必须使用机箱管理器或 FXOS CLI。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **机箱 (Chassis)**
使用序列号将设备注册 Firepower 1000/2100 和 Cisco Secure Firewall 3100 到防火墙管理中心的零接触调配。	7.4.0	管理中心可公开访问：7.2.0 管理中心不可公开访问：7.2.4/7.4.0	通过零接触调配（也称为低接触调配），您可以按序列号将 Firepower 1000/2100 和 Cisco Secure Firewall 3100 设备注册到防火墙管理中心，而无需在设备上执行任何初始设置。防火墙管理中心与 SecureX 和Security Cloud Control集成以实现此功能。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备 (Device)** > **序列号 (Serial Number)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
合并的管理接口和诊断接口。	7.4.0	7.4.0	**升级影响。升级后合并接口。** 对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。 如果您已升级到 7.4 或更高版本，并且： • 您没有为诊断接口进行任何配置，则接口将自动合并。 • 您已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 对于平台设置，这意味着： • 您无法再启用 HTTP、ICMP 或 SMTP 进行诊断。 • 对于 SNMP，可以允许“管理”而不是“诊断”上的主机。 • 对于系统日志服务器，您可以通过“管理”而不是“诊断”来访问它们。 • 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 • 如果不指定接口，DNS 查找不会再回退到管理专用路由表。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** 新增/经修改的命令： **show management-interface convergence**
将 Firepower 1000/2100 迁移到 Cisco Secure Firewall 3100。	7.4.0	任意	您现在可以将配置从 Firepower 1000/2100 轻松迁移到 Cisco Secure Firewall 3100。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **迁移 (Migrate)** 平台限制：不支持从 Firepower 1010 或 1010E 迁移。
下载所有已注册设备的报告。	7.4.0	任意	现在您可以下载所有已注册设备的报告。在**设备 (Devices)** > **设备管理 (Device Management)**中，点击页面右上角新的**下载设备列表报告 (Download Device List Report)** 链接。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
使用数据接口管理 Firewall Threat Defense 高可用性对。	7.4.0	7.4.0	Firewall Threat Defense高可用性现在支持使用常规数据接口与防火墙管理中心通信。以前，只有独立设备才支持这一功能。 请参阅：设备管理
ISA 3000 系统 LED 支持关闭。	7.0.5/7.3.0	7.0.5/7.3.0	关闭 ISA 3000 时，系统 LED 会熄灭。至少等待 10 秒，然后再断开电源。
ISA 3000 支持关闭。	7.0.2/7.2.0	7.0.2/7.2.0	您现在可以关闭 ISA 3000；以前，您只能重新启动设备。
多管理器支持	7.2.0	7.2.0	我们引入了云交付的管理中心。云交付的管理中心使用 Security Cloud Control (Security Cloud Control) 平台，并会跨多个思科安全解决方案统一管理。我们负责管理器的更新。 运行版本 7.2+ 的硬件或虚拟管理中心可以“共同管理”云托管设备，但仅限于事件日志记录和分析目的。您无法从硬件或虚拟管理中心将策略部署到这些设备。 新增/修改的命令： **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** 新增/修改的屏幕： • 将云托管设备添加到硬件或虚拟管理中心时，请使用新的**Security Cloud Control托管设备**复选框将其指定为仅用于分析。 • 在 **设备** > **设备管理**中查看哪些设备仅用于分析。 有关详细信息，请参阅 Security Cloud Control文档。
Cisco Secure Firewall 3100 上的 SSD 支持 RAID。	7.1.0	7.1.0	SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，则它们会组成软件 RAID。 新增/经修改的命令： **configure raid, show raid, show ssd**
管理连接支持 TLS 1.3。	7.1.0	7.1.0	FMC 设备管理连接现在使用 TLS 1.3。以前支持 TLS 1.2。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
使用 FDM 将 FTD 配置为由 FMC 进行管理。	7.1.0	7.1.0	如果使用 FDM 执行初始设置，那么在切换到 FMC 进行管理时，除管理和 FMC 访问设置外，会保留在 FDM 中完成的所有接口配置。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 FMC CLI 时，仅保留管理和管理器访问设置（例如，不保留默认的内部接口配置）。 切换到 FMC 后，您将无法再使用 FDM 管理 FTD。 新增/修改 FDM 屏幕：**系统设置 (System Settings)** > **管理中心 (Management Center)**
按升级状态过滤设备。	6.7.0	6.7.0	**设备管理 (Device Management)** 页面现在提供有关托管设备的升级信息，包括设备是否正在升级（及其升级路径），以及上次升级是成功还是失败。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**
一键访问 Firepower 机箱管理器。	6.4.0	6.4.0	对于 Firepower 4100/9300 系列设备，“设备管理”(Device Management) 页面会提供指向 Firepower 机箱管理器 Web 界面的链接。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**
按运行状况和部署状态过滤设备；查看版本信息。	6.2.3	6.2.3	“设备管理”(Device Management) 页面现在提供托管设备的版本信息，并且能够按运行状况和部署状态过滤设备。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**



第 2 章

使用设备模板进行设备注册

您可以使用设备模板将设备添加到 防火墙管理中心。

- 关于使用设备模板进行设备注册， 第 87 页
- 使用设备模板进行设备注册的先决条件， 第 91 页
- 使用设备模板进行设备注册的许可证， 第 91 页
- 使用设备模板进行设备注册的准则， 第 92 页
- 使用设备模板进行设备管理的工作流程， 第 95 页
- 配置设备模板， 第 95 页
- 将模板与设备一起使用， 第 115 页
- 监控设备模板， 第 117 页
- 设备模板故障排除， 第 119 页
- 使用设备模板进行设备管理的历史记录， 第 121 页

关于使用设备模板进行设备注册

通过设备模板，可以部署具有预配置初始设备配置的多个分支设备。您可以使用设备模板对多台设备执行批量零接触调配，对具有不同接口配置的多台设备应用 day 2 配置更改，以及从现有设备克隆配置参数。 您也可以使用序列号一次向 防火墙管理中心 注册多个设备。

使用基本初始配置注册设备时，可以应用访问控制策略和许可证等有限配置。然后，您必须在设备注册后单独配置其他设备设置，如接口、路由和站点间VPN配置。设备模板可让您预先配置这些设置及其他设置，以便在注册时应用。每个设备需要唯一的值，如 IP 地址，可以使用在注册时定义的变量和网络对象覆盖来定义。

您还可以在设备模板中配置站点间 VPN 连接。这些配置定义了设备应加入的站点间 VPN 拓扑。VPN 配置以及其他设备模板策略和配置可使分支设备轻松部署到网络中。设备模板仅支持将设备配置为分支设备。一台设备可以是多个中心辐射型站点间 VPN 拓扑的一部分。

将配置的设备模板应用于设备后，解析变量，配置受保护的网络覆盖，然后将该设备添加为指定 VPN 拓扑中的分支。

使用模板注册设备的方法

您可以通过以下方法，使用设备模板在 防火墙管理中心 上注册设备并设置 Day 0 配置：

- 注册密钥 - 您可以通过在 防火墙管理中心 中指定注册密钥并定义变量来注册单个设备。
- 序列号 - 您可以使用零接触调配按序列号注册一个或多个设备。对于序列号注册，请在您上传的 CSV 文件中定义所有变量和覆盖。

变量和网络对象覆盖

您可以使用变量和网络对象覆盖对模板配置进行参数化。

变量是模板配置支持的对象类型。模板中的变量定义设备的特定配置值。您可以在设备注册和在设备上应用模板时定义这些变量的值。您可以在使用变量的字段看到变量图标 (x)。变量显示时使用 $ 前缀，以区别这些值和其他值。

有关支持的变量类型和创建变量的信息，请参阅支持的变量和添加变量。

网络对象覆盖类似于变量。但是，这些值用于为网络对象提供覆盖值。您可以在模板中声明网络对象列表，并为这些对象创建网络对象覆盖。然后，您就可以在设备上应用模板时为这些网络对象覆盖提供值。例如，如果在模板中定义了主机网络对象，则可以在设备上应用模板之前添加网络对象覆盖，然后在设备上应用模板时提供相关值。

有关受支持的网络对象和添加网络对象覆盖的详细信息，请参阅支持的网络对象覆盖和添加网络对象覆盖。

型号映射

由于不同型号设备的接口配置各不相同，因此必须将模板中的接口配置复制到设备上的目标接口。通过模型映射，可以定义模板中定义的接口与所需 Firewall Threat Defense 模型接口的映射。在设备上应用模板时，接口配置中的变量会被替换为您提供的值，并复制到设备上的映射接口。请注意，在设备上开始应用模板之前，必须在模板中创建模型映射。有关设置模型映射的详细信息，请参阅添加模型映射。

模板和高可用性

设备注册后，可以在 Firewall Threat Defense 高可用性设备上应用设备模板。设备模板不支持特定于高可用性的配置。目标高可用性设备对配置中已包含的任何高可用性配置和受监控接口不会被修改。您无法将任何模板接口映射到故障转移接口。

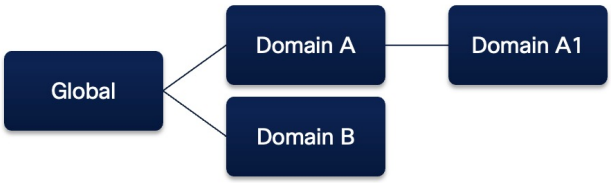
可以从高可用性设备对生成设备模板。模板操作（如在设备上应用模板、生成模板、导入和导出模板）只能在主用设备上执行。不能在备用设备上执行这些操作。

模板和域

设备模板可以存在于任何域中。如果您在子域中，则对域层次结构中您上面的模板具有只读访问权限。您可以将模板应用于其域或其父域中的设备。您可以从设备生成模板，并将该模板应用于域层次结构中任意域的设备。

下面给出了一个域层次结构示例，以及一个显示支持的设备模板应用和生成场景的表格。

请考虑以下情景：



- 域 A 和域 B 是全局域的子域。
- 域 A1 是域 A 的子域。

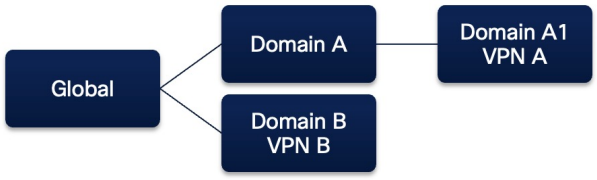
模板域	设备领域	支持的设备模板应用/生成
全局	A1	是
全局	B	是
A	A1	是
A	B	否
B	A1	否
B	B	是
A1	A1	是
A1	B	否

域和 VPN 连接

- 您可以在全局域或子域/枝叶域中定义模板，但只能在枝叶域中定义 VPN 拓扑。
- 您可以在模板中为所有域配置 VPN 连接。在模板应用过程中，只有当设备与 VPN 拓扑处于同一域时，VPN 连接才会应用到设备。

下面给出了一个域层次结构示例，以及一个显示支持的设备模板应用和生成场景的表格。

请考虑以下情景：



- 域 A 和域 B 是全局域的子域。
- 域 A1 是域 A 的子域。
- VPN A 是域 A1 的一部分。
- VPN B 是域 B 的一部分。

模板域	模板中的 **VPN** 拓扑	设备领域	支持的设备模板应用/生成
全局	VPN A VPN B	A1	否
全局	VPN B	B	是
A	VPN A	A1	是
B	VPN B	A1	否
B	VPN B	B	是
A1	VPN A	A1	支持

在设备上应用模板前后验证模板配置

在设备上应用模板前后执行模板配置验证。

任务开始时会执行以下验证检查，以便在设备上应用模板：

- 确保支持目标设备型号和版本。
- 集群和容器检查 - 设备不得是集群或多实例的一部分。
- 模型映射验证 - 目标设备型号的模型映射存在且有效。
- 对模板参数值进行合理性检查。例如，用作接口 IP 地址的两个变量的值不能相同。

任务结束时将执行以下验证检查，以便在设备上应用模板，确保应用的配置有效：

- 接口配置验证。例如，两个或多个接口的 IP 地址字段所用变量的 IP 地址值不得相同。
- 路由策略验证。例如，BGP 邻居配置中的 IPv4 地址不得与任何接口的 IP 地址重叠。

如果在设备上应用模板的任务结束时进行的验证检查失败，任何应用的配置都将回滚，设备将恢复到原始状态。

使用设备模板进行设备注册的先决条件

型号支持

本地 防火墙管理中心、云交付的防火墙管理中心 (cdFMC) 以及运行 Secure Firewall 版本 7.4.1 及更高版本的以下型号支持设备模板：

- Secure Firewall 200
- Firepower 1010
- Firepower 1100
- Secure Firewall 1200
- Secure Firewall 3100

设备模板中 VPN 连接的前提条件

- 配置设备模板中必须使用的站点间 VPN 拓扑。
- 确保已配置所有与中心和 VPN 拓扑相关的配置，例如身份验证方法、IKE 和 IPsec 策略。
- 支持的 VPN 中心辐射型拓扑类型包括：
  - 基于策略
  - 基于路由
  - SD-WAN
- 为Firewall Threat Defense设备的接口分配适当的逻辑名称和 IP 地址。例如，使用 内部 表示连接到 LAN 的接口，使用 外部 表示连接到互联网或 WAN 的接口。
- 分支设备的版本必须为 7.4.1 及更高版本。

使用设备模板进行设备注册的许可证

- 设备模板没有任何特定的许可证要求。
- 智能许可账户中必须有目标设备的许可权限。
- 要在模板中配置 VPN 连接，Essential 许可证必须允许出口控制功能。选择 **管理** > **许可证** > **智能许可证** 在 防火墙管理中心 中验证此功能。
- 在设备上应用模板时，请注意以下有关安全客户端许可的条件：

具有安全客户端许可证的设备	具有安全客户端许可证的模板	设备模板应用后的安全客户端许可证
支持	支持	模板许可证
支持	否	设备许可证
否	支持	模板许可证

使用设备模板进行设备注册的准则

一般准则

- 支持 VNI 和 VTEP 以外的所有设备配置。
- 您可以将共享策略和 S2S VPN 策略附加到模板。这些策略是在模板应用期间分配的。
- 模板可在 HA 设备上应用。但是，不支持在 HA 设备对注册期间应用设备模板。您也无法管理与 HA 相关的配置，例如故障切换链路、备用 IP 地址等。有关详细信息，请参阅威胁防御 HA 设备上的设备模板操作。
- 仅在活动 防火墙管理中心 中支持设备模板操作。备用对等体不支持设备模板操作。
- 确保模板名称和设备显示名称不相同。
- 确保在设备备份或还原操作期间不创建或删除模板。
- 在设备上应用模板后，如果管理器访问从管理接口改为数据接口（反之亦然），则必须重新建立与设备的管理连接。请注意，在模板应用过程中不能更改管理器访问接口。
- 您最多可以将 250 个设备模板添加到 防火墙管理中心。
- 为通过数据接口管理的设备创建和配置的模板不能用于注册和应用到通过管理接口管理的设备。
- 设备注册和模板应用不属于变更管理工作流程。只使用经批准的数据，如访问策略、模板、模板变量、模板中声明的网络覆盖以及模板应用操作中使用的模板配置。
- 每次只支持一台设备使用序列号和访问控制策略进行设备注册。
- 在使用序列号添加设备时，不支持具有 IPv6 DHCP 可发现性的设备。
- 在将模板应用于已注册设备时，模板中的配置只会复制到目标设备。然后，您可以选择在设备上手动部署配置，或者让复制的配置留在设备上，稍后再部署。但是，如果在设备载入过程中应用模板，模板中的配置就会复制到目标设备，并按照现有行为，在设备注册后自动部署到设备上。
- 模型映射中的任何更改都会导致设备被标记为“不同步”(Out of Sync)。如果您对相应模型映射中的接口映射进行了更改，或者在上次应用模板后对配置进行了更改，请考虑将模板重新应用到设备上。

- 设备模板只支持合并的管理和诊断接口。有关详细信息，请参阅合并管理接口和诊断接口。
- 变更管理支持模板配置更新。变更管理不支持创建和应用设备模板。
- 您无法将配置更改从设备同步到模板。下面列出了一些可能需要使用模板更改设备配置的场景以及推荐的解决方案：
  - 如果您想先在一台设备上测试新的配置更改，然后再将更改传播到多台设备上，则建议您在模板中进行更改，并将模板应用到一台设备上。验证该设备上的更改，然后将模板应用到其他设备。
  - 如果要在一台设备上进行大量更改，从而导致与当前配置有明显偏差，然后将这些更改传播到其他设备，则可以选择以下选项之一：
    - 导出当前模板以获取模板副本。然后，您就可以在模板中进行所需的更改，并应用到单个设备。验证该设备上的更改，然后将模板应用到其他设备。
    - 您也可以在设备上进行所需的更改，然后从该设备创建模板。然后，您就可以在其他设备上应用和验证更改。但我们不建议这样做，因为创建的模板中不会出现变量和网络对象覆盖等模板参数。
  - 如果特定设备上的配置与模板中的配置开始出现显着差异，您也可以选择对此设备不使用模板，并从**关联设备 (Associated Devices)** 窗口中删除设备-模板关联。

VPN 连接的准则

- VPN 拓扑支持的接口包括：

拓扑类型	接口类型

基于策略的 SD-WAN	• 物理接口
	  • 非管理
	  • 接口模式必须为“路由”或“无”
	• 子接口
	• 冗余接口
	• Etherchannel 接口
	• VLAN 接口

基于路由	静态虚拟隧道接口

- 在作为VPN拓扑一部分的设备上应用模板时，必须确保模板包含拓扑中使用的所有接口的接口配置。
- 在将具有 VPN 连接的模板应用于多个设备时，请注意以下事项：

模板会按照您选择设备的顺序应用于多个设备。如果模板有 VPN 连接，则会锁定相应的 VPN 拓扑。

- 对于 SD-WAN 拓扑 VPN 连接：确保接口的 IP 地址子网与 SD-WAN 中心的 IP 地址池子网不存在冲突。
- 域：
  - 您可以在全局域或枝叶域中定义模板。但只能在枝叶域中定义 VPN 拓扑。
  - 您可以在模板中为所有域配置 VPN 连接。在模板应用过程中，只有当设备与 VPN 拓扑处于同一域时，VPN 连接才会应用到设备。

  有关详细信息，请参阅 模板和域，第 89 页。
- 变更管理：在将设备模板应用到设备之前，确保 VPN 拓扑未被变更管理故障单锁定。

不支持的配置

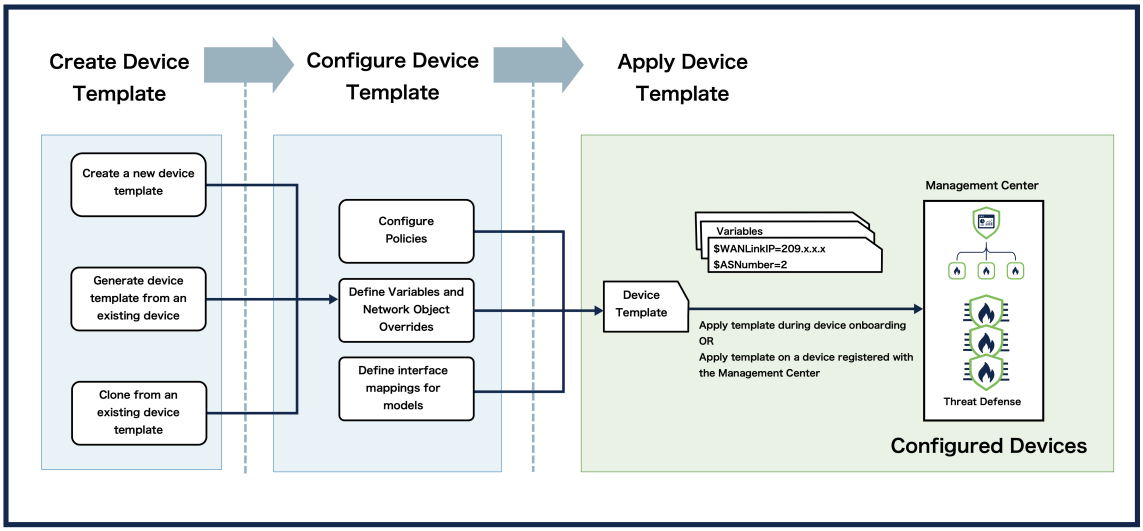
- 使用设备模板不支持以下功能和配置：
  - 多实例模式
  - 集群
  - 非融合管理接口
  - 透明模式
  - HA 故障转移配置
  - 机箱配置
  - 逻辑设备
  - 嵌套对象的变量
  - 覆盖对网络组和其他对象类型的支持

VPN 连接的限制

- 当您从属于 VPN 拓扑的设备创建模板时（**设备 > 设备管理** 更多 (⋮) **> 从设备生成模板**），VPN 配置不包含在模板中。您必须重新配置模板上的 VPN 配置。
- 当您导出具有一个或多个 VPN 连接的设备模板时（**模板设置 (Template Settings) > 常规 (General) > 常规 (General)** 面板 > **导出 (Export)**），不会导出 VPN 连接。您必须在导入的模板上重新配置 VPN 连接。
- 基于证书的身份验证：
  - 设备模板不支持设备的自动证书注册。

- 在使用带有 VPN 配置的模板载入设备时，如果 VPN 拓扑使用基于证书的身份验证，则设备的首次部署将失败。确保在设备注册后手动注册设备证书，并再次在设备上部署配置。

使用设备模板进行设备管理的工作流程



配置设备模板

添加模板，然后在模板中配置设置。

添加设备模板

您可以添加具有所需配置的新设备模板，或从现有设备生成设备模板。

创建新设备模板

您可以指定设备模板名称、说明、访问控制策略和路由模式。在创建模板后，您可以添加更多配置。执行以下程序来创建设备模板。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击**添加设备模板 (Add Device Template)**。

步骤 3 在**添加设备模板 (Add Device Template)** 窗口中，为模板输入**名称**。

步骤 4 （可选） 输入模板的**描述**。

步骤 5 从下拉列表中选择**访问控制策略 (Access Control Policy)**。

步骤 6 从下拉列表中选择**模式**。

步骤 7 点击**确定**。

从现有设备生成新设备模板

您可以从已在防火墙管理中心注册的设备中生成新的设备模板。新模板的配置与生成模板的设备相同。您可以从独立设备和 HA 设备生成新的设备模板。但是，如果从 HA 设备生成模板，新模板将不包含故障转移配置。

执行以下指定的程序，从现有设备生成新设备模板。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **更多** (⋮) 图标，然后点击**从设备生成模板 (Generate Template from Device)**。

步骤 3 在**从设备生成模板 (Generate template from device)** 窗口中，为模板输入**名称**。

步骤 4 （可选） 输入模板的**描述**。

步骤 5 从下拉列表中选择**访问控制策略 (Access Control Policy)**。

注释
此策略将被分配给生成的模板。与生成模板的设备相关联的任何其他共享策略，只有在这些策略在生成模板的域中可见时，才会分配给生成的模板。

步骤 6 点击**确定**。要查看模板创建状态，请前往**通知**，然后点击**任务**选项卡。

步骤 7 选择**设备** > **模板管理**，以查看新创建的模板。

导入设备模板

您可以将模板导入防火墙管理中心或将模板导出到您的本地系统。此功能在以下情况下非常有用：

- 从设备生成模板副本并将其导出，然后将该设备导入另一个 防火墙管理中心 或 云交付的防火墙管理中心。
- 生成模板副本并将其导出，根据需要修改以创建现有模板的变体，然后将模板导入 防火墙管理中心。
- 生成模板的副本并将其导出，然后将该模板导入到源模板在其中不可见的其他域中。

在将模板导入域时，如果导入模板的域中存在同名对象，则配置中的任何对象都会被新建或重复使用。由于域层次结构的原因，任何名称匹配但不可见的对象都会作为新对象导入，名称后缀为 _x。

如果要在使用从其他域克隆的模板的域中导入设备时出现变量名不匹配的情况，则必须在 .csv 文件中指定新的变量名才能导入设备。

执行以下程序，将设备模板从本地系统导入 防火墙管理中心。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要替换为导入模板的模板对应的 **更多** (⋮) 图标。

步骤 3 点击**导入 (Import)**，然后再次点击**导入 (Import)**。

如果要导出模板，点击**导出**，然后点击**确定**。

步骤 4 要查看导入任务的状态，请点击**通知**，然后点击**任务**选项卡。

步骤 5 选择本地系统上的模板 SFO 文件，然后点击**打开 (Open)**。导入的模板 SFO 文件可以新创建、从设备生成或从现有模板克隆。

步骤 6 要查看导入任务的状态，请点击**通知**，然后点击 **任务** 选项卡。您将看到一条通知，告知您导入或导出任务已成功完成。如果要导出模板，请点击**通知**，然后点击**任务**选项卡。在选项卡页面中，点击**下载导出数据包**将模板配置下载为 SFO 文件。

注释
或者，您也可以转到**模板管理 (Template Management)** 窗口，然后点击模板的 **编辑** (✎) 图标。然后，转至**模板设置**，点击**常规**。在**常规**磁贴中点击**导入**或**导出**以导入或导出模板。

在模板中配置设备设置

创建模板后，您可以设置设备配置，并通过编辑模板配置要在设备上应用的设置。

添加物理接口

默认情况下，设备模板将使设备能够提供以下物理接口：

- 管理接口
- 内部接口
- 外部接口

执行以下程序来创建物理接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加物理接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击**添加物理接口 (Add Physical Interface)**。

步骤 4 从下拉列表中选择一个**插槽 (Slot)** 和**端口索引 (Port Index)** 数字。

步骤 5 点击**创建接口 (Create Interface)**。

添加逻辑接口

您可以采用与在防火墙管理中心上相同的方式来创建逻辑接口，而不使用模板。执行以下程序以创建逻辑接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加逻辑接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击**添加接口 (Add Interface)**，然后从下拉列表中选择要创建的接口类型。您可以创建以下类型的接口：

- 子接口
- 以太网通道接口
- 桥接组接口
- VLAN 接口
- Virtual Tunnel Interface
- 环回接口

有关详细信息，请参阅接口概述和常规防火墙接口。

编辑接口

您可以采用与在防火墙管理中心上相同的方式来编辑接口，而不使用模板。使用模板变量设置IPv4和 IPv6 地址。设备模板支持 Firepower 1000、Secure Firewall 1200、 Firepower 2100 和 Cisco Secure Firewall 3100 Firewall Threat Defense 设备上支持的配置。执行以下程序以编辑接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中编辑物理接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击要编辑的接口的**编辑**图标。

步骤 4 在**编辑物理接口 (Edit Physical Interface)** 窗口中，您可以编辑以下任何设置：

- 常规
- PoE
- IPv4
- IPv6
- 路径监控
- 硬件配置
- 管理器访问
- 高级

注释
使用变量配置 IPv4 和 IPv6 地址。有关模板化变量的详细信息，请参阅配置模板参数。

有关编辑上述设置的详细信息，请参阅接口概述和常规防火墙接口。

配置其他设备设置

在不使用模板的情况下，以与 防火墙管理中心 相同的方式配置其他设备设置。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中配置设置的模板的 **编辑** (✎) 图标。

步骤 3 点击窗口顶部的选项卡可配置以下任何设置：

- 内联集
- 路由
- DHCP
- VPN
- 模板设置

配置模板设置

这些是特定于模板的设置，在设备上应用模板时会复制到设备上。在**模板设置 (Template Settings)** 窗口中，您可以配置以下模板设置：

- 常规
  - 常规
  - 许可
  - 应用的策略
  - 高级设置
  - 部署设置
- 模板参数
  - 变量
  - 网络对象覆盖
- 型号映射

编辑常规设置

在**常规 (General)** 磁贴中，您会看到以下字段：

- **模板名称 (Template Name)** – 模板的名称。
- **传输数据包 (Transfer Packets)** - 显示托管设备是否将数据包数据随事件一起发送到管理中心。
- **模式 (Mode)** - 显示设备管理界面的模式：已路由。
- **配置 (Configuration)** - 点击**导出 (Export)** 可将模板配置导出为 SFO 文件。点击**导入 (Import)** 以导入具有所需模板配置的 SFO 文件。
- **按数据接口管理设备 (Manage device by Data Interface)** - 切换按钮以启用或禁用使用数据接口进行设备管理。

执行以下程序编辑设备名称，即可启用或禁用数据包传输。

过程

步骤 1 点击**常规 (General)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 根据您的要求更改**模板名称**。

步骤 3 选中**转换数据包 (Transfer Packets)** 复选框以允许数据包数据随事件一起存储在 防火墙管理中心 上。

步骤 4 点击**保存**。

编辑许可证

在**许可证 (License)** 磁贴中，您可以根据模板中使用的配置查看所需的**许可证类型**。在此处选择许可证不会消耗设备上的许可证。只有在将模板应用于设备时才会使用许可证。

执行下面给出的程序，根据您的要求编辑许可证类型。

过程

步骤 1 点击**许可证 (License)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 选中或取消选中要为托管设备启用或禁用的许可证旁边的复选框。

步骤 3 点击**保存**。

编辑应用的策略

在**应用的策略 (Applied Policies)** 磁贴中，您可以查看与模板关联的访问控制策略。

对于包含链接的策略，您可以点击链接以查看策略。

执行下面给出的程序，按要求编辑政策任务。

过程

步骤 1 点击**已应用的策略 (Applied Policies)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 对于每种策略类型，请从下拉列表选择一个策略。只有现有的策略会被列出。

步骤 3 点击**保存**。

编辑高级设置

高级设置 (Advanced Settings) 磁贴显示高级配置设置，如下所述。您可以编辑任何这些设置。

表 *8:*“高级”*(Advanced)* 部分表字段

字段	说明
应用绕行	设备上“自动应用绕行”的状态。
旁路阈值	“自动应用绕行”阈值（以毫秒为单位）。

字段	说明
对象组搜索	设备上对象组搜索的状态。运行时，Firewall Threat Defense 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在防火墙管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。 **注释** 默认情况下，在 防火墙管理中心 中首次添加 Firewall Threat Defense 时会启用**对象组搜索**。
接口对象优化	设备上的接口对象优化状态。部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

执行以下程序以编辑高级设置。

过程

步骤 1 点击**高级设置 (Advanced Settings)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 您可以根据需要更改设置。有关详细信息，请参阅以下各节：

- 配置自动应用旁路
- 配置对象组搜索
- 配置接口对象优化

步骤 3 点击**保存**。

编辑部署设置

部署设置 (Deployment Settings) 磁贴显示下表所述信息。

表 *9:* 部署设置

字段	说明
连接失败时自动回滚部署	“启用”(Enabled) 或“禁用”(Disabled)。 您可以在管理连接因部署而失败时启用自动回滚；特别是如果您将数据用于防火墙管理中心访问，然后又错误地配置了数据接口。
连接监控间隔（分钟）	显示在回滚配置之前等待的时间。

部署设置包括在管理连接因部署而失败时启用部署自动回滚；特别是如果您将数据用于防火墙管理中心访问，然后又错误地配置了数据接口。您也可以使用 **configure policy rollback** 命令手动回滚配置。

执行下面给出的程序以编辑部署设置。

过程

步骤 1 点击**部署设置 (Deployment Settings)** 磁贴中的**编辑 (Edit)** 图标。

步骤 2 设置**连接监控间隔（分钟）(Connectivity Monitor Interval [in Minutes])** 以设置在回滚配置之前要等待的时间。默认值为 20 分钟。

步骤 3 如果发生回滚，请参阅以下内容以了解后续步骤。

- 如果自动回滚成功，您会看到一条成功消息，指示您执行完整部署。
- 您还可以点击**部署**并转到**高级部署**屏幕，然后点击**预览**图标以查看已回滚的配置部分（请参阅部署配置更改）。 点击**显示回滚更改 (Show Rollback Changes)** 以查看更改，然后点击**隐藏回滚更改 (Hide Rollback Changes)** 以隐藏更改。
- 在部署历史记录预览中，您可以查看回滚更改。

步骤 4 检查管理连接是否已重新建立。

在 防火墙管理中心中，在连接状态 (Connection Status) 页面上检查管理连接状态。导航到 **设备 > 设备管理** 页面，然后导航到**设备**选项卡下的**管理**区域。然后，在 **FMC 访问详细信息**屏幕中，点击**连接状态**。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要10分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障。

模板模板参数

您可以使用变量和网络对象覆盖等模板参数将配置模板化。

支持的变量

设备模板支持以下变量类型。

变量名称	说明	类型 (Type)
AS 编号	定义唯一的自治系统(AS)编号。	整数 示例：2
FQDN	定义单个完全限定域名(FQDN)。	字符串 示例：abc.example.com
IPv4 主机	定义主机的 IPv4 地址。	字符串 示例：209.165.201.8
IPv4 网络	定义 IPv4 网络地址块。	字符串 示例：209.165.200.224/27
IPv4 范围	定义 IPv4 地址的范围。	字符串 示例：209.165.200.225-209.165.200.250
IPv6 主机	定义主机的 IPv6 地址。	字符串 示例：2001:DB8::1
IPv6 网络	定义 IPv6 网络地址块。	字符串 示例：2001:DB8:0:CD30::/60
密码	定义密码字符串。	字符串 示例：E28@2OiUrhx!
路由器 ID	定义路由器的标识符。	整数 示例：21
字符串	定义自定义字符串。	字符串 示例：testvalue2

添加变量

执行以下步骤添加变量。

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**变量 (Variable)**。

步骤 3 点击**添加变量 (Add Variable)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从下拉列表中选择**变量类型 (Variable Type)**：

步骤 6 （可选） 输入**说明**。

步骤 7 点击**保存**。

支持的网络对象覆盖

支持以下网络对象。

网络对象名称	说明	类型 (Type)
网络	地址块，也称为子网。	字符串 示例： IPv4 - 209.165.200.224/27 IPv6 - 2001:DB8::/48
Host	主机的 IP 地址。	字符串 示例： IPv4 - 209.165.200.225 IPv6 - 2001:DB8:1::1
范围	IP 地址范围。	字符串 示例： IPv4 - 209.165.200.225-209.165.200.250 IPv6 - 2001:DB8::1 - 2001:DB8:FFFF:FFFF:FFFF:FFFE:FFFF:FFFF
FQDN	单个完全限定域名 (FQDN)。	字符串 示例：abc.example.com

添加网络对象覆盖

执行下面给出的程序以添加网络对象覆盖。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加网络对象覆盖的模板的 **编辑** (✎) 图标。

步骤 3 依次选择**模板设置 (Template Settings)** > **模板参数 (Template Parameters)**。

步骤 4 在**网络对象覆盖 (Network Object Overrides)** 部分中，点击**添加或删除网络对象覆盖 (Add or Remove Network Object Overrides)**。

步骤 5 在**添加或删除网络对象覆盖 (Add or Remove Network Object Overrides)** 窗口中，从**可用网络 (Available Networks)** 窗口中选择要为其创建网络对象覆盖的网络对象，然后点击 > 按钮。

步骤 6 点击**保存**。

添加模型映射

对于每个模型，您可以指定哪个模板接口与哪个模型接口对应。只要接口配置对所有映射型号都有效，就可以将模板映射到一个或多个型号。例如，如果模板包含交换机端口和 VLAN 接口，则该模板只能应用于 Firepower 1010 或 Cisco Secure Firewall 1210/1220。

执行下面给出的程序来添加型号映射。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 对于要在其中创建模型映射的模板，点击**添加模型映射 (Add Model Mapping)**。或者，您可以点击模板的 **编辑** (✎) 图标，然后依次选择**模板设置 (Template Settings)** > **模型映射 (Model Mapping)**。

步骤 3 点击**添加模型映射 (Add Model Mapping)**。

步骤 4 从下拉列表中选择**设备模型 (Device Model)**。

步骤 5 从**模型接口 (Model Interface)** 下拉列表中选择接口，将模板接口映射到设备模型接口。

注释
您可以点击**清除映射 (Clear Mapping)** 以删除已定义的模型映射。点击**重置映射 (Reset Mappings)** 进行默认接口映射，其中映射是根据接口名称的插槽和端口索引顺序进行的。

步骤 6 点击**保存**。接口映射会与设备模型和映射状态一起在**模型映射 (Model Mapping)** 窗口中列出。

注释
可能并非所有设备型号都支持模板中的某些配置。不受支持的配置（如有）不会应用于设备。设备模板应用报告会提供有关此类配置的详细信息。

无效模型映射

可能并非所有设备型号都支持模板中的某些配置。不受支持的配置（如有）不会应用于设备。修改模板配置时，有效的模型映射也可能会失效。例如，在模板上添加新接口并为其分配名称时，必须将新接口映射到设备模型上的相应接口。

以下任意原因都可能让模型映射失效：

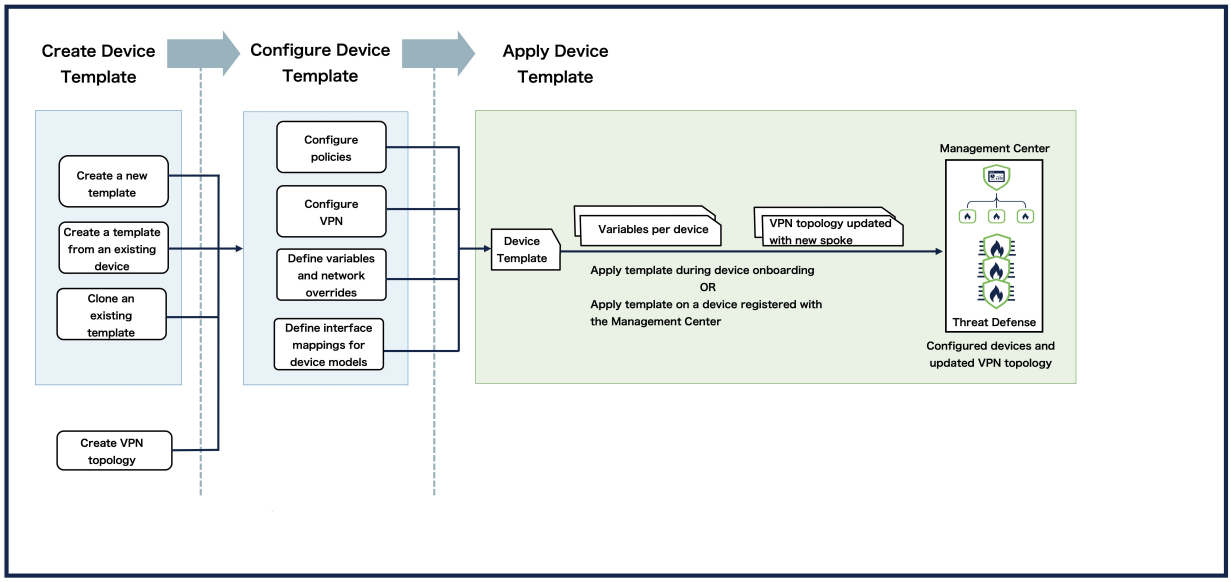
- 配置的 VRF 实例数量超过特定型号的限制。
- 接口映射到不兼容的型号、版本或接口。有关详细信息，请参阅要求和前提条件。
- 接口数量超过型号限制。
- 删除了映射的接口。
- 新添加的物理接口没有映射到兼容的模型接口。
- 未对已命名接口完成模型映射。
- 对于与其他逻辑接口（如子接口、PC 接口等）相关的接口，不进行模型映射。
- 更改某些设备型号不支持的策略或配置。例如，在接口上启用交换机端口配置。

您也可以保存带有无效模型映射的模板。但是，在设备上开始应用模板之前，您必须检查并修复模型映射。

您可以将鼠标悬停在**映射状态 (Mapping Status)** 下的**无效 (Invalid)** 上，以查看导致映射状态无效的错误。在设备上开始应用模板之前，先更正错误。

在设备模板中配置站点间 VPN 连接

具有站点间 VPN 连接的设备模板工作流程



配置 SD-WAN VPN 连接

您可以配置 SD-WAN VPN 连接，使用设备模板将分支添加到 SD-WAN 拓扑中。

开始之前

- 配置至少一个 SD-WAN 拓扑（**安全连接** > **站点间 VPN 和 SD-WAN**）。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择 SD-WAN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。此列表包含设备模板上配置的所有接口。

b) **使用 VPN 接口的 IP 地址 (Use IP Address from the VPN Interface)** - 此下拉列表使用 IP 地址变量自动填充。对于 IPv6 地址，请从下拉列表中选择 IPv6 地址。

c) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

d) **身份类型 (Identity Type)** - 密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以创建新的密钥 ID 变量。

e) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 在设备模板中为分支配置路由策略。
2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

配置基于路由的站点间 VPN 连接

您可以配置基于路由的站点间 VPN 连接，使用设备模板将分支添加到基于路由的站点间 VPN 拓扑中。

开始之前

- 配置至少一个基于路由的站点间 VPN 拓扑（**安全连接** > **站点间 VPN 和 SD-WAN**）。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择基于路由的站点间 VPN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 在**虚拟隧道接口 (VTI) (Virtual Tunnel Interface [VTI])** 下拉列表中选择一个 VTI 接口，或点击 (+) 创建一个新的 VTI。

VTI 是用于建立基于路由的 VPN 隧道的虚拟接口。您必须为 VTI 配置路由策略以设置 VPN 隧道。此列表包含设备模板上配置的所有 VTI。有关创建 VTI 的详细信息，请参阅添加 VTI 接口，第 1470 页。

b) 选中**使用公共 IP 地址 (Use Public IP Address)** 复选框以覆盖隧道源 IP 地址，并为 VTI 配置公共 IP 地址变量。点击 (+) 以创建一个新的公共 IP 地址变量。

此 IP 地址是 VPN 隧道的源 IP 地址。默认情况下，这是 VPN 接口的 IP 地址。但是，如果设备位于 NAT 之后，则 VPN 接口具有专用地址，但应配置 NAT 后的公共 IP 地址。

c) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

d) **身份类型 (Identity Type)**：密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以创建新的密钥 ID 变量。

e) （可选）选中**启用辅助 VPN 隧道 (Enable Secondary VPN Tunnel)** 复选框以配置辅助 VPN 隧道的参数。

f) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 在设备模板中为分支配置路由策略。
2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

配置基于策略的站点间 VPN 连接

您可以配置基于策略的站点间 VPN 连接，使用设备模板将分支添加到基于策略的站点间 VPN 拓扑中。

开始之前

- 配置至少一个基于策略的站点间 VPN (**安全连接** > **站点间 VPN 和 SD-WAN**)。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择基于策略的站点间 VPN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。

此列表包含设备模板上配置的所有接口。

执行以下操作之一来配置 VPN 接口的 IP 地址：

- 点击**使用来自 VPN 接口的 IP 地址 (Use IP Address from the VPN Interface)** 单选按钮以使用 VPN 接口的 IP 地址。

  此 IP 地址会自动填充。对于 IPv6 地址，请从下拉列表中选择 IPv6 地址。

- 点击**使用公共 IP 地址 (Use Public IP Address)** 单选按钮，为 VPN 接口配置一个公共 IP 地址。

  从下拉列表中选择 IP 地址变量，或点击 (+) 以添加 IP 地址变量。

b) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

c) **身份类型 (Identity Type)**：密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以添加新的密钥 ID 变量。

d) **受保护的网络 (Protected Networks)**：点击 (+)，为 VPN 连接配置受保护的网络。

执行以下操作之一：

- 选择受保护的网络，然后点击**确定**。
- 点击**添加**以配置网络对象，然后点击**保存**。

  创建受保护的网络对象时，请注意以下事项：

  - 点击**主机 (Host)** 或**网络 (Network)** 单选按钮。
  - 请勿选中**允许覆盖 (Allow Overrides)** 复选框。

e) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 请注意，在将模板应用于设备之前，要为受保护的网络配置设备特定的值，可在**模板设置 (Template Settings) > 模板参数 (Template Parameters) > 添加网络对象覆盖 (Add Network Objects Overrides)** 中添加这些对象。

2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

使用设备模板注册设备并将其添加到基于路由的 VPN 拓扑中

本节介绍使用设备模板注册设备并将其添加到基于路由的 VPN 拓扑。

准备工作

确保拥有基于路由的 VPN 拓扑。

步骤	任务	GUI 路径	更多信息
1	创建设备模板。	设备 > 模板管理，然后点击添加设备模板	创建新设备模板，第 95 页
2	在模板中配置接口。	设备 > 模板管理，然后点击接口	编辑接口，第 98 页
3	在模板中配置基于路由的 VPN 连接。	设备 > 模板管理，然后点击 VPN > 添加 VPN 连接	配置基于路由的站点间 VPN 连接，第 109 页
4	在模板中配置路由策略。	设备 > 模板管理，然后点击路由	—
5	为模板中的设备模型添加模型映射。	设备 > 模板管理，然后点击模板设置 > 型号映射	添加模型映射，第 106 页
6	使用设备模板注册设备。	设备 > 设备管理，然后点击添加 > 设备（向导）	使用注册密钥添加设备-设备模板，第 36 页
7	在 VPN 拓扑的中心上部署配置。	Deploy	—

在双 ISP 部署中为 SD-WAN 拓扑添加设备

本节介绍在双 ISP 部署中使用设备模板将设备添加到 SD-WAN 拓扑的说明。

准备工作

确保有两个使用相同中心的 SD-WAN VPN 拓扑。有关配置 SD-WAN 拓扑的详细信息，请参阅使用 SD-WAN 向导配置 SD-WAN 拓扑，第 1512 页。

步骤	任务	GUI 路径	更多信息
1	创建设备模板。	**设备 > 模板管理**	创建新设备模板，第 95 页
2	在模板中添加物理接口。 默认情况下，一个模板只有一个外部接口。重命名外部接口，例如，ISP1, ISP2。	**设备 > 模板管理**，然后点击**接口 > 添加物理接口**	添加物理接口，第 97 页
3	使用 ISP1 接口配置 SD-WAN VPN 连接。	**设备 > 模板管理**，然后点击 **VPN > 添加 VPN 连接**	配置 SD-WAN VPN 连接，第 108 页
4	使用 ISP2 接口配置 SD-WAN VPN 连接。		
5	从 ISP1 和 ISP2 接口添加静态路由到 SD-WAN 中心网络。	**设备 > 模板管理**，然后点击**路由 > 静态路由**	-
6	将 ISP1 和 ISP2 接口添加到 ECMP 区域。	**设备 > 模板管理**，然后点击**路由 > ECMP**	-
7	配置网络对象覆盖。	**设备 > 模板管理**，然后点击**模板设置 > 模板参数 > 添加网络对象覆盖**	添加网络对象覆盖，第 105 页
8	将模板接口映射到设备模型接口（模型映射）。	**设备 > 模板管理**，然后点击**模板设置 > 型号映射**	添加模型映射，第 106 页
9	将模板应用到设备。	**设备 > 模板管理**	应用模板，第 116 页
10	在设备上部署配置。	**Deploy**	—
11	在 SD-WAN 拓扑的中心部署配置。	**Deploy**	—

有关使用 SD-WAN 向导的双 ISP 部署的详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例，第 1517 页。

为使用数据接口管理的 Firewall Threat Defense 设备配置模板

要配置想应用于使用 防火墙管理中心 连接的数据接口管理的 Firewall Threat Defense 设备的模板，请确保设备的连接参数与模板匹配。这可确保威胁防御设备在应用模板后不会失去与 防火墙管理中

心 的连接。为使用数据接口管理的 Firewall Threat Defense 设备配置的模板不能应用于非数据接口管理的设备。

以下是连接参数列表：

- 用于管理 Firewall Threat Defense 设备的数据接口。例如，**Ethernet1/1**。
- 接口的名称。例如，**outside**。
- 在数据接口上配置的 IP 地址。例如，DHCP 或静态 IP。
- 为数据接口配置的路由。这可以是在用于 Firewall Threat Defense 设备与 防火墙管理中心之间的连接的数据接口上定义的默认路由或特定路由。
- 数据接口上的 DDNS 主机名配置。

如果模板上的连接参数与设备上的参数不匹配，则为确保模板成功应用于设备而进行的模板验证检查将失败。这样，模板就不会被应用到设备上。模板验证检查不会强制要求某些参数（如 IP 地址或 DDNS 主机名）完全匹配。但是，请确保配置此类参数，以便在部署后保持 Firewall Threat Defense 设备与 防火墙管理中心 之间的连接。

以下是为确保使用数据接口管理 Firewall Threat Defense 设备所需的配置的正确性而进行的模板验证检查列表：

- 您不能将管理器访问设备配置为管理接口的模板应用到管理器访问设备配置为数据接口的设备上。
- 您不能将管理器访问设备配置为数据接口的模板应用到管理器访问设备配置为管理接口的设备上。
- 您不能将管理器访问设备配置为单 WAN 数据接口的模板应用到管理器访问设备配置为双 WAN 数据接口的设备上。
- 如果任何连接参数不匹配，则不能将管理器访问设备配置为数据接口的模板应用到管理器访问设备配置为数据接口的设备上。

执行下面指定的程序，配置模板以使用数据接口来管理 Firewall Threat Defense 设备。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要配置的模板的 **编辑** (✎) 图标，以使用数据接口来管理 Firewall Threat Defense 设备。

步骤 3 点击**模板设置 (Template Settings)** 选项卡。

步骤 4 在**常规 (General)** 磁贴中，切换**按数据接口管理设备 (Manage device by Data Interface)** 按钮。

步骤 5 您将看到一个弹出窗口，要求您选择一个数据接口供管理器访问。点击**确定**。

步骤 6 点击**接口 (Interfaces)** 选项卡。

步骤 7 点击要用于管理器访问的数据界面的**编辑 (Edit)** 图标。第一个数据接口 - Ethernet1/1（外部接口）是最常用于管理器访问的数据接口。

步骤 8 在**编辑物理接口 (Edit Physical Interface)** 窗口中，点击**管理器访问 (Manager Access)** 选项卡。

步骤 9 选中**启用管理访问 (Enable management access)** 复选框。

步骤 10 点击**确定**。您将看到您选择用于管理器访问的接口已标记为**管理器访问 (Manager Access)**。

步骤 11 点击 **DHCP** 选项卡。

步骤 12 点击 **DDNS 更新方法 (DDNS Update Methods)** 选项卡。

步骤 13 点击 **+添加 (+Add)** 以添加 DDNS 更新方法。

步骤 14 在**添加 DDNS 更新方法 (Add DDNS Update Method)** 窗口中，输入**方法名称 (Method Name)**，然后选择**仅 FMC (FMC only)**。

步骤 15 根据您的要求设置**更新间隔 (Update Interval)**。

步骤 16 点击**确定**。您将在 **DDNS 更新方法 (DDNS Update Methods)** 表中看到您创建的方法。

步骤 17 点击 **DDNS 接口设置 (DDNS Interface Settings)** 选项卡。

步骤 18 点击 **+ 添加 (+Add)** 以添加动态 DNS 配置。

步骤 19 在**添加动态 DNS (Add Dynamic DNS)** 配置窗口中，选择以下字段的值：

- **接口 (Interface)** - 选择为管理器访问启用的接口
- **方法名称 (Method Name)** - 选择您创建的方法。
- **主机名 (Host Name)** - 选择主机名变量。

不要编辑此窗口中的其他字段。

步骤 20 点击**确定**。使用您创建的条目填充 **DDNS 接口设置 (DDNS Interface Settings)** 表。

步骤 21 要配置模型映射以确保模板中为管理器访问设置的数据接口与设备上为管理器访问选择的数据接口匹配，请点击**模板设置 (Template Settings)** 选项卡，然后点击**模型映射 (Model Mapping)**。

步骤 22 点击**添加模型映射 (Add Model Mapping)**。

步骤 23 从下拉列表中选择**设备模型 (Device Model)**。

步骤 24 通过从**模型接口 (Model Interface)** 下拉列表中选择接口，将模板中为管理器访问设置的日期接口映射到设备上的相应数据接口。

步骤 25 点击**保存**。接口映射会与设备模型和映射状态一起在**模型映射 (Model Mapping)** 窗口中列出。现在，您可以在使用数据接口管理的设备上应用模板。

将模板与设备一起使用

在向 防火墙管理中心 注册设备时，您可以选择兼容的模板进行初始配置。您也可以将模板应用于已向 防火墙管理中心 注册的设备。

使用设备模板向管理中心添加设备

您可以使用设备模板通过以下选项将设备添加到 防火墙管理中心：

- 使用注册密钥添加设备-设备模板 ， 第 36 页
- 使用序列号来添加设备（零接触调配）- 设备模板 ， 第 46 页



注释 任何与模板配置相关的变更管理票据都必须获得批准，才能将相应的变更纳入模板应用工作流程。在模板应用过程中，只使用已批准的模板配置。

将模板应用于现有设备

您可以将模板应用或重新应用模板到现有设备。

应用模板

您可以将模板应用于已向 防火墙管理中心 注册的设备。在设备上应用模板会清除现有配置并应用模板中的配置。但是，Firewall Threat Defense HA 故障转移配置不会被清除。

应用模板仅会更改 防火墙管理中心 上的设备配置。您必须将这些设备配置更改显式部署到 Firewall Threat Defense 设备上。已应用的配置更改无法回滚。但是，您也可以使用另一个模板来进行所需的配置。



注释 任何与模板配置相关的变更管理票据都必须获得批准，才能将相应的变更纳入模板应用工作流程。在模板应用过程中，只使用已批准的模板配置。

执行以下程序可在现有设备上应用模板。

过程

步骤 1 要从**模板管理**窗口应用模板，请选择**设备** > **模板管理**。

a) 点击要应用的模板旁边的 **更多** (⋮) 图标，然后点击**应用 (Apply)**。
b) 从**设备 (Device)** 下拉列表中选择要应用模板的**设备**。
c) 点击**确认 (Confirm)** 以在设备上启动模板应用。

步骤 2 （可选） 要从**关联设备 (Associated Devices)** 窗口应用模板，请依次选择**设备 (Devices)** > **模板管理 (Template Management)**。

a) 点击您要应用于设备的模板的 **编辑** (✎) 图标。
b) 点击**关联设备 (Associated Devices)**。
c) 在**关联设备 (Associated Devices)** 窗口中，点击**应用模板 (Apply Template)**。
d) 从**设备 (Device)** 下拉列表中选择要应用模板的**设备**。
e) 输入**变量**和**网络对象覆盖**字段的值。

f) 点击**应用 (Apply)** 以在设备上启动模板应用。

重新应用模板

如果对设备或模板进行了任何更改，导致配置不同步，则可以重新应用模板，使配置与模板同步。

执行以下程序在设备上重新应用模板。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击您要重新应用到设备的模板的 **编辑** (✎) 图标。

步骤 3 点击**关联设备 (Associated Devices)**。

步骤 4 在**关联的设备 (Associated Devices)** 窗口中，点击要重新**应用模板 (Reapply Template)** 的设备旁边的重新应用模板。

注释
如果要在模板中的所有关联设备上重新应用模板，请点击**批量重新应用 (Bulk Reapply)**，然后点击**确认 (Confirm)**。

步骤 5 在**重新应用模板 (Reapply template)** 窗口中，您可以重复使用自动填充的**变量 (Variables)** 和**网络对象覆盖 (Network object overrides)** 值或输入新值。

步骤 6 点击**确认 (Confirm)** 以在设备上启动模板的重新应用。

监控设备模板

您可以通过查看**关联设备 (Associated Devices)** 窗口中列出的设备并查看**模板应用报告 (Template Apply Report)** 来监控和验证模板的应用情况。

查看关联设备

与模板关联的设备列在**关联设备 (Associated Devices)** 窗口中。每个设备行将显示**设备名称**、**同步状态**、**模板应用状态**和**应用日期**。您还可以点击**重新应用模板 (Reapply template)** 以重新应用模板。点击**变量摘要 (Variable Summary)** 图标以显示模板中的变量摘要，然后点击 **报告** (📋) 图标以下载设备模板应用报告。点击 **删除** (🗑) 图标从设备中删除模板。

如果要从**关联设备 (Associated Devices)** 窗口在设备上应用模板，请点击**应用模板 (Apply Template)**。如果要在模板中的所有关联设备上重新应用模板，请点击**批量重新应用 (Bulk Reapply)** ，然后点击**确认 (Confirm)**。

同步状态 (Sync Status) 可以为**同步 (Sync)** 或**不同步 (Out-of-Sync)**。如果状态显示为**同步 (Sync)**，则表示模板和设备配置相同或正在同步。如果状态显示为**不同步 (Out-of-Sync)**，则表示自上次应用模板以来，设备上或模板中的配置发生了更改。

设备与模板的关联不会因以下情况而改变：

- 设备上的待处理配置更改 - 如果设备上存在必须应用的待处理配置更改，则**同步状态**不会发生变化。
- 在设备上部署待处理配置更改 - 在设备上部署待处理配置更改后，**同步状态**不会发生变化。

下表显示了可能出现的**同步**和**不同步**场景。

在设备上应用模板后修改的设备配置	在设备上应用模板后修改的模板配置	关联状态
否	否	同步
支持	否	不同步
否	支持	不同步
支持	支持	不同步

生成模板应用报告

模板应用报告 PDF 会在模板应用任务完成后生成。无论在设备上应用模板成功还是失败，都会生成该报告。要访问该报告的链接，请点击**通知**，然后点击**任务**选项卡。

模板应用报告包含以下详细信息：

- 模板名称
- 设备型号名称
- 从其中应用模板的域
- 开始和结束时间
- 设备上的模板应用状态
- 接口映射信息
- 变量值

由于设备型号或版本不兼容，模板上的某些配置可能无法应用于设备。报告还包含有关此类配置的详细信息。报告还包含应用模板失败时遇到的任何错误。由于以下原因，在设备上应用模板可能会失败：

- 所使用的设备型号不存在型号映射。
- 变量和网络对象覆盖使用的值不符合路由策略或接口配置规则。例如，两个 IPv4 地址接口变量使用了相同的 IPv4 地址。

- 由于正在执行其他任务（如应用或修改模板），设备或模板被锁定。

审核日志

与设备模板应用、配置更新、设备模板创建和删除相关的日志记录在审计日志下。设备模板审核日志会在任务开始和结束时添加到日志中，以便在设备上应用模板。

系统还会生成一个审核差异文件，让您能够查看在设备上应用模板期间所做的配置更改。执行下面给出的程序以查看差异文件。

过程

步骤 1 选择**事件和日志** > **分析** > **审核日志** 。

步骤 2 设备模板日志记录在子系统 **设备** > **模板管理** 下。点击**差异 (diff)** 图标可打开一个新窗口，其中显示在设备上应用模板期间完成的配置更改。

设备模板故障排除

初步故障排除

要初步排除故障，我们建议查看模板应用报告中的信息，以及遇到错误时 防火墙管理中心 UI 上显示的通知。防火墙管理中心 日志文件还包含详细的调试和故障排除信息。

请按照以下步骤进行初始故障排除。

1. 检查**模板应用报告**中提到的错误。有关详细信息，请参阅模板、应用报告。
2. 查看变量值并检查重叠和不兼容情况。
3. 检查模型映射，确保是否存在正确的模型映射。相应地删除或添加映射。
4. 请参阅 防火墙管理中心 审核日志，以查找并解决任何其他问题。

请考虑以下错误场景。在设备模板中，内部接口使用静态 IPv4 变量 - *$insideIPv4* 来进行配置。

BGP IPv4 地址与 IPv4 BGP 邻居一起配置。

为 BGP 邻居和接口配置一个重叠的 IPv4 地址。

由于上述问题，设备模板的应用会失败并显示错误。

要排除此错误，请从 UI 上显示的通知中确定错误。

```
IP Address 192.168.10.1 same as ip address of interface - 'inside'(Ethernet1/1)
```

有关详细信息，请查看**模板应用报告**。

输入正确的变量值并再次应用模板，以确保在设备上成功应用模板。

设备注册故障排除

- 问题：管理员密码不正确或注册时未提供密码

  场景：如果设备上未设置管理员密码，并且您在注册时未提供管理员密码，则 Firewall Threat Defense 设备调配将失败。在这种情况下，系统会显示调配错误和**输入密码**链接。

  解决方法：点击**输入密码**，输入新密码，然后点击**保存**。点击**确认并继续 (Confirm and Proceed)**以再次触发载入。

- 如果设备上已经设置了管理员密码，而您在注册时又提供了另一个管理员密码，则设备调配将失败。

- 问题：防火墙管理中心 中的设备注册失败

  解决方法：按照现有的设备注册故障排除步骤操作。有关详细信息，请参阅 Firepower 设备注册配置、验证和故障排除。

- 问题：在 防火墙管理中心 中的批量注册请求失败

  场景： 批量注册请求可能会在几种情况下失败：

  - 您没有执行模板相关操作所需的权限
  - 从请求域看不到模板
  - 提供的 CSV 文件无效

  解决方法：您可以在 VMS 共享和 USM 共享日志文件中看到这些错误的日志。修复错误并重新启动注册。

- 问题：由于某些一般错误（例如与设备的通信失败），Security Cloud Control 中的设备调配失败

  解决方法：点击调配错误中的重试，以便再次触发 Security Cloud Control 中的自行激活。您还可以参阅 Security Cloud Control 工作流程，以了解有关错误和故障排除的更多信息。

思科安全云集成故障排除

问题：思科安全云集成不成功

解决方法：执行思科安全云集成故障排除步骤。有关详细信息，请参阅思科安全云集成。

设备模板配置问题故障排除

问题：设备模板配置错误，导致注册后部署失败

解决方法：请按照以下步骤进行初始故障排除。

1. 检查模板应用报告中提到的错误。
2. 查看变量值并检查重叠和不兼容情况。
3. 检查模型映射，确保是否存在正确的模型映射。相应地删除或添加映射。
4. 请参阅 防火墙管理中心 审核日志，以查找并解决任何其他问题。

Security Cloud Control 问题故障排除

- 问题：已申领序列号的设备

  解决方法：验证序列号并重新启动载入。

- 问题：Security Cloud Control 未能申领设备。

  解决方法：在 Security Cloud Control **安全设备 (Security Devices)** 窗口中选择设备，以了解有关错误的更多详细信息。您可以在 VMS 共享和 USM 共享日志文件中看到与设备申领问题相关的日志。点击**重试 (Retry)** 以再次启动注册。

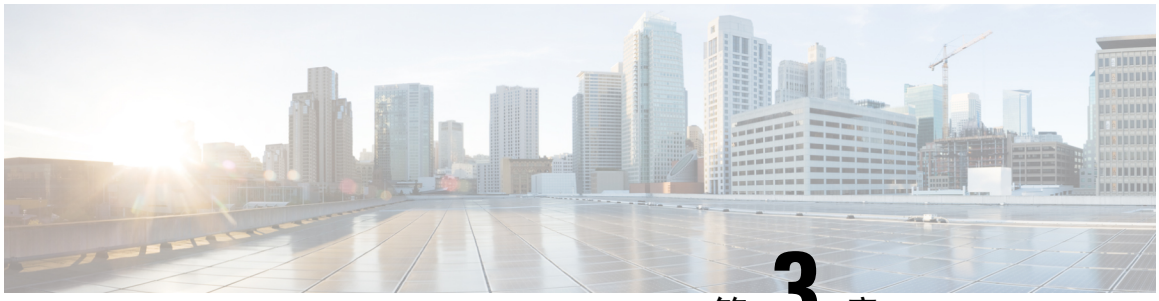
- 问题：防火墙管理中心 和 Security Cloud Control 之间的通信失败

  场景：防火墙管理中心 和 Security Cloud Control 之间的通信故障可能会导致零接触调配 (ZTP) 设备注册请求失败。

  解决方法：刷新 ZTP 设备状态，重新尝试注册 ZTP，然后再删除 ZTP 设备。您可以在身份验证后台守护程序日志中查看有关 防火墙管理中心 和 Security Cloud Control 之间通信失败的日志。对于与 ZTP 相关的操作故障，您可以查看 VMS 共享和 USM 共享日志文件中的日志。

使用设备模板进行设备管理的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
使用设备模板进行设备管理	7.6.0	7.4.1	通过设备模板，可以部署具有预配置初始设备配置的多个分支设备。您可以使用设备模板对多台设备执行批量零接触调配，对具有不同接口配置的多台设备应用 day 2 配置更改，以及从现有设备克隆配置参数。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备（向导）(Device [Wizard])** • **设备 (Devices)** > **模板管理 (Template Management)** > **添加设备模板 (Add Device Template)** • **设备 (Devices)** > **模板管理 (Template Management)** > **添加模型映射 (Add Model Mapping)** • **设备 (Devices)** > **模板管理 (Template Management)** > **编辑模板 (Edit a template)** > **模板设置 (Template Settings)** • **集成 (Integration)** > **思科安全云 (Cisco Security Cloud)**



第 3 章

透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式下的工作方式。

注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。有关仅 IPS 接口的详细信息，请参阅内联集和被动接口，第 833 页。内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与本章介绍的透明防火墙模式或防火墙类型接口无关。

小心

- 使用 FTD CLI 命令设置“防火墙模式”。

- 关于防火墙模式，第 123 页
- 默认设置，第 131 页
- 防火墙模式准则，第 131 页
- 设置防火墙模式，第 132 页

关于防火墙模式

Firewall 威胁防御面向普通防火墙接口支持两种防火墙模式：路由防火墙模式和透明防火墙模式。

关于路由防火墙模式

在路由模式中，Firewall 威胁防御设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。

通过集成路由和桥接，您可以使用您用来对网络的多个接口进行分组的“网桥组”，Firewall 威胁防御设备使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。Firewall 威胁防御设备在 BVI 与正规的路由接口之间进行路由。如果您不需要集群或 EtherChannel 成员接口，则可以考虑使用路由模式而非透明模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。但是，与其他防火墙一样，接口之间的访问控制是受控制的，需要进行通常的所有防火墙检查。

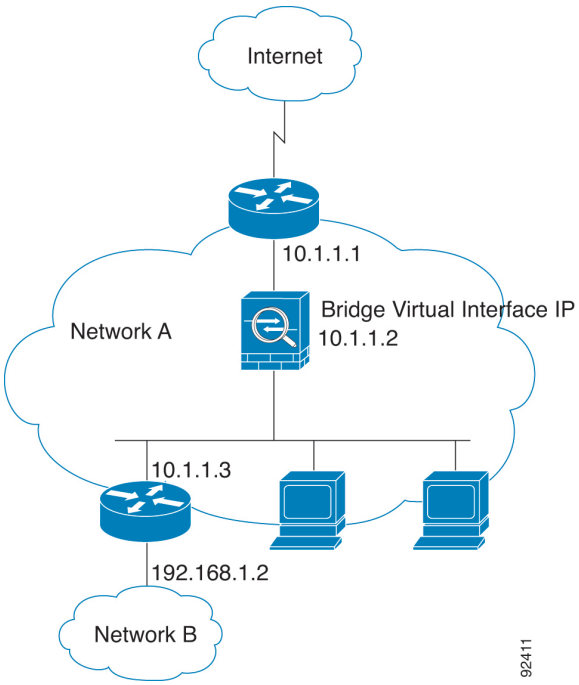
第 2 层连接使用您用来对网络的内部和外部接口进行分组的“网桥组”来实现，Firewall 威胁防御设备使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。多个网络可以有多个网桥组。在透明模式下，这些网桥组无法相互通信。

在网络中使用透明防火墙

Firewall 威胁防御设备 在其接口之间连接同一个网络。由于防火墙不是路由跃点，因此可以将透明防火墙轻松引入到现有网络中。

下图显示典型的透明防火墙网络，其中的外部设备与内部设备在同一个子网上。内部路由器和主机显示为与外部路由器直接连接。

图 *30:* 透明防火墙网络



允许路由模式功能通过流量

对于透明防火墙不直接支持的功能，您可以允许流量通过，以便上游和下游路由器能够支持这些功能。例如，通过使用访问规则，可以允许 DHCP 流量（而不是不受支持的 DHCP 中继功能）或组播流量（例如 IP/TV 产生的流量）。还可以通过透明防火墙建立路由协议邻接；可以根据扩访问规则允许 OSPF、RIP、EIGRP 或 BGP 流量通过。同样，诸如 HSRP 或 VRRP 之类的协议也可以通过 Firewall 威胁防御设备。

关于网桥组

网桥组是指 Firewall 威胁防御设备 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。与任何其他防火墙接口一样，接口之间的访问控制将受控制，并将部署所有普通防火墙检查。

网桥虚拟接口 (BVI)

每个网桥组包括一个网桥虚拟接口 (BVI)。Firewall 威胁防御设备使用该 BVI IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与网桥组成员接口位于同一子网。BVI 不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。

在透明模式下：只有网桥组成员接口会被命名并可以与基于接口的功能配合使用。

在路由模式下：BVI 充当网桥组和其他路由接口之间的网关。要在网桥组/路由接口之间进行路由，必须为 BVI 命名。对于一些基于接口的功能，您可以单独使用 BVI：

- DHCPv4 服务器 - 只有 BVI 支持 DHCPv4 服务器配置。
- 静态路由 - 可以为 BVI 配置静态路由；不能为成员接口配置静态路由。
- 系统日志服务器和其他源自 Firewall 威胁防御设备的流量 - 当指定系统日志服务器（或 SNMP 服务器，或流量源自 Firewall 威胁防御设备的其他服务）时，可以指定 BVI 或成员接口。

如果您在路由模式下没有命名 BVI，则 Firewall 威胁防御设备不会路由网桥组流量。此配置将为网桥组复制透明防火墙模式。如果您不需要集群或EtherChannel成员接口，则可以考虑改用路由模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

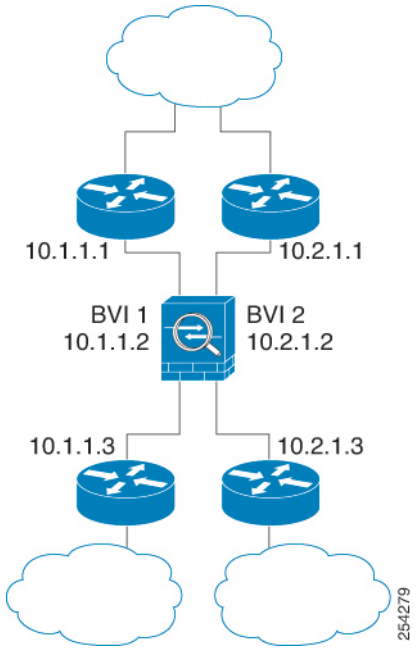
透明防火墙模式下的网桥组

网桥组的流量相互分离；流量不会路由至 Firewall 威胁防御设备 中的另一个网桥组，并且流量必须退出Firewall威胁防御设备 后才能通过外部路由器路由回Firewall威胁防御设备 中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或 AAA 服务器的配置。

可以在每个网桥组中包含多个接口。有关支持的网桥组和接口的确切数量，请参阅防火墙模式准则，第 131 页。如果您在每个网桥组中使用的接口数超过 2 个，则可以控制同一网络上多个网段之间的通信，而不只是在内部和外部之间的通信。例如，如果您有三个不需要彼此通信的内部网段，则可以将每个网段设置在单独的接口上，并且仅允许它们与外部接口通信。或者，您可以自定义接口之间的访问规则，以根据需要允许任意程度的访问。

下图显示连接到 Firewall 威胁防御设备且具有两个网桥组的两个网络。

图 *31:* 具有两个网桥组的透明防火墙网络

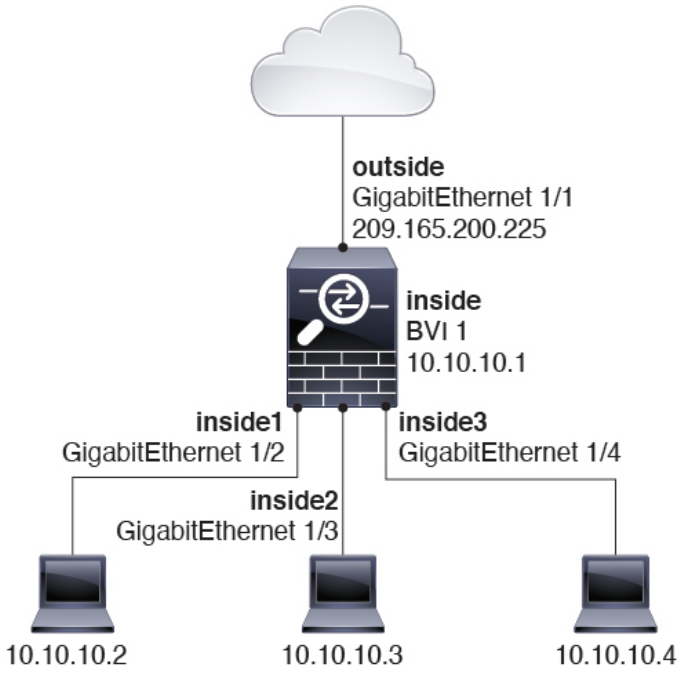


路由防火墙模式下的网桥组

网桥组流量可以路由到其他网桥组或路由接口。您可以选择通过不为网桥组的 BVI 接口分配名称来隔离网桥组流量。如果命名了 BVI，则 BVI 将像其他任何普通接口一样参与路由。

路由模式下网桥组的一种用途是在 Firewall 威胁防御上而非外部交换机上使用额外接口。例如，某些设备的默认配置包括一个外部接口作为普通接口，还包括分配给内部网桥组的其他接口。由于此网桥组的目的是替换外部交换机，因此您需要配置访问策略，以便所有网桥组接口都可以自由通信。

图 *32:* 具有内部网桥组和外部路由接口的路由防火墙网络



允许第 3 层流量

- 单播 IPv4 和 IPv6 流量需要允许一个访问规则通过网桥组。
- 允许 ARP 双向通过网桥组，而无需访问规则。ARP 流量可通过 ARP 检测进行控制。
- IPv6 邻居发现和路由器请求数据包可以使用访问规则传递。
- 可使用访问规则允许广播和组播流量通过。

允许的 MAC 地址

如果得到您的访问策略的允许，将允许以下目标 MAC 地址通过网桥组（请参阅允许第 3 层流量，第 127 页）。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。

默认情况下，BPDU 也会被转发以进行高级检测，这对此类型数据包并无必要，并且有可能导致例如由于检测重启而被阻止的问题发生。我们建议您始终免除对 BPDU 进行高级检测。为此，请使用 FlexConfig 配置信任 BPDU 的 EtherType ACL，并在每个成员接口上免除对其进行高级检测。请参阅 FlexConfig 策略。

FlexConfig 对象应部署以下命令，在其中将 <if-name> 替换为接口名称。添加所需数量的 access-group 命令以涵盖设备上的每个网桥组成员接口。您还可以为 ACL 选择其他名称。

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

MAC 地址与路由查找

对于网桥组中的流量，通过执行目标 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下情况是必要的：

- 源自 Firewall 威胁防御设备的流量 - 例如，在 Firewall 威胁防御设备上为发往系统日志服务器所在的远程网络的流量添加一个默认/静态路由。
- 在透明防火墙模式下启用的 SSL 策略 —
  - TLS 1.3 流量会通过 Firewall 威胁防御设备 设备。
  - Firewall 威胁防御设备 充当 TCP 代理。它会终止客户端 TCP 连接，并启动单独的服务器端连接。Firewall 威胁防御设备 TCP 堆栈拥有会话状态。
  - 对于空闲的代理会话，Firewall 威胁防御设备 会生成 TCP ACK 保持连接探测以保留连接状态。这些不是直通数据包 — 防火墙生成它们并根据 TLS 传输连接的状态将它们发送到客户端或服务器。
  - 由于 Firewall 威胁防御设备 发起这些保持连接，因此即使在透明模式下也必须执行邻接表查找（下一跳或出口 MAC 解析）。
  - 如果对其中一个代理生成的数据包的邻接查找失败，则 Firewall 威胁防御设备 会记录系统日志 110003。

    要阻止这些系统日志消息，请在 Firewall 威胁防御设备 上为传输连接终端（客户端和服务器 IP 地址）配置路由。正确的路由有助于成功查找保持连接数据包的邻接关系。

    如果 Firewall 威胁防御设备 成功发送 TCP 保持连接并收到应答，它会让传输连接保持活动状态。如果设备无法发送保持连接，或没有收到回复，它会在大约 240 秒后删除中转连接。
- IP 语音 (VoIP) 和 TFTP 流量，并且终端至少在一跳之外 - 在 Firewall 威胁防御设备上为发往成功建立辅助连接的远程终端的流量添加静态路由。Firewall 威胁防御设备会在访问控制策略中创建一个临时“针孔”以允许辅助连接；由于连接可能会使用一组不同于主连接的 IP 地址，所以 Firewall 威胁防御设备需要执行路由查找以便在正确的接口上安装针孔。

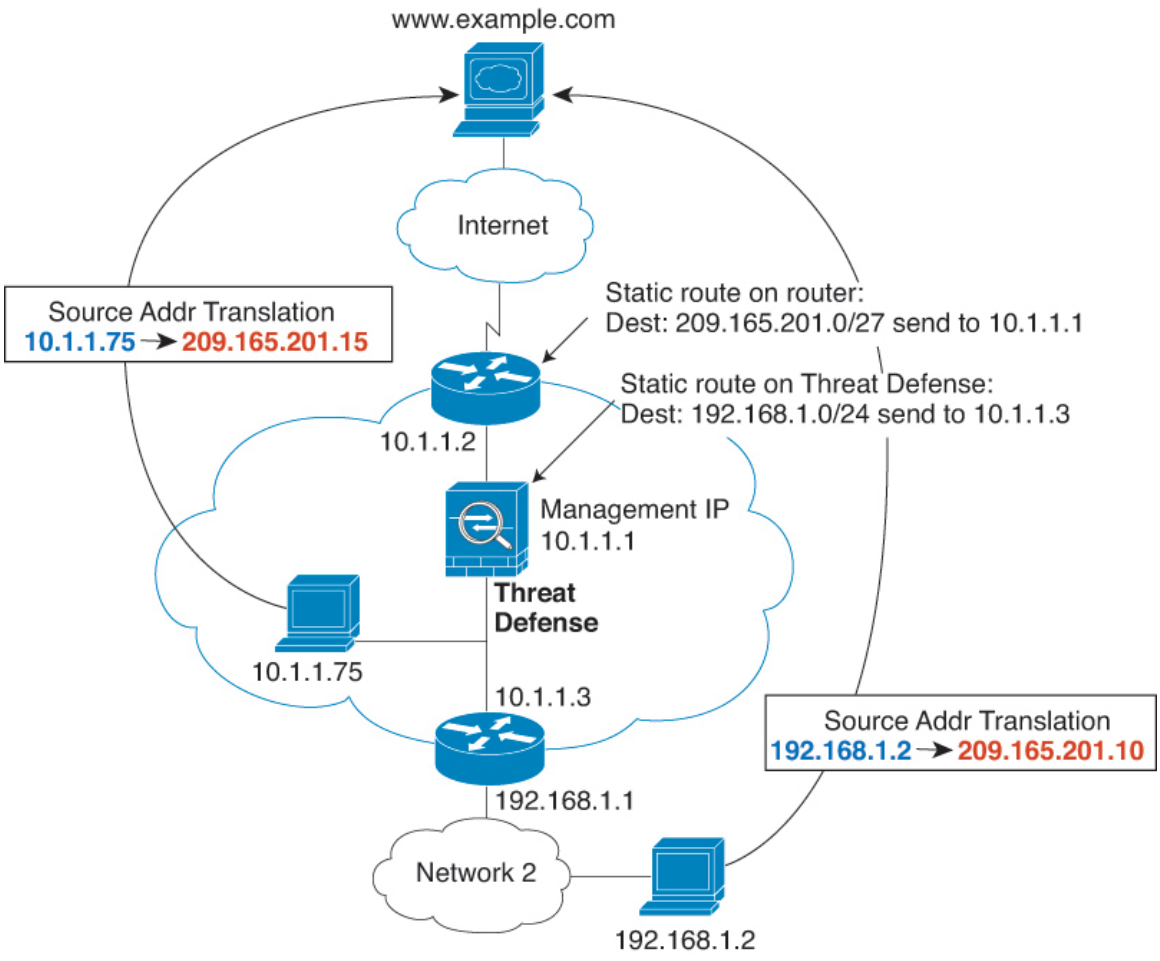
  受影响的应用包括：
  - H.323

- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- Firewall 威胁防御设备对其执行 NAT 的至少一跳开外的流量 - 在 Firewall 威胁防御设备上为发往远程网络的流量配置静态路由。您还需要在上游路由器上为要发送到 Firewall 威胁防御设备的已映射地址的流量配置静态路由。

  此路由要求也适用 NAT 的 VoIP 和 DNS 的嵌入式 IP 地址，这些嵌入式 IP 地址都必须至少在一跳之外。Firewall 威胁防御设备需要识别正确的出口接口，以便可以执行转换。

图 *33: NAT* 示例：网桥组中的 *NAT*



透明模式下网桥组不支持的功能

下表列出了在透明模式下网桥组中不受支持的功能。

表 *10:* 在透明模式下不支持的功能

功能	说明
动态 DNS	—
DHCPv6 无状态服务器	在网桥组成员接口上仅支持 DHCPv4 服务器。
DHCP 中继	透明防火墙可作为 DHCPv4 服务器，但它不支持 DHCP 中继。不需要使用 DHCP 中继，因为可使用两个访问规则来允许 DHCP 流量通过：一个规则用于允许从内部接口向外部发送 DCHP 请求；另一个用于允许来自另一个方向的服务器的应答。
动态路由协议	但是，对于网桥组成员接口，可以为 Firewall 威胁防御设备上发起的流量添加静态路由。您还可以使用访问规则来允许动态路由协议通过 Firewall 威胁防御设备。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 Firewall 威胁防御设备。
QoS	—
针对直通流量终止 VPN	透明防火墙仅支持在网桥组成员接口上使用站点间的VPN隧道传输管理连接。它不会针对通过 Firewall 威胁防御设备 的流量终止 VPN 连接。您可以Firewall 威胁防御设备使用访问规则允许 VPN 流量通过 ASA，但它不会终止非管理连接。

路由模式下网桥组不支持的功能

下表列出了在路由模式下网桥组中不支持的功能。

表 *11:* 路由模式下不受支持的功能

功能	说明
EtherChannel 成员接口	仅支持物理接口、冗余接口和子接口作为网桥组成员接口。 管理 接口也不受支持。
集群	集群中不支持网桥组。
动态 DNS	—
DHCPv6 无状态服务器	只有 DHCPv4 服务器在 BVI 上受支持。

功能	说明
DHCP 中继	路由防火墙可以作为 DHCPv4 服务器，但它不支持在 BVI 或网桥组成员接口上使用 DHCP 中继。
动态路由协议	但您可以为 BVI 添加静态路由。您还可以使用访问规则来允许动态路由协议通过 Firewall 威胁防御设备。非网桥组接口支持动态路由。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 Firewall 威胁防御设备。非网桥组接口支持组播路由。
QoS	非网桥组接口支持 QoS。
针对直通流量终止 VPN	您无法终止 BVI 上的 VPN 连接。非网桥组接口支持 VPN。 网桥组成员接口仅支持将站点间 VPN 隧道用于管理连接。它不会针对通过 Firewall 威胁防御设备 的流量终止 VPN 连接。您可以使用访问规则通过网桥组传递 VPN 流量，但它不会终止非管理连接。

默认设置

网桥组默认设置

默认情况下，所有 ARP 数据包都在网桥组内通过。

防火墙模式准则

桥接组准则（透明和路由模式）

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- Firewall 威胁防御设备不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 Firewall 威胁防御设备。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。

- 对于具有桥接 ixgbevf 接口的 VMware 上的 Firewall Threat Defense Virtual，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。20012101220
- 对于 Firepower 4100/9300，不支持将数据共享接口作为网桥组成员。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 Firewall 威胁防御另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的 Threat Defense Virtual 实例不支持透明模式。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，Firewall 威胁防御 - 不支持将 EtherChannel 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 Firewall 威胁防御。如果 Firewall 威胁防御 的一端有两个邻居运行 BFD，则 Firewall 威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

设置防火墙模式

在 CLI 中执行初始系统设置时，可以设置防火墙模式。我们建议在安装过程中设置防火墙模式，因为更改防火墙模式会清除您的配置，以确保不存在不兼容的设置。如果以后需要更改防火墙模式，则必须从 CLI 中执行此操作。

过程

步骤 1 从 防火墙管理中心注销 Firewall Threat Defense 设备。

在取消注册设备之前，您不能更改模式。

a) 性能配置文件会在防火墙模式更改后保留，并且在重新注册后不能更改。您必须将性能配置文件设置为默认值。请参阅平台设置策略中的**性能配置文件**页面（选择 **设备** > **平台设置**，然后点击您的策略的 **编辑** (✎)）。

此外，如果您为设备启用了通用 Zero Trust 网络访问（通用 ZTNA）（这也启用了特殊的通用 ZTNA 性能配置文件），则需要在Security Cloud Control中禁用它。请参阅**设备管理** > **通用 Zero Trust 访问设置**。

部署配置以完成这些更改。

b) 选择**设备** > **设备管理**。

c) 在要取消注册的设备旁边点击 **更多** (⋮)，然后点击**删除 (Delete)**。

步骤 2 访问 Firewall Threat Defense设备 CLI，首选使用控制台端口。

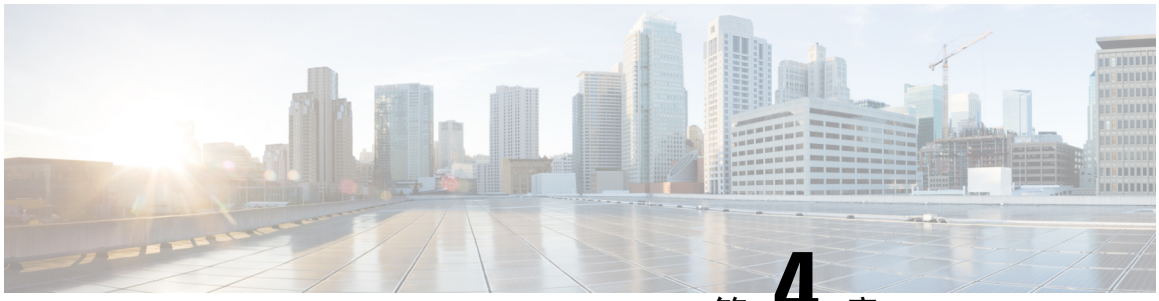
步骤 3 更改防火墙模式：

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

示例：

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

步骤 4 向 防火墙管理中心重新注册。请参阅 使用 CLI 完成Firewall Threat Defense初始配置 和 使用注册密钥添加设备 - 基本配置 。



第 4 章

CLI 用户

托管设备中有一个用于 CLI 访问的默认**管理员**账户。本章介绍如何创建自定义用户帐户。

- 关于 CLI 用户，第 135 页
- CLI 用户准则，第 136 页
- 在 CLI 中添加内部用户，第 137 页
- 配置 FTD 的外部身份验证，第 139 页
- LDAP 身份验证连接故障排除，第 151 页
- CLI 用户的历史记录，第 153 页

关于 CLI 用户

您可以在托管设备上作为内部用户添加自定义用户账号，也可以作为 LDAP 或 RADIUS 服务器上的外部用户添加自定义用户账号。每个托管设备单独维护用户账号。例如，将某个用户添加到 防火墙管理中心时，该用户只能访问防火墙管理中心；您不能使用该用户名直接登录托管设备。您必须单独在托管设备上添加用户。

内部和外部用户

托管设备支持两种用户类型：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

CLI 访问

Firepower 设备包括一个在 Linux 上运行的 Firepower CLI。您可以使用 CLI 在设备上创建内部用户。您可以使用 防火墙管理中心在 Firewall Threat Defense 设备上建立外部用户。

⚠

注意 拥有 CLI 配置级别访问权的用户可以使用 **expert** 命令来访问 Linux 外壳，并在 Linux 外壳中获得 `sudoers` 权限，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在 Firepower 用户文档明确指示时使用 Linux 外壳。
- 请确保相应地限制具有 CLI 访问权限的用户列表。
- 在授予 CLI 访问权限时，请显示具有“配置”级别访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。
- 除非思科 TAC 指示或 Firepower 用户文档中有明确说明，否则请不要使用 CLI 专家模式来访问 Firepower 设备。

CLI 用户角色

在托管设备上，用户在 CLI 中的命令访问权限取决于您所分配的角色。

无

用户无法在命令行上登录设备。

配置

用户可以访问所有命令，包括配置命令。请谨慎将此访问级别分配给用户。

基本

用户只能访问非配置命令。允许的命令包括 dig、ping 和 traceroute。只有内部用户和 Firewall Threat Defense 外部 RADIUS 用户支持基本角色。

CLI 用户准则

用户名

- 不能为内部和外部用户添加相同的用户名。如果外部服务器使用重复的用户名，则部署到设备会失败。
- 用户名必须对 Linux 有效：
  - 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
  - 全部小写
  - 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

默认值

所有设备都包括一个 **admin** 用户作为本地用户帐户；您不能删除 **admin** 用户。默认初始密码为 **Admin123**；系统会强制您在初始化过程中更改此设置。代理将修改后的凭证存储在 Windows 注册表中，并使用与防火墙管理中心相同的加密方式，即密码块链(CBC)。有关系统初始化的详细信息，请参阅您的型号的入门指南 。

用户账户数量

您最多可以为 Firepower 1100系列设备创建 43 个用户账户。

在 CLI 中添加内部用户

使用 CLI 可在 Firewall Threat Defense上创建内部用户。

过程

步骤 1 使用具有配置权限的帐户登录设备 CLI。

管理员用户账号具有所需的权限，但具有配置权限的任何帐户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些 Firewall Threat Defense型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 Firewall Threat Defense CLI。

步骤 2 创建用户账号。

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

- 用户名-设置用户名。用户名必须对 Linux 有效：
  - 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
  - 全部小写
  - 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)
- **basic**- 提供用户基本访问权限。此角色不允许用户输入配置命令。允许的命令包括 dig、ping 和 traceroute。
- **config**- 提供用户配置访问权限。此角色将赋予用户完整管理员权限，让其可以输入所有配置命令。

示例：

以下示例将添加一个名为 johncrichton 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add johncrichton config
```

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

注释
告知用户他们可以使用 **configure password** 命令更改自己的密码。

步骤 3 （可选） 根据安全要求调整该帐户的特性。

您可以使用以下命令更改默认帐户行为。

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

  设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建帐户时，密码没有到期日。

- **configure user forcereset** *username*

  强制用户下次登录时更改密码。

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

  设置在锁定帐户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁帐户。新帐户的默认值为 5 次连续失败登录。除非已启用安全认证合规性，否则管理员账户不会在达到最大失败登录次数后被锁定。

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

  设置最小密码长度，此值介于 1 至 127 之间。

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

  启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4 根据需要管理用户账号。

用户可能被锁定在帐户之外了，也可能您需要删除帐户或解决其他问题。使用以下命令管理系统中的用户账号。

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

  更改用户账号的权限。

- **configure user delete** *username*

  删除指定的帐户。

- **configure user disable** *username*

  禁用指定的帐户，而不将其删除。用户无法登录，直到您启用该帐户为止。

- **configure user enable** *username*

  启用指定的帐户。

- **configure user password** *username*

  更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

  注意
  请不要在专家模式下使用 Linux **passwd** 命令更改管理员用户密码。此命令可能会导致文件系统损坏。仅使用常规的 Firewall Threat Defense CLI **configure user password admin** 命令（如果您不是管理员）或 **configure password** 命令（如果您是管理员）。如果您不知道密码并且根本无法登录，请参阅 密码恢复 程序。

- **configure user unlock** *username*

  解锁因超出最大连续失败登录尝试次数而被锁定的用户账号。

注释
Firewall Threat Defense使用可插拔身份验证模块 (PAM) 框架进行用户身份验证。在此框架中，pam_unix.so 模块使用 SHA-512 算法处理密码散列和验证。

密码使用 SHA-512 算法进行散列处理。

配置 FTD 的外部身份验证

要启用 FTD 设备的外部身份验证，您需要添加一个或多个外部身份验证对象。

关于Firewall Threat Defense外部身份验证

在为 Firewall Threat Defense 用户启用外部身份验证时，Firewall Threat Defense 会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

防火墙管理中心 和 Firewall Threat Defense 设备可使用外部身份验证对象。不同应用/设备可共享同一个对象，也可以为它们创建不同的对象。对于 Firewall Threat Defense，您智能在部署到设备的平台设置中激活一个外部身份验证对象。

注释 Firewall Threat Defense 和 防火墙管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense 外部身份验证配置将不起作用。

只有外部身份验证对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果对于其他设备类型也使用此对象，系统将使用这些字段。

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

您可以在 RADIUS 服务器上（通过 Service-Type 属性）定义用户，也可以预定义外部身份验证对象中的用户列表。对于 LDAP，您可以指定过滤器来匹配 LDAP 服务器上的 CLI 用户。



注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。确保：

- 限制具有 Linux 外壳访问权限的用户列表。
- 请勿创建 Linux 外壳用户。

关于 LDAP

通过轻量级目录访问协议(LDAP)，可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

如果您尚未执行此操作，我们建议您开始使用 TLS / SSL 加密对 Active Directory 服务器进行身份验证。

关于 RADIUS

远程身份验证拨入用户服务 (RADIUS) 是用于验证/授权和说明用户对网络资源的访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

Secure Firewall 设备支持使用 SecurID 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并使用此代码作为其登录密码。在 Secure Firewall 设备上无需配置任何其他信息来支持 SecurID。

准则

- 默认 RADIUS 身份验证端口为 1812。
- 默认 RADIUS 记账端口为 1813（比 RADIUS 身份验证端口大 1）。

如果更改 RADIUS 身份验证端口，RADIUS 记账端口会相应更改。确保 防火墙管理中心 可以连接到新 RADIUS 服务器；否则，可能会出现认证延迟。

为 Firewall Threat Defense 添加 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行 Firewall Threat Defense 管理。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

共享外部身份验证对象

防火墙管理中心 和 Firewall Threat Defense 设备可使用外部 LDAP 对象。防火墙管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。确保即使您未共享对象，Firewall Threat Defense 和 防火墙管理中心 也都可以访问 LDAP 服务器。防火墙管理中心 对于检索用户列表并将其下载到设备至关重要。



注释 对于 LDAP，Firewall Threat Defense 和 防火墙管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则到 Firewall Threat Defense 的部署将失败。

Firewall Threat Defense 支持的字段

只有 LDAP 对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 防火墙管理中心，则将使用这些字段。此程序仅涵盖 Firewall Threat Defense 支持的字段。有关其他字段，请参阅《*Cisco Secure Firewall Management Center* 管理指南》中的“为 防火墙管理中心 添加 LDAP 外部身份验证对象’ ”。

用户名

用户名必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

不能为外部身份验证添加 **admin** 或 **sshd** 用户。

只能在防火墙管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在CLI中添加他们。请注意，内部用户只能在 CLI 中添加，不能在防火墙管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 Firewall Threat Defense 首先对照此内部用户检查密码，如果失败，再检查 LDAP 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。

特权等级

LDAP 用户始终具有“配置”权限。

开始之前

您必须在设备上指定 DNS 服务器用于域名查找。即使您在此程序中为 LDAP 服务器指定了 IP 地址而非主机名，LDAP 服务器也可能返回可能包括主机名的身份验证 URI。解析主机名需要进行 DNS 查询。请参阅在 CLI 中修改 Firewall Threat Defense 管理接口，第 879 页来添加 DNS 服务器。

过程

步骤 1 选择**管理** > **用户**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击 (+) **添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **LDAP** 。

步骤 5 输入**名称**和可选**说明**。

步骤 6 从下拉列表中选择**服务器类型**。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 输入 **LDAP 特定参数**。

a) 在**基础 DN** 中为要访问的 LDAP 目录输入基础 DN。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN (Fetch DNs)**，然后从下拉列表中选择相应的基本可分辨名称。

b) （可选） 输入**基本过滤器**。

例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

要检索所有 cn 名称（禁止的用户 admin 和 sshd 除外），请输入 `(&(cn=*)(!(|(cn=sshd)(cn=admin)))`。

c) 为有足够凭证浏览 LDAP 服务器的用户输入**用户名**。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

d) 在**密码**和**确认密码**字段中输入用户密码。

e) （可选） 点击**显示高级选项**配置以下高级选项。

- **加密 (Encryption)** - 点击**无 (None)**、**TLS** 或 **SSL**。

  如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径 (SSL Certificate Upload Path)** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件 (Choose File)** 选择一个证书。

  如果之前已上传证书并要将其替换，请上传新证书并将该配置重新部署到设备，以复制转移新证书。

  注释

TLS 加密要求所有平台上均有证书。对于 SSL，Firewall Threat Defense 同样要求有证书。对于其他平台，SSL 不要求有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- （未使用）**用户名模板** - Firewall Threat Defense 未使用。
- **超时（秒）**-输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

  注释
  Firewall Threat Defense 和 防火墙管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense LDAP 配置将不起作用。

步骤 11 配置**属性映射 (Attribute Mapping)** 以基于属性检索用户。

- 输入 **UI 访问属性 (UI Access Attribute)**。**注意**：此字段不用于设备 CLI 访问；但是，它是必填字段，因此您需要输入一个值。您可以输入与为 **CLI 访问属性**输入的值相同的值。
- 如果要使用用户可分辨类型之外的 CLI 访问属性，请设置 **CLI 访问属性**。例如，在 Microsoft 活动目录服务器上，通过键入 `sAMAccountName`可使用 `sAMAccountName` 外壳 CLI 访问属性来检索外壳访问用户。

  注释
  具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

  注释
  部署允许大量具有 CLI 访问权限的用户的外部身份验证对象可能会导致部署超时并在等待创建用户时失败。

步骤 12 设置 **CLI 访问过滤器**。

选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选中 **与基本过滤器相同**复选框。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

有关用户名准则，请参阅此程序之前的用户名。

步骤 13 点击**保存**。

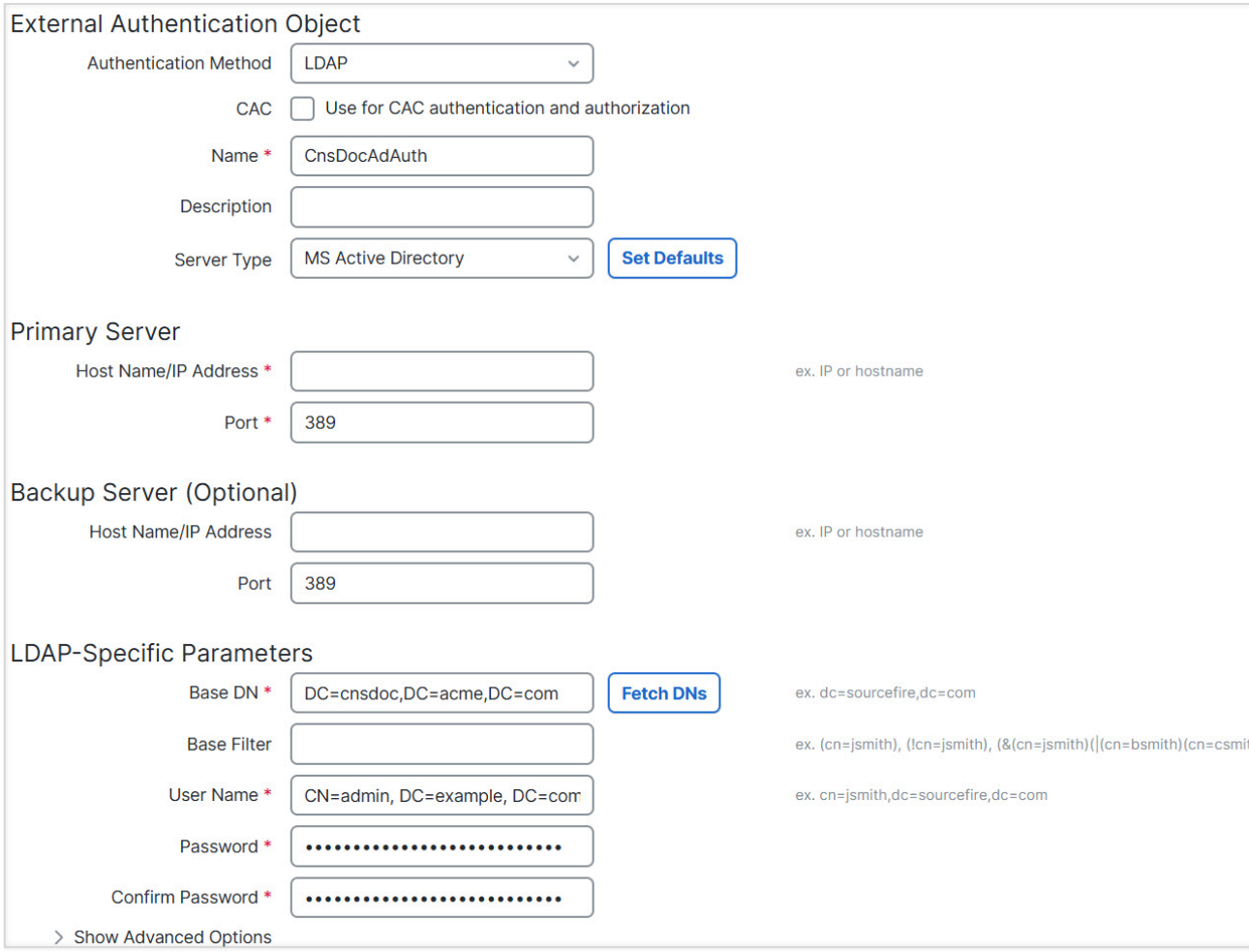
步骤 14 启用此服务器。请参阅外部身份验证，第 980 页。

步骤 15 如果以后在 LDAP 服务器上添加或删除用户，必须在托管设备上重新部署“平台设置”。防火墙管理中心 会重新下载用户列表并将其部署到设备。请参阅部署配置更改，第 180 页。

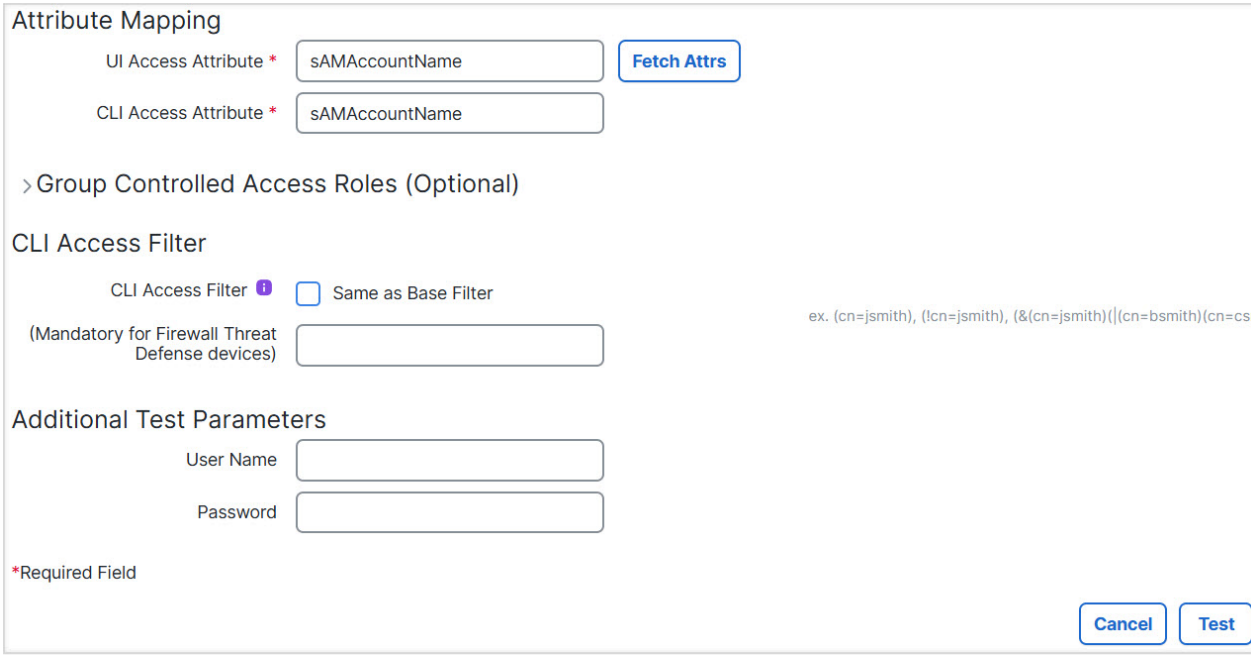
示例

基本示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。

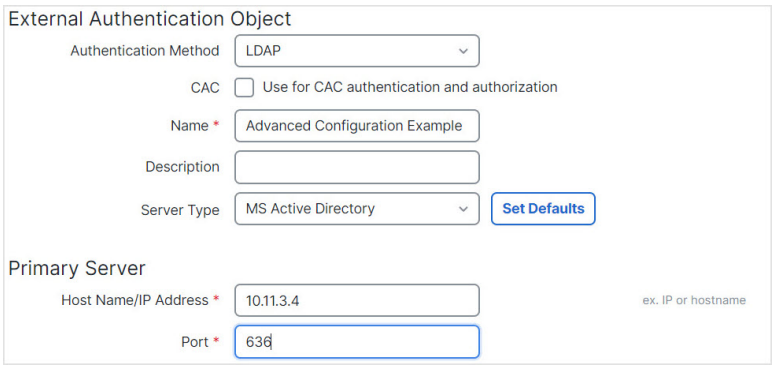


当用户登录 Firewall Threat Defense 时，`sAMAccountName` 的 **CLI 访问属性**会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

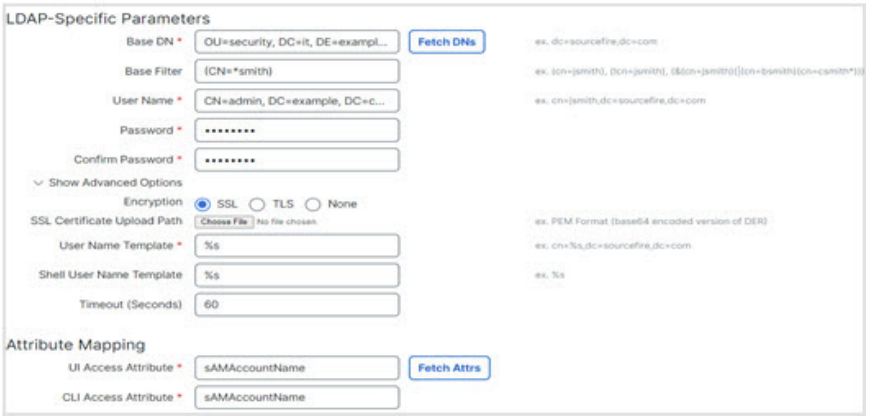
请注意，由于未对此服务器应用基本过滤器，因此 Firewall Threat Defense 会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

高级示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。该过滤器将从服务器检索到的用户限制为公用名称以 `smith` 结尾的用户。

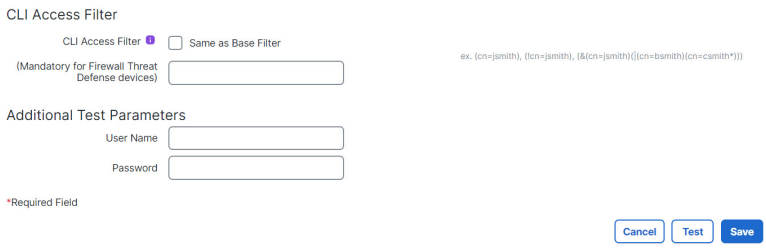


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **超时（秒）** 设置，与服务器的连接在 60 秒后将超时。

由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。

当用户登录 Firewall Threat Defense 时，`sAMAccountName` 的 **CLI 访问属性**会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

在以下示例中，CLI 访问过滤器设置为与基本过滤器相同。



为 Firewall Threat Defense 添加 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户进行Firewall Threat Defense。

共享外部身份验证对象

防火墙管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意，Firewall Threat Defense 支持在 RADIUS 服务器上定义用户，而 防火墙管理中心 要求您在外部身份验证对象中预定义用户列表。您可以选择针对 Firewall Threat Defense使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 Firewall Threat Defense 和 防火墙管理中心创建单独的对象。

注释 Firewall Threat Defense 和 防火墙管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense RADIUS 配置将不起作用。

Firewall Threat Defense 支持的字段

只有 RADIUS 对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于防火墙管理中心，则将使用这些字段。此程序仅涵盖 Firewall Threat Defense 支持的字段。有关其他字段，请参阅*Cisco Secure Firewall Management Center* 管理指南中的为 防火墙管理中心 添加 RADIUS 外部身份验证对象。

用户名

不能为外部身份验证添加**管理员**用户。只能在防火墙管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在防火墙管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 Firewall Threat Defense 首先对照此内部用户检查密码，如果失败，再检查 RADIUS 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

过程

步骤 1 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤 12，第 148 页）。要在为 Firewall Threat Defense使用 Service-Type 属性的同时对 Firewall Threat Defense 和 防火墙管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 防火墙管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 Firewall Threat Defense）。

步骤 2 在 防火墙管理中心上，选择 **管理** > **用户**。

步骤 3 点击**外部身份验证 (External Authentication)**。

步骤 4 点击 (+)**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 5 将**身份验证方法**设置为 **RADIUS**。

步骤 6 输入**名称**和可选**说明**。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

仅支持 IPv4。

注释
如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 输入 **RADIUS 服务器密钥**。

步骤 10 （可选） 输入**备份服务器**参数。

步骤 11 （可选） 输入 **RADIUS 特定参数**。

a) 在**超时（秒）** 中输入重试主服务器之前允许的秒数（介于 1 和 300 之间）。默认值为 30。

注释
Firewall Threat Defense 和 防火墙管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense RADIUS 配置将不起作用。

b) 输入滚动到备份服务器之前允许的**重试次数**。默认值为 3。

步骤 12 （可选） 不要使用 RADIUS 定义的用户（请参阅 步骤 1，第 147 页），在 **CLI 访问过滤器 (CLI Access Filter)** 区域**管理员 CLI 访问用户列表 (Administrator CLI Access User List)** 字段中，输入应具有 CLI 访问权限的用户名并以逗号分隔。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

您可能想要使用 Firewall Threat Defense 的 **CLI 访问过滤器** 方法以便对 Firewall Threat Defense 和其他平台类型使用相同的外部身份验证对象。

注释
如果想要使用 RADIUS 定义的用户，则必须将 **CLI 访问过滤器 (CLI Access Filter)** 留空。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释
具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释
部署允许大量具有 CLI 访问权限的用户的外部身份验证对象可能会导致部署超时并在等待创建用户时失败。

步骤 13 （可选） 点击**测试 (Test)** 以测试与 RADIUS 服务器的 防火墙管理中心 连接。

此功能只能测试 防火墙管理中心 与 RADIUS 服务器的连接；没有用于托管设备与 RADIUS 服务器的连接的测试功能。

步骤 14 （可选）此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名**和**密码**，然后点击**测试**。

提示
如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

步骤 15 点击**保存**。

步骤 16 启用此服务器。请参阅 外部身份验证，第 980 页

示例

简单的用户角色指定

下图说明端口 1812 上 IP 地址为 10.10.10.98 的运行 Cisco Identity Services Engine (ISE) 的服务器的示例 RADIUS 登录身份验证对象。未定义备份服务器。



以下示例显示 RADIUS 特定参数，包括超时（30 秒）和系统尝试联系备份服务器（如有）之前的失败重试次数。

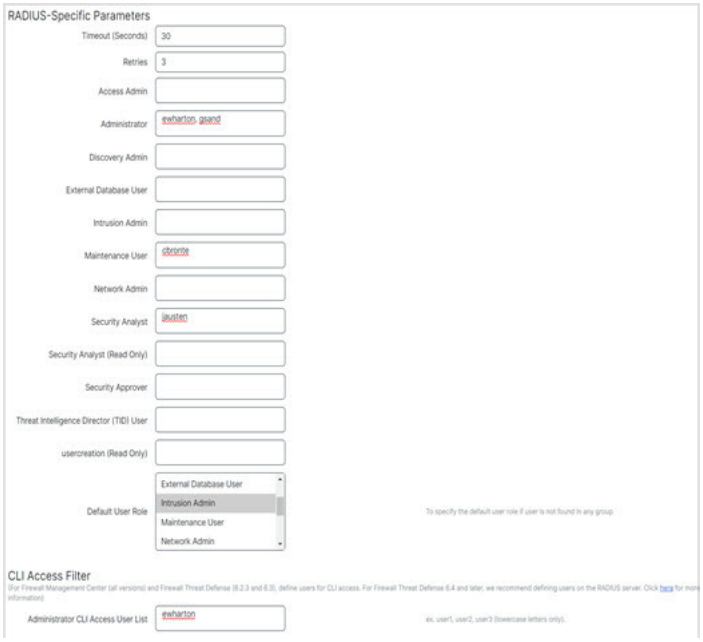
此示例说明 RADIUS 用户角色配置的重要方面：

授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

授予用户 `cbronte` Web 界面“维护用户”权限。

授予用户 `jausten` Web 界面“安全分析师”权限。

用户 `ewharton` 可以使用 CLI 帐户登录到设备中。



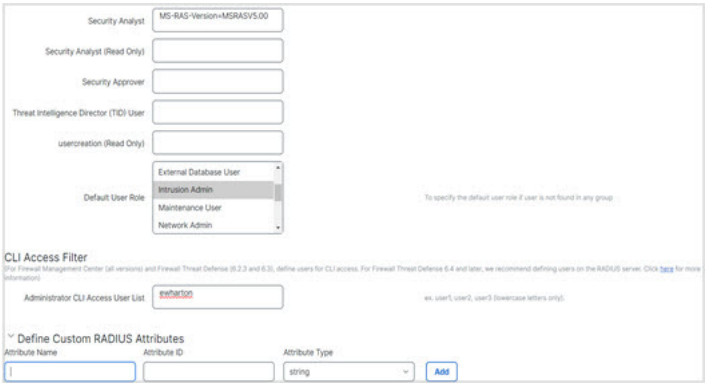
下图说明示例的角色配置：

匹配属性-值对的用户角色

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 ISE 服务器的示例 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



为 FTD 设备上的用户启用外部身份验证

在 Firepower 威胁防御平台设置中启用“外部身份验证”(External Authentication)，然后将这些设置部署到托管设备。有关详细信息，请参阅外部身份验证，第 980 页。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用 Web 界面屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效：
  - 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基本可分辨名称中指示的目录。
  - 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
  - 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用对服务器进行身份验证，以了解通过该连接进行的绑定是否也失败。
  - 配置 LDAP 身份验证时，请避免在绑定密码中使用反斜线（“\”）。密码中存在反斜线会导致 LDAP 绑定过程失败，从而导致外部身份验证失败。
- 检查是否已正确识别服务器：
  - 检查服务器 IP 地址或主机名是否正确。
  - 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问权限。
  - 检查对服务器的访问是否未被防火墙阻止，以及在对象中配置的端口是否已打开。
  - 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
  - 如果是对 CLI 访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
  - 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击**设置默认值 (Set Defaults)** 以重置默认值。
- 如果键入了基本可分辨名称，请点击**获取 DN (Fetch DNs)** 以检索服务器上的所有可用基本可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。

- 如果使用的是基本过滤器或 CLI 访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符（包括括号在内，最大450个字符）。
- 要测试受限更多的基本过滤器，请尝试将其设置为基本可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
  - 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
  - 检查是否未对加密服务器连接使用 IPv6 地址。
- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过连接到 LDAP 服务器并使用以下语法测试使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

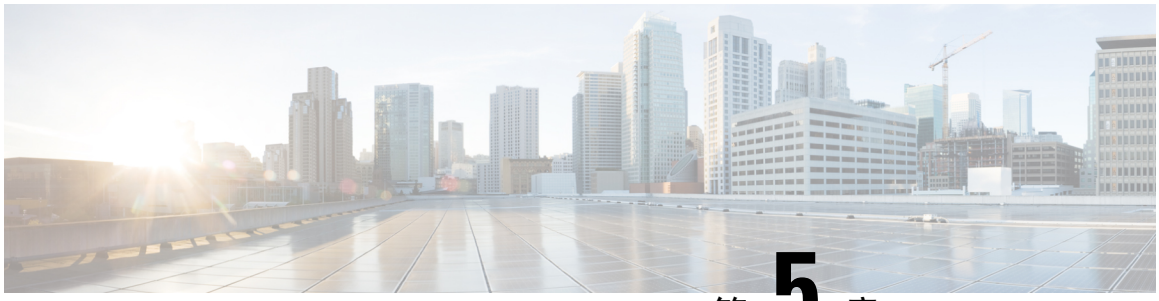
如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的平台设置策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或CLI访问过滤器，或者使用限制较多或较少的基本 DN。

在对与 Active Directory (AD) 服务器的连接进行身份验证时，尽管与 AD 服务器的连接成功，但连接事件日志很少指示受阻 LDAP 流量。当 AD 服务器发送重复的重置数据包时，会出现此不正确的连接日志。防火墙威胁防御设备将第二个重置数据包识别为新连接请求的一部分，并使用“阻止”操作记录连接。

CLI 用户的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
威胁防御CLI基本用户的有限用户权限。	7.7.0	7.7.0	威胁防御 CLI 基本用户权限的范围现在仅限于以下命令：dig、ping、traceroute。如果创建的用户具有基本权限，请评估是否需要将其更改为配置权限。您可以使用 **configure user access** 命令来更改用户的权限级别。 请参阅： *Cisco Secure Firewall Threat Defense 命令参考*
对RADIUS服务器上定义的 Firewall Threat Defense用户的 Service-Type 属性的支持。	6.4.0	任意	对于 Firewall Threat Defense CLI 用户的 RADIUS 身份验证，以往，您须预定义RADIUS外部身份验证对象中的用户名，且须手动确保该列表匹配 RADIUS 服务器上定义的用户名。现在，您可以使用 Service-Type 属性在 RADIUS 服务器上定义 CLI 用户，亦可同时定义“基本”和“配置”用户角色。要使用此方法，请务必将外部身份验证对象中的外壳访问过滤器留空。 新增/修改的屏幕：**系统** > **用户** > **外部身份验证** > **添加外部身份验证对象** > **外壳访问筛选器**
用于 Firewall Threat Defense SSH 访问的外部身份验证。	6.2.3	任意	现在，您可以配置外部身份验证以便对使用 LDAP 或 RADIUS 的 Firewall Threat Defense进行 SSH 访问。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **外部身份验证 (External Authentication)**



第 5 章

变更管理

如果您的组织需要实施更加正式的配置变更流程，包括在部署变更之前进行审核跟踪和正式审批，则可以启用变更管理。

- 关于变更管理， 第 155 页
- 变更管理的要求和前提条件， 第 159 页
- 变更管理的准则和限制， 第 160 页
- 启用或禁用更改管理， 第 160 页
- 管理工单， 第 161 页
- 变更管理的历史记录， 第 166 页

关于变更管理

一些组织需要实施正式的方法来部署配置更改。这可能包括更多审核，以及在对设备进行配置更改之前必须进行的正式审批流程。

如果您的组织使用更正式的配置更改流程，您可以启用更改管理来实施该流程。使用变更管理时，管理员必须先创建故障单，然后才能进行配置更改。然后，更改完成后，他们必须提交故障单进行审批，然后才能部署建议的更改。这使您可以执行正式的审批流程，并确保由合适的员工做出最终决策。

使用“更改管理”时，管理员可以在故障单中查看自己的更改，但无法查看其他人在故障单中所做的更改。由于一旦用户在故障单中进行更改，策略就会被锁定，因此用户应该无法进行干扰性更改。但是，当其他用户进行了等待审批的更改时，用户将无法进行更改。

管理员可以创建多个故障单，以便单个故障单仅包含逻辑相关的策略更改。范围更有限的故障单也更容易快速评估和批准。

以下主题介绍变更管理工作流程以及哪些策略和对象需要提交故障单和审批流程。

如何在变更管理工作流程中配置设备

当您启用更改管理时，配置设备的用户需要稍微更改其方法。对支持的策略和对象进行配置更改时，配置专家需要采用以下方法。

过程

步骤 1 创建故障单。

步骤 2 打开故障单。

步骤 3 对配置进行更改。

请注意，在线帮助和用户指南中介绍的程序假定“变更管理”处于非活动状态，并省略创建、打开或提交故障单的任何步骤。

步骤 4 或者，预览并验证故障单，以确保更改完整且正确。

步骤 5 提交故障单。此时，审批人可以批准或拒绝故障单。

- 如果故障单获得批准，请部署更改。
- 如果故障单被拒绝，请解决问题，然后重新提交故障单。

创建独立的审批人和配置角色

某些系统定义的角色具有修改（创建/打开/丢弃）和审核（批准/拒绝）故障单的权限：

- 要修改和查看故障单，请执行以下操作：
  - 管理员
  - 网络管理员
- 仅修改故障单：
  - 访问管理员
  - 入侵管理员
- 仅查看故障单：
  - 安全审批人

如果您的组织要求需要更精细的角色来分隔这些活动，则可以创建单独的角色，以确保仅将故障单审批分配给具有审批更改的组织权限的用户。要创建新用户，请转到 **管理** > **用户** > **用户角色**。

以下是 **管理** > **配置** > **更改管理** 文件夹中与故障单使用和审批相关的权限。请注意，这些权限仅在启用更改管理后可用。

- 修改故障单 - 创建故障单（为自己）、使用配置更改故障单，以及丢弃故障单。
- 审核故障单 - 批准或拒绝故障单。

- 修改和查看通知单 - 要为自己和他人创建通知单，请使用通知单，并批准/拒绝通知单。您还可以接管分配给其他用户的通知单。

您所采取的方法取决于精细的要求。例如：

- 如果还应允许您的审批人进行配置更改，您只需为他们分配系统定义的角色，例如管理员。然后，创建包含相同权限但不包含“审核故障单”权限的自定义仅配置角色。
- 如果您需要完全分离审批者和进行配置更改的人员，请为两者创建自定义角色，将角色限制为“修改故障单”或“审核故障单”权限，以及查看或更改支持的策略和对象所需的所有其他权限。

支持变更管理的策略和对象

如果策略或对象支持更改管理工作流程，则必须在未解决的故障单中创建、编辑或删除策略或对象，包括将策略分配给设备。

可以创建、编辑或删除不支持更改管理工作流程的任何操作、策略或对象，而无需打开故障单。即使故障单处于未决状态，对不受支持的策略所做的更改也不会包含在已发出故障单的更改中，并且可以立即进行部署。

以下列表包括支持的策略和对象。未列出的任何内容均不受支持。

支持的策略

- 访问控制，包括规则、对其他策略的引用和继承设置。故障单中不包含克隆访问控制策略。该克隆将被立即接受并提供给所有用户。
- 设备配置策略：
  - 接口
  - 内联集
  - DHCP
  - VTEP
  - 所有路由
- 解密策略
- DNS 策略
- FlexConfig
- 入侵策略和网络分析策略 (NAP)，仅 Snort 3。
- 恶意软件及文件策略
- 网络地址转换 (NAT)
- 网络发现策略

- 平台设置
- 预过滤器策略
- QoS
- Splunk 集成
- Umbrella SASE 拓扑
- VPN 策略，站点间和远程访问
- Zero Trust 访问

支持的对象

- AAA 服务器
- 访问列表
- 地址池
- AS 路径
- 密码套件列表
- 社区列表
- 可分辨名称对象
- DHCP IPv6 池
- DNS 服务器组
- FlexConfig 对象
- 组策略
- 接口
- 密钥链
- 网络
- PKI 证书，所有对象
- 策略列表
- 端口
- 前缀列表
- 路由映射
- Sinkhole
- SLA 监视器

- 时间范围
- 时区
- 隧道区域
- URL
- 变量集
- VLAN 标记
- VPN 对象（IKEv1、IKEv2 IPSec 和策略、PKI 注册、证书映射）

变更管理的要求和前提条件

型号支持

管理中心

支持的域

任意

用户角色

- 要启用或禁用变更管理：管理员。
- 要修改和查看故障单，请执行以下操作：
  - 管理员
  - 网络管理员
- 仅修改故障单：
  - 访问管理员
  - 入侵管理员
- 仅查看故障单：
  - 安全审批人

变更管理的准则和限制

- 在更改管理模式下运行时，用户可以对支持的策略进行更改，但无法保存更改。例如，您可以在没有打开故障单的情况下通过对话框创建新的平台设置策略，但是当您点击确定实际创建策略时，您将收到错误消息，并且不会创建策略。
- 以下活动要求所有故障单都处于终止状态，即已批准或已丢弃：备份/恢复、在域之间移动设备、升级 防火墙管理中心。
- 从资产中删除设备需要批准或丢弃涉及该设备的所有故障单。
- 某些进程（例如部署和备份/恢复）会阻止您更改更改管理模式。等待该过程完成以更改模式。
- 根据更改管理是否支持功能和对象，您在配置功能时创建对象的能力受到限制。例如，更改管理不支持导入配置。因此，在导入期间无法创建受支持的安全区域对象。另一方面，您可以在配置访问控制规则时创建新对象，因为这两种规则都受支持。
- 使用 云交付的防火墙管理中心时，只有在 Security Cloud Control 中定义的用户至少交叉启动一次 cdFMC 后，才能为其分配故障单。在第一次交叉启动之前，用户不存在于 cdFMC中。

启用或禁用更改管理

默认情况下，更改管理工作流程处于禁用状态。用户在进行配置更改时不需要打开故障单并获得批准。如果要实施更改管理工作流程，则必须为系统全局启用它。

开始之前

有几个系统进程会阻止您启用/禁用更改管理。如果正在执行以下任何操作，则需要等待它们完成后才能更改这些设置：备份/恢复；导入/导出；域移动；升级； Flexconfig迁移；设备注册；高可用性注册、创建、中断或切换；集群创建、注册、中断、编辑、添加或删除节点； EPM 中断或加入。

更改这些设置时，无法锁定访问控制策略。如果策略已锁定，则必须等待锁定被释放，然后才能启用/禁用此功能。

过程

步骤 1 选择**管理** > **配置**。

步骤 2 点击 **变更管理**。

步骤 3 选择 **启用变更管理**。

要禁用该功能，请取消选择该选项。要禁用变更管理，必须批准或丢弃所有故障单。无法禁用变更管理，如果任何故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。

步骤 4 选择 **需要审批的数量**，即要批准和部署故障单，必须有多少管理员批准更改。默认值为 1，但每个故障单最多可以有 5 个审批人。用户可以在创建故障单时覆盖此编号。

步骤 5 选择 **故障单清除持续时间**，即保留已批准的故障单的天数，范围为 1-100 天。默认值为 5 天。

步骤 6 （可选。）输入**回复地址**和**审批者列表地址**的邮件地址。您还必须配置邮件通知系统设置，邮件才能正常工作。

步骤 7 点击**保存**。

系统将 **工单** (▣) 快捷方式添加到菜单栏，并添加 **管理** > **更改管理工作流程** 命令。用户可以使用这些方法来管理故障单。

管理工单

当您启用变更管理时，受支持策略的配置更改必须在工单的上下文中完成。您可以打开故障单，进行更改，然后提交故障单进行审批。

您可以在“更改管理”页面上或通过“故障单”快速访问菜单查看故障单列表并创建新故障单。所有故障单更改都在每个菜单中同步，因此您可以在方便时来回切换，并使用您喜欢的任何方法。

注释 当您打开故障单并对受支持的策略进行更改时，该策略将被其他用户或通过其他故障单锁定。策略保持锁定，直到故障单被批准或丢弃。

过程

步骤 1 执行以下任一操作：

- 选择 **管理** > **更改管理工作流程** 打开显示现有故障单的页面。
- 点击 **工单** (▣) 快速访问菜单。图标可以命名为“选择故障单”（如果未打开故障单）、故障单名称（如果已打开故障单）或未命名（如果不存在故障单）。

两个页面的组织方式相同。**故障单** 选项卡列出所有故障单，而 **审核** 选项卡列出已提交审批的故障单。默认视图仅显示您的故障单。

步骤 2 在 **故障单** 选项卡上，执行以下任何操作：

- 要创建新故障单，请点击 **添加故障单**。
- 要查看故障单的详细信息，请点击故障单名称旁边的>。“详细信息”页面包括UUID、名称、说明、用户、上次修改日期和注释。历史记录页面包括故障单的状态更改。顶部的图像显示了故障单在整个工作流程中的位置。
- 要预览未解决的故障单的配置更改，请点击 **预览** (🔍)。

- 要验证未解决的故障单中的配置更改，请点击 **验证** () 或 **更多** () > **验证** 。如果存在任何验证错误，系统将打开一个对话框，显示错误、警告和参考消息。
- 要创建故障单，请点击 **打开** () 或 **更多** () > **打开** 。
- 要关闭未解决的故障单，请点击 **暂停故障单 (X)** 或 **更多** () > **暂停故障单**。关闭故障单不会将其提交进行审核，也不会解除对已编辑策略的任何锁定。
- 要提交未解决的故障单以供审核和批准，请点击 **提交供审批** () 或 **更多** () > **提交以供批准** 。故障单必须处于打开状态才能提交。
- 要丢弃故障单，请点击 **丢弃** () 或 **更多** () > **丢弃** 。
- 要接管或重新分配故障单，请 **更多** () > **在查看系统中的所有故障单时点击接管故障单** 。
- 要搜索故障单，请在搜索框中键入字符串。搜索将查看故障单名称、描述和负责用户。
- 要按工单状态筛选列表（在变更管理工作流程页面上），点击列表上方的状态：**新建**、**打开**、**搁置**（工单已关闭）、**已拒绝**、**待审批**、**已批准**。每个状态都有该状态的故障单数量的计数。点击 **我的故障单** 下的 **全部** 可恢复显示所有故障单的默认设置，或点击 **系统** 故障单下的 **全部** 以查看每个人的故障单。

步骤 3 在 **审核** 选项卡上，对已提交的故障单执行以下任何操作。如果没有已提交的故障单，则列表为空。此外，只有具有审核故障单权限的用户才能看到此选项卡。

- 要预览故障单的配置更改，请点击 **预览** ()。
- 要验证未解决的故障单中的配置更改，请点击 **验证** () 或 **更多** () > **验证** 。
- 要批准故障单，请点击 **批准** () 或 **更多** () > **批准**。
- 要拒绝请求，请点击 **拒绝** () 或 **更多** () > **拒绝**。

创建变更管理工单

使用变更管理工作流程时，必须在已开启的工单上下文中执行所有配置更改。如果您还没有故障单，则必须创建一个新的故障单。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** () 快捷菜单。

步骤 2 点击 **添加故障单**。

步骤 3 配置故障单选项：

- **名称**- 故障单的名称。名称可以包含字母、数字、空格和以下特殊字符：#-_!

- **说明**-您打算使用此故障单进行配置的可选说明。例如，如果您有一个与您打算使用此故障单修复的问题相关的案例编号，这将是说明中的有用信息。
- **审批的数量**-要批准和部署故障单，必须有多少管理员批准更改。您可以指定 1-5。
- **分配到** -选择将拥有故障单并负责实施更改的用户。选择 **自己** 将其分配给自己。

步骤 4 点击以下选项之一：。

- **创建**-故障单已添加到故障单列表，但未打开。您需要先打开它，然后才能在故障单的上下文中工作。
- **创建并打开** - 通知单将添加到通知单列表并打开。

为配置更改开单

必须先打开故障单，然后才能在故障单中进行更改。

如果您有另一个待处理的故障单，系统会在打开新的故障单之前为您搁置（关闭）该故障单。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** (🖥) 快捷菜单。

步骤 2 在 **故障单** 选项卡上，点击 **打开** (📂) 或 **更多** (⋮) > **打开** 故障单。

步骤 3 或者，输入操作的注释。

步骤 4 点击**打开 (Open)**。

现在，您可以开始部署配置更改。工单图标名称将更改为已开工单的名称。

预览工单

您可以在更改配置时或在批准故障单之前预览故障单。预览显示在故障单上下文中进行的所有配置更改。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** (🖥) 快捷菜单。

步骤 2 点击 **预览** (🔍) 获取故障单。

系统会显示“预览”对话框。更改根据对话框顶部的图例进行颜色编码。

步骤 3 在已更改的策略列表中选择要查看其更改的策略。

您将看到 Secure Firewall Management Center 中定义的当前策略版本（位于左侧）以及故障单中定义的建议更改。

对于包含“平台设置”等页面的策略，您可以在“已更改的策略”列表中选择整体策略以查看所有更改，或选择策略中的特定页面。

您无法在预览中更改更改。如果您需要更改某些内容，则必须关闭预览并返回到要更改的策略。

步骤 4 或者，点击 **下载为 PDF** 将预览保存为 PDF 文件，以供离线查看或存档。

步骤 5 点击**确定**。

提交工单

完成故障单所需的更改后，您可以预览并验证更改。然后，当您对更改感到满意时，请提交故障单以供审核和批准。

在您提交故障单并且故障单获得批准之前，不会应用在故障单中所做的更改。在获得批准之前，故障单中修改的所有策略都将锁定到该故障单，其他任何人都无法更改。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** (▣) 快捷菜单。

步骤 2 点击 **提交供审批** (🗎) 或 **更多** (⋮) > **提交待批准** 请求。

步骤 3 或者，为您的操作输入注释。

步骤 4 点击**提交 (Submit)**。

丢弃工单

如果您不再需要对其创建故障单的更改，则可以丢弃该故障单。当您丢弃故障单时，您在故障单中所做的任何更改都将被删除。

您无法撤消此操作并检索故障单及其更改。如果需要，您必须创建一个新的故障单并重新开始。

您无法在提交故障单后将其丢弃。但是，如果审批人拒绝了该故障单，您可以将其丢弃。



注释 如果您有权修改故障单，则可以丢弃属于其他用户的故障单。这样就可以处理管理员正在休假或无法管理处理中的故障单的情况。 如果您有“审核故障单”权限，则可以重新分配或接管故障单，而不是将其丢弃。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** (▣) 快捷菜单。

步骤 2 点击 **丢弃** (🗑) 或 **更多** (⋮) > **丢弃** 该故障单。

步骤 3 或者，为您的操作输入注释。

步骤 4 点击 **丢弃**。

批准或拒绝工单

当用户提交故障单时，必须批准该故障单中所做的更改才能变为活动状态并可供部署。

您是否可以批准自己的故障单，还是有单独的审批人，取决于您的工作场所策略和用户角色的分配方式，而不是管理软件。

详细信息视图包括故障单所需的审批人数量以及故障单的审批人。

如果更改不充分或不需要，您可以拒绝故障单。被拒绝的故障单返回给提交者，然后提交者可以进行其他更改并重新提交故障单，或者直接丢弃故障单及其包含的配置更改。

过程

步骤 1 选择 **管理** > **更改管理工作流程**或点击 **工单** (▣) 快捷菜单。

步骤 2 在 **审核** 选项卡上，点击故障单的 **预览** (🔍) 并评估建议的更改。

您还可以点击 **验证** (☐) 或 **更多** (⋮) > **验证** 来检查错误。

步骤 3 完成评估后，请执行以下操作之一：

- 要批准故障单，请点击 **批准** (✓) 或 **更多** (⋮) > **批准**。
- 要拒绝请求，请点击 **拒绝** (✗) 或 **更多** (⋮) > **拒绝**。

步骤 4 或者，为您的操作输入注释。

步骤 5 根据需要点击 **批准** 或 **拒绝**。

接管或重新分配工单

有时可能需要接管其他人创建的故障单。例如，故障单所有者可能正在休假或不可用，并且故障单阻止了需要部署的更新。

您也可以使用此程序将您自己的故障单重新分配给其他人。

开始之前

以下是接管通知单所需的权限：

- 管理员用户 - 您可以将通知单分配给自己或其他用户。
- 修改或查看通知单 + 系统 > 用户管理 > 用户（自定义角色）- 您可以将通知单分配给自己或其他用户。

但是，仅当用户具有与当前故障单所有者或管理员角色相同的角色时，才能分配用户。这可确保新用户具有配置故障单中当前修改的功能所需的权限。

您无法重新分配已提交审批的故障单。

过程

步骤 1 选择**管理** > **更改管理工作流程**。

步骤 2 点击 **系统中故障单下的 全部**。

步骤 3 点击 **更多** (⋮) > **接管故障单**。

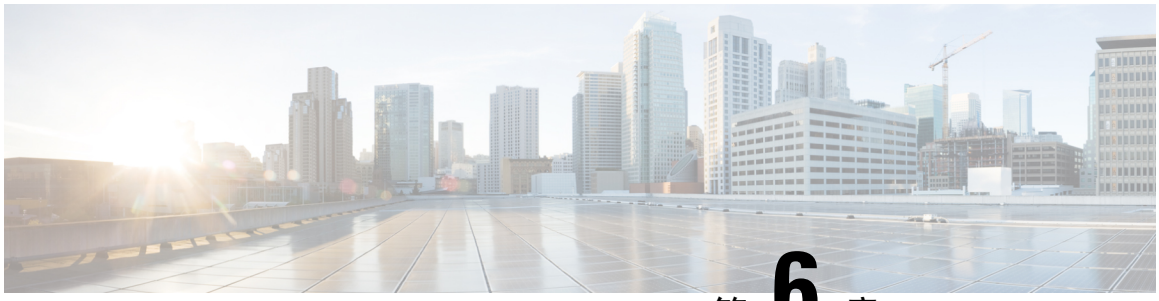
步骤 4 选择现在应拥有该故障单的用户。

用户列表仅限于具有编辑故障单中已更改策略所需权限的用户。例如，如果故障单包含对访问控制策略的更改，则用户列表仅包含允许修改访问控制策略的用户。

步骤 5 输入可选注释，然后点击 **接管**。

变更管理的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
接管工单并为变更管理提供额外支持。	7.6.0	任意	您可以接管其他用户的故障单。如果故障单阻止了策略的其他更新，并且用户不可用，这将非常有用。此外，变更管理审批工作流现在还包括以下功能：解密策略、DNS 策略、文件和恶意软件策略、网络发现、证书和证书组、密码套件列表、可分辨名称对象、Sinkhole 对象。
变更管理。	7.4.1	任意	如果您的组织需要实施更加正式的配置变更流程，包括在部署变更之前进行审核跟踪和正式审批，则可以启用变更管理。 我们添加了**系统**（⚙）> **配置 (Configuration)** > **更改管理 (Change Management)** 页面来启用此功能。启用后，将在菜单中显示**系统**（⚙）> **更改管理工作流程 (Change Management Workflow)** 页面和新的**故障单**（📄）快速访问图标。



第 6 章

配置部署

本章介绍如何将配置更改下载到一台或多台托管设备。

- 关于配置部署， 第 167 页
- 策略管理的要求和前提条件， 第 178 页
- 部署配置更改的最佳实践， 第 178 页
- 部署配置， 第 179 页
- 管理部署， 第 187 页
- 配置部署的历史记录， 第 199 页

关于配置部署

所有设备配置均由 防火墙管理中心 管理，然后部署到托管设备。

需要部署的配置更改

系统使用红色状态文本标记过期策略，表明其需要策略更新的目标设备的数量。要清除此状态，必须将策略重新部署到设备。

需要部署

需要部署的配置更改包括：

- 修改访问控制策略：对访问控制规则、默认操作、策略目标、安全智能过滤、高级选项（包括预处理）等等的任何更改。
- 修改访问控制策略调用的任何策略：SSL 策略、网络分析策略、入侵策略、文件策略、身份策略或 DNS 策略。
- 更改访问控制策略或其调用的策略中所使用的任何可重用对象或配置：
  - 网络、端口、VLAN 标记、URL 和地理位置对象。
  - 安全智能列表和源
  - 应用过滤器或检测器

- 入侵策略变量集
- 文件列表
- 与解密相关的对象和安全区域

- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

请记住，可以从 Web 界面中的多个位置更改其中某些配置。例如，可以使用对象管理器（**对象**）修改安全区域，但是修改设备配置（**设备** > **设备管理**）中的接口类型还可更改区域并要求部署。

不需要部署

请注意，以下更新 **不** 要求部署：

- 使用上下文菜单自动对安全智能源进行更新和对安全智能全局阻止或不阻止列表进行添加
- 对 URL 过滤数据的自动更新
- 计划的地理位置数据库 (GeoDB) 更新

部署预览

预览提供要在设备上部署的所有策略和对象更改的快照。策略更改包括新策略、现有策略的更改以及已删除的策略。对象更改包括策略中使用的已添加和修改的对象。未使用的对象更改不会显示，因为它们没有部署在设备上。

点击部署作业旁边的**预览**图标，查看待部署到设备上的作业的配置更改日志。更改日志包括：

- **比较视图 (Comparison View)**：并排比较自上次部署以来所做的所有设备配置更改。
- **高级视图 (Advanced View)**：显示要应用于设备的待处理 CLI 命令。

有关查看部署预览的详细信息，请参阅部署配置更改，第 180 页。

首次添加接口或平台设置策略时，预览中显示所有默认值（即使未有变更）以及其他配置的设置。同样，在高可用性对配置或中断后的首次预览中也会显示设置的高可用性相关策略和默认值（即使未有变更）。

要查看自动回滚导致的更改，请参阅编辑部署设置。

不支持的功能

- 仅当对象与任何设备或接口关联时，预览中才会显示添加的对象和属性的更改。删除的对象不显示。
- 以下策略不支持预览：
  - 高可用性
  - 网络发现

- 网络分析
- 设备设置

- 规则级别的用户信息不可用于入侵策略。
- 预览不会显示跨策略的规则重新排序。

  对于DNS策略，重新排序的规则作为规则添加和删除项显示在预览列表中。例如，将规则从规则顺序中的位置 1 移动到位置 3 显示为好像该规则已从位置 1 中删除，并作为新规则添加到位置 3 中。同样，删除规则时，其下的规则会列为已编辑的规则，因为它们的位置已更改。更改按它们在策略中出现的最终顺序显示。

- 以下 HA 场景不支持预览：
  - 如果设备处于单机模式并已建立链，则会触发自动部署。对于该特定作业，不支持预览。将鼠标悬停在 **预览** () 上时会显示一条消息，指明这是 HA 引导程序部署，并且不支持预览。
  - **配置组** - 考虑设备最初为独立设备的流程。随后进行了三个部署。在第四个部署中，设备是 HA 引导程序部署。在这些之后，用户会部署设备 5、6 和 7。部署 7 是 HA 中断部署，而用户会部署设备 8、9 和 10。

    在此流程中，不支持 3 和 5 之间的预览，因为 4 是 HA 部署。同样，也不支持 8 和 3 之间的预览。仅支持从 3 到 1、7、6、5、4 和 10、9 和 8 的预览。
  - 如果设备已损坏（HA 已损坏），则新设备会被视为新设备。

选择性策略部署

防火墙管理中心 允许您在设备上应该部署的所有更改的列表内选择特定的策略，并只部署所选的策略。选择性部署仅可用于以下策略：

- 访问控制策略
- 入侵策略
- 恶意软件和文件策略
- DNS 策略
- 身份策略
- SSL 策略
- QoS 策略
- 预过滤策略
- 网络发现
- NAT 策略

- 路由策略
- VPN 策略

选择性部署策略有特定的限制。按照下表中的内容，了解何时可以使用选择性策略部署。

表 *12*: 选择性部署的限制

类型	说明	情景
完整部署	对于特定部署场景，完整部署是必要的， 防火墙管理中心 在这类场景下不支持选择性部署。如果在这类场景下遇到错误，可选择要部署在设备上的所有更改以继续。	需要完整部署的场景包括： • 升级 Firewall Threat Defense 或 防火墙管理中心后的第一次部署。 • 恢复 Firewall Threat Defense 后的第一次部署。 • 修改 Firewall Threat Defense 接口设置后的第一次部署。 • 修改虚拟路由器设置后的第一次部署。 • Firewall Threat Defense 设备移动到新域（从全局域到子域或从子域到全局域）时。
关联策略部署	防火墙管理中心 识别相互关联和依赖的策略。选择一个相互关联的策略时，其余相互关联的策略将自动选中。	自动选择关联策略的场景： • 新对象与现有策略关联时。 • 修改现有策略的对象时。 自动选择多个策略的场景： • 当新对象与现有策略关联并且同一对象已与其他策略关联时，所有关联的策略将自动选中。 • 修改共享对象时，所有关联的策略将自动选中。

类型	说明	情景
相互依赖的策略更改（使用彩色标记显示）	防火墙管理中心动态检测策略之间以及共享对象与策略之间的依赖关系。对象或策略的相互依赖关系使用彩色标记显示。	自动选择以彩色显示的互相依赖策略或对象的场景： • 所有过期策略都有相互依赖的更改时。 例如，当访问控制策略、入侵策略和NAT策略过期时。由于访问控制策略和 NAT 策略共享一个对象，因此系统将同时选择所有策略进行部署。 • 所有过期策略共享一个对象，而该对象被修改时。
访问策略组规范	当您点击**视图**()时，访问策略组的策略将同时在预览窗口中的**访问策略组 (Access Policy Group)** 下列出。	访问策略组策略的场景和预期行为如下： • 如果访问控制策略过期，则在选择访问控制策略进行部署时，将选择该组下的所有其他过期策略，但文件策略和入侵策略除外。 但是，如果访问控制策略已过期，则无论是否选择访问控制策略，都可以单独选择或取消选择入侵和文件策略，除非有任何相关更改。例如，如果为访问控制规则分配了新的入侵策略，则表明存在相关更改，则选择访问控制策略和入侵策略中的任何一个时，都会自动选择访问控制策略和入侵策略。 • 如果没有过期的访问控制策略，可以选择此组中的其他过期策略单独部署。

系统用户名

防火墙管理中心 将用户名显示为 **system** 以执行以下操作：

- 回滚
- 升级
- Firewall Threat Defense 备份和恢复
- SRU 更新
- LSP 更新
- VDB 更新

自动启用应用检测器

如果执行的是应用控制，但是禁用所需的检测器，则系统会在策略部署时自动启用系统提供的适当检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

网络发现策略更改带来的资产重新发现

将更改部署到网络发现策略时，系统会删除并重新发现受监控网络中主机的网络映射中的 MAC 地址、TTL 和跳数信息。此外，受影响的托管设备还会放弃任何尚未发送到 防火墙管理中心的发现数据。

Snort 重新启动场景

当托管设备上的流量检测引擎（称为 *Snort* 进程）重启时，检测会中断，直到该进程继续运行。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。 此外，无论 Snort 进程是否重新启动，部署时的资源需求都可能导致少量数据包未经检测即被丢弃。

以下任一场景都将导致 Snort 进程重新启动：

- 部署需要 Snort 进程重新启动的特定配置。请参阅部署或激活时重启 Snort 进程的配置，第 176 页。
- 所做的更改将立即重新启动 Snort 进程。请参阅会立即重新启动 Snort 进程的更改，第 177 页。
- 流量激活当前部署的自动应用旁路 (AAB) 配置。请参阅配置自动应用旁路，第 918 页。
- 启用或禁用“将连接事件记录到 RAM 磁盘”功能。请参阅排除 FMC 未处理事件耗尽故障中的**记录到 Ramdisk 部分**。

以下主题提供有关 Snort 进程重启的更多详细信息。

设备的重启警告

部署过程中，“部署”页中的 **检查中断** 列会指定部署的配置是否在 Firewall Threat Defense 设备上重启 Snort 进程。当名为 *Snort* 进程的流量检测引擎重启时，检测会中断，直到该进程恢复为止。流量将会中断还是在中断期间允许未经检测而通过，取决于设备对流量的处理方式。请注意，您可以继续进行部署，取消部署并修改配置，也可以将部署推迟到部署对网络的影响最低时执行。

当**检查中断**列显示**是**并展开设备配置列表时，系统会以**检查中断**（）指示任何将重启 Snort 进程的特定配置类型。将鼠标指针悬停在图标上时，会显示一条消息，通知您部署配置可能会中断流量。

下表总结了“部署”页面中显示的检测中断警告。

表 *13:* 检测中断指示器

类型	检测中断	说明
Firewall Threat Defense	**检查中断**（）是	至少有一个配置（如果已部署）会中断设备上的检测并可能会中断流量，具体取决于设备对流量的处理方式。展开设备配置列表可以了解详细信息。
	--	部署的配置不会中断设备上的流量。
	未确定	系统无法确定部署的配置是否可能会中断设备上的流量。 进行软件升级后，有些情况下是在呼叫支持期间，首次部署之前会显示“不确定”状态。
	错误（）	系统因内部错误而无法确定状态。 取消操作，然后再次点击**部署 (Deploy)**，以便系统可以重新确定**检测中断 (Inspect Interruption)** 状态。如果问题仍然存在，请与支持人员联系。
sensor	--	被识别为 传感器 的设备不是 Firewall Threat Defense 设备；系统无法确定部署的配置是否会中断此设备上的流量。

有关会为各类设备重启 Snort 进程的所有配置的信息，请参阅部署或激活时重启 Snort 进程的配置，第 176 页。

在策略应用期间检测流量

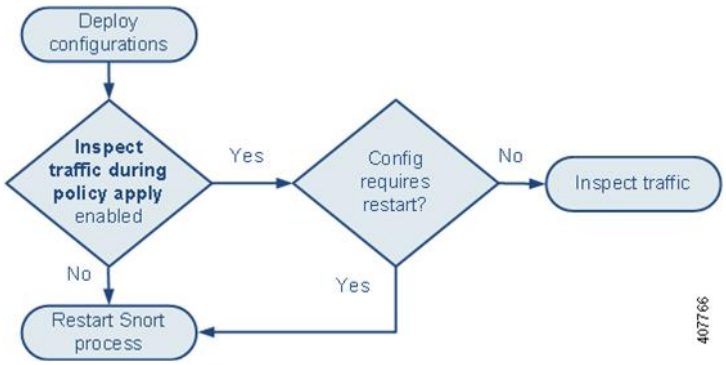
在策略应用期间检查流量是一项高级访问控制策略常规设置，支持托管设备在部署配置更改时检查流量；该设置在部署的配置需要重启 Snort 进程时不适用。可以按如下方式配置此选项：

- 已启用 - 在部署过程中会检查流量，除非某些配置要求重启 Snort 进程。

  当部署的配置不需要 Snort 重启时，系统最初使用当前部署的访问控制策略检查流量，并在部署期间切换到您正在部署的访问控制策略。

- 已禁用 - 部署期间不会检查流量。Snort 进程在您部署时总是会重启。

下图展示了当启用或禁用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 时，Snort 如何重启。



注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。 请参阅Snort 重启流量行为，第 174 页和部署或激活时重启 Snort 进程的配置，第 176 页。

Snort 重启流量行为

下表说明在 Snort 进程重新启动时不同设备处理流量的方式。

表 *14: Firewall Threat Defense* 和 *Firewall Threat Defense Virtual* 重新启动流量影响

接口配置	重启流量行为
内联：**Snort 故障时自动打开：关闭：**禁用	被丢弃
内联：**Snort 故障时自动打开：关闭：**启用	不检查直接通过 在系统识别 Snort 已关闭之前，某些数据包可能会在缓冲区中延迟几秒钟。此延迟可能因负载分布而异。但是，缓冲的数据包最终会通过。

接口配置	重启流量行为
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**启用（**configure snort preserve-connection enable**；默认） 有关详细信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*。	现有 TCP/UDP 流：只要在 Snort 关闭时至少有一个数据包到达，无需检查即可通过 新 TCP/UDP 数据流和所有非 TCP/UDP 数据流：丢弃 请注意，即使启用 **preserve-connection**，以下流量也会丢弃： • 纯文本、与**Analyze**规则操作或**Analyze all tunnel traffic** 默认策略操作匹配的贯通式隧道流量 • 与访问控制规则不匹配，并由默认操作处理的连接。 • 解密的 TLS/SSL 流量 • 安全搜索流量 • 强制网络门户流量
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**禁用 (**configure snort preserve-connection disable**)	被丢弃
内联：分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查

注释 除了当 Snort 进程在重启时关闭这一情况下的流量处理外，在 Snort 进程繁忙时，流量也可不检查直接通过或丢弃，具体取决于 Snort 故障时自动打开**繁忙**选项（请参阅配置内联集，第 841 页）的配置。设备只支持“故障保护”选项或“Snort 故障时自动打开”选项，不同时支持这两个选项。

注释 如果 Snort 进程在部署期间正忙但未关闭，则在 CPU 总负载超过 60% 的情况下，路由式、交换式或透明接口上可能会丢弃某些数据包。

警告 在 Snort 规则更新过程中，请勿重新启动系统。

当 snort 无法足够快速地处理数据包时，会出现 Snort-busy 丢弃。Lina 不知道 Snort 是否由于处理延迟而繁忙，是否卡住或由于呼叫阻塞。当传输队列已满时，发生 snort-busy 丢弃。根据传输队列利用率，Lina 将尝试在队列服务正常时进行访问。

部署或激活时重启 Snort 进程的配置

如下所述，部署以下任何配置（AAB 除外）都会重启 Snort 进程。部署 AAB 不会导致重启，但过多的数据包延迟会激活当前部署的 AAB 配置，从而导致 Snort 进程的部分重启。

访问控制策略高级设置

- 禁用**应用策略期间检查流量**时部署。
- 添加或删除 SSL 策略。

文件策略

首先或最后部署以下任一配置；请注意，尽管以其他方式部署这些文件策略配置不会导致重启，但部署非文件策略配置则可能会导致重启。

- 执行下列操作之一：
  - 当部署的访问控制策略包括至少一个文件策略时，启用或禁用**检查存档**。
  - 当已启用**检查存档**时，添加第一个文件策略规则或删除最后一个文件策略规则（请注意，需要至少一个规则才能使**检查存档**生效）。
- 在 **Detect Files** 或 **Block Files** 规则中启用或禁用 **Store files**。
- 添加第一个将**恶意软件云查找**或**阻止恶意软件**规则操作与分析选项（**Spero 分析**或 **MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**正常**或**自定义**）组合到一起的活动文件规则，或删除最后一个符合上述条件的活动文件规则。

请注意，仅在您的配置满足以下条件时，将这些文件策略配置部署到安全区或隧道区域的访问控制规则才会导致重启：

- 您的访问控制规则中的源或目标安全区必须匹配与目标设备上的接口相关的安全区。
- 除非您的访问控制规则中的目标区域为任何，否则规则中的源隧道区域必须与分配给预过滤器策略中隧道规则的隧道区域相匹配。

身份策略

- 当禁用 SSL 解密时（即，当访问控制策略不包含 SSL 策略时），请添加第一个或删除最后一个主动身份验证规则。

  主动身份验证规则具有**主动身份验证**规则操作或**被动身份验证**规则操作，并且**如果无法建立被动或 VPN 识别，则使用主动身份验证**已选中。

网络发现

- 使用网络发现策略，通过 HTTP、FTP 或 MDNS 协议启用或禁用基于流量的非授权用户检测。

设备管理

- MTU：在设备上的所有非管理接口中更改最高 MTU 值。
- 自动应用旁路 (AAB)：当前部署的 AAB 配置会在 Snort 进程出现故障或设备误配置导致单个数据包使用过多处理时间时激活。结果是Snort进程部分重启，以缓解极高的延迟或防止流量彻底停顿。此部分重启会导致几个数据包在不检查的情况下通过或丢弃，具体取决于设备处理流量的方式。

TLS 服务器身份发现

启用或禁用 **TLS 服务器身份发现** 将导致 Snort 2 重新启动。



注释 启用或禁用 **TLS 服务器身份发现**时，Snort 3 不会重启。

更新

- 系统更新：在包含新版本 Snort 二进制或数据采集库 (DAQ) 的软件更新后首次部署配置。
- 对于运行 Snort 3 的托管设备，在安装漏洞数据库 (VDB) 更新后首次部署配置可能会暂时中断应用检测，但不会出现流量中断。

相关主题

部署配置更改，第 180 页
Snort 重新启动场景，第 172 页

会立即重新启动 Snort 进程的更改

以下更改将立即重新启动 Snort 进程，而不执行部署过程。 重启对流量的影响取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

- 采取以下任何涉及应用或应用检测器的操作：
  - 激活或者停用系统或自定义应用检测器。
  - 删除激活的自定义检测器。
  - **保存并重新激活**已激活的自定义检测器。
  - 创建用户定义的应用。

  系统会提醒您继续操作会重新启动所有托管设备上的Snort进程，并允许您取消；重启会在当前域或其任何子域中的任何托管设备上发生。

- 创建或中断 Firewall Threat Defense 高可用性对。

  消息会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的Snort进程，并允许您取消。

策略管理的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 网络管理员
- 安全审批人

部署配置更改的最佳实践

以下是部署配置更改的准则。

可靠的管理连接

防火墙管理中心 与设备之间的管理连接是一个安全的 TLS-1.3 加密通信通道。

出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

⚠

注意 建议不要通过在设备本身上终止的 VPN 隧道进行设备的管理连接。如果部署的配置更改导致 VPN 关闭，则管理连接将被断开，如果不直接连接到设备，将无法恢复配置。

如果管理流量从 VPN 终端接口流出，请确保将管理流量排除在 VPN 隧道之外。

最大并发部署数

在同一作业中，部署的设备数不应超过 防火墙管理中心 允许的最大设备数的 25%。例如，对于 FMCv300，最大作业大小应为 75 台设备（300 台的 25%）。并发部署到更多设备可能会导致性能问题。

部署共享策略

为获得最佳性能，请部署到使用相同策略的设备。为共享策略的每组设备创建单独的部署作业。

部署时间和内存限制

部署所需的时间取决于多个因素，包括（但不限于）：

- 发送至设备的配置。例如，如果阻止的安全智能条目数显示增加，部署时间可能要长一些。
- 设备型号和内存。内存较低的设备，部署时间可能要长一些。

请勿超过设备的能力。如果超过目标设备所支持的规则或策略最大数量，系统会显示警告。最大值取决于许多因素 - 不仅包括设备内存及处理器的数量，还与策略和规则复杂性有关。有关优化策略和规则的信息，请参阅访问控制规则的最佳实践，第 1758 页。

使用维护窗口减轻流量中断的影响

我们强烈建议在维护窗口或在中断的影响最低时部署。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 174 页和部署或激活时重启 Snort 进程的配置，第 176 页。

对于 Firewall Threat Defense 设备，如果部署中断了流量或检测，“部署”(Deploy) 对话框中的**检测中断 (Inspect Interruption)** 列会显示警告。您可以继续，也可以取消或延迟部署；有关详细信息，请参阅设备的重启警告，第 172 页。

相关主题

Snort 重新启动场景，第 172 页

部署配置

在配置部署后，无论何时对该配置进行更改，您都必须向受影响设备部署更改。您可以在消息中心查看部署状态。

部署会更新以下组件：

- 设备和接口配置
- 与设备相关的策略：NAT、VPN、QoS、平台设置
- 访问控制策略以及相关策略：DNS、文件、身份、入侵、网络分析、预过滤器、SSL
- 网络发现策略
- 入侵规则更新
- 与其中任一元素相关联的配置和对象

您可以将系统配置为自动部署，方法如下：安排一个部署任务，或者将系统设置为在导入入侵规则更新时进行部署。如果允许入侵规则更新修改系统提供的基本策略以进行入侵和网络分析，则自动部署策略的方法尤其有用。入侵规则更新还可修改访问控制策略中高级预处理和性能选项的默认值。

部署配置更改

更改配置后，将其部署到受影响的设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动Snort进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。 请参阅Snort 重启流量行为，第 174 页和部署或激活时重启 Snort 进程的配置，第 176 页。

开始之前

- 确保所有托管设备都使用安全区域对象的相同修订版。如果已编辑安全区域对象：在编辑要同步的全部设备上接口的区域设置前，请勿将配置更改部署到任何设备。您必须同时部署到所有托管设备。。
- 要预览部署更改，请启用 REST API 访问。要启用 REST API 访问，请执行*Cisco Secure Firewall Management Center* 管理指南中启用 *REST API* 访问中的步骤。

注释 如果在部署过程中正在通过设备CLI读取设备配置，则部署过程将失败。请勿在部署期间执行命令，例如 **show running-config**。

过程

步骤 1 在 防火墙管理中心 菜单栏上，点击**部署 (Deploy)**。

步骤 2 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**，或者点击**全部部署 (Deploy All)** 以部署到所有设备。否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

此程序的其余部分适用于**高级部署 (Advanced Deploy)** 屏幕。

图 *34:* 快速部署

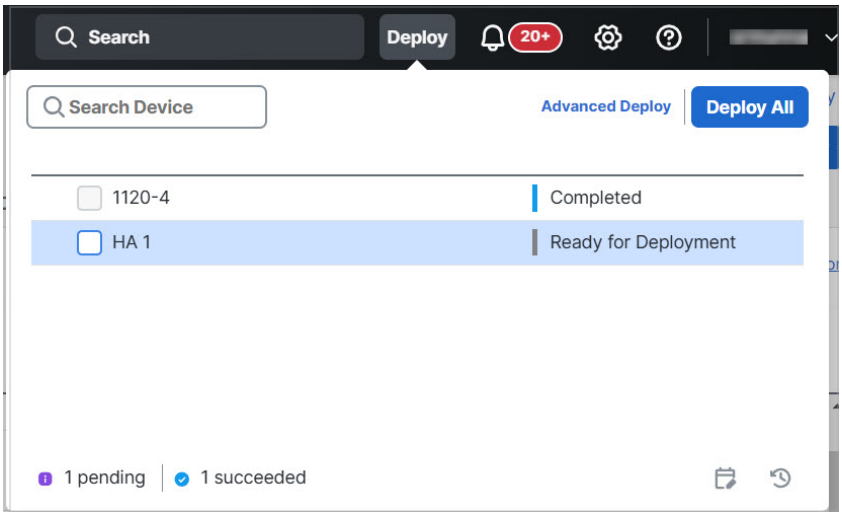
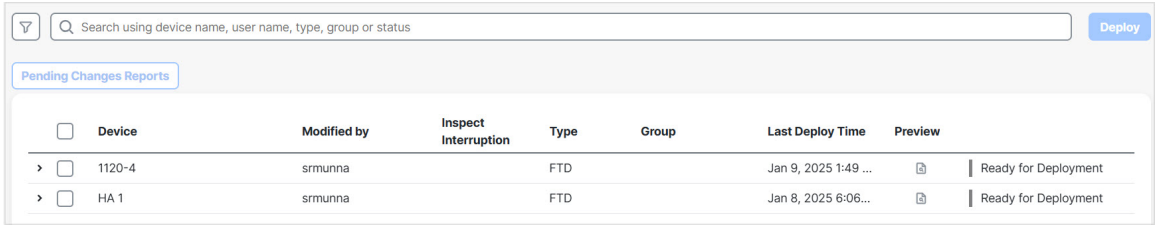
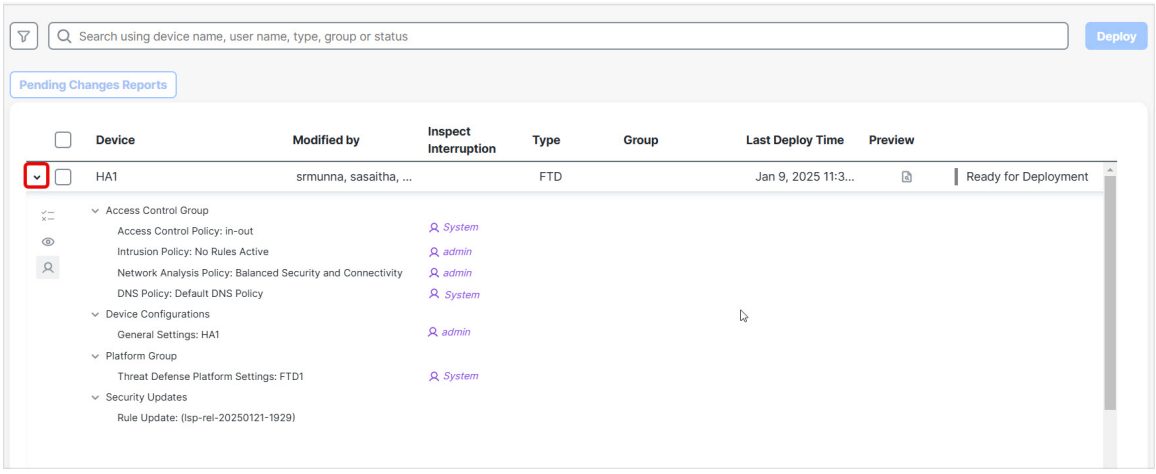


图 *35:* 高级部署



步骤 3 点击 **展开箭头**（**>**） 以查看要部署的设备特定的配置更改。

图 *36:* 扩展



- **修改者**列列出了修改策略或对象的用户。展开设备列表时，您可以参照每个策略列表查看修改了策略的用户。有关何时显示**系统**用户（而不是已登录用户）的信息，请参阅系统用户名，第 171 页。

注释
没有为已删除的策略和对象提供用户名。

- **检查中断**列指示在部署过程中是否可能导致设备中的流量检查中断。

  当状态指示（是）部署会中断 Firewall Threat Defense 设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（ ） 指示导致中断的特定配置。

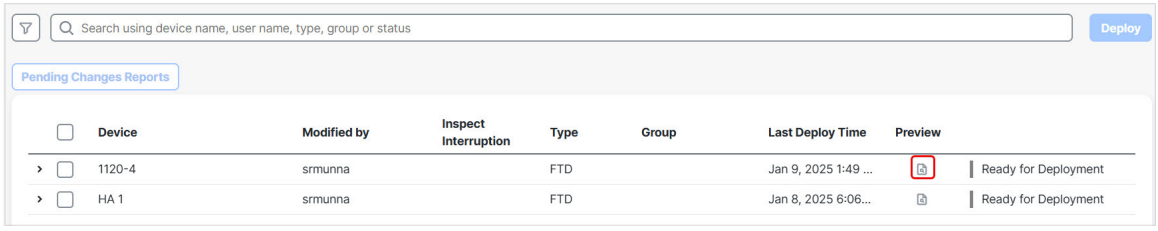
  如果设备的此列中这一条为空白，则表明在部署过程中该设备上不会出现流量检查中断。

  请参阅 设备的重启警告，第 172 页 中的信息，可帮助您识别在部署到 Firewall Threat Defense 设备时会中断流量检查并可能中断流量的配置。

- **上次修改时间**列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。
- **状态**列提供每个部署的状态。有关详细信息，请参阅查看部署状态，第 187 页。

步骤 4 在**预览 (Preview)** 列中，点击 **预览** ( ) 以查看可以部署的配置更改。

图 *37:* 预览

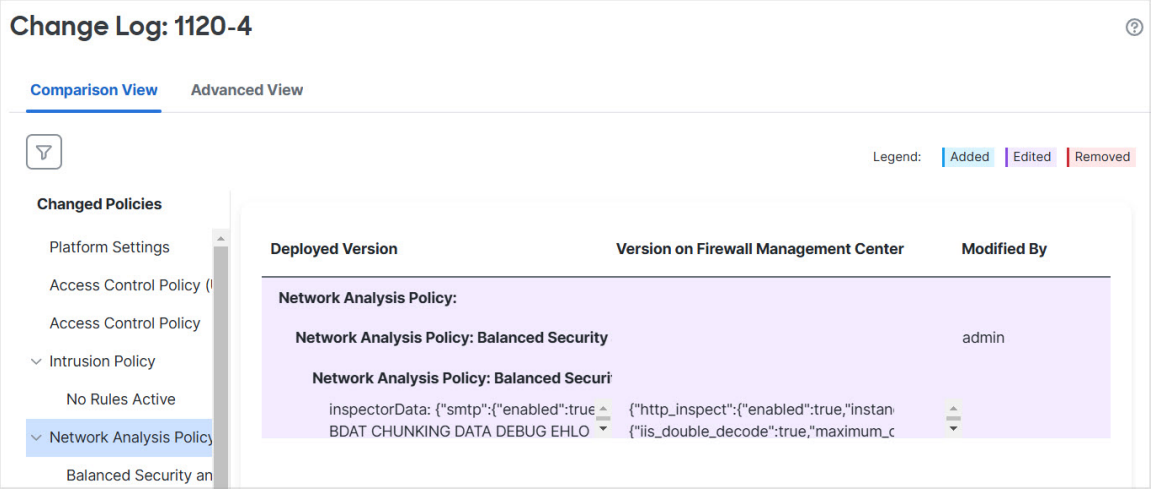


注释
如果您在 **管理** > **配置** > **信息** 中更改 防火墙管理中心 名称，则部署预览不会指定此更改，但它需要部署。

有关预览不支持的功能，请参阅部署预览，第 168 页。

比较视图 (Comparison View) 选项卡列出了所有策略和对象更改。左侧窗格以树状结构组织列出设备中更改的所有不同策略类型。

图 *38:* 比较视图



过滤器（ ） 允许您在用户级别和策略级别过滤策略。

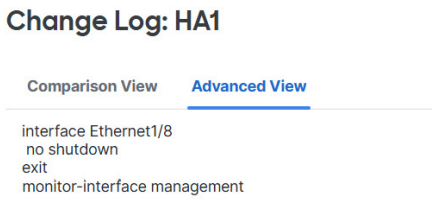
左侧窗格中列出策略中的所有添加、更改或删除项，或者在左侧窗格中选择的对象。右侧窗格中的两个列提供上次部署的配置设置（在 **“部署版本”** 列中）与应该部署的更改（在 **“待处理版本”** 列中）。上次部署的配置设置源自防火墙管理中心中上次保存的部署的快照，而不是来自设备。设置的背景颜色根据页面右上角的图例分类显示。

修改者 (Modified By) 列列出了修改或添加了配置设置的用户。在策略级别， 防火墙管理中心 显示所有修改过策略的用户，而在规则级别， 防火墙管理中心 只显示最后修改规则的用户。

您可以点击**下载报告 (Download Report)** 按钮下载更改日志的副本。

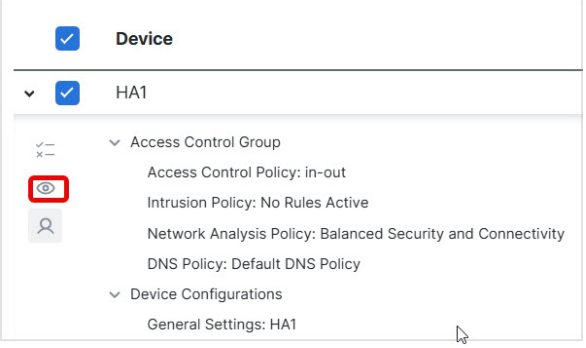
高级视图 (Advanced View) 选项卡显示将应用的 CLI 命令。如果您熟悉用于 Firewall Threat Defense 后端的 ASA CLI，则此视图非常有用。

图 *39:* 高级视图



步骤 5 使用 **显示或隐藏策略** （ ） 可选择性地查看或隐藏关联的未修改策略。

图 *40:* 显示或隐藏策略



步骤 6 选中设备名称旁边的复选框以部署所有配置更改，或点击 **策略选择**（ ） 以选择部署个别策略或配置，而保留其余的更改不予部署。

您也可以使用此选项查看特定策略或配置之间相互依赖的更改。防火墙管理中心 动态检测策略之间的依赖关系（例如，访问控制策略和入侵策略之间），以及共享对象和策略之间的依赖关系。相互依赖的更改以彩色标记表示，以指定一组相互依赖的部署更改。选择一个部署更改时，相互依赖的更改将自动选中。

有关详细信息，请参阅选择性策略部署，第 169 页。

注释

- 部署共享对象的更改后，受影响的策略也应随其一起部署。在部署过程中选择共享对象时，受影响的策略会自动选中。
- 计划部署和使用 REST API 的部署不支持选择性部署。在这些情况下，您只能选择完全部署所有更改。
- 部署前对警告和错误的检查不仅在所选策略上执行，还在所有过期的策略上执行。因此，警告或错误列表也显示取消选择的策略。
- 同样，“部署”页上**检查中断**列的指示会考虑所有过时的策略，而不仅是选定的策略。有关**检查中断**列的信息，请参阅设备的重启警告，第 172 页。

步骤 7 选择要部署的设备或策略后，点击**估计 (Estimate)** 以粗略估计部署持续时间。

图 *41:* 估价

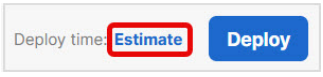
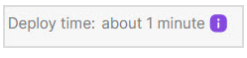


图 *42:* 部署时间



持续时间是一个粗略估计值（精确度约为 70%），在少数情况下，部署所花费的实际时间可能有所不同。如果部署不超过 20 台设备，该估计值是可靠的。

当估计值不可用时，表示数据不可用，因为所选设备上的第一次成功部署还未完成。这种情况可能发生在 防火墙管理中心 重新映像、版本升级或高可用性故障转移之后。

注释
当批量更改策略（在批量策略迁移的情况下）和选择性部署时，估计值不正确且不可靠，因为估计值基于启发式技术。

步骤 8 点击**部署 (Deploy)**。

步骤 9 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。选中**忽略警告 (Ignore warnings)** 复选框，以忽略警告并部署更改。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

- （可选）监控部署状态；请参阅*Cisco Secure Firewall Management Center* 管理指南中的查看部署消息。
- 如果部署失败，请参阅部署配置更改的最佳实践，第 178 页。
- 在部署期间，如果部署中存在特定的配置更改，则部署失败可能导致流量中断。例如，在集群环境中，接口上配置的 IP 地址与站点 IP 不在同一子网中。由于此错误，部署会失败，并且设备会在处理回滚操作时尝试清除配置。这些事件会共同导致部署失败，从而中断流量。

  请参阅下表，了解在部署失败时可能导致流量中断的配置更改。

配置更改	存在？	流量受影响？
访问控制策略中的**威胁防护服务**更改	支持	支持
VRF	支持	支持
接口	支持	支持
QoS	支持	支持

注释 仅当 防火墙管理中心 和 Firewall Threat Defense 版本为 6.2.3 或更高版本时，部署期间中断流量的配置更改才是有效的。

相关主题

Snort 重新启动场景，第 172 页

将现有配置重新部署到设备

可以将现有（未改变）的配置强制部署到单台托管设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动Snort进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。 请参阅Snort 重启流量行为，第 174 页和部署或激活时重启 Snort 进程的配置，第 176 页。

开始之前

查看部署配置更改的最佳实践，第 178 页中所述的准则。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要强制部署的设备旁边的 **编辑** (✎) 。

步骤 3 点击**设备 (Device)**。

步骤 4 点击 **常规** 部分标题旁边的 **编辑** (✎) 。

步骤 5 请点击 **强制部署** (→)。

注释
强制部署比常规部署需要更多时间，因为它涉及要在 Firewall Threat Defense 上部署的策略规则的完整生成。

步骤 6 点击**部署 (Deploy)**。

系统会识别出您正在部署的配置中的所有错误或警告。您可以点击**继续**继续，而不解决警告状况。但是，如果系统识别到错误，则无法继续。

下一步做什么

- （可选）监控部署状态；请参阅*Cisco Secure Firewall Management Center* 管理指南中的 查看部署消息 。
- 如果部署失败，请参阅部署配置更改的最佳实践，第 178 页。

相关主题

Snort 重新启动场景，第 172 页

管理部署

查看部署状态

在“部署”页上，**状态**列提供每个设备的部署状态。如果正在进行部署，则会显示部署进度的实时状态，否则会显示以下状态之一：

- 待处理 - 表示设备中有要部署的更改。
- 警告或错误 - 表示部署前检查已发现部署的警告或错误之处，而且您没有继续部署。如果出现任何警告，可以继续进行部署，但如果有任何错误，则不能继续。



注释 “状态”列仅提供“部署”页上单个用户会话的警告或错误状态。如果您离开或刷新该页面，状态将变为“待处理”。

- 失败 - 表示先前的部署失败。点击状态以查看详细信息。
- 排队中 - 表示部署已启动，而系统尚未开始部署过程。
- 已完成 - 表示部署已成功完成。

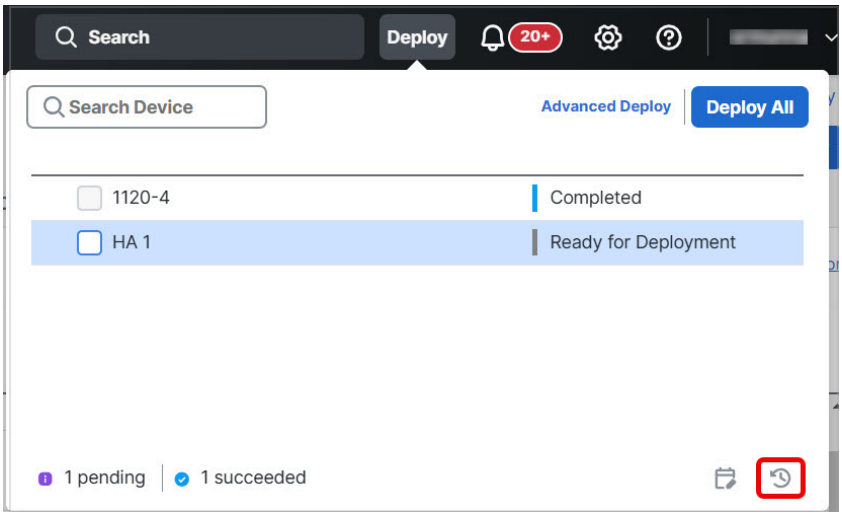
查看部署历史记录

在部署历史记录中，将捕获最近 10 次成功部署、最近 5 次失败部署以及最近 5 次回滚部署。

过程

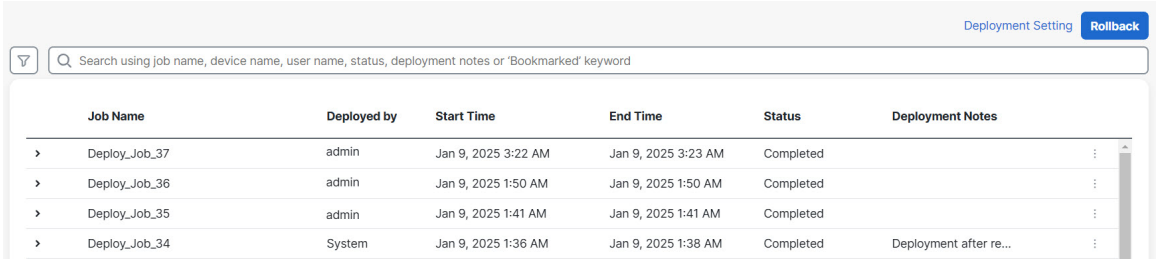
步骤 1 在 防火墙管理中心 菜单栏上，点击**部署 (Deploy)**，然后点击 **部署历史记录** ()。

图 *43:* 部署历史记录图标



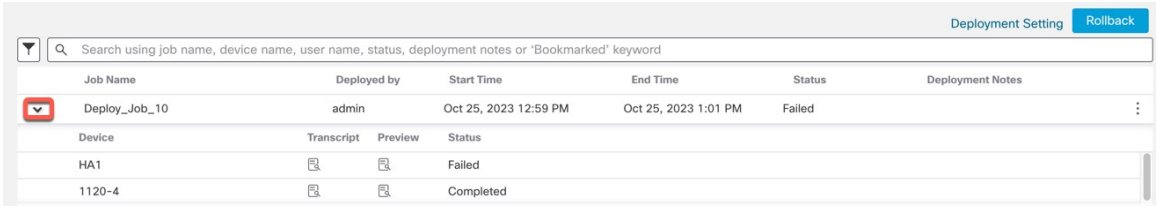
所有先前部署和回滚作业的列表按时间倒序显示。

图 *44:* 部署历史记录页面



步骤 2 点击所需部署作业旁边的 **展开箭头**（›），以便查看作业中包含的设备及其部署状态。

图 *45:* 扩展



- 查看**部署说明 (Deployment Notes)** 列中的说明。

  部署说明是用户可以在部署过程中添加的自定义说明，而这些说明是可选的。

步骤 3 （可选）点击 **脚本详细信息** （ ）以查看发送到设备的命令以及收到的响应。

图 *46:* 脚本详细信息图标

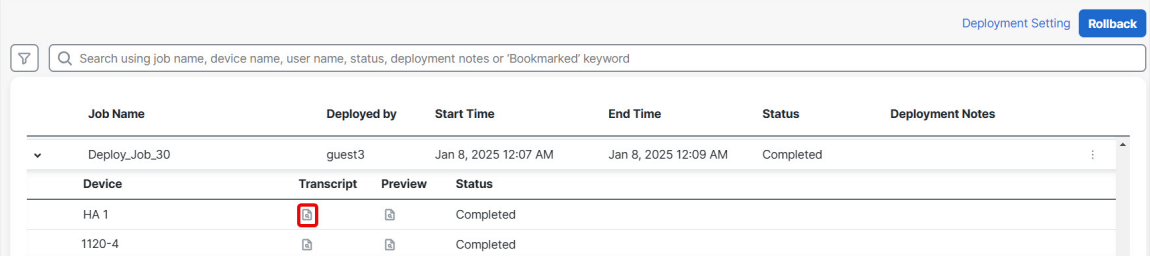
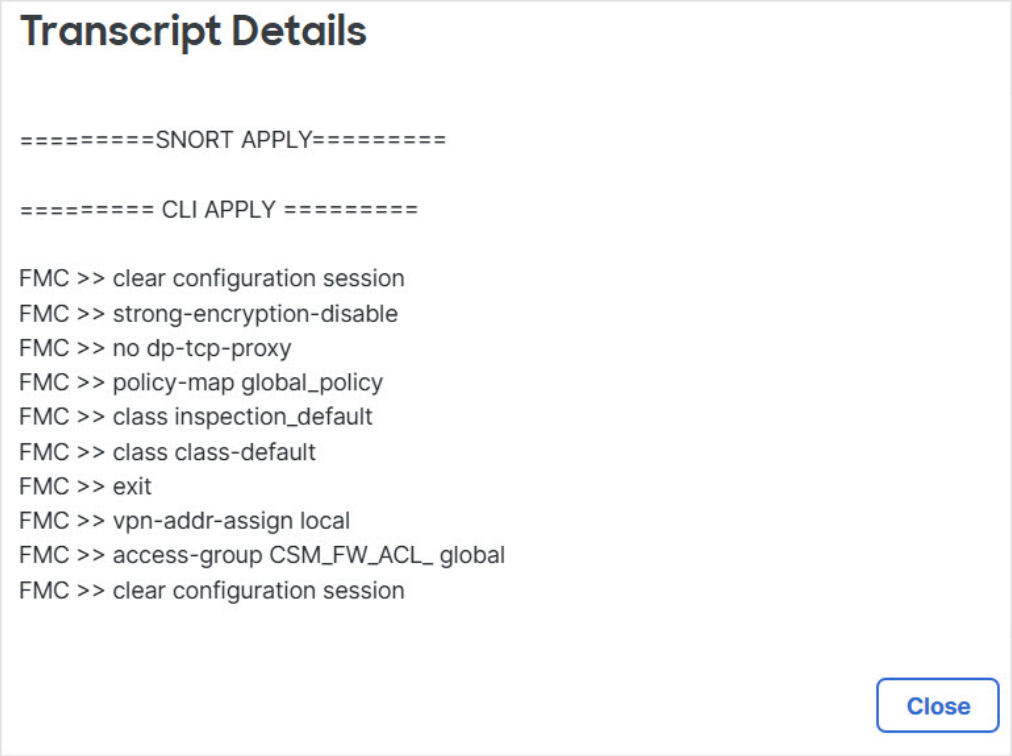


图 *47:* 脚本详细信息



该脚本包含以下各节：

- **Snort 应用 (Snort Apply)** - 如果 Snort 相关的策略中有任何故障或响应，则此部分中会显示消息。通常，该部分为空。
- **CLI 应用 (CLI Apply)** - 此部分涵盖使用发送到设备的命令配置的功能。

  注释
  回滚操作的脚本不会提供 CLI 命令信息。要查看回滚命令，请参阅查看部署回滚脚本，第 196 页。

- **Infrastructure Messages** - 此部分显示不同部署模块的状态。

在 **CLI 应用 (CLI Apply)** 部分中，部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示命令错误的消息。如果您正在使用 FlexConfig 策略配置自定义的功能，则检查这些错误特别有用。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释
为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

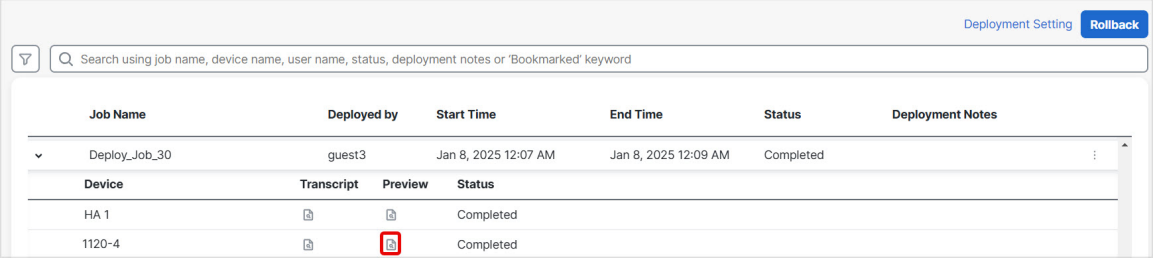
例如，以下序列显示防火墙管理中心 发送了命令来为 GigabitEthernet0/0 配置**外部**逻辑名。设备的响应是自动将安全级别设置为 0。Firewall Threat Defense 不会将安全级别用于任何操作。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

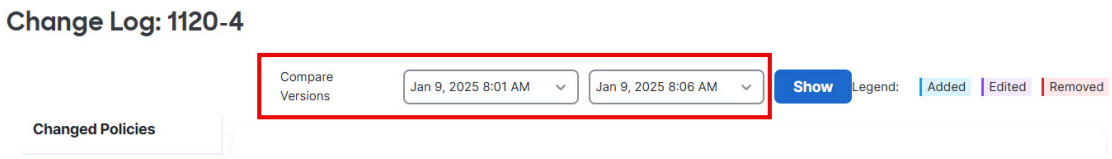
步骤 4 （可选）点击**预览** ()以查看设备上部署的策略和对象更改与之前部署的版本。

图 *48:* 预览图标



1. 要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。下拉框会显示部署作业名称和部署结束时间。

   图 *49:* 比较版本

   注释
   下拉框还会显示失败的部署。

2. **修改者**列列出了修改策略或对象的用户。
   1. 在策略级别，防火墙管理中心 会显示已修改策略的所有用户名。
   2. 在规则级别，防火墙管理中心 会显示最后修改规则的用户。

3. 您还可以点击**下载为报告 (Download Report)** 按钮下载更改日志的副本。

注释

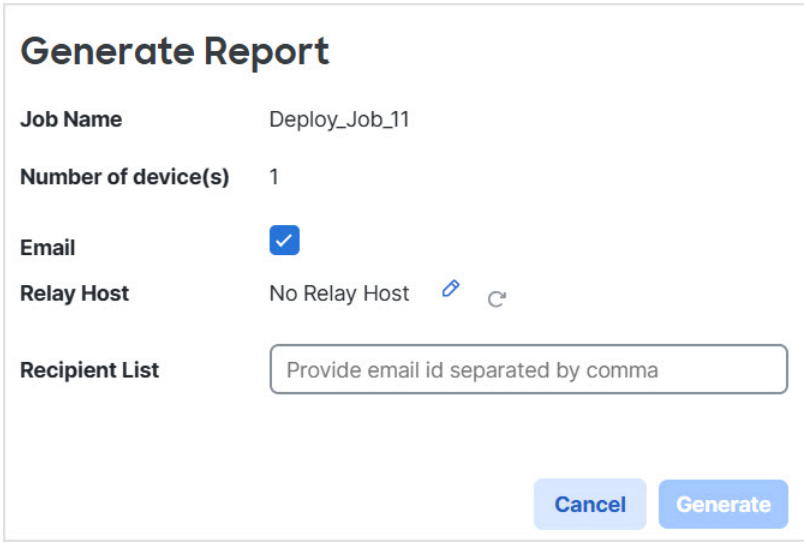
- 认证登记、HA 操作和失败的部署不支持部署历史记录预览。
- 注册设备后，创建的作业历史记录不支持预览。

步骤 5 （可选）针对每个部署作业，点击 **更多** (⋮) 图标并执行其他操作：

- **书签 (Bookmark)** - 为部署作业添加书签。
- **编辑部署说明 (Edit Deployment Notes)** - 编辑为部署作业添加的自定义部署说明。
- **生成报告 (Generate Report)** - 生成可用于审核的部署报告。此报告包括具有预览和脚本信息的作业属性，并且报告可以作为 PDF 文件下载。

1. 点击**生成报告 (Generate Report)** 以再次生成报告。

   图 *50:* 生成报告



2. 在**生成报告 (Generate Report)** 弹出窗口中，选中**邮件 (Email)** 复选框。
3. 如果配置了邮件中继主机，也可以通过邮件发送报告。如果未配置邮件中继主机，请使用**编辑** (✎) 图标来配置或修改邮件中继主机。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的配置邮件中继主机和通知地址。
4. 在**收件人列表 (Recipient List)** 中，您可以输入多个邮件地址并以分号分隔。
5. 点击**生成 (Generate)** 以生成报告，然后此报告将通过邮件发送给收件人。
6. 在“通知任务”(Notifications task) 选项卡中，您可以跟踪进度。完成报告生成后，点击通知任务选项卡中的链接以下载 PDF 报告。

设置配置版本数

防火墙管理中心 将设备配置文件历史记录作为配置版本存储在磁盘上。您可以指定要为每台设备保留的配置版本数。此设置允许您估计磁盘上设备配置文件的大小，并将其保持在允许的限制内。减少配置版本的数量可以减少备份大小并提高 防火墙管理中心 HA 同步速度。

在 防火墙管理中心 高可用性部署中，配置版本设置仅在主用 防火墙管理中心上可用。

开始之前

版本 7.4.0 不支持此功能。

过程

步骤 1 在 防火墙管理中心 菜单栏上，选择 **部署** > **部署历史记录** ()。

步骤 2 点击 **部署设置**。

步骤 3 从 **要保留的版本数** 下拉列表中选择要为每台设备保留的配置版本数。

注释
减少版本数量会删除最早的配置版本，以匹配您选择的版本大小。您无法回滚或预览已删除的版本。

- **最大允许磁盘大小**：用于存储配置版本的最大大小为 20 GB。 防火墙管理中心 会定期计算配置版本的大小，并在配置版本的大小超过 20 GB 时发送运行状况警报。要解决运行状况警报，请选择估计配置版本大小小于 20 GB 的 **要保留的版本数** 。
- **当前配置版本大小**：上一次在 防火墙管理中心 部署的配置文件的大小。
- **估计配置版本大小**： 防火墙管理中心上配置文件的大致大小。它是根据您选择保留的配置版本数计算的。

步骤 4 点击**保存**。

回滚部署

您可以将设备回滚到以前部署的配置。在策略部署后，如果通过设备的流量以非预期方式受到影响，则回滚提供了一个选项，可将设备恢复到故障部署之前存在的较早状态。

回滚为中断操作：所有现有的连接和路由都会被丢弃，并且流量会中断。

识别破坏性配置

如果部署出现问题并以非预期方式导致流量中断，您应确定导致该情况的部署更改并进行修复，下次部署将成功。

请参阅以下方法来比较配置。

回滚之前

1. 请选择**部署 (Deploy)** > **部署历史记录 (Deployment History)**，展开上一个部署的作业（导致流量中断的作业），然后点击 **预览** ()。

   预览页面提供了一个用于比较部署的选项，可用于识别与先前部署相比的部署的特定更改。

2. 确定导致问题的更改后，请纠正配置并将其重新部署到设备上。

回滚之后

1. 成功执行回滚操作后，选择 **部署** > **部署**，然后点击回滚设备旁边的 **预览** 图标。
2. 查看回滚配置和待定部署 防火墙管理中心 中的当前更改之间的更改。
3. 确定导致问题的更改后，请纠正配置并将其重新部署到设备上。

回滚准则和限制

- 您可以回滚到当前部署的版本之前的最后10个版本中的任何一个。不支持回滚到之前的版本。对于不支持的版本，回滚图标将呈灰色显示。
- 您必须先执行部署，然后才能再次回滚。
- 执行回滚后，回滚的设备在 防火墙管理中心上标记为过期。您对配置所做的更改仍在等待下一次部署。要查看待处理的更改，请选择 **部署** > **部署**，然后点击回滚设备旁边的 **预览** 图标。
- 对于访问列表非常大的设备，如果**对象组搜索** 设置被禁用，回滚操作可能需要更长时间才能完成。要验证**对象组搜索**设置，请选择 **设备** > **设备管理**，然后选择设备并点击**编辑高级设置**。
- 对于 Firepower 4100/9300，请确保任何回滚版本的当前 防火墙机箱管理器 接口配置都相同。否则，回滚接口配置可能与您的实际接口不匹配。
- 如果回滚版本和当前版本的管理器访问接口（管理器或数据接口）不同，则不支持回滚。
- 独立认证登记也会在“部署历史记录”(Deployment History) 页面中列为部署作业。但是，您无法回滚到这些版本。从证书注册后创建的部署版本回滚也会恢复证书关联。在回滚后的下一次部署中，请在继续部署之前手动关联证书。
- 如果您升级 防火墙管理中心，则以前软件版本的所有回滚版本都将不再可用于设备，即使您没有升级设备。
- 如果升级设备，则只能回滚到当前软件版本的版本。
- 如果回滚了 FlexConfig 对象且部署频率被设为**一次**的设备的部署，则您将无法重新部署该对象，即使该对象在“预览”(Preview) 页面上显示为过期。在回滚后，您必须手动取消分配，然后在下一次部署之前将 FlexConfig 对象重新分配给设备。
- 对于高可用性，以下场景不支持回滚：
  - 当要回滚到的版本包含高可用性引导程序配置时。换句话说，首次为独立设备形成高可用性时的部署。
  - 当前处于独立模式的设备是先前部署版本中高可用性对的一部分时。

- 有关集群，请参阅以下准则：
  - 当前处于独立模式的设备是先前部署版本中集群的一部分时，回滚不受支持。
  - （Cisco Secure Firewall 3100/4200 和私有云中的 Firewall Threat Defense Virtual ）如果更改集群引导程序配置或添加或删除节点，则无法回滚到这些更改之前的版本。

在回滚之后未恢复的配置

回滚会恢复设备上的所有配置，但个别配置除外。有关详细信息，请参阅下表。

在回滚期间已恢复的配置	在回滚期间未恢复的配置
• 所有策略配置 • 接口配置 • SRU 配置 • VDB 配置 • LSP 配置 • VPN 配置 • FXOS 配置	• Snort 二进制文件 • 地理位置数据库

执行回滚

您可以将设备回滚到以前部署的配置。在策略部署后，如果通过设备的流量以非预期方式受到影响，则回滚提供了一个选项，可将设备恢复到故障部署之前存在的较早状态。

回滚仅恢复所选设备上的配置。

过程

步骤 1 选择 **部署 >部署历史记录** ()。

所有先前部署作业的列表将按时间倒序显示。

步骤 2 点击**回滚 (Rollback)**。

步骤 3 通过点击 **作业** 并从 **所选作业** 下拉列表中选择作业，或者选择 **设备列表**来过滤显示的设备列表。

步骤 4 （可选） 在 **搜索设备** 搜索框中输入设备名称，以便过滤设备列表。

步骤 5 选中要回滚的设备旁边的复选框，然后从 **回滚版本** 下拉列表中选择每个设备的版本。

图 *51:* 所选作业列表

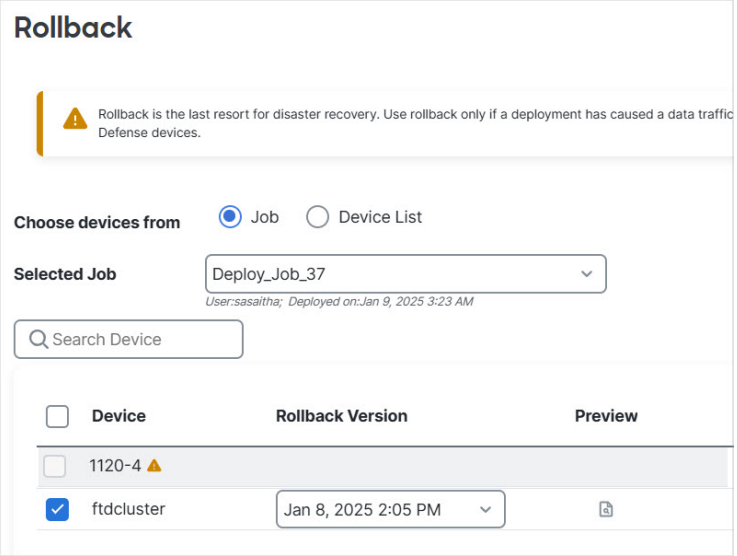
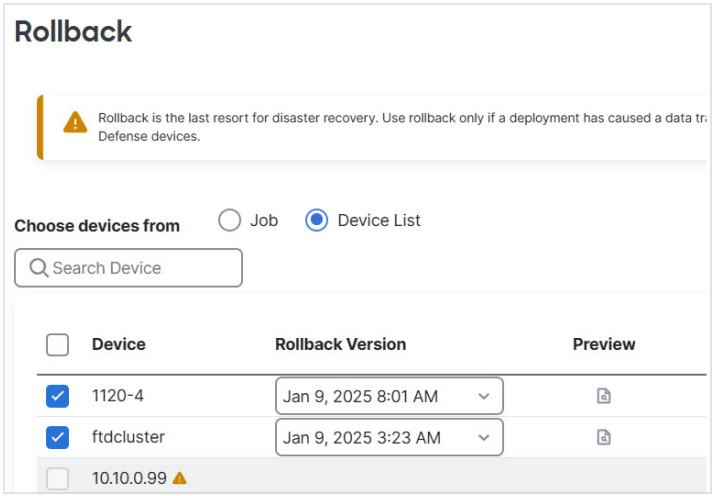


图 *52:* 设备列表



此外，还会列出特定回滚版本的作业名称和关联的部署说明。

步骤 6 （可选） 点击 **预览** (🔍) 查看所选版本中部署的更改。

步骤 7 点击**回滚 (Rollback)**。

下一步做什么

要了解回滚的状态，请选择**部署 (Deploy)** > **部署 (Deployment)**。您可以在设备名称旁边查看回滚状态。

查看部署回滚脚本

回滚脚本是发送到设备的命令以及从设备返回的响应的书面版本。如果回滚操作失败，可以点击 **部署 (Deploy)**，然后点击 **部署历史记录** ()([])来查看失败原因。但是，要了解为成功执行回滚操作而执行的CLI命令，请在回滚操作完成后执行以下步骤。请注意，这些信息仅在下一次部署之前可用。



注释 CLI 命令信息在回滚完成后并且仅在下一次部署之前可用。回滚操作后的第一次部署会清除所有与回滚相关的信息。



注释 对于任何回滚部署，部署说明会随回滚作业自动更新。在**部署历史记录 (Deployment History)** 页面中，用户可以使用“搜索”(Search) 选项轻松过滤回滚作业。

过程

步骤 1 在 Secure Firewall Management Center 菜单栏上，选择 > **运行状况** > **监控器故障排除** 。

步骤 2 从左窗格中选择已回滚的设备。

步骤 3 点击**查看系统和故障排除详细信息 (View System & Troubleshooting Details)** 链接。

步骤 4 点击**高级故障排除 (Advanced Troubleshooting)**。

步骤 5 点击**威胁防御 CLI (Threat Defense CLI)**。

步骤 6 从**命令 (Command)** 下拉框中选择 **show**。

步骤 7 在**参数 (Parameter)** 字段中输入 **`running`**。

步骤 8 点击**执行 (Execute)**

下载多个设备的策略更改报告

下载有关自上次部署多台设备以来所做 Firewall Threat Defense 的策略和对象更改的报告。您可以以包含以下报告的 zip 文件的形式下载报告：

- 每台设备的待处理变更报告，在其中预览策略中的添加、更新或删除，或将在设备上部署的对象。有关详细信息，请参阅 部署配置更改，第 180 页 和 部署预览。
- 根据报告状态对每台设备进行分类的合并报告。

过程

步骤 1 选择 **部署** > **高级部署**。

步骤 2 选中要为其生成待处理策略更改报告的设备旁边的复选框，然后点击 **待处理更改报告**。

步骤 3 点击 **待处理更改报告**。报告在后台生成。

步骤 4 在 防火墙管理中心 菜单栏上，选择 **通知** > **任务** 以查看报告生成任务。

报告请求任务完成后，下载链接将显示在任务通知中。

步骤 5 点击 **下载报告** 链接以下载报告。

比较策略

要查看策略更改是否符合您的组织的标准或优化系统性能，您可以检查两个策略之间的区别，或者已保存策略和正在运行策略之间的区别。

您可以比较以下策略类型：

- DNS
- 文件
- 健康状况
- 身份
- 网络分析
- SSL

比较视图以并排形式显示两个策略。突出显示两个策略之间的差异：

- 蓝色表示两个策略中此突出显示的设置存在不同，并且用红色文本注明其不同之处。
- 绿色表示突出显示的设置出现在一个策略中但未出现在另一个策略中。

开始之前

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能比较策略。

过程

步骤 1 访问要比较的策略的管理页面：

- DNS - **策略** > **安全策略** > **DNS**
- 文件 - **策略** > **安全策略** > **恶意软件和文件**
- 运行状况 - **故障排除** > **+ 显示更多** > **运行状况** > **策略**
- 身份 - **策略** > **安全策略** > **身份**

- 网络分析 (Network Analysis) -**策略** > **安全策略** > **访问控制**，然后点击 **网络分析策略 (Network Analysis Policy)** 或 **策略** > **安全策略** > **入侵**，然后点击 **网络分析策略 (Network Analysis Policies)**。

  注释
  如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略** > **安全策略** > **解密**

步骤 2 点击**比较策略 (Compare Policies)**。

步骤 3 从**对比 (Compare Against)** 下拉列表中，选择要进行的比较类型：

- 要比较两个不同的策略，请选择**其他策略 (Other Policy)**。
- 要比较同一策略的两个版本，请选择**其他版本 (Other Revision)**。
- 要将其他策略与当前有效的策略进行比较，请选择**运行配置 (Running Configuration)**。

步骤 4 根据所选的比较类型，您将具有以下选项：

- 如果要比较两个不同的策略，请从**策略 A (Policy A)** 和**策略 B (Policy B)** 下拉列表中选择要比较的策略。
- 如果要比较运行配置与其他策略，请从**策略 B (Policy B)** 下拉列表中选择第二个策略。

步骤 5 点击**确定**。

步骤 6 查看比较结果：

- 比较查看器 - 要使用比较查看器逐个浏览策略差异，请点击标题栏上方的**上一个 (Previous)**或**下一个 (Next)**。
- 比较报告 - 要生成 PDF 报告来列出两个策略之间的差异，请点击**比较报告 (Comparison Report)**。

生成当前策略报告

对于大多数策略，可以生成两种报告。有关单个策略的报告提供该策略的当前已保存配置的详细信息，而比较报告仅列出两个策略之间的区别。您可以为运行状况策略之外的所有策略类型生成单策略报告。



注释 入侵策略报告将基本策略中的设置与策略层的设置组合在一起，不区分源自基本策略或策略层的设置。

开始之前

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能生成策略报告。

过程

步骤 1 访问要为其生成报告的策略的管理页面：

- 访问控制 -**策略** > **安全策略** > **访问控制**
- DNS - **策略** > **安全策略** > **DNS**
- 文件 - **策略** > **安全策略** > **恶意软件和文件**
- 运行状况 - **故障排除** > **+ 显示更多** > **运行状况** > **策略**
- 身份 - **策略** > **安全策略** > **身份**
- 入侵 - **策略** > **安全策略** > **入侵**
- NAT-**策略** > **网络策略** > **NAT**
- 网络分析 -**策略** > **安全策略** > **访问控制**，然后点击 **网络分析策略** 或 **策略** > **安全策略** > **入侵**，然后点击 **网络分析策略**

  注释
  如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略** > **安全策略** > **解密**

步骤 2 点击要生成报告的策略旁边的**报告** ( )。

配置部署的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
设置为设备回滚保留的部署历史文件数量。	7.2.6 7.4.1	任意	现在可以设置为设备回滚保留的部署历史文件数量，最多为 10 个（默认值）。这样可以帮助你节省防火墙管理中心的磁盘空间。 新增/修改的屏幕：**部署** > **部署历史** > **部署设置** > **配置版本设置**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
查看并生成有关自上次部署以来的配置更改的报告。	7.2.6 7.4.1	任意	您可以生成、查看和下载（作为 zip 文件）以下关于上次部署后配置更改的报告： • 每台设备的策略变更报告，在其中预览策略中的添加、变更或删除，或将在设备上部署的对象。 • 根据策略变更报告生成的状态对每台设备进行分类的合并报告。 这在升级防火墙管理中心或Firewall Threat Defense后尤其有用，这样就能在部署前看到升级所做的更改。 新增/修改的屏幕：**部署 (Deploy)** > **高级部署 (Advanced Deploy)**。
在部署配置更改时生成报告并通过邮件发送。	7.2	任意	您现在可以为任何部署生成报告。 新增/修改的屏幕：**部署** > **部署历史图标** > **更多** > **生成报告**
部署预览和预览中的用户信息。	7.0	任意	“部署”(Deployment) 页面具有以下新添加的功能： • 在**部署 (Deployment)** 页面上，**修改者 (Modified By)** 列会根据每个策略列表列出已修改策略的用户。 • 过滤器部署支持 - **部署 (Deployment)** 页面上的过滤器图标会提供一个选项，用于过滤待部署的设备列表。过滤器图标提供了根据所选设备和用户名过滤列表的选项。 • 部署历史预览 - 点击**预览 (Preview)** 以查看设备上部署的策略和对象更改与之前部署的版本。在部署历史记录中，将捕获最近 10 次成功部署、最近 5 次失败部署以及最近 5 次回滚部署。 • 部署说明 - **部署说明 (Deployment Notes)** 是用户可以在部署过程中添加的自定义和可选说明。您可以在**部署历史记录 (Deployment History)** 页面中查看**部署说明 (Deployment Notes)** 列。 • 部署回滚也可用于 Snort 3 策略。
在 Firewall Threat Defense 设备上回滚部署。	6.7	6.7	回滚是一种部署功能，用于删除 Firewall Threat Defense 设备上的现有部署，并可以使用以前部署的配置来重新配置设备。 新增/修改的页面：**部署 (Deploy)** > **部署历史 (Deployment History)** 页面提供了一个带有回滚图标的新回滚列。展开作业时也会看到类似的回滚图标，以便在设备级别启动回滚。

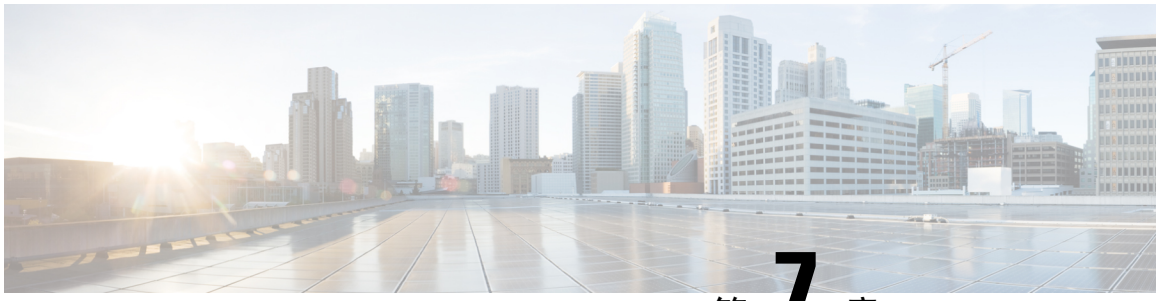
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
新部署 Web 界面。	6.6	任意	防火墙管理中心 菜单栏上的**部署 (Deploy)** 按钮更改为**部署 (Deploy)** 菜单。它下面包含两个新的子菜单选项。这些是**部署 (Deployment)** 和**部署历史 (Deployment History)**。“部署”(Deployment) 页面经过改进，添加了新功能，新的“部署历史”(Deployment History) 页面提供所有以前部署的图例。 “部署”(Deployment) 页面具有以下新添加的功能： • 部署状态 - 在“部署”(Deployment) 页上，状态列提供每个设备的部署状态。 • 部署估计 - 选择设备、策略或配置后，“部署”(Deployment) 页上将提供**估计 (Estimate)**链接。点击**估计 (Estimate)** 链接后会显示部署持续时间的估计值。 • 部署预览 - 预览可提供要在设备上部署的所有策略和对象更改的快照。策略更改包括新策略、现有策略的更改以及已删除的策略。对象更改包括策略中使用的已添加和修改的对象。 • 选择性策略部署 - 防火墙管理中心 允许您在设备上应该部署的所有更改的列表内选择特定的策略，并只部署所选的策略。



第 II 部分

高可用性和可扩展性

- 多实例模式， 第 205 页
- Firepower 4100/9300 上的逻辑设备， 第 273 页
- 设备的高可用性， 第 333 页
- 群集技术：Cisco Secure Firewall 3100/4200/6100， 第 373 页
- 群集技术：私有云， 第 447 页
- 群集技术：公共云， 第 501 页
- 集群：Firepower 4100/9300， 第 637 页



第 7 章

多实例模式

您可以将 Cisco Secure Firewall 3100/4200 作为单个设备（设备模式）或多个容器实例（多实例模式）进行部署。本章介绍如何在多实例模式下部署设备。

- 关于多实例模式， 第 205 页
- 实例的许可证， 第 218 页
- 实例的要求和前提条件， 第 218 页
- 实例的准则和限制， 第 220 页
- 配置实例， 第 222 页
- 监控多实例模式， 第 267 页
- 多实例模式的历史记录， 第 270 页

关于多实例模式

在多实例模式下，您可以在单个机箱上部署多个容器实例充当完全独立设备。

多实例模式与应用模式

您可以在多实例模式或设备模式下运行设备。

设备模式

设备模式为默认模式。设备运行本地 Firewall Threat Defense 映像并充当单个设备。唯一可用的机箱级配置（在 **机箱管理器** 页面上）用于网络模块管理（分支端口或启用/禁用网络模块）。

多实例模式

如果更改为多实例模式，则设备在机箱上运行 Cisco Secure Firewall 可扩展操作系统 (FXOS)，而每个实例运行单独的 Firewall Threat Defense 映像。您可以使用 FXOS CLI 配置模式。

由于多个实例在同一机箱上运行，因此您需要对以下项执行机箱级管理：

- 使用资源配置文件的 CPU 和内存资源。
- 接口配置和分配。

- 部署和监控实例。

对于多实例设备，将 机箱 添加到 防火墙管理中心 并在 **机箱管理器** 页面上配置机箱级别设置。

机箱管理接口

机箱管理

机箱使用设备上的专用管理接口。多实例模式不支持将数据接口用于机箱管理，也不支持将 DHCP 寻址用于管理接口。

您只能在 Firewall Threat Defense CLI（初始设置时）或 FXOS CLI（转换为多实例模式后）中配置机箱管理接口。请参阅 在 FXOS CLI 中更改机箱管理设置，第 265 页 以更改多实例模式下的管理接口设置。



注释 默认情况下，除非您启用 SSH 服务器和 SSH 访问列表，否则在多实例模式下不允许 SSH 访问此接口。这种差异意味着您可以使用 SSH 连接到应用模式威胁防御管理接口，但在转换为多实例模式后，默认情况下无法再使用 SSH 进行连接。请参阅配置 SSH 和 SSH 访问列表，第 247 页。

实例管理

所有实例共享机箱管理接口，并且每个实例在管理网络上都有自己的 IP 地址。添加实例并指定 IP 地址后，您可以在Firewall Threat Defense CLI 中更改网络设置。

默认情况下，实例管理 IP 地址允许 SSH。

实例事件接口

Cisco Secure Firewall 4200/6100 包括可用于事件的第二个专用接口管理 1/2。您可以在每个实例的 Firewall Threat Defense CLI 中配置此接口。为每个实例分配同一网络上的 IP 地址。请参阅配置事件接口，第 27 页。

实例接口

要确保灵活使用实例的物理接口，可以在机箱上创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。请参阅共享接口可扩展性，第 209 页和配置子接口，第 233 页。



注释 本章仅讨论 机箱 VLAN 子接口。您还可以在Firewall Threat Defense实例内单独创建子接口。有关详细信息，请参阅机箱接口与实例接口，第 207 页。

接口类型

物理接口、VLAN 子接口和 EtherChannel 接口可以是下列类型之一：

- 数据 - 用于常规数据或故障切换链路。数据接口无法在实例之间共享，并且实例无法通过背板与其他实例通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个实例。您可以将 VLAN 子接口添加到数据接口，以便为每个高可用性对提供单独的故障切换链路。
- 数据共享 - 用于常规数据。这些数据接口可以由一个或多个实例共享。每个实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、或故障转移链路。

机箱接口与实例接口

在机箱层面，管理物理接口、实例的 VLAN 子接口和 EtherChannel 接口的基本以太网设置。在实例中，您可以配置更高级别的设置。例如，您只能在机箱中创建 EtherChannel；但是，您可以为实例中的 EtherChannel 分配 IP 地址。

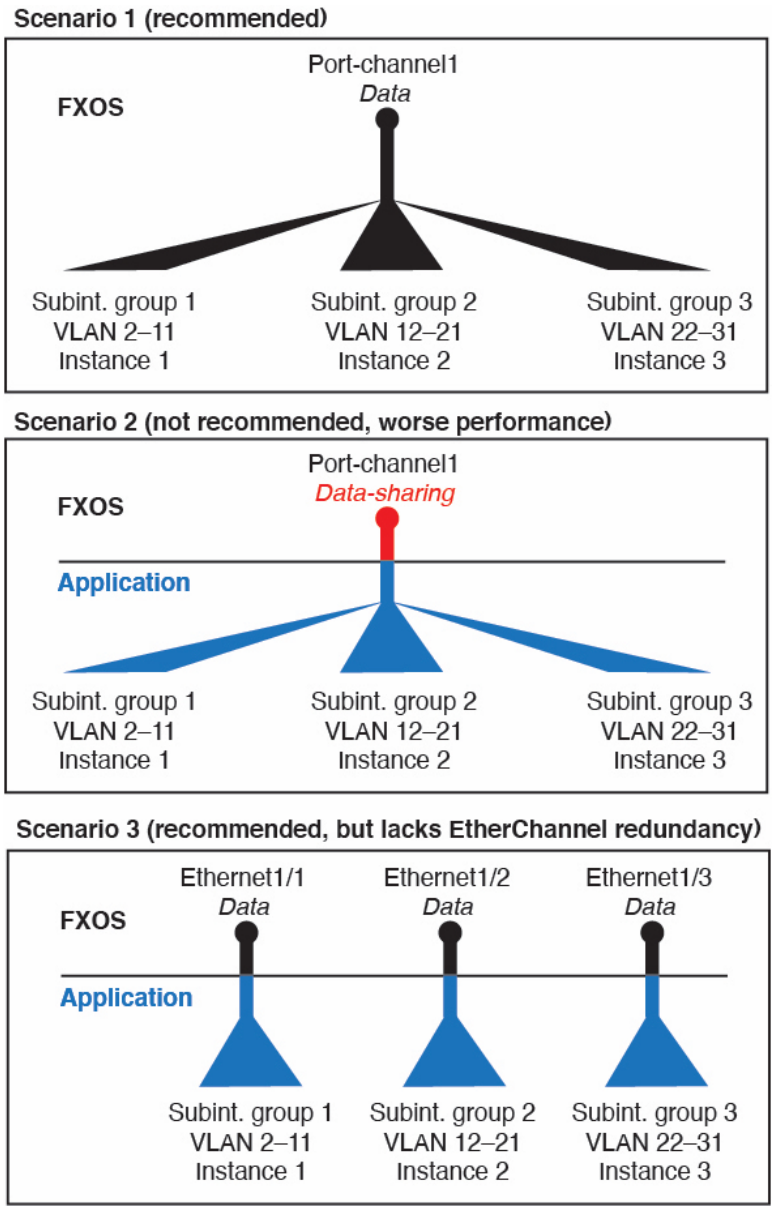
下文将介绍机箱接口与实例接口之间的交互。

VLAN 子接口

您可以在实例中创建 VLAN 子接口，就像创建任何设备一样。

您 还 可以在机箱中创建 VLAN 子接口。实例定义的子接口不受机箱限值的约束。选择在哪个位置创建子接口取决于网络部署和个人偏好。例如，要共享子接口，必须在机箱创建子接口。偏好机箱子接口的另一种场景包含将单个接口上的单独子接口组分配至多个实例。例如，您想要结合使用端口通道 1 与实例 A 上的 VLAN 2-11、实例 B 上的 VLAN 12-21 和实例 C 上的 VLAN 22-31。如果您在实例内创建这些子接口，则必须在机箱中共享父接口，但这可能并不合适。有关可以用于实现这种场景的三种方法，请参阅下图：

图 *53:* 机箱中的 ***VLAN*** 与实例



机箱和实例中的独立接口状态

您可以从管理上启用和禁用机箱和机箱中的接口。必须在两个位置中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与实例之间可能出现不匹配的情况。

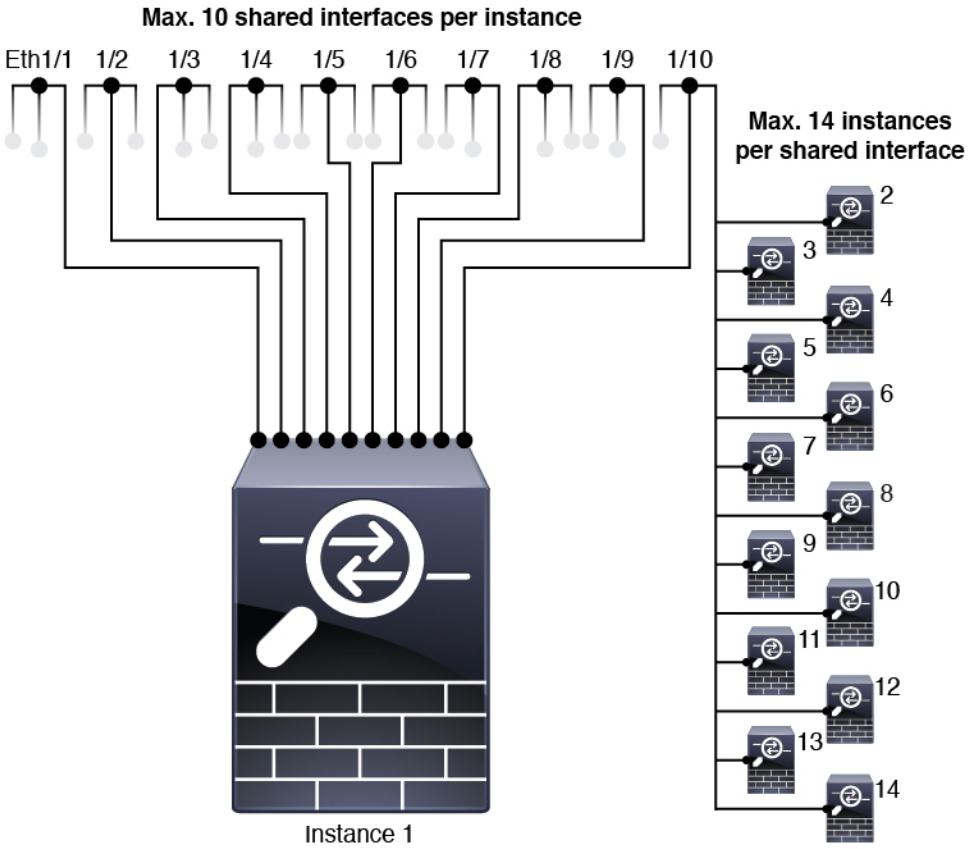
实例内接口的默认状态取决于接口类型。例如，在实例内，默认禁用物理接口或 EtherChannel，但默认启用子接口。

共享接口可扩展性

实例可以共享数据共享型接口。此功能允许您保存物理接口的使用情况，以及支持灵活的网络部署。当您共享接口时，机箱会使用唯一 MAC 地址将流量转发至适当实例。然而，由于需要在机箱内实现全网状拓扑，因此共享接口将导致转发表规模扩大（每个实例都必须能够与共享同一接口的所有其他实例进行通信）。因此，您可以共享的接口存在数量限制。

除转发表外，机箱还维护用于 VLAN 子接口转发的 VLAN 组表。 您最多可以创建 500 个 VLAN 子接口。

请参阅共享接口分配的以下限制：



共享接口最佳实践

为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

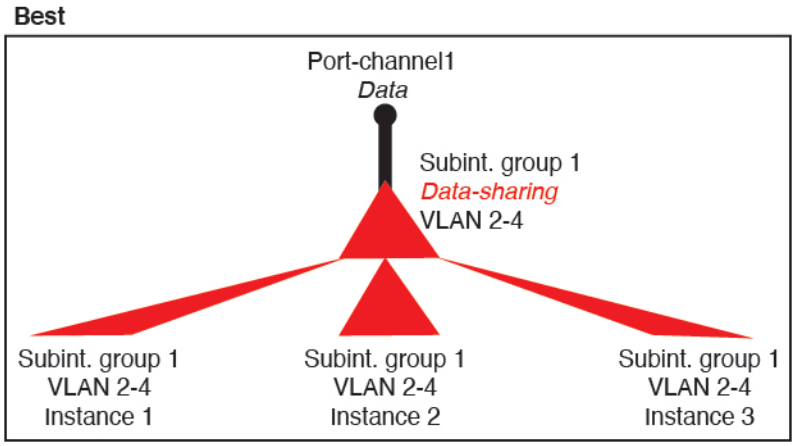
共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

1. 最佳 - 共享单父项下的子接口，并结合使用相同集合的子接口和同组实例。

   例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：Port-Channel1.2, 3 和 4 而不是 Port-Channel2、Port-Channel3 和 Port-Channel4。与跨父项共

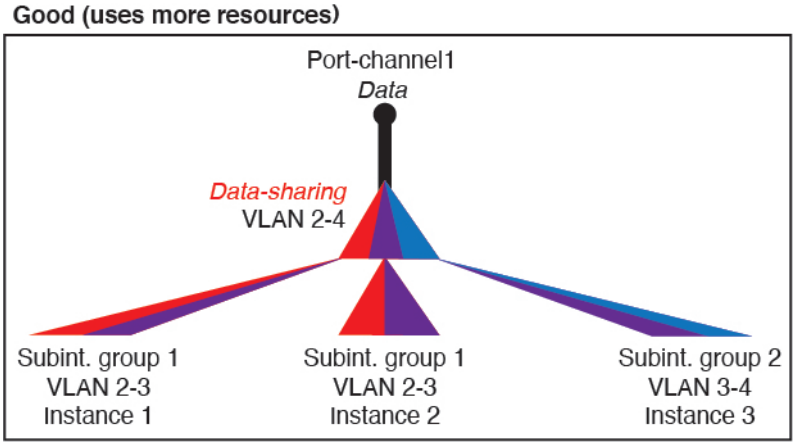
享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

图 *54:* 最佳：一个父项上的共享子接口组



如果未与一组实例共享相同集合的子接口，则配置会提高资源使用率（更多 VLAN 组）。例如，与实例 1、2 和 3（一个 VLAN 组）共享 Port-Channel1.2, 3 和 4 而不是与实例 1 和 2 分享 Port-Channel1.2 和 3，同时与实例 3（两个 VLAN 组）共享 Port-Channel1.3 和 4。

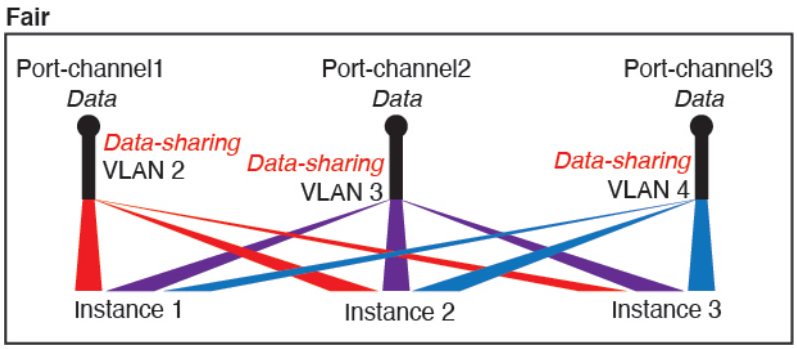
图 *55:* 良好：一个父项上共享多个子接口组



2. 一般 - 跨父项共享子接口。

   例如，共享 Port-Channel1.2、Port-Channel2.3 和 Port-Channel3.4 而不是 Port-Channel2、Port-Channel4 和 Port-Channel4。虽然这种使用方法的效率低于仅共享同一父项上的子接口，但仍可利用 VLAN 组。

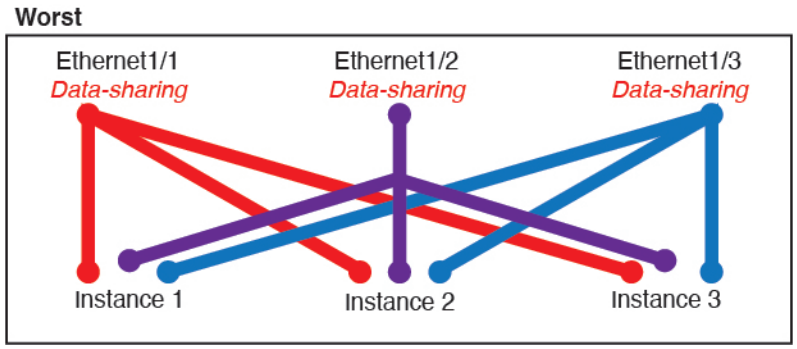
图 *56:* 一般：独立父项上的共享子接口



3. 最差 - 共享单个父接口（物理或 EtherChannel）。

   此方法使用的转发表条目最多。

图 *57:* 最差：共享父接口



机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的实例。在应用内配置每个接口时，您也可以手动设置MAC地址。

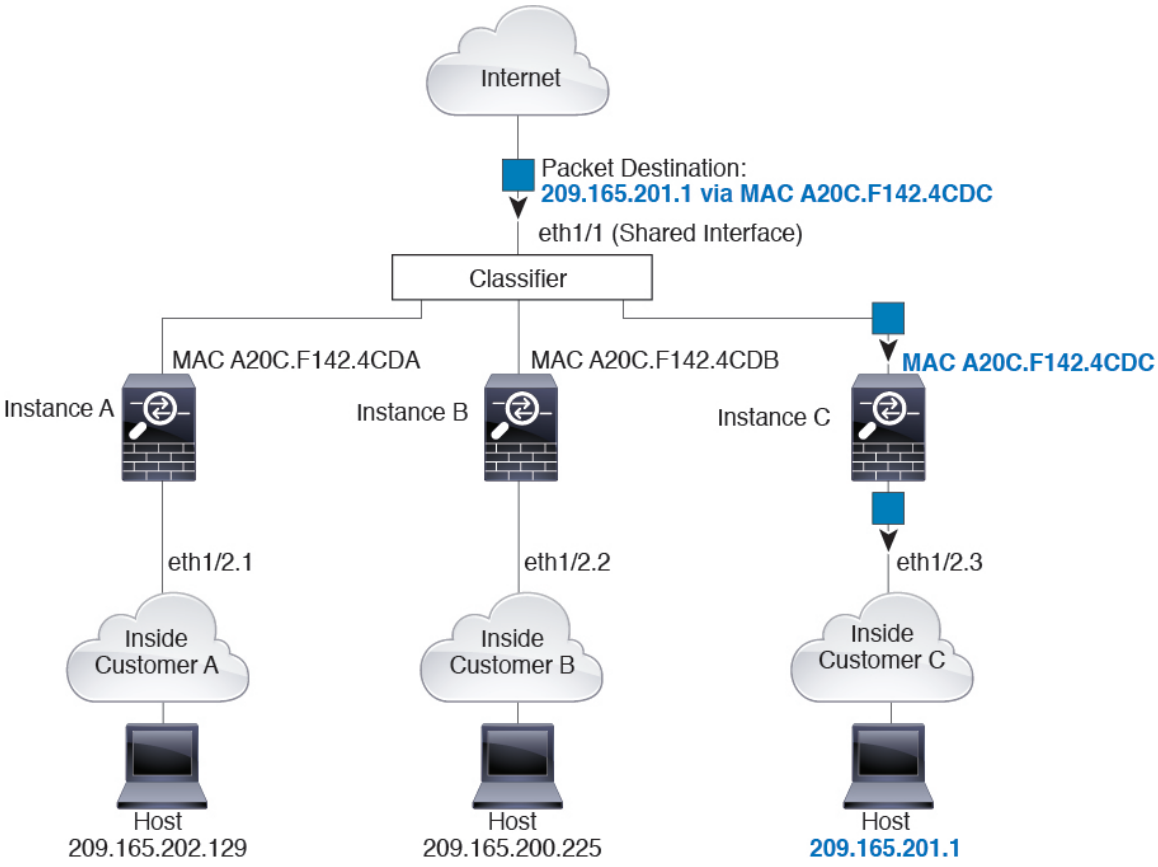
注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

使用 MAC 地址通过共享接口进行数据包分类

下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

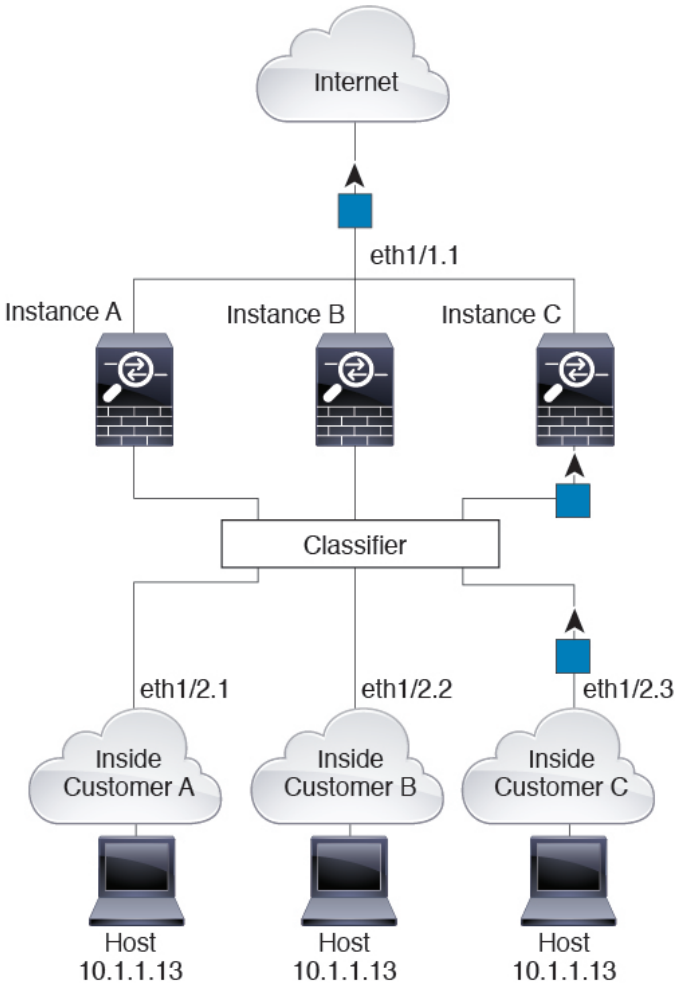
图 *58:* 使用 *MAC* 地址通过共享接口进行数据包分类



来自内部网络的传入流量

请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

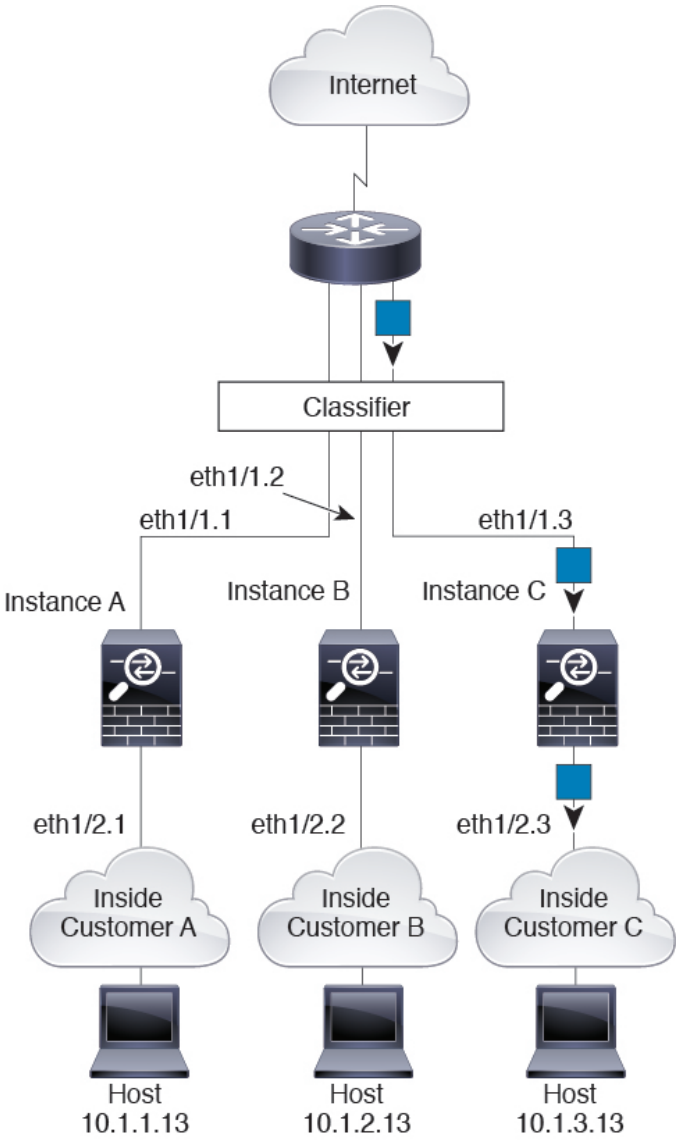
图 *59:* 来自内部网络的传入流量



透明防火墙实例

对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

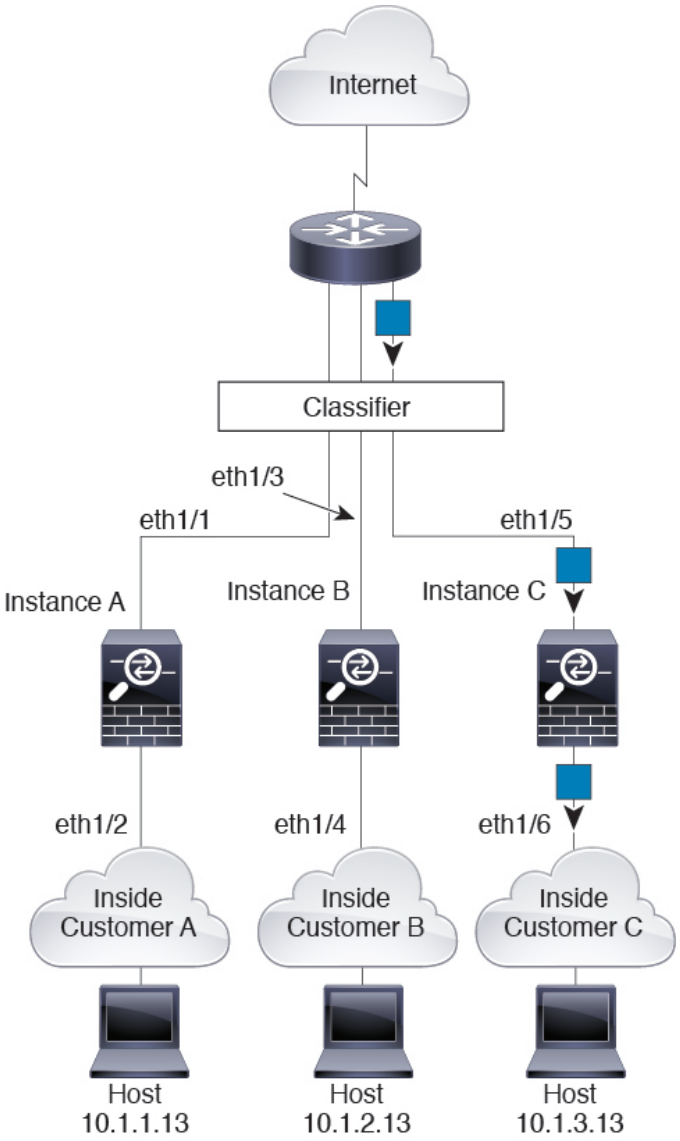
图 *60:* 透明防火墙实例



内联集

对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 *61:* 内联集

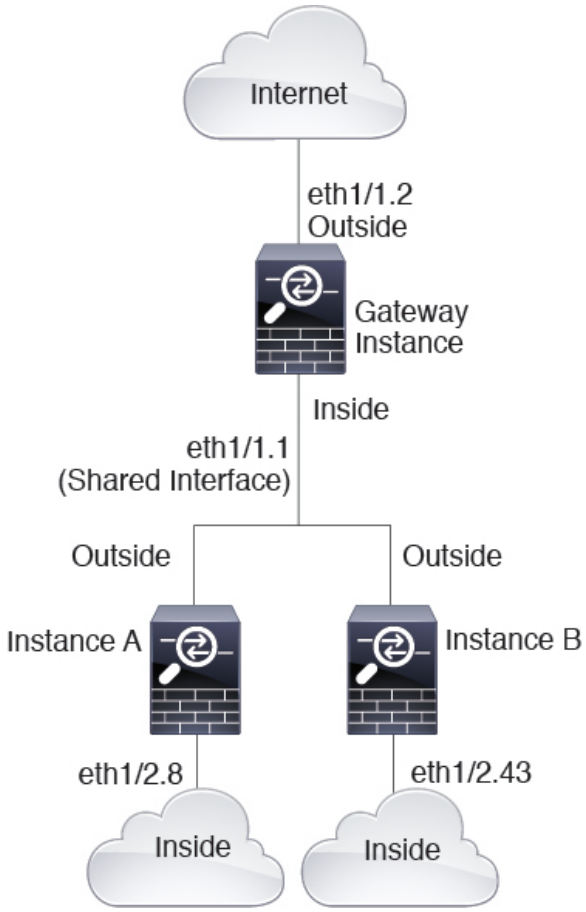


级联实例

直接在一个实例前面放置另一个实例的行为称为 级联实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

图 *62:* 级联实例



注释 请勿使用具有高可用性的级联实例（使用共享接口）。发生故障转移且备用设备重新加入后，MAC 地址可能会暂时重叠并导致中断。您应改为为网关实例和内部实例使用唯一接口，使用外部交换机在实例之间传递流量。

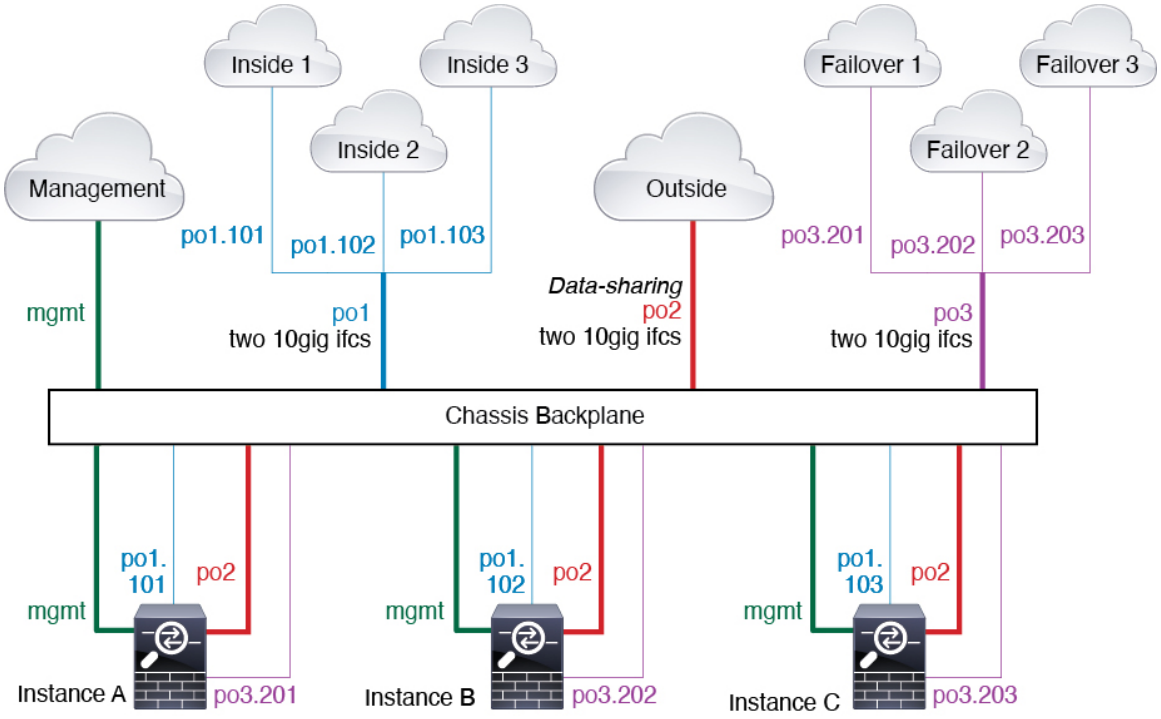
典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例和机箱均使用专用管理接口。在每个实例（和机箱）中，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 1 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 2 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一外部网络上的唯一 IP 地址。

- 故障切换 - 每个实例都使用端口通道 3 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。

图 *63:* 典型多实例部署



实例接口的自动 MAC 地址

机箱会自动为实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一 MAC 地址。

如果您手动为实例中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在实例中为接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。

机箱使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中， *xx.yy* 是用户定义的前缀或系统定义的前缀，*zz.zzzz* 是由机箱生成的内部计数器。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与机箱的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数）是为了得出设备的内存和CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但实例可用的吞吐量可能低于应用可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html。

实例与高可用性

您可以在 2 个独立机箱上使用实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建10个高可用性对。您还可以在高可用性实例所在的机箱上设置独立实例。有关详细要求，请参阅 实例的要求和前提条件，第 218 页。

注释 不支持群集。

实例的许可证

所有许可证均按机箱使用，而不是按实例使用。请查看以下详细信息：

- 基础版 许可证作为一个整体分配给机箱，每个机箱一个。
- 功能许可证分配到每个实例；但每个机箱每个功能只能 使用 一个许可证。

实例的要求和前提条件

型号支持

- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245

注释 不支持 Cisco Secure Firewall 3105。

每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的CPU核心数量（或更具体地说，线程数）。我们通常使用术语“核心”来表示不同的硬件架构。系统会根据核心数量动态分配RAM，并将每个实例的磁盘空间设为 40 GB。

表 *15:* 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 CPU 核心（线程数）
Cisco Secure Firewall 3110	3	22
Cisco Secure Firewall 3120	5	30
Cisco Secure Firewall 3130	7	46
Cisco Secure Firewall 3140	10	62
Cisco Secure Firewall 4215	10	62
Cisco Secure Firewall 4225	21	126
Cisco Secure Firewall 4245	34	254

软件要求

- 您可以在每个实例上运行不同版本的 Firewall Threat Defense 软件，只要它们都与机箱上运行的 FXOS 版本兼容。
- 您无法部署带有 Firewall Threat Defense 软件补丁程序版本的实例，因为它不是一个完整的捆绑包。您需要先部署主要或维护版本，然后在部署后安装补丁程序。

高可用性要求

- 高可用性配置中的两个实例必须：
  - 位于单独的机箱上。
  - 位于相同的型号。
  - 分配相同的接口。启用高可用性之前，所有接口必须在机箱中进行相同的预配置。

- 使用相同的资源配置文件属性。配置文件名称可以不同，但定义需要匹配。

防火墙管理中心 要求

对于机箱管理和机箱上的所有实例，由于许可实施，您必须使用相同的 防火墙管理中心 。

实例的准则和限制

一般准则

- 单个 防火墙管理中心 必须管理机箱上的所有实例，以及管理机箱本身。
- 对于实例，不支持以下功能：
  - TLS 加密加速
  - 集群
  - 防火墙管理中心 UCAPL/CC 模式
  - 到硬件的数据流分流
  - LLDP
- 不支持通过 Security Cloud Control 云交付 防火墙管理中心 对机箱进行主要管理，也不支持通过本地部署 防火墙管理中心 对机箱进行单独的仅分析管理。但是，您可以将 Security Cloud Control 托管的实例添加到本地分析专用 防火墙管理中心。

管理界面

- 不支持用于机箱管理的数据接口；只能使用专用的管理接口
- 管理接口无 DHCP 寻址
- 管理连接需要 TCP 端口 8305；不要更改默认值。

VLAN 子接口

- 本文档仅讨论 机箱 VLAN 子接口。您还可以在实例内单独创建子接口。
- 如果将父接口分配至实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。
- 子接口在数据或数据共享型接口。
- 最多可以创建 500 个 VLAN ID。
- 不得将子接口用于内联集或用作被动接口。

- 如果将子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。不得将某些子接口用作故障转移链路，而将某些用作常规数据接口。

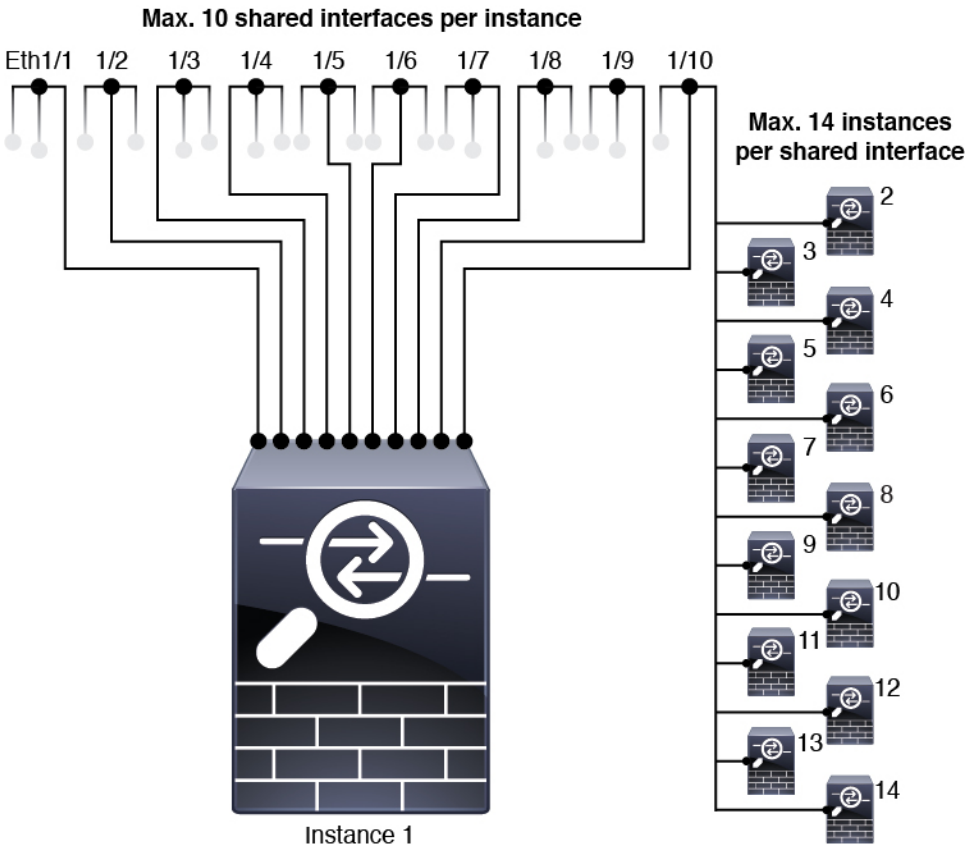
EtherChannel

- 您最多可以配置 48 个 EtherChannel，受物理接口数量限制。
- EtherChannel 最多可以有 8 个主用接口。
- EtherChannel 中的所有接口必须具有相同的介质类型和速度容量。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。除非将速度设置为**检测 SFP**，否则不能通过将较大容量接口的速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口）;在这种情况下，您可以使用不同的接口容量，并使用最低的通用速度。
- 机箱不支持带有 VLAN 标记的 LACPDU。如果使用思科 IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则机箱将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 在低于 15.1(1)S2 的思科 IOS 软件版本中，机箱不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接机箱 EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为一个足够大的值，以考虑重新加载时间；例如，8 分钟或无限接近 0。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

数据共享接口

- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。

  每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。



- 不得结合使用数据共享接口和透明防火墙模式接口。
- 不得结合数据共享接口和内联集或被动接口。
- 不得将数据共享接口用于故障转移链路。

默认 MAC 地址

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅实例接口的自动 MAC 地址，第 217 页。

配置实例

在配置实例之前，您需要启用多实例模式，将机箱添加到 防火墙管理中心，并配置机箱接口。您还可以自定义机箱设置。

将设备转换为多实例模式

使用此程序将 防火墙管理中心 中的设备转换为多实例模式。转换大约需要 15 分钟。系统将重新启动，并在更改模式时清除配置，但管理网络设置和管理员密码除外。机箱主机名设置为“firepower-*model*”。管理 IP 地址分配给机箱，用于通过 防火墙管理中心 进行管理连接。当您添加实例时，它们将在管理接口上使用单独的 IP 地址并维护自己的管理连接。

在转换为多实例模式后，您可以使用 防火墙管理中心 配置所有机箱设置以及实例。不支持 FXOS CLI 上的 Cisco Secure Firewall 机箱管理器 或配置。

注释 如果您希望在将设备添加到 防火墙管理中心 之前使用 CLI 转换为多实例模式，请参阅在 CLI 启用多实例模式，第 260 页。

开始之前

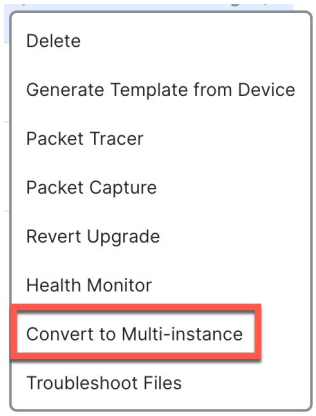
将设备模式设备作为独立设备添加到 防火墙管理中心 。此设备无法使用：

- 用于管理器访问的数据接口
- 管理接口的 DHCP
- 零接触调配

过程

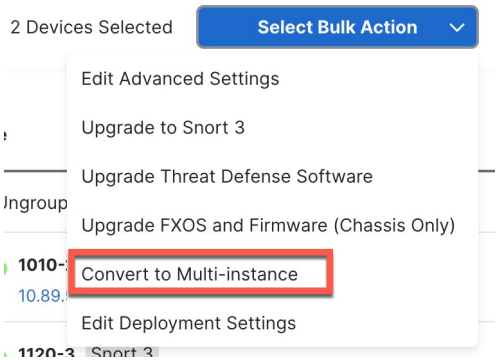
步骤 1 在 **设备** > **设备管理** 上，在要转换为多实例模式的设备旁边，选择 **更多** (⋮) > **转换为多实例**。

图 *64:* 转换为多实例



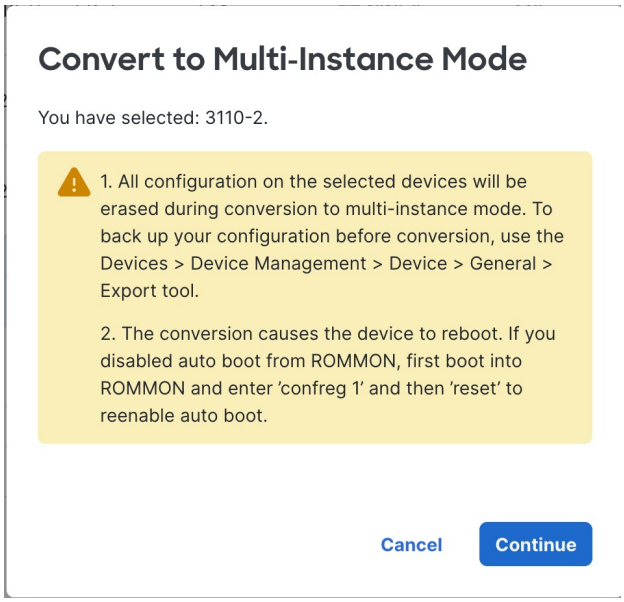
您也可以选中要转换的多个设备旁边的复选框，然后选择**选择批量操作 (Select Bulk Action)** > **转换为多实例 (Convert to Multi-Instance)**。

图 *65:* 批量转换



步骤 2 确认您要执行转换，然后点击**继续**。

图 *66:* 转换确认



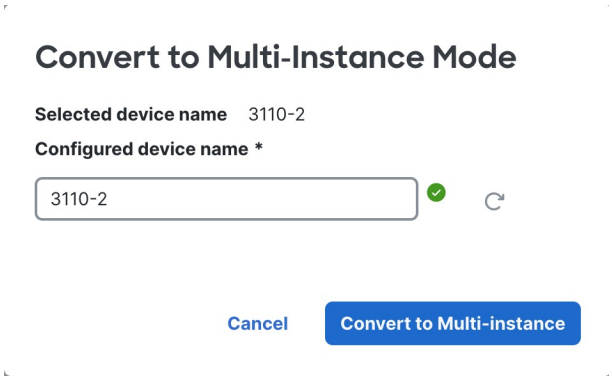
执行就绪性检查。例如，如果部署正在进行，则检查可能会失败。

步骤 3 或者，更改机箱的名称，然后点击**转换为多实例 (Convert to Multi-Instance)**。默认情况下，使用设备名称，但您可能需要为多实例机箱使用不同的命名约定。

注释

如果就绪性检查失败（例如，由于正在进行部署），您可以等待该过程完成，然后点击 以重新运行就绪性检查，以便继续。

图 *67:* 重命名机箱

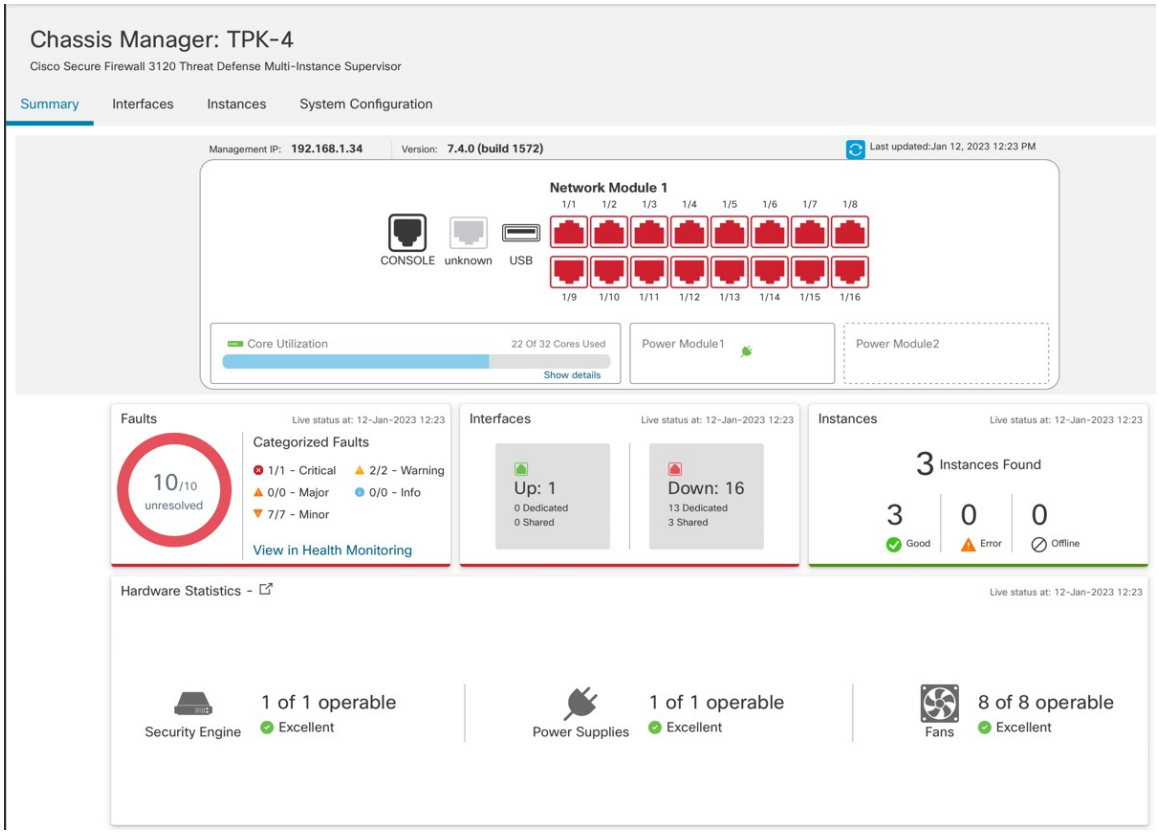


等待大约 15 分钟，在此期间设备将从设备列表中删除，然后在转换后将其重新添加为机箱。

步骤 4 要查看和配置机箱，请点击 **机箱** 列中的 **管理** ，或点击 **编辑** ()。

打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

图 *68:* 机箱摘要



配置机箱接口

在机箱层面，配置物理接口、实例的 VLAN 子接口和 EtherChannel 接口的基本以太网设置。默认情况下，物理接口处于禁用状态。

注释 要配置分支端口并执行其他网络模块操作，请参阅 管理 Cisco Secure Firewall 3100/4200/6100的网络模块 ， 第 728 页。

注释 有关 **同步设备** 按钮的信息，请参阅 与 防火墙管理中心同步接口更改 ， 第 727 页。

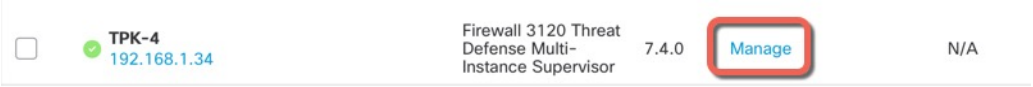
配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工及其他硬件设置。要使用某一接口，必须为机箱以物理方式启用它，并在ASA中以逻辑方式启用它。默认情况下，物理接口处于禁用状态。对于 VLAN 子接口，其管理状态继承自父接口。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

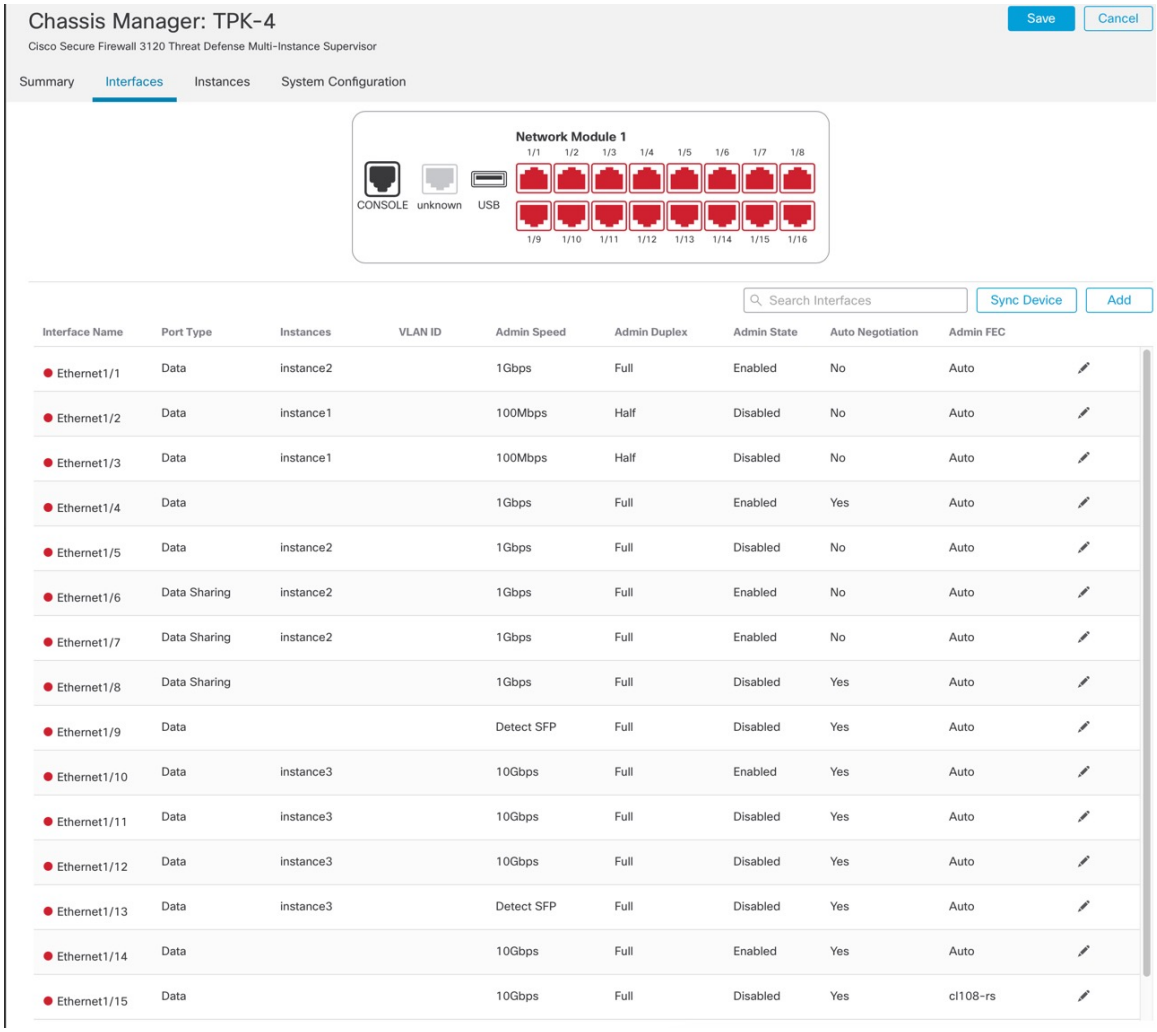
图 *69:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

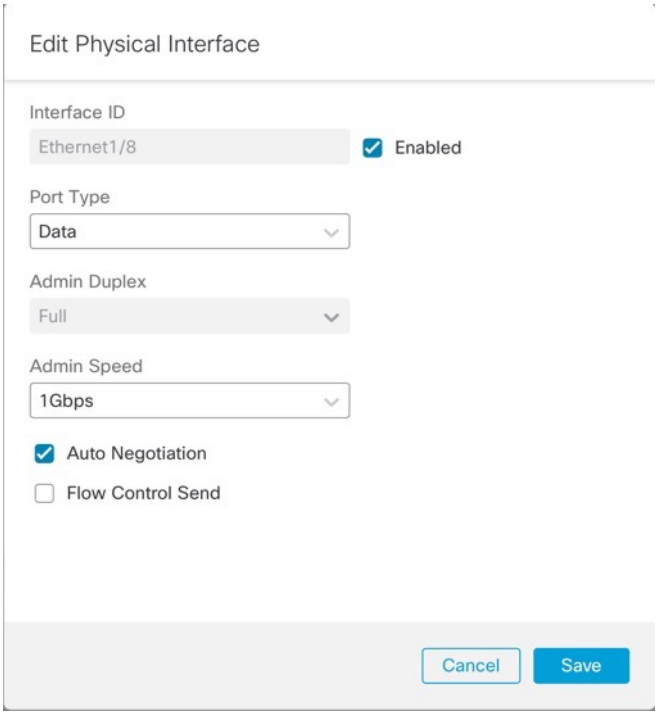
步骤 2 点击**接口 (Interfaces)**。

图 *70:* 接口



步骤 3 点击要编辑的接口的 **编辑** (✎)。

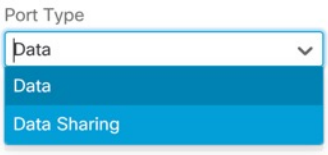
图 *71:* 编辑物理接口



步骤 4 选中**启用**复选框以启用此接口。

步骤 5 对于 **端口类型**，选择 **数据** 或 **数据共享**。

图 *72:* 端口类型



步骤 6 设置 **管理员双工**。

1Gbps 及更高的速度仅支持 **全双工** 。SFP 接口仅支持 **全** 复用。

步骤 7 设置 **管理员速度**。

对于 SFP，选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。

步骤 8 （可选） 选中 **流量控制发送** 以启用暂停 (XOFF) 帧以进行流量控制。

流量控制通过允许拥塞节点在另一端暂停链路操作，从而让连接的以太网端口能够在拥塞期间控制流量速率。如果威胁防御端口遇到拥塞（内部交换机上的排队资源耗尽）并且无法接收更多流量，则它会通过发送暂停帧来通知另一个端口停止发送，直到状况恢复正常为止。在收到暂停帧后，发送设备会停止发送任何数据包，从而防止在拥塞期间丢失任何数据包。

注释
Firewall Threat Defense 支持传输暂停帧，以便远程对等体可以对流量进行速率控制。

但是，不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池，而每个缓冲区都有 250 个字节，并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记（2 MB [8000 个缓冲区]）时，会在每个启用了流量控制的接口上发送暂停帧；当特定接口的缓冲区超过端口高水位标记（0.3125 MB [1250 个缓冲区]）时，会从该接口发送暂停帧。在发送暂停后，如果缓冲区使用率降低至低水位标记之下（全局 1.25 MB [5000 个缓冲区]；每个端口 0.25 MB [1000 buffers]），则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 9 （可选） 选中 **自动协商** 以设置接口以协商速度、链路状态和流量控制。对于低于 1 Gbps 的速度，无法编辑此设置。对于 SFP 接口，只能在速度设置为 1 Gbps 时禁用自动协商。

步骤 10 点击 **保存**，然后点击 **接口** 页面右上角的 **保存**。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

配置 EtherChannel

EtherChannel（也称为端口通道）最多可以包含 8 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。除非将速度设置为**检测 SFP**，否则不能通过将较大容量接口的速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口）;在这种情况下，您可以使用不同的接口容量，并使用最低的通用速度。

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

机箱创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。将 EtherChannel 添加到实例时，它将退出此 **挂起** 状态。

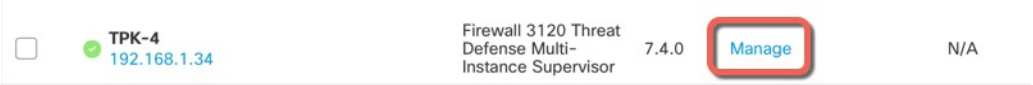
开始之前

启用物理接口并设置硬件参数。请参阅配置物理接口，第 226 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

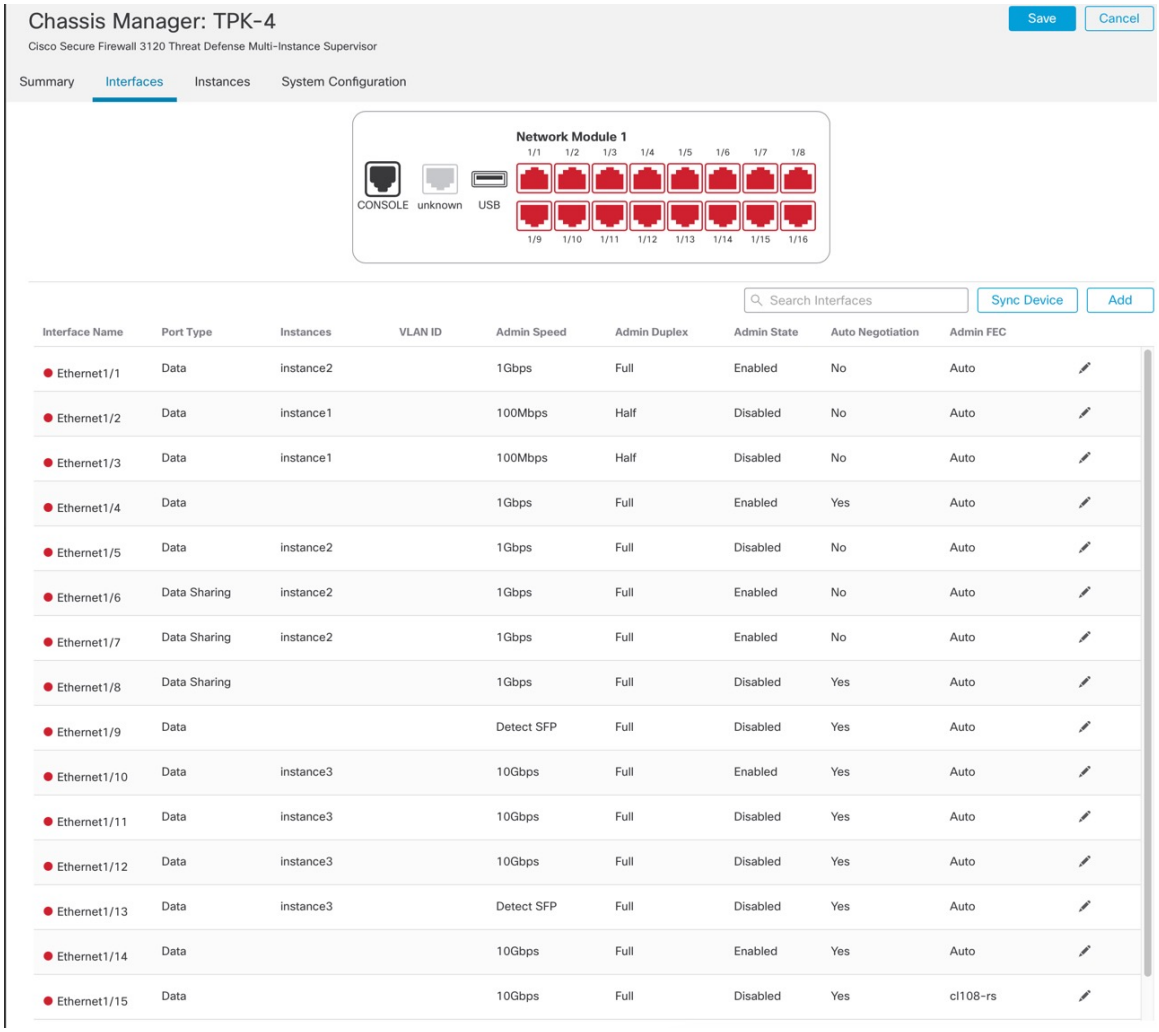
图 *73:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

步骤 2 点击**接口 (Interfaces)**。

图 *74:* 接口



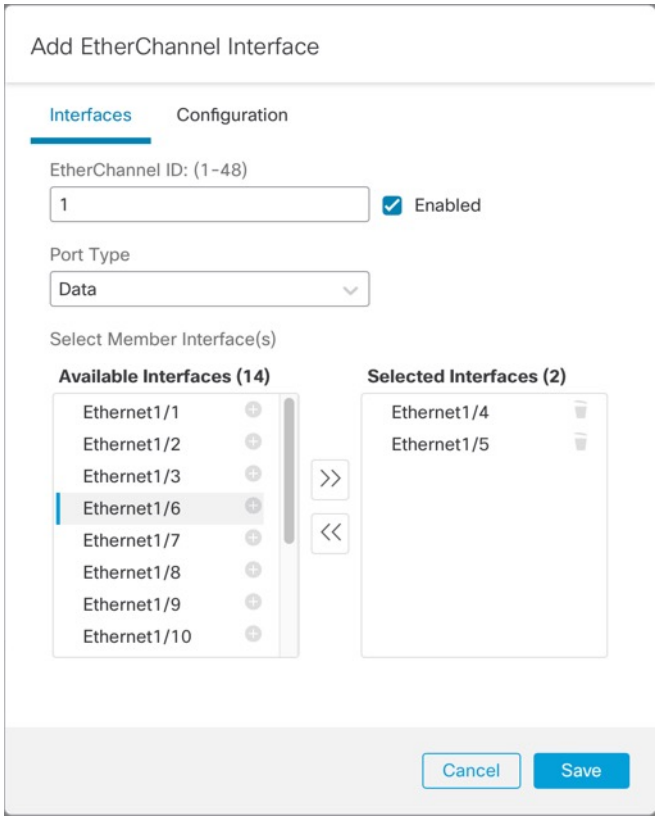
步骤 3 点击 添加 > **EtherChannel** 通道接口

图 *75:* 添加 ***EtherChannel***



步骤 4 设置以下 **接口** 参数。

图 *76:* 接口设置



a) 对于 **EtherChannel ID**，请指定一个介于 1 和 48 之间的 ID。

b) 点击**已启用**。

c) 对于 **端口类型**，请选择 **数据** 或 **数据共享**。

有关端口类型的信息，请参阅 接口类型 ， 第 206 页。

d) 要将物理接口添加到 EtherChannel，请在**可用接口**列表中选择点击 **添加** (⊕) 以将其移动到**选定的接口**列表。

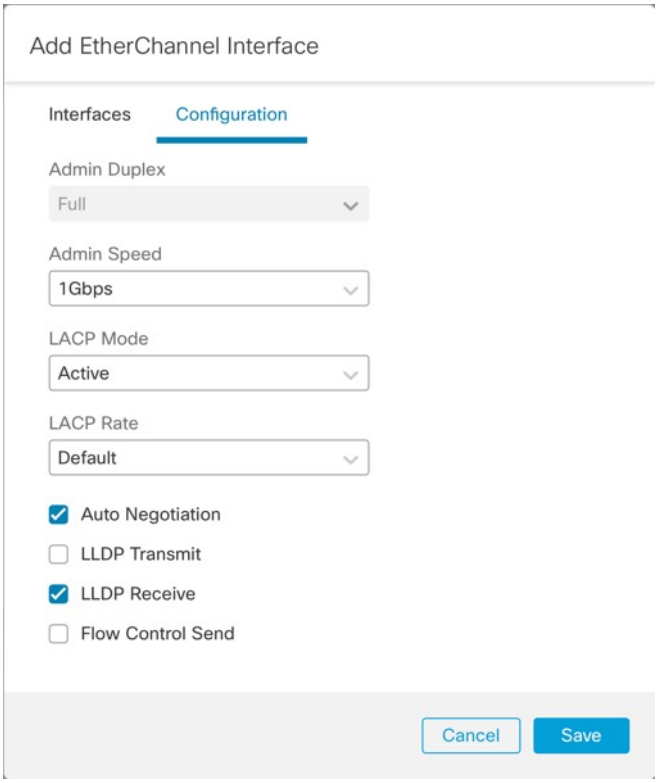
要添加或删除所有接口，请点击双箭头按钮。

注释
不能添加已分配给实例的接口。

步骤 5 （可选） 设置以下 **配置** 参数。

其中许多设置（不包括 LACP 设置）为要包含在 EtherChannel 中的接口设置了要求；它们不会覆盖成员接口的设置。例如，如果选中**LLDP 传输**，则应仅添加具有该设置的接口。如果将 **管理速度** 设置为 1Gbps，则只能包括 1Gbps 接口。

图 *77*: 配置设置



a) 为成员接口、 **全双工** 或 **半双工** 选择所需的 **管理双工** 。

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。

b) 从下拉列表选择成员接口要求的 **管理速度**。

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。

c) 选择 **LACP 模式**、 **活动** 或 **打开**。

- **主用**-发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开启** - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释
如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

d) 选择 **LACP Rate**、 **Default**、 **Fast**或 **Normal**。

默认值为 **Fast**。

e) 通过选中 **LLDP 传输** 和/或 **LLDP 接收**，为成员接口选择所需的链路层发现协议 (LLDP) 设置。

f) 检查成员接口所需的 **流量控制发送** 设置。

步骤 6 点击 **保存**，然后点击 **接口** 页面右上角的 **保存** 。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

配置子接口

您最多可以将 500 个子接口连接到您的机箱。

每个接口的 VLAN ID 都必须具有唯一性，并且在实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的实例，您就可以在 单独 接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

本部分仅讨论 *FXOS* VLAN 子接口。您还可以在实例内单独创建子接口。请参阅机箱接口与实例接口，第 207 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

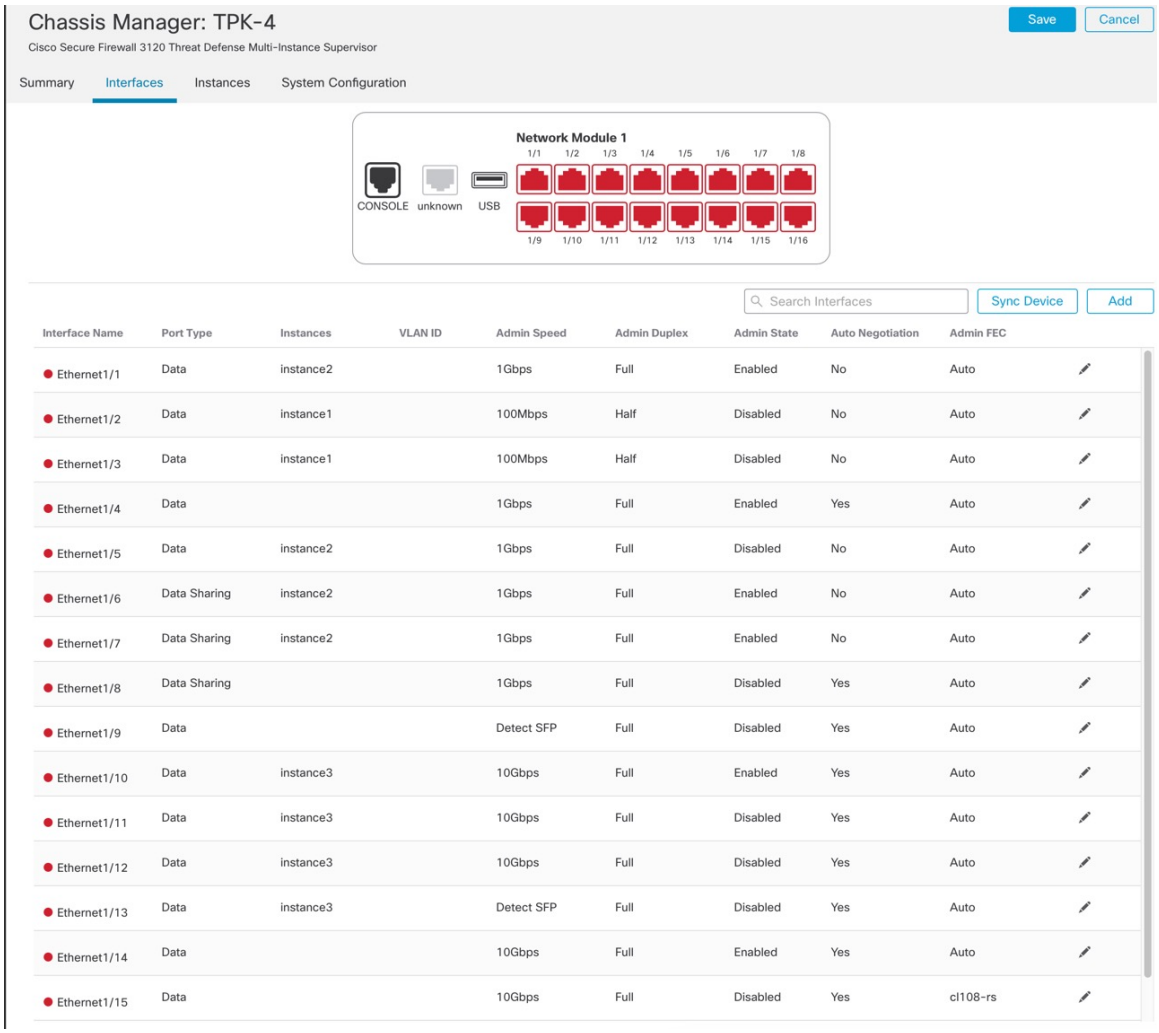
图 *78:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

步骤 2 点击**接口 (Interfaces)**。

图 *79:* 接口



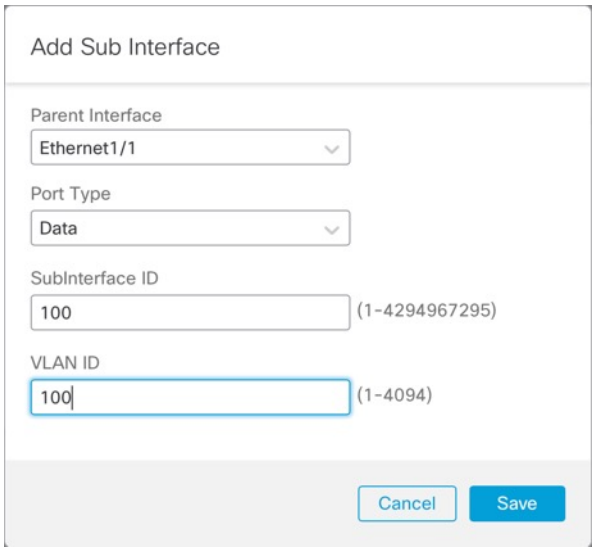
步骤 3 点击 添加 > 子接口

图 *80:* 添加子接口



步骤 4 设置以下参数。

图 *81:* 子接口设置



a)

步骤 5 点击 **保存**，然后点击 **接口** 页面右上角的 **保存**。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

添加实例

您可以在多实例模式下将一个或多个实例添加到机箱。支持的实例数量取决于您的型号；请参阅 实例的要求和前提条件，第 218 页。

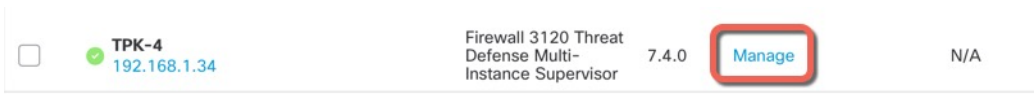
开始之前

将设备转换为多实例模式，第 223 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

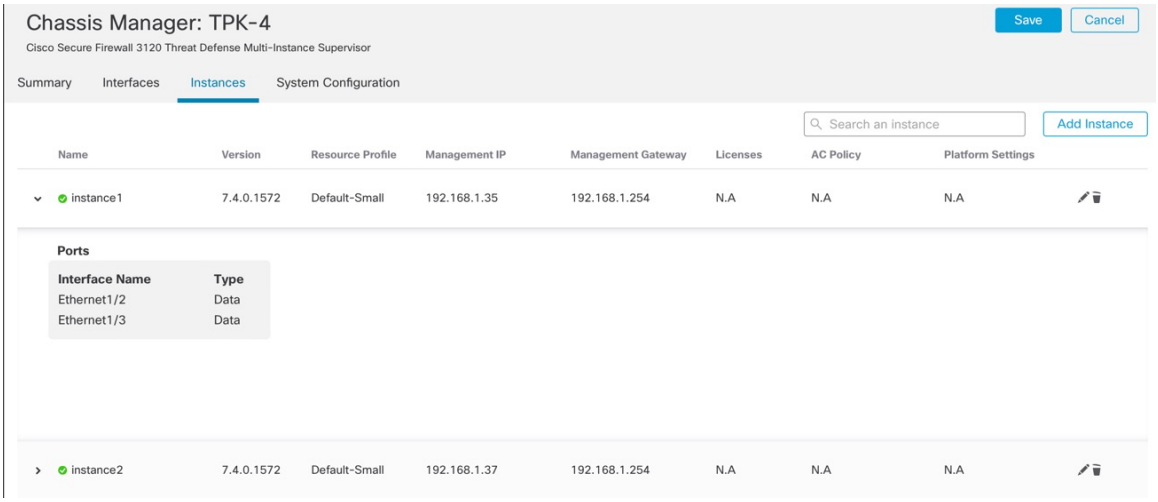
图 *82:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

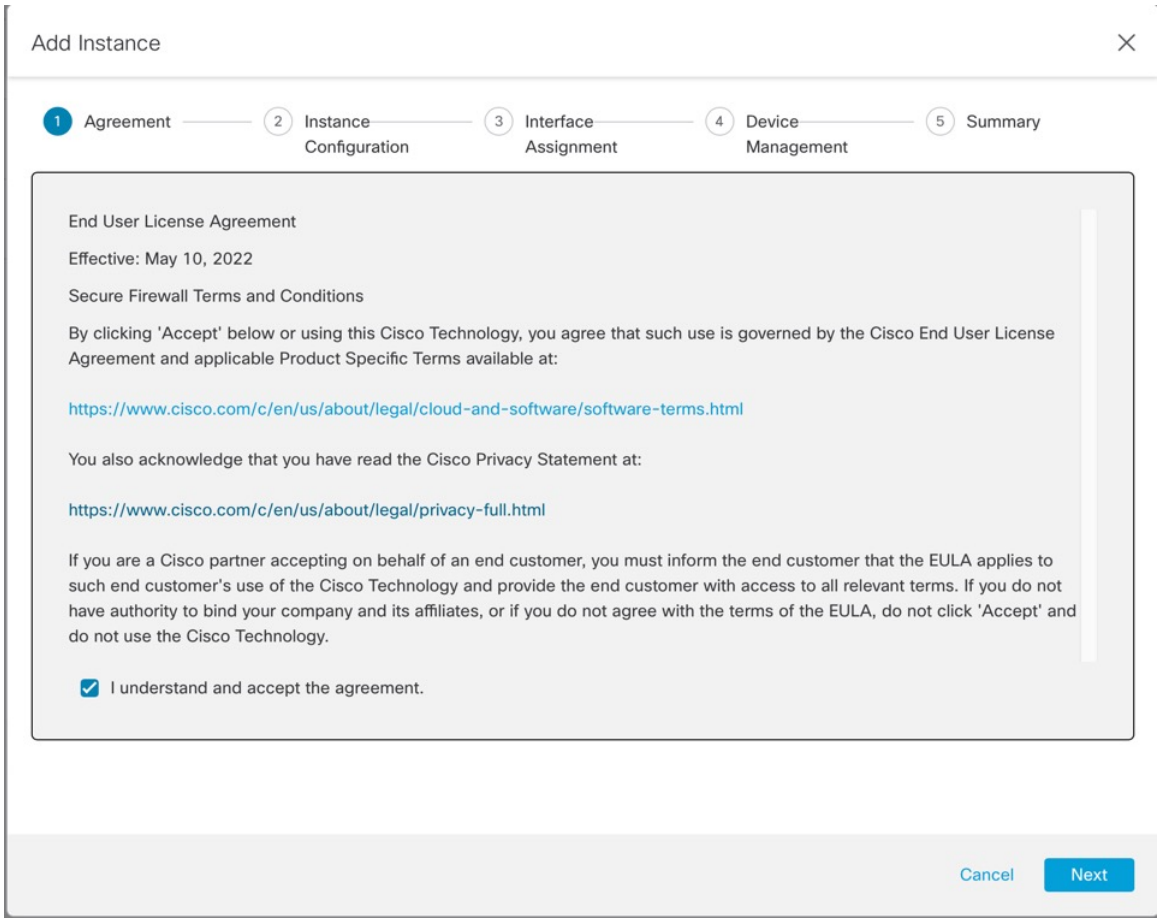
步骤 2 点击 **实例**，然后点击 **添加实例**。

图 *83:* 实例



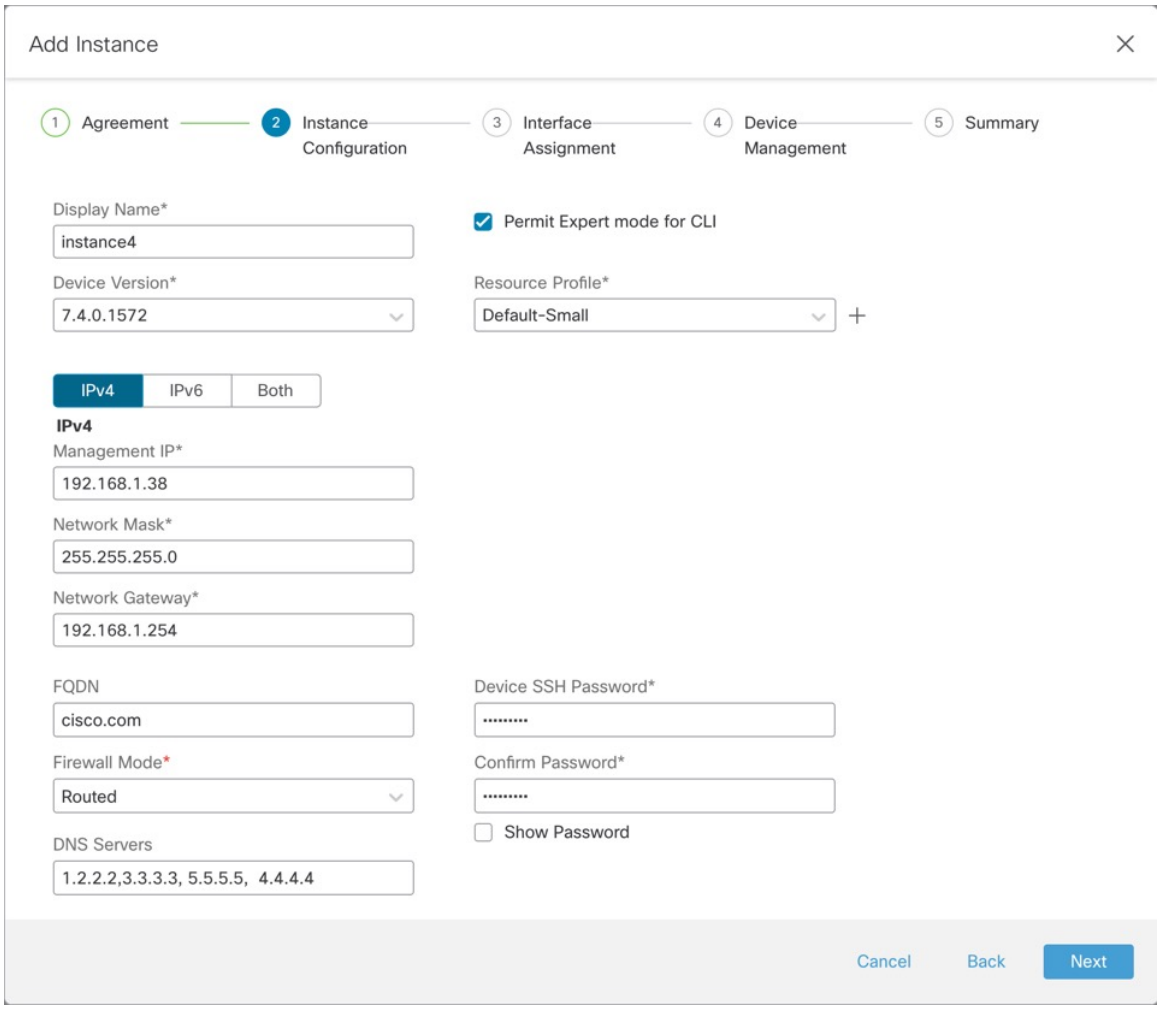
步骤 **3** 在 **协议**中，选中 **我了解并接受协议**，然后点击 **下一步**。

图 *84:* 协议



步骤 4 在 **实例配置**中，设置实例参数，然后点击 **下一步**。

图 ***85:*** 实例配置



- **显示名称**
- **设备版本**-列出的版本是当前下载到机箱的软件包。补丁版本没有列出，也不能使用，因为它们未包含整个软件包。要升级到新软件包，请参阅 **设备** > **+ 显示更多** > **升级** > **机箱升级**。升级时，旧 Firewall Threat Defense 版本和新 Firewall Threat Defense 版本都将在菜单中列出。要下载较旧的软件包，您需要使用 FXOS CLI。注意：FXOS 和 Firewall Threat Defense 映像都包含在同一软件包中。有关详细信息，请参阅 故障排除指南 。

  例如：

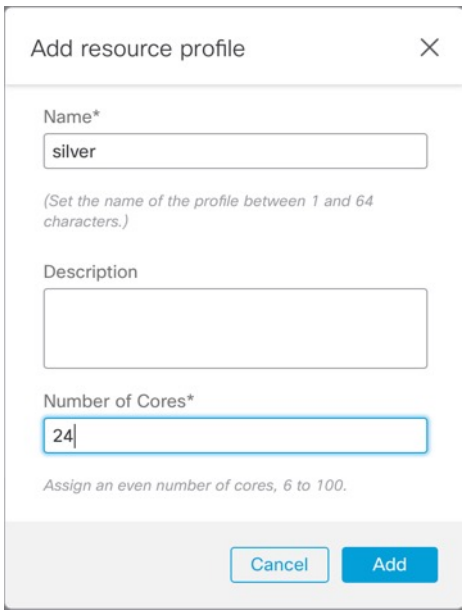
```
firepower-3110# scope firmware
firepower-3110# download image
https://10.10.7.89/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar : completed successfully.
```

- **IPv4、IPv6 或两者 (Both)** - 在与机箱管理接口相同的网络上设置**管理 IP (Management IP)** 地址。设置**网络掩码 (Network Mask)** 和网关（可能与机箱相同）。机箱管理接口与每个实例共享，每个实例在网络上都有自己的 IP 地址。默认情况下，您可以通过 SSH 连接到此 IP 地址以访问 Firewall Threat Defense CLI。
- （可选） **FQDN**
- **防火墙模式** - **路由** 或 **透明**。有关防火墙模式的详细信息，请参阅透明或路由防火墙模式，第 123 页。
- **DNS 服务器**- 输入仅用于管理流量的 DNS 服务器列表（以逗号分隔）。
- （可选）**适用于 CLI 的专家模式许可**-专家模式提供 Firewall Threat Defense 外壳访问权限以确保实现高级故障排除。

  如果启用此选项，拥有直接从 SSH 会话访问实例的权限的用户可以输入专家模式。如果禁用此选项，只有拥有从 FXOS CLI 访问实例的权限的用户可以输入专家模式。我们建议禁用此选项以加强实例之间的隔离。

  仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在Firewall Threat Defense CLI 中使用 **专家** 命令。
- **资源配置文件** - 资源配置文件会设置 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。机箱包括以下默认资源配置文件：Default-Small、Default-Medium 和 Default-Large。您可以通过点击 **添加** (+)为此机箱添加其他配置文件。以后无法编辑资源配置文件。

图 *86:* 添加资源配置文件



  - 最小核心数量为 6。

    注释

与具有较大内核数量的实例相比，具有较小核心数量的实例可能具有相对更高的CPU利用率。具有较小核心数量的实例对流量负载变化更敏感。如果出现流量丢弃情况，请尝试分配更多核心。

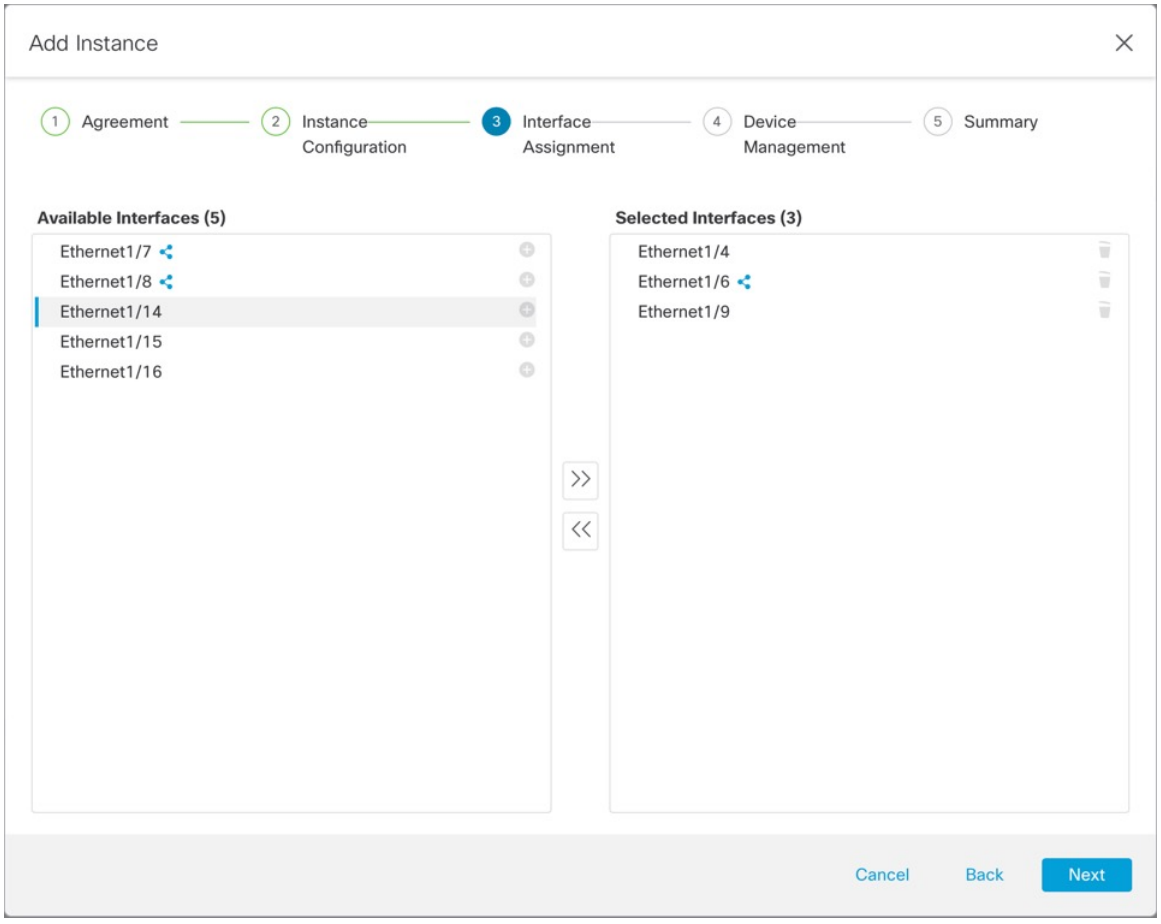
- 您可以分配偶数（6、8、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于型号，请参阅实例的要求和前提条件，第 218 页。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约5分钟的时间。请注意，对于已建立的高可用性对，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

- **设备 SSH 密码** - 为 CLI 访问（SSH 或控制台）设置Firewall Threat Defense管理员用户密码。在**确认密码**字段中重复密码。

步骤 5 在 **接口分配**中，将机箱接口分配给实例，然后点击 **下一步**。

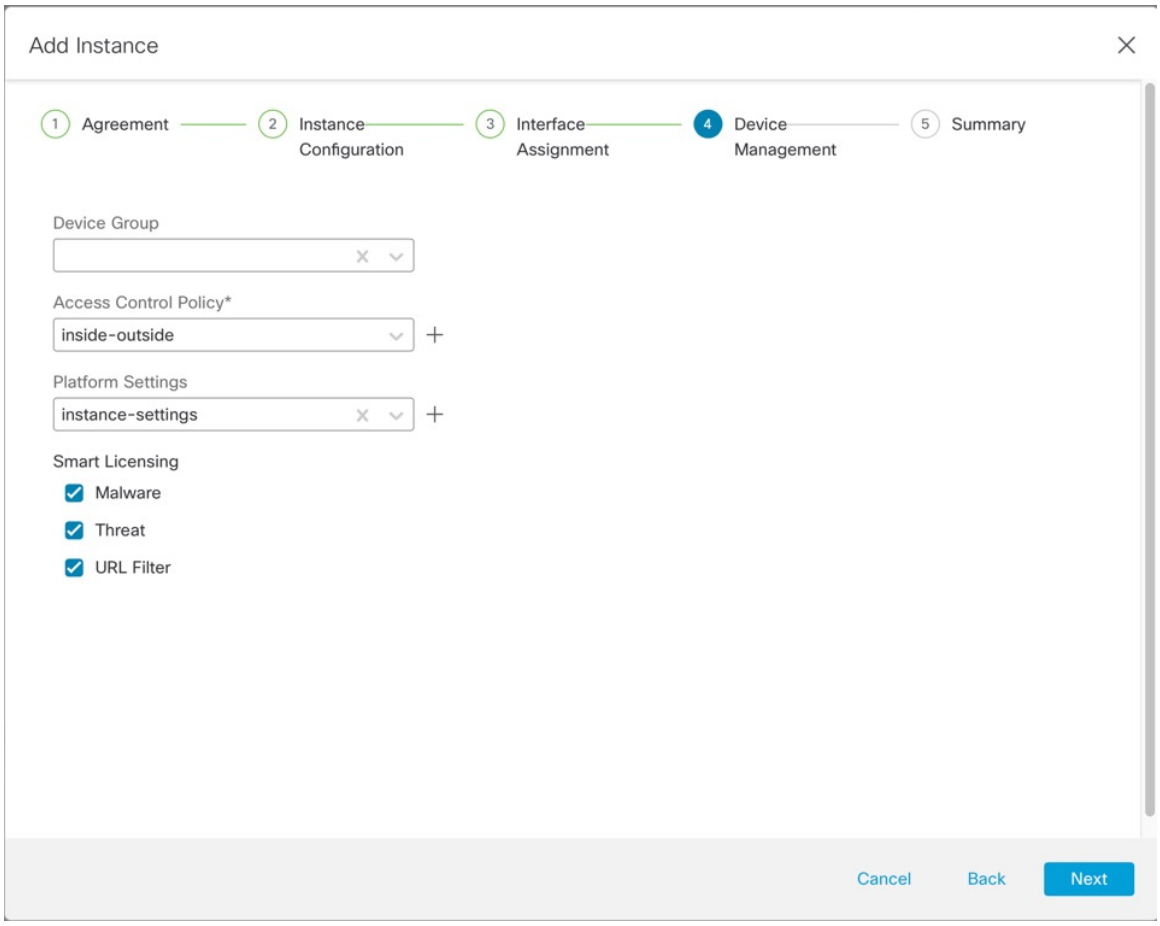
图 *87:* 接口分配



共享接口显示共享图标 ( )。

步骤 6 在 **设备管理**上，设置设备特定的设置，然后点击 **下一步**。

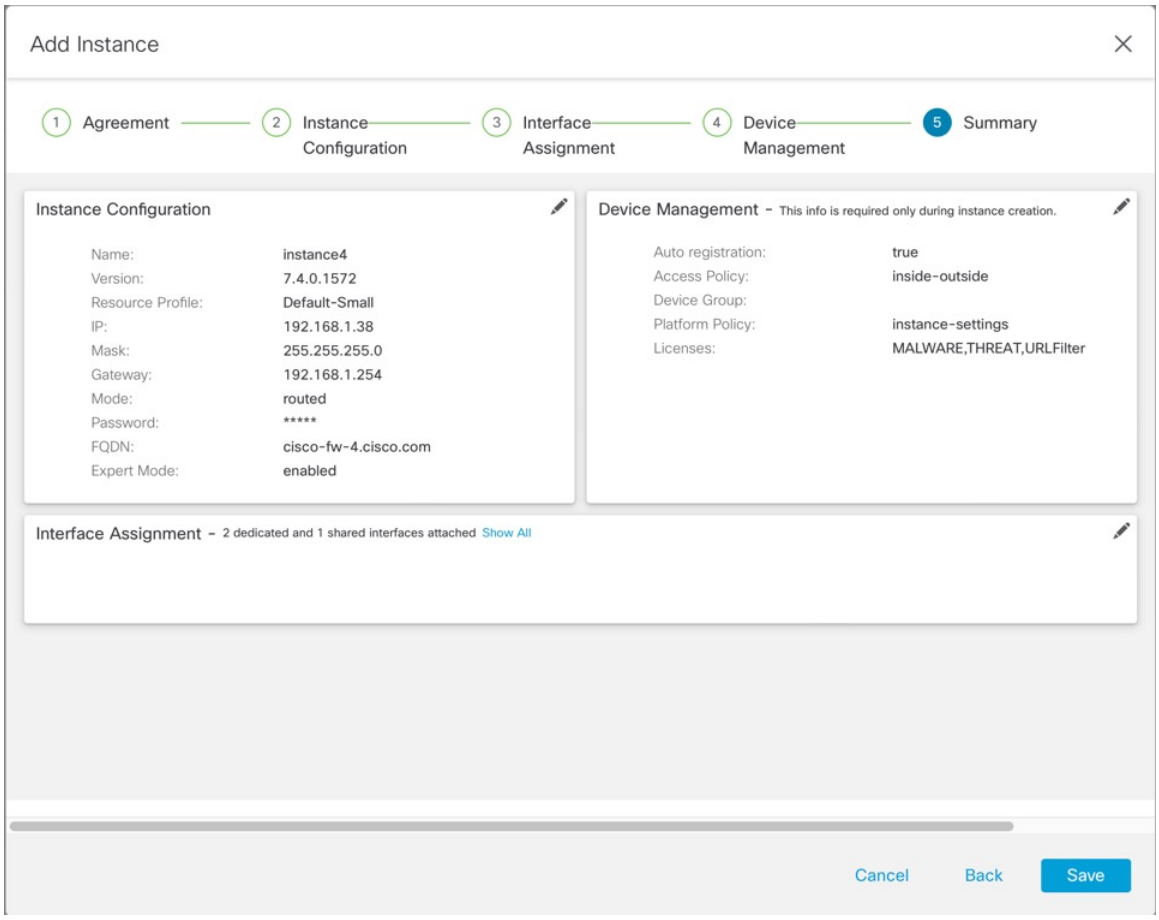
图 *88:* 设备管理



- **设备组**
- **访问控制策略**- 选择现有访问控制策略，或创建新策略。
- **平台设置**-选择现有平台设置策略或创建新策略。
- **智能许可**

步骤 7 在 **摘要**中，确认您的设置，然后点击 **保存**。

图 *89:* 摘要



您可以在保存实例之前编辑此屏幕上的任何设置。保存后，实例将添加到 **实例** 屏幕。

步骤 8 在 **实例** 屏幕上，点击 **保存**。

步骤 9 部署机箱配置。

部署后，该实例将在**设备管理**页面上添加为设备。

注释
在删除实例之前，必须先在**设备管理**页面上取消注册该实例。如果在未取消注册实例的情况下删除该实例，该实例将在**设备管理**中保留为过时条目。

自定义系统配置

您可以配置机箱级别的设置，例如 SNMP。您还可以导入或导出机箱 FXOS 配置。

配置 SNMP

您可以通过在机箱系统配置中指定的其中一个实例的数据接口访问机箱级 MIB。您只能将此实例用于机箱 SNMP 信息。您无法通过机箱管理接口访问 SNMP。

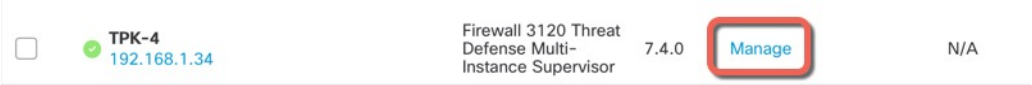
开始之前

- 为其中一个实例配置 SNMP。请参阅SNMP，第 994 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** ()。

图 *90:* 管理机箱

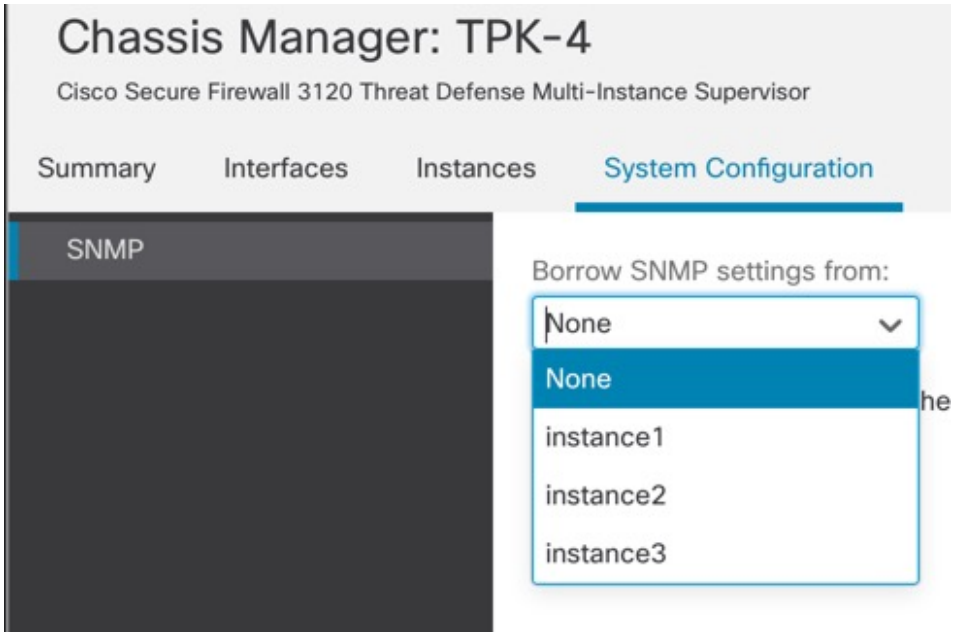


打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

步骤 2 点击 **系统配置**。

步骤 3 选择 **SNMP**，然后从下拉列表中选择实例。

图 *91: SNMP*



可从所选实例访问机箱上的 SNMP。

步骤 4 点击**保存**。

步骤 5 部署机箱配置。

导入或导出机箱配置

使用配置导出功能将包含机箱配置设置的 XML 文件导出到本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于机箱，以返回到已知的正确配置，或从系统故障中恢复。

注释 如果需要将配置导入到相同型号的新机箱中，请联系思科 TAC。

导出时，仅导出机箱配置；不导出实例配置设置。需要使用设备备份/恢复功能单独备份实例。

导入时，机箱上的所有现有配置都将替换为导入文件中的配置。

开始之前

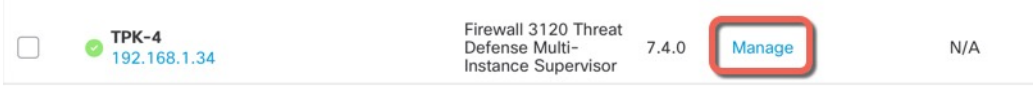
将配置导入到同一机箱时，请确保机箱匹配以下各项：

- 相同的机箱软件版本
- 相同的 Firewall Threat Defense 实例映像
- 相同的网络模块

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

图 *92:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

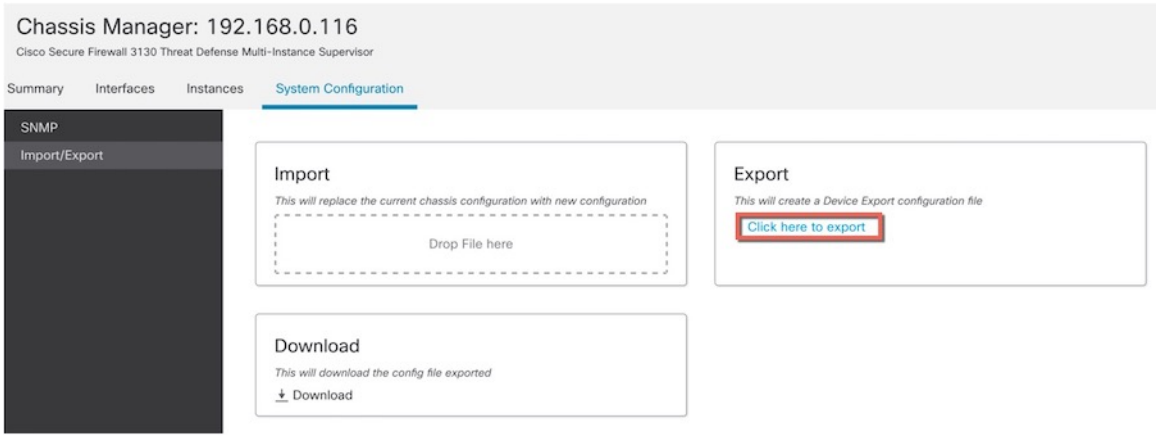
步骤 2 点击 **系统配置**。

步骤 3 点击 **导入/导出**。

步骤 4 要导出配置，请执行以下步骤。

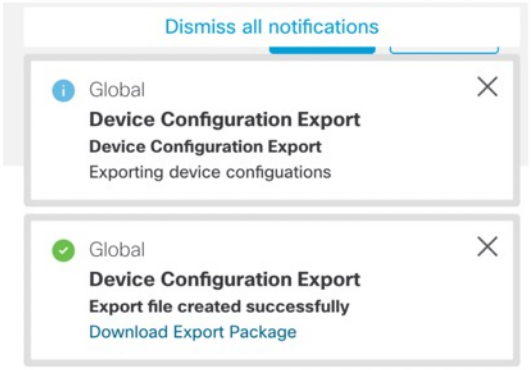
a) 在 **导出** 区域中，点击 **点击此处导出**。

图 *93:* 创建导出文件



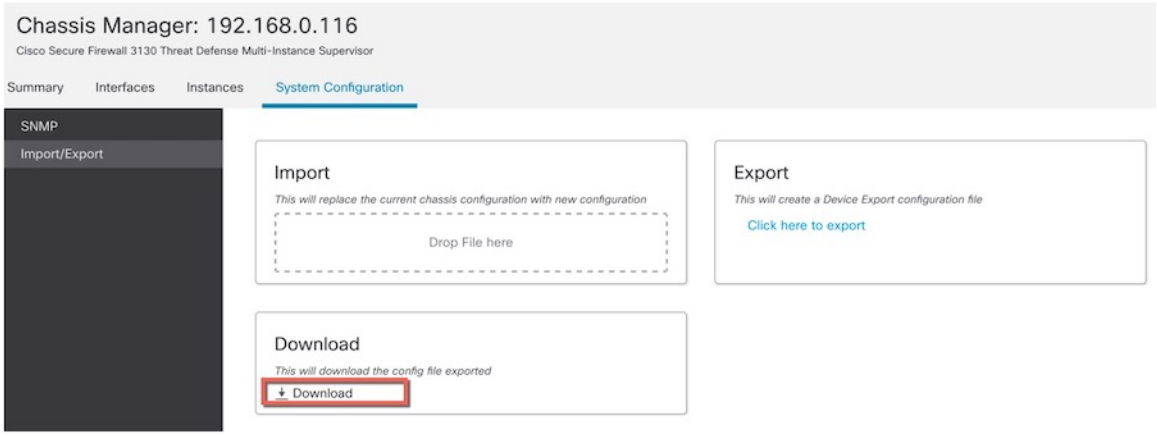
b) 监控 **导出文件创建成功** 消息的通知。

图 *94:* 创建的文件导出成功



c) 点击通知消息（**下载导出包**）或点击 **下载**，下载导出文件。

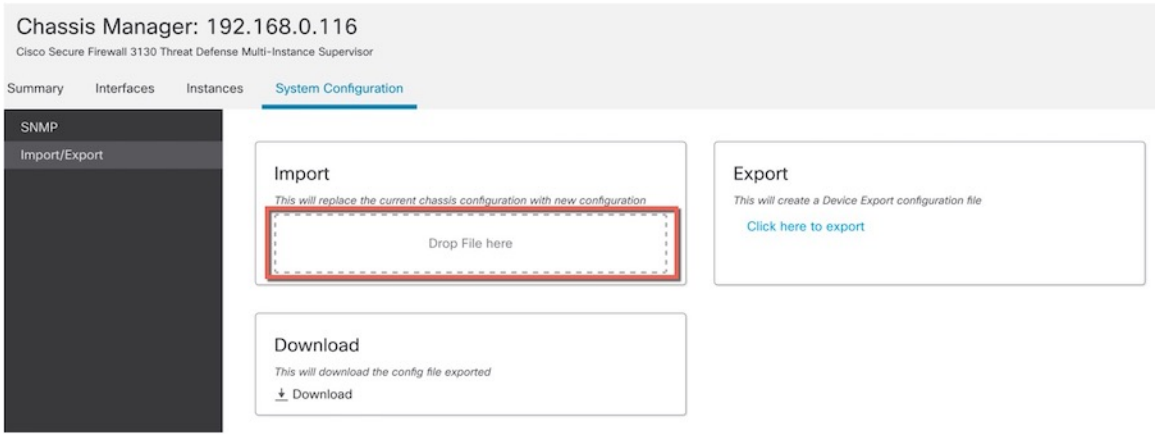
图 *95:* 下载



文件以 **.sfo** 扩展名保存。

步骤 5 要导入配置，请将 **.sfo** 文件拖动到**导入** > **放置文件**区域。

图 ***96:*** 导入



配置机箱平台设置

机箱平台设置可配置一系列用于管理机箱的功能。您可以在多个机箱之间共享策略。如果您希望每个机箱使用不同的设置，则必须创建多个策略。

创建机箱平台设置策略

使用 **平台设置** 页面（**设备** > **平台设置**）管理平台设置策略。此页面指示每个策略的设备类型。 **状态** 列显示策略的设备目标。

过程

步骤 1 选择**设备** > **平台设置**。

步骤 2 对于现有策略，您可以**复制** ()、**编辑** ()或**删除** ()策略。

注意
不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

步骤 3 要创建新策略，请点击**新建策略 (New Policy)**。

a) 从下拉列表中选择 **机箱平台设置** 。
b) 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。
c) （可选）选择要应用策略的**可用机箱**，然后点击**添加 (Add)**（或拖放）以添加所选机箱。

d) 点击**保存**。

系统创建策略，并打开以进行编辑。

步骤 4 要更改策略的目标机箱，请点击要编辑的平台设置策略旁边的 **编辑** (✎) 图标。

a) 点击**策略分配 (Policy Assignment)**。
b) 要将机箱分配给策略，请在 **可用机箱** 列表中选择该机箱，然后点击 **添加**。
c) 要删除机箱分配，请点击 **所选机箱** 列表中机箱旁边的 **删除** (🗑) 。
d) 点击**确定**。

配置 DNS

如果机箱要求将主机名解析为 IP 地址，则您需要指定 DNS 服务器。这些机箱 DNS 设置独立于每个实例的 DNS 设置，后者在设备平台设置中配置。

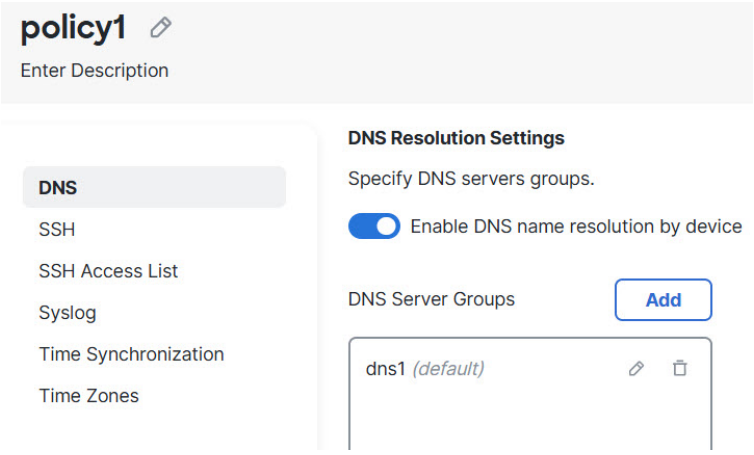
配置多个 DNS 服务器时，机箱仅以任意随机顺序使用服务器。您最多可以在四个 DNS 服务器组中配置四个服务器。例如，可以为单个服务器组配置四台服务器，也可以为四个服务器组配置每组一台服务器。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **DNS**。

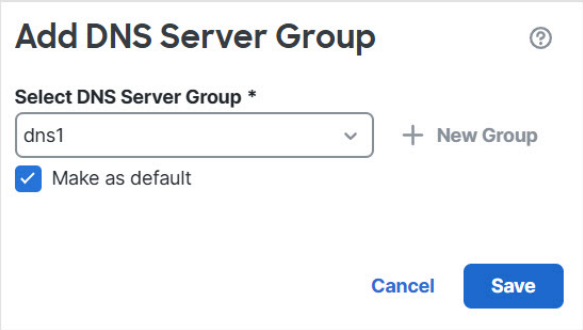
图 ***97: DNS***



步骤 3 启用 **启用按设备 DNS 域名解析** 滑块。

步骤 4 点击 **添加** 以添加 DNS 服务器组。

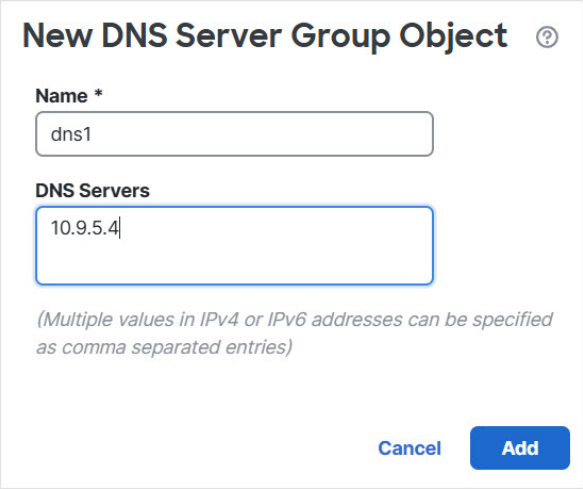
图 *98:* 添加 ***DNS*** 服务器组



步骤 5 选择现有的 DNS 服务器组（请参阅创建 DNS 服务器组对象，第 2640 页），或点击 (+) **新建组 (New Group)**。

如果添加新组，您会看到以下对话框。以逗号分隔值提供名称和最多四个 DNS 服务器 IP 地址，然后点击 **添加**。

图 *99:* 新建 ***DNS*** 服务器组对象



步骤 6 点击 **保存**，将 DNS 服务器添加到列表中。

步骤 7 重复这些步骤添加其他服务器组。

确保在所有合并的组中最多只能识别四个 DNS 服务器。

步骤 8 点击**保存** 以保存对策略的所有更改。

配置 SSH 和 SSH 访问列表

要在管理接口上允许从管理员用户到机箱的 SSH 会话，请启用 SSH 服务器并配置允许的网络。

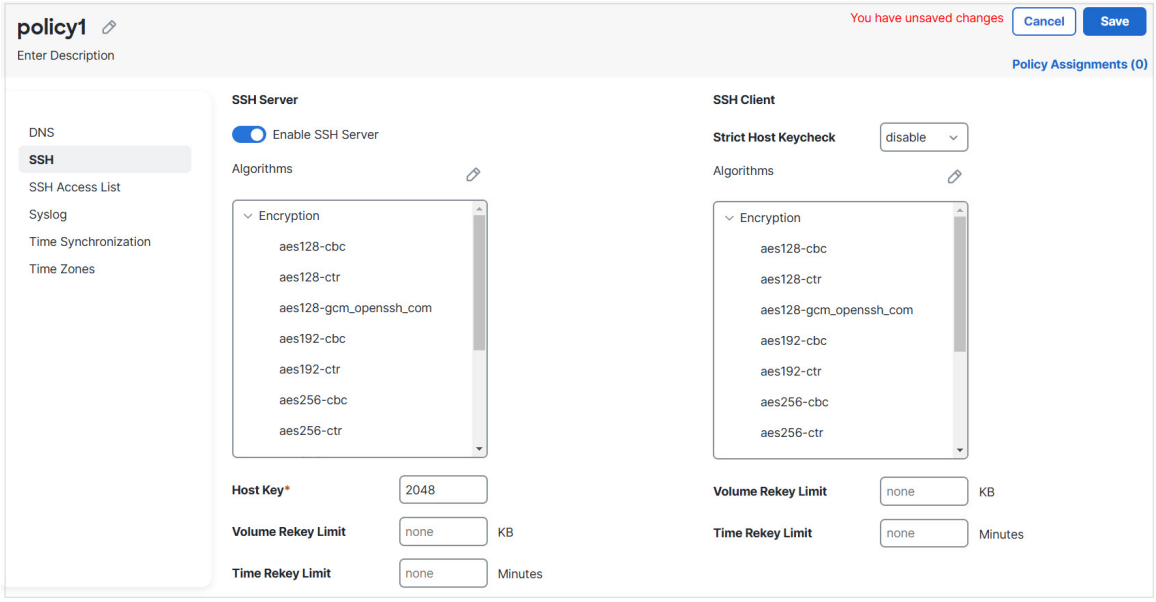
过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **SSH**。

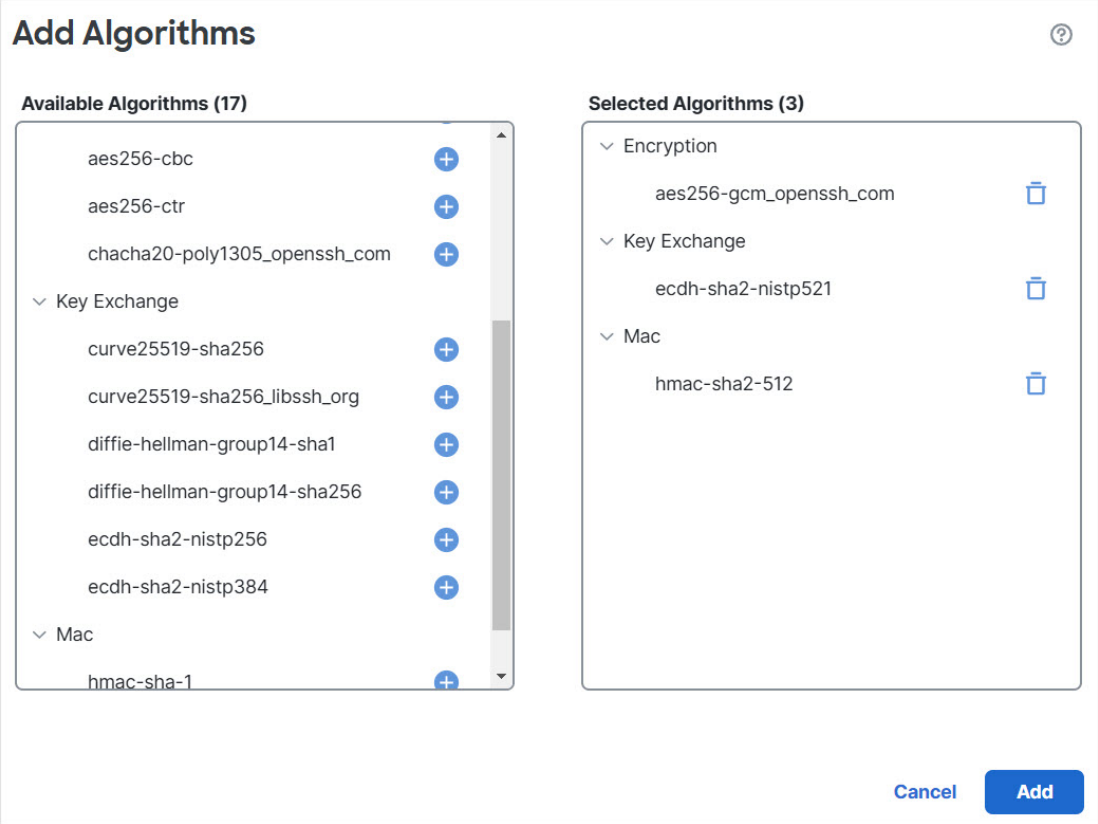
步骤 3 要启用到机箱的 SSH 访问，请选中 **启用 SSH (Enable SSH)** 滑块。

图 *100: SSH*



步骤 4 要设置允许的**算法**，请点击 **编辑** ()。

图 *101:* 添加算法



a) 选择**加密**算法：

b) 选择**密钥交换**算法。

密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。

c) 选择 **Mac** 完整性算法。

步骤 5 对于**主机密钥**，请输入 RSA 密钥对的模块大小。

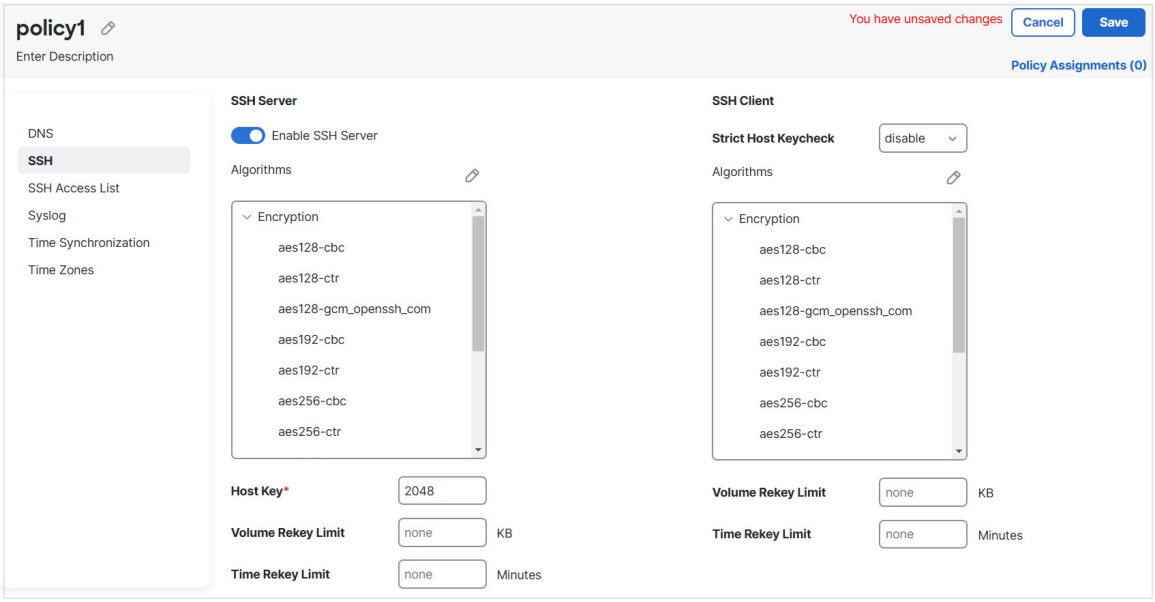
模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

步骤 6 对于服务器**密钥更新数量限制**，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。

步骤 7 对于服务器**密钥更新时间限制**，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

步骤 8 对于 **SSH 客户端**，请配置以下设置。

图 *102: SSH*

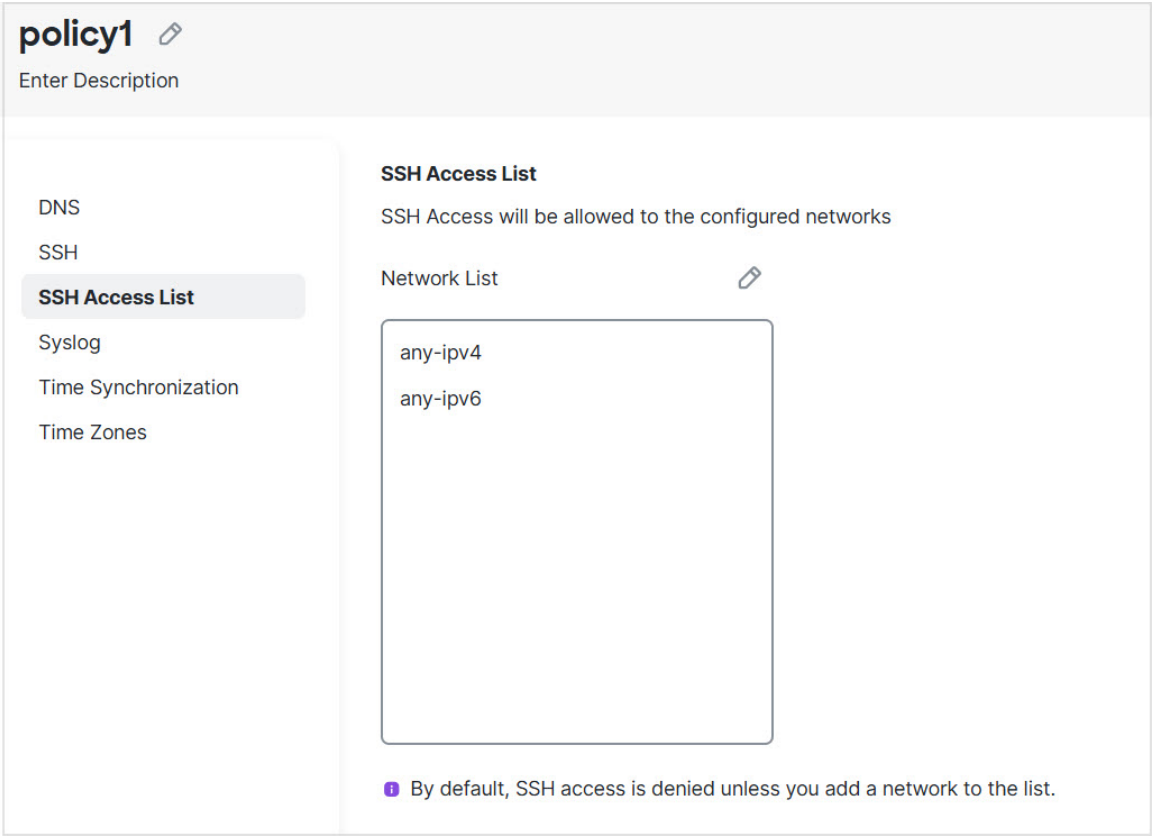


- **严格主机密钥检查 (Strict Host Keycheck)** - 选择**启用 (enable)**、**禁用 (disable)**或**提示 (prompt)**来控制 SSH 主机密钥检查。
  - **启用 (enable)** - 如果 FXOS 已知的主机文件中不包括主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
  - **提示 (prompt)** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
  - **禁用 (disable)** -（默认）机箱将自动接受以前未存储的主机密钥。
- **算法 (Algorithms)** - 点击 **编辑** ()，然后选择**加密 (Encryption)**、**密钥交换 (Key Exchange)** 和 **Mac** 算法。
- **密钥更新数量限制 (Volume Rekey Limit)** - 请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。
- **密钥更新时间限制 (Time Rekey Limit)** - 请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

步骤 9 选择 **SSH 访问列表 (SSH Access List)**。您需要先允许访问 IP 地址或网络，然后才能使用 SSH。

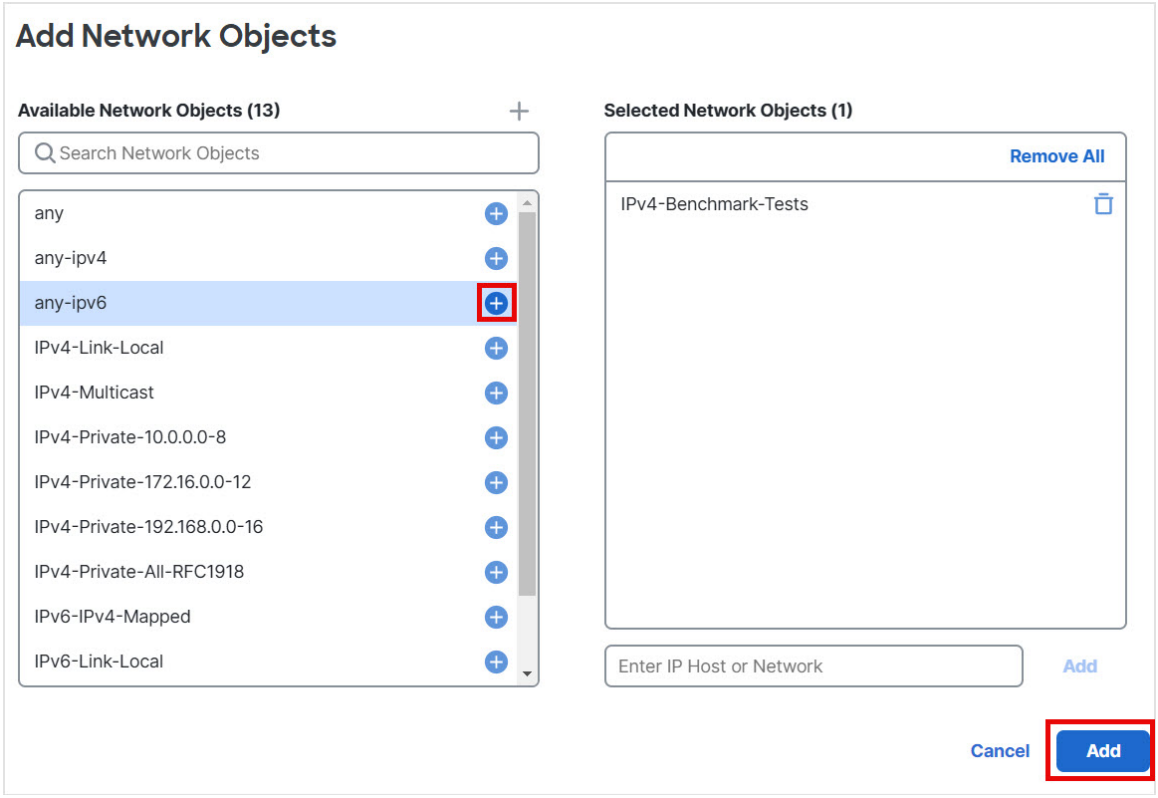
您最多可以添加 25 个 CRL。

图 *103: SSH* 访问列表



步骤 10 点击 **编辑** (✎) 添加网络对象，然后点击**保存**。您也可以手动输入 IP 地址。

图 *104:* 网络对象



步骤 11 点击**保存** 以保存对策略的所有更改。

配置系统日志

您可以从机箱启用系统日志。这些系统日志来自机箱的 FXOS 操作系统。

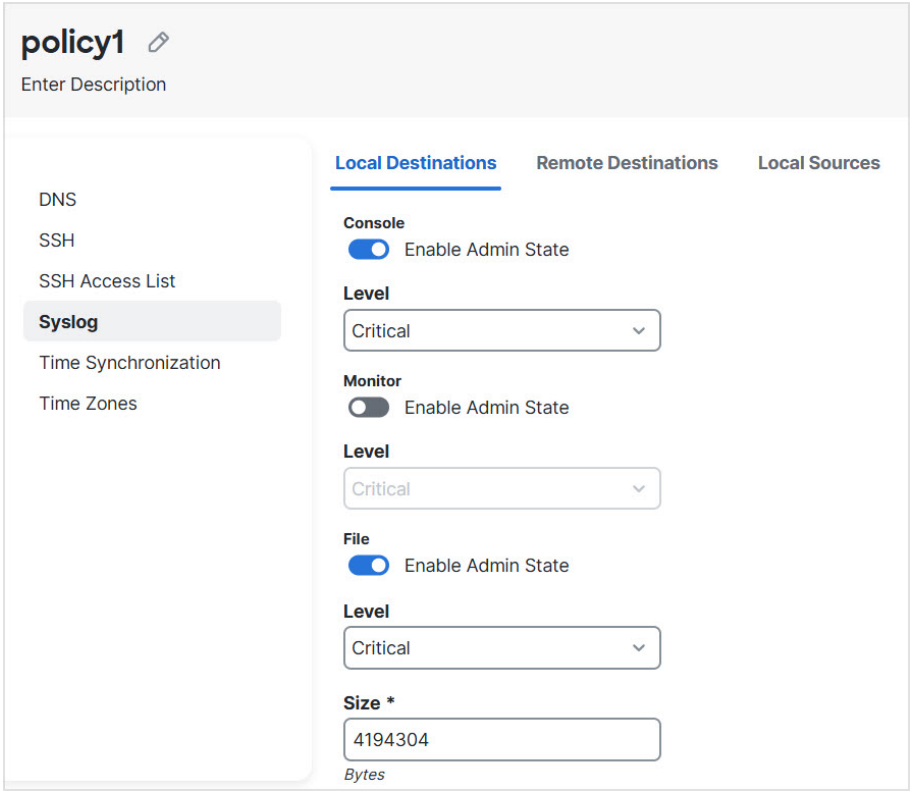
过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **系统日志**。

步骤 3 在 **本地目的** 选项卡上，填写以下字段。

图 *105:* 系统日志本地目标

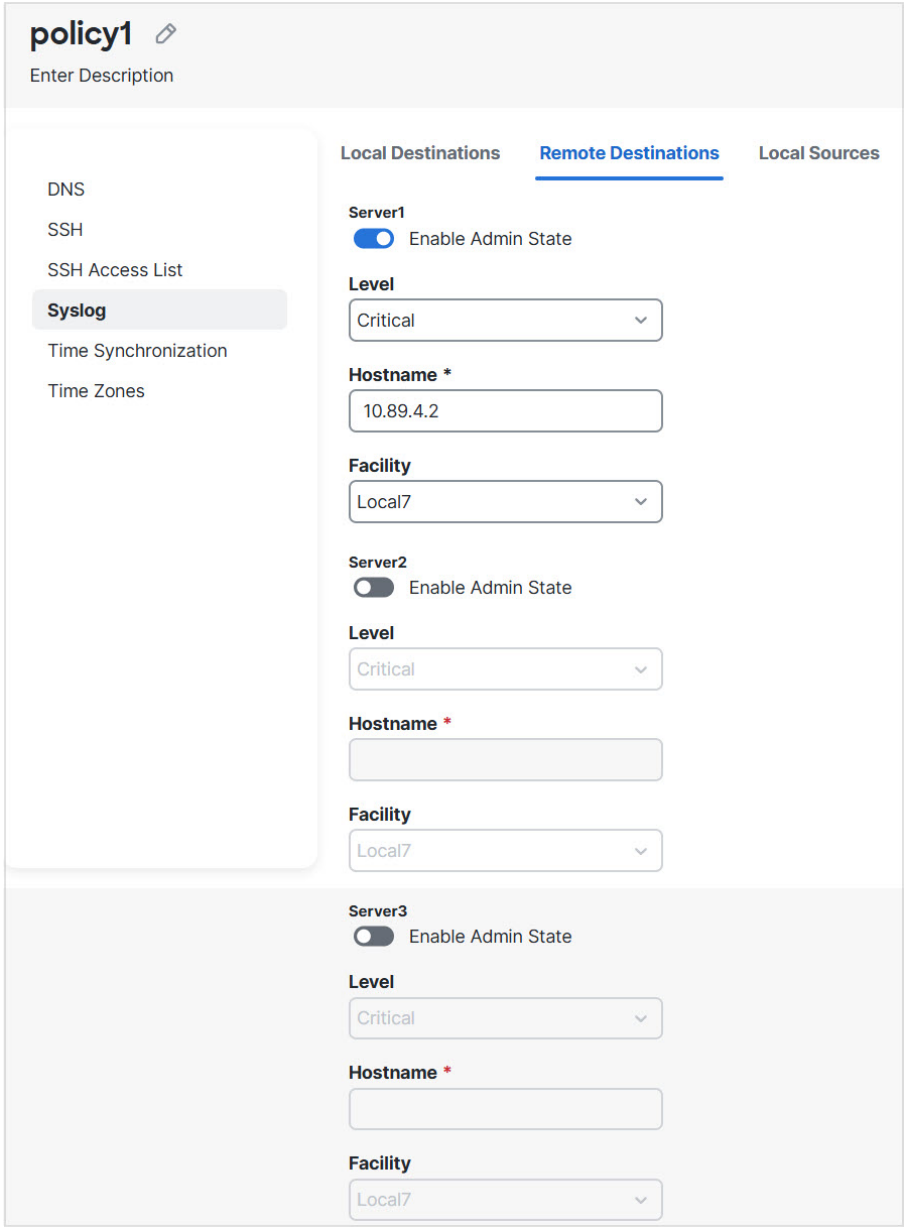


名称	说明
控制台 (Console) 部分	
管理状态 (Admin State) 字段	机箱是否在控制台上显示系统日志消息。 如果您想在控制台上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在控制台上。
级别 (Level) 字段	如果选中了**控制台 - 管理状态 (Console - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在控制台上显示的最低消息级别。机箱在控制台上显示此级别及以上消息。这可以是以下其中一项： • 紧急 • 提醒 • 严重
监视器 (Monitor) 部分	

名称	说明
管理状态 (Admin State) 字段	机箱是否在监视器上显示系统日志消息。 如果您想在监视器上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在监视器上。
级别 (Level) 下拉列表	如果选中了**监视器 - 管理状态 (Monitor - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在监视器上显示的最低消息级别。系统在监视器上显示此级别及以上消息。这可以是以下其中一项： • **紧急** • **提醒** • **严重** • **错误** • **警告** • **通知** • **信息** • **调试**

步骤 4 在**远程目的 (Remote Destinations)** 选项卡上，为最多三个外部日志填写下列字段，这些日志可以存储机箱生成的消息：

图 *106:* 系统日志远程目的



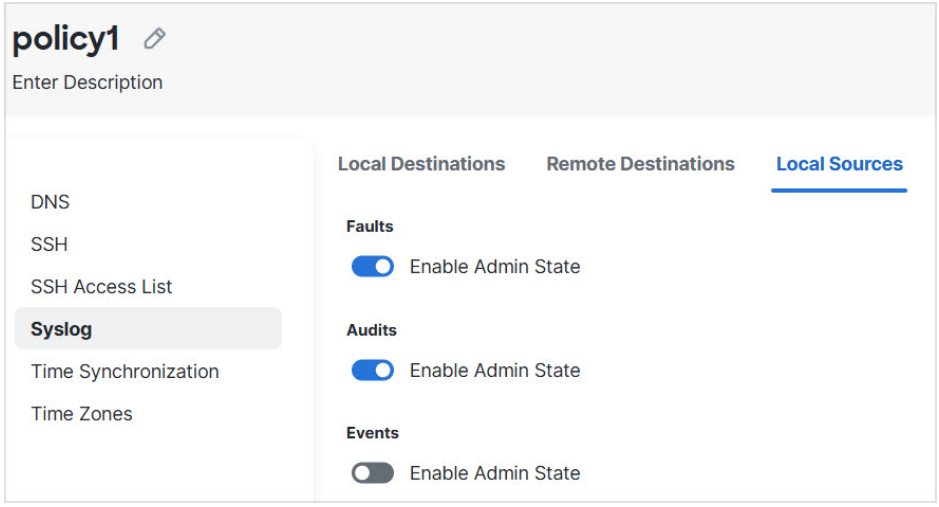
通过将系统日志消息发送到远程目的，您可以根据外部系统日志服务器上的可用磁盘空间存档消息，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

名称	说明
管理状态 (Admin State) 字段	如果您想在远程日志文件中存储系统日志消息，请选中**启用 (Enable)** 复选框。

名称	说明
级别 (Level) 下拉列表	选择您想让系统存储的最低消息级别。系统在远程文件中存储此级别及以上消息。这可以是以下其中一项： • 紧急 • 提醒 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
主机名/IP 地址 (Hostname/IP Address) 字段	远程日志文件所驻留的主机名或 IP 地址。 注释 如果使用主机名而不使用 IP 地址，必须配置 DNS 服务器。
设备 (Facility) 下拉列表	为系统日志服务器选择要用作文件消息基础的系统日志设备。这可以是以下其中一项： • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

步骤 5 在 **本地源** 选项卡上，填写以下字段。

图 *107:* 系统日志本地源



名称	说明
故障 > **启用管理状态**	启用系统故障日志记录。
审核 > **启用管理状态**	启用审核日志。
事件 > **启用管理状态**	启用系统事件日志记录。

步骤 6 点击**保存** 以保存对策略的所有更改。

配置时间同步

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。您最多可以配置 4 个 NTP 服务器。

注释

- FXOS 使用 NTP 版本 3。
- 如果外部NTP服务器的层值为13或更大，则应用实例无法同步到FXOS机箱上的NTP服务器。每次 NTP 客户端同步到 NTP 服务器时，层值就会增加 1。

  如果您已设置自己的 NTP 服务器，则可以在服务器上的 /etc/ntp.conf 文件中找到它的层值。如果 NTP 服务器的层值大于或等于 13，则可以更改 ntp.conf 文件中的层值并重新启动服务器，或者使用其他 NTP 服务器（例如：pool.ntp.org）。

开始之前

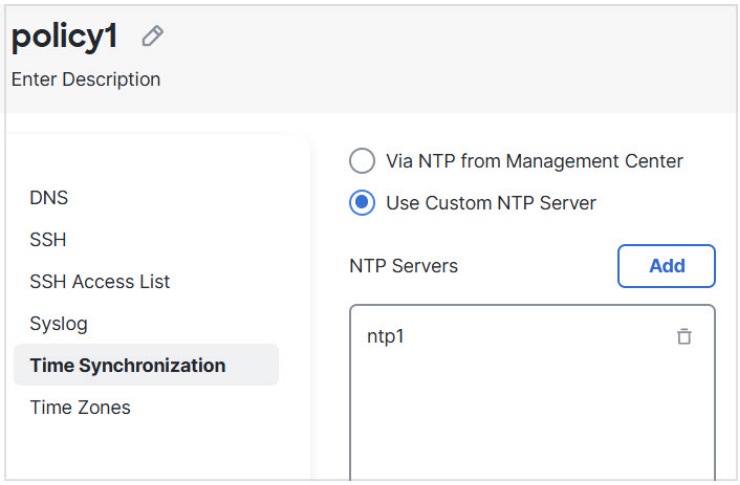
如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 配置 DNS，第 246 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **时间同步**。

图 ***108:*** 时间同步



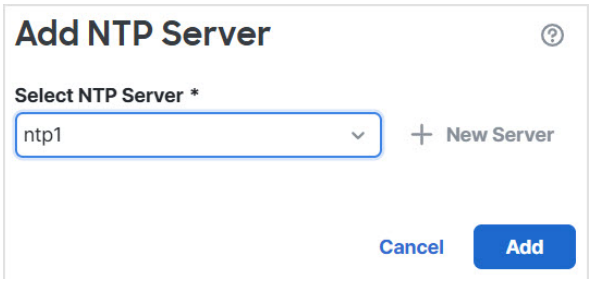
步骤 3 如果要从 防火墙管理中心获取时间，请 **从管理中心点击通过 NTP**。

此选项可确保机箱和 防火墙管理中心 具有相同的时间。

步骤 4 要使用外部 NTP 服务器，请点击 **使用自定义 NTP 服务器**。

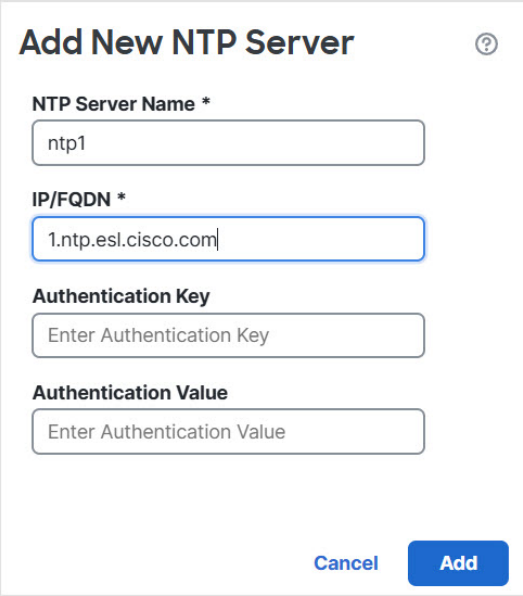
a) 点击 **添加** 来添加服务器。

图 ***109:*** 添加 ***NTP*** 服务器



b) 从下拉菜单中选择任何已定义的服务器，然后点击 **添加**，或点击 **新建服务器** 以添加新服务器。

图 *110:* 添加新的 *NTP* 服务器



c) 对于新服务器，请输入以下字段，然后点击 **添加**。

- **NTP 服务器名称**- 用于标识此服务器的名称。
- **IP/FQDN**- 服务器的 IP 地址或主机名。
- **验证密钥**和**验证值** - 从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

  仅支持使用 SHA1 进行 NTP 服务器身份验证。

步骤 5 点击**保存** 以保存对策略的所有更改。

配置时区

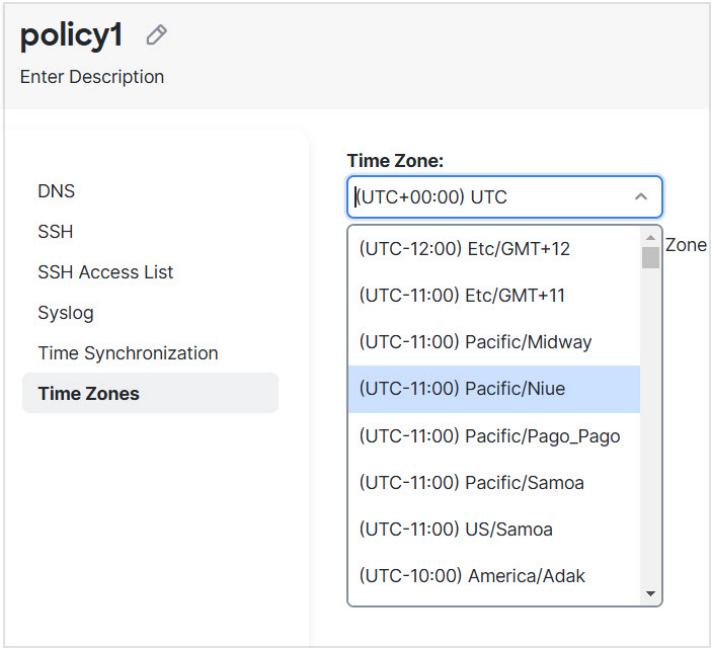
设置机箱的时区。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **时区**。

图 *111:* 时区



步骤 3 从下拉菜单中选择 **时区** 。

步骤 4 点击**保存** 以保存对策略的所有更改。

管理多实例模式

本节介绍不太常见的任务，包括在 FXOS CLI 中更改设置或更改分配给机箱的接口。

在 CLI 启用多实例模式

如果要在将设备添加到防火墙管理中心之前将其预配置为多实例模式，则可以执行此程序。要使用防火墙管理中心 来转换为多实例模式，请参阅 将设备转换为多实例模式 ，第 223 页。

您需要在控制台端口连接到 Firewall Threat Defense CLI，以启用多实例模式。配置模式后，可以将其添加到 防火墙管理中心。

注释 虽然您可以在管理端口上连接到 SSH，但我们建议使用控制台端口来避免多次断开连接。此程序涉及控制台端口。

过程

步骤 1 连接到机箱控制台端口。

控制台端口连接到 FXOS CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

第一次登录FXOS时，系统会提示您更改密码。

注释
如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关重新映像程序的信息，请参阅 FXOS 故障排除指南。

示例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

步骤 3 检查您当前的模式：本地模式或容器模式。如果模式为本地模式，您可以继续执行此程序以转换为多实例（容器）模式。

show system detail

示例：

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

步骤 4 连接到 Firewall Threat Defense CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

步骤 5 首次登录 Firewall Threat Defense 时，系统会提示您接受一般条款。然后，系统将显示 CLI 设置脚本。

设置脚本允许您设置管理接口 IP 地址和其他设置。但是，当您转换为多实例模式时，仅保留以下设置。

- 管理员密码（您在初始登录时设置）
- DNS 服务器
- 搜索域

您将在多实例模式命令中重置管理 IP 地址和网关。转换为多实例模式后，您可以在 FXOS CLI 中更改管理设置。请参阅在 FXOS CLI 中更改机箱管理设置，第 265 页。

步骤 6 启用多实例模式，设置机箱管理接口设置，并识别 防火墙管理中心。您可以使用 IPv4 和/或 IPv6 静态寻址；不支持 DHCP。输入命令后，系统将提示您清除配置并重新启动。输入 **ERASE**（全部大写）。系统将重新启动，并在更改模式时清除配置，但您在 命令中设置的管理网络设置和管理员密码除外。机箱主机名设置为“firepower-*model*”。

IPv4：

configure multi-instance network ipv4 *ip_address network_mask gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv4_address* | **DONTRESOLVE**} *registration_key nat_id*

IPv6：

configure multi-instance network ipv6 *ipv6_address prefix_length gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv6_address* | **DONTRESOLVE**} *registration_key nat_id*

请参阅以下 **manager** 组件：

- {*hostname* | *ipv4_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the 防火墙管理中心. 必须至少有一个设备（防火墙管理中心 或机箱）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信信道。如果未在此命令中指定管理器主机名或 IP 地址，然后输入 **DONTRESOLVE**；这种情况下，机箱必须具有可访问的 IP 地址或主机名，并且必须指定 *nat-id*。
- *registration_key*-输入您选择的一次性注册密钥，注册时也要在 防火墙管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。
- *nat_id*-指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 防火墙管理中心 上指定它。如果您不指定管理器地址或主机名，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。

要将模式更改回设备模式，必须使用 FXOS CLI 并输入 **scope system** 及 **set deploymode native**。请参阅在 FXOS CLI 中更改机箱管理设置，第 265 页。

示例：

```
> configure multi-instance network ipv4 172.16.0.104 255.255.255.0 172.16.0.1 manager
fmc1 172.16.0.103 impala67 winchester1
```

```
WARNING: This command will discard any FTD configuration (except admin's credentials).
Make sure you backup your content. All previous content will be lost. System is going to
be re-initialized.
Type ERASE to confirm:ERASE
Exit...
>
```

步骤 7 将机箱添加到 防火墙管理中心。请参阅添加机箱，第 52 页。

更改分配给实例的接口

您可以在实例上分配或取消分配接口。添加新接口或删除未使用接口对实例配置的影响最小。您也可以编辑已分配的 EtherChannel 的成员，而不影响实例。但是，删除安全策略中使用的接口会影响配置。

可以直接在实例配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。

引用安全区域的策略不受影响。

注释 为实现高可用性，您需要对另一台设备进行相同的接口更改。否则，高可用性可能无法正常运行。

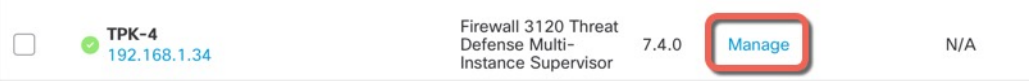
开始之前

- 根据配置实例，第 222 页配置接口。
- 如果您要将已分配的接口添加到 EtherChannel，则需要先从实例取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到实例。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

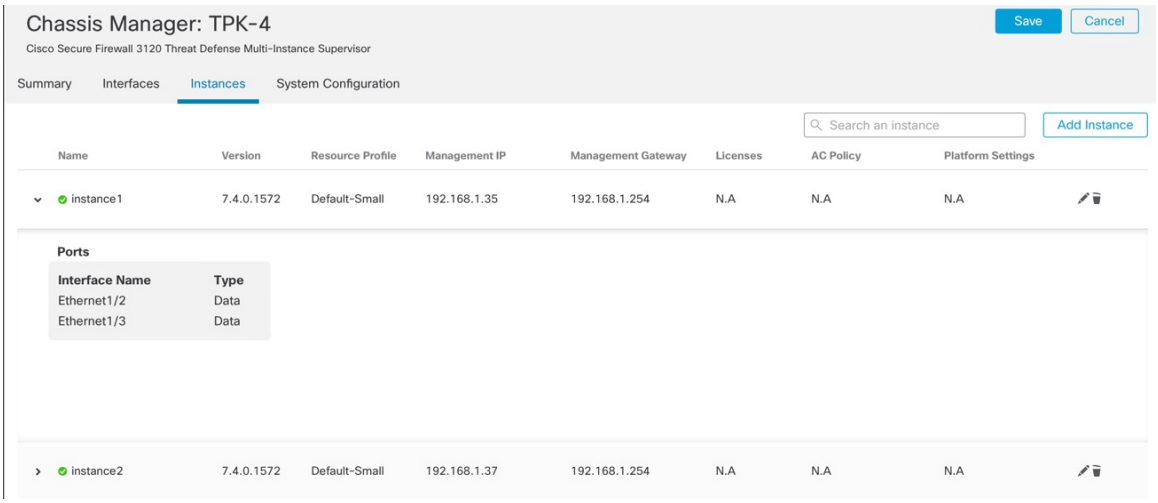
图 *112:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

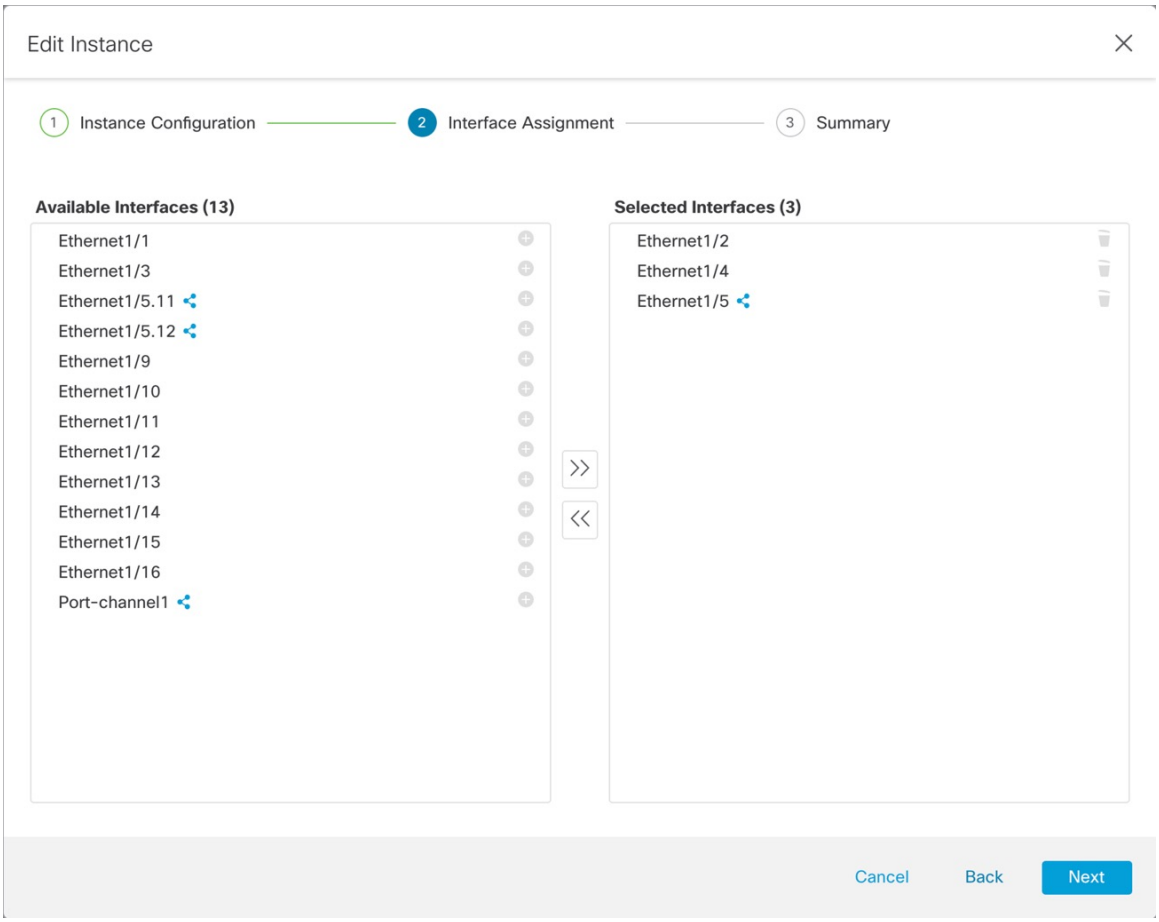
步骤 2 点击 **实例**，然后点击要为其更改接口的实例旁边的 **编辑** (✎) 。

图 *113:* 实例



步骤 3 点击 **下一步**，直到进入 **接口分配** 屏幕。

图 *114:* 接口分配



共享接口显示共享图标 ( )。

步骤 4 更改接口，然后点击 **下一步**。

步骤 5 点击 **摘要** 屏幕上的 **保存**。

步骤 6 为实现高可用性，您需要对另一台设备进行相同的接口更改。否则，高可用性可能无法正常运行。

在 FXOS CLI 中更改机箱管理设置

如果要更改机箱管理接口 IP 地址和网关，将 防火墙管理中心 更改为新的管理器、更改管理员密码或禁用多实例模式，可以从 FXOS CLI 执行此操作。

过程

步骤 1 连接到机箱控制台端口。

控制台端口连接到 FXOS CLI。

注释
我们建议使用控制台端口。您还可以使用SSH连接到管理接口（如果在防火墙管理中心中的机箱平台设置中进行了配置）；但是，如果更改管理 IP 地址，则会断开连接。

步骤 2 使用用户名 **admin** 和初始设置期间设定的密码登录。

步骤 3 更改管理 IP 地址。您可以使用静态 IPv4 和/或 IPv6 地址。

IPv4：

scope fabric-interconnect

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

IPv6：

scope fabric-interconnect

scope ipv6-config

set out-of-band static ipv6 *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

示例：

IPv4：

```
firepower-3110# scope fabric-interconnect
firepower-3110 /fabric-interconnect # set out-of-band static ip 10.5.23.8 netmask
255.255.255.0
gw 10.5.23.1
```

IPv6：

```
firepower-3110# scope fabric-interconnect
firepower-3110 / fabric-interconnect # scope ipv6-config
firepower-3110 / fabric-interconnect /ipv6-config # set out-of-band static ipv6 2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

步骤 4 更改 防火墙管理中心。

您应先从当前 防火墙管理中心取消注册机箱。

enter device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

系统将提示您输入注册密钥。

您可以从任何范围输入此命令。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the 防火墙管理中心。必须至少有一个设备（防火墙管理中心或机箱）具有可访问的IP地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果未在此命令中指定 **hostname**，则机箱必须具有可访问的 IP 地址或主机名，并且必须指定 **nat-id**。
- **nat-id** *nat_id*- 指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 防火墙管理中心 机箱上指定它。如果您不指定 **hostname**，则必须设置，但我们建议您始终设置NAT ID，即使您指定了主机名或IP地址。NAT ID不得超过37个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。
- **Registration Key:** *reg_key*- 系统将提示您输入选择的一次性注册密钥，注册机箱时也要在 防火墙管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

示例：

```
firepower-3110# enter device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

步骤 5 更改 admin 密码。

scope security

set password

输入密码：*password*

确认密码：*password*

示例：

```
firepower-3110# scope security
firepower-3110 /security # set password
Enter new password: Sw@nsong67
Confirm new password: Sw@nsong67
firepower-3110 /security #
```

步骤 6 禁用多实例模式并将系统设置回设备模式。

scope system

set deploymode native

系统会提示您重新启动 。

示例：

```
firepower-3110# scope system
firepower-3110 /system # set deploymode native
All configuration and bootable images will be lost and system will reboot.
If there was out of band upgrade, it might reboot with the base version and
need to re-image to get the expected running version.
Do you still want to change deploy mode? (yes/no):yes
firepower-3110 /system #
```

要将模式更改回多实例模式，请输入 **set deploymode container**。您可以使用 **show system detail** 命令来检测当前模式。

监控多实例模式

本部分可帮助您对多实例模式机箱和实例进行故障排除和诊断。

监控多实例设置

显示系统详细信息

此 FXOS 命令显示当前模式：本地或容器。如果模式为本地（也称为设备模式），则可以转换为多实例（容器）模式。请注意，多实例模式下的提示/名称是通用的“firepower-<model> "，而设备模式下的提示符是您为 Firewall Threat Defense 设置的主机名（默认情况下为“firepower”）

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

范围系统 > 显示

此 FXOS 命令以表格格式显示当前模式。请注意，多实例模式下的提示/名称是通用的“firepower-<model> "，而设备模式下的提示符是您为 Firewall Threat Defense 设置的主机名。

```
firepower-3110# scope system
firepower-3110 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- ------------------
    firepower-3110
               Stand Alone Container   10.89.5.42        ::


3110-1# scope system
3110-1 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- ------------------
    3110-1     Stand Alone Native      10.89.5.41        ::
3110-1 /system #
```

监控实例接口

show portmanager switch forward-rules hardware mac-filter

此命令显示两个实例的内部交换机转发规则，为每个实例分配一个专用物理接口。以太网接口 1/2 分配给 ftd1，以太网接口 1/1 分配给 ftd2。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

```
secfw-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT      PKT_CNT       DMAC
1        0          17        0        17          19        29164  0:0:0:0:0:0
2        0          19        0        19          17        67588  0:0:0:0:0:0
3        0           1        0       101        1541            0  a2:5b:83:0:0:15
4        0           1        0       101        1541         8181  ff:ff:ff:ff:ff:ff
5        0           2        0       102        1540            0  a2:5b:83:0:0:18
6        0           2        0       102        1540          431  ff:ff:ff:ff:ff:ff
7        0          17        0         0           0        11133  0:0:0:0:0:0
8        0          17        0         0           0            0  0:0:0:0:0:0
```

此命令显示共享物理接口分配给两个实例的两个实例的内部交换机转发规则。以太网接口 1/1 在 ftd1 和 ftd2 之间共享。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

MCAST 组 4096 用于在 ftd1 和 ftd2 之间复制广播流量。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT      PKT_CNT       DMAC
1        0          17        0        17          19         2268  0:0:0:0:0:0
2        0          19        0        19          17         4844  0:0:0:0:0:0
3        0           1        0       101        1541            0  a2:5b:83:0:0:9
4        0           1        0       101        4096          546  ff:ff:ff:ff:ff:ff
```

```
5         0          1        0      101      1540            0  a2:5b:83:0:0:c
6         0         17        0        0         0         1263  0:0:0:0:0:0
7         0         17        0        0         0            0  0:0:0:0:0:0
```

此命令显示分配给两个实例的共享子接口的两个实例的内部交换机转发规则。以太网接口 1/1.2452 在 ftd1 和 ftd2 之间共享。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

MCAST 组 4097 用于在 ftd1 和 ftd2 之间复制广播流量。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19        21305  0:0:0:0:0:0
2        0         19       0       19         17        50976  0:0:0:0:0:0
3     2452          1       0      101       1541          430  a2:5b:83:0:0:f
4     2452          1       0      101       4097            0  ff:ff:ff:ff:ff:ff
5     2452          1       0      101       1540            0  a2:5b:83:0:0:12
6        0         17       0        0         0        11038  0:0:0:0:0:0
7        0         17       0        0         0            0  0:0:0:0:0:0
```

show portmanager switch ecmp-groups detail

使用此命令可列出每个实例 Ecmp-Vport-物理端口映射详细信息。



注释 物理端口 18 是内部交换机和实例之间的背板上行链路接口。

```
firepower-3140(local-mgmt)# show portmanager switch ecmp-groups detail
       ECMP-GROUP  VPORT      PHYSICAL-PORT
1      1536        256        18
2      1537        257        18
3      1538        258        18
4      1539        259        18
5      1540        260        18
6      1541        261        18
7      1542        262        18
8      1543        263        18
9      1544        264        18
10     1545        265        18
```

show portmanager switch mcast-groups detail

使用此命令可列出 MCAST 组成员身份详细信息。

```
firepower-3140(local-mgmt)# show portmanager switch mcast-groups detail
       MCAST-GROUP
1      4096
       Member-ports
       Ethernet 1/1
       ECMP-ID 1541
       ECMP-ID 1540
```

show portmanager counters mcast-group

使用此命令可检查 MCAST 组数据包计数器。

```
firepower-3140(local-mgmt)# show portmanager counters mcast-group 4096
PKT_CNT: 8106
```

show portmanager counters ecmp

使用此命令可检查 ECMP 组数据包计数器。

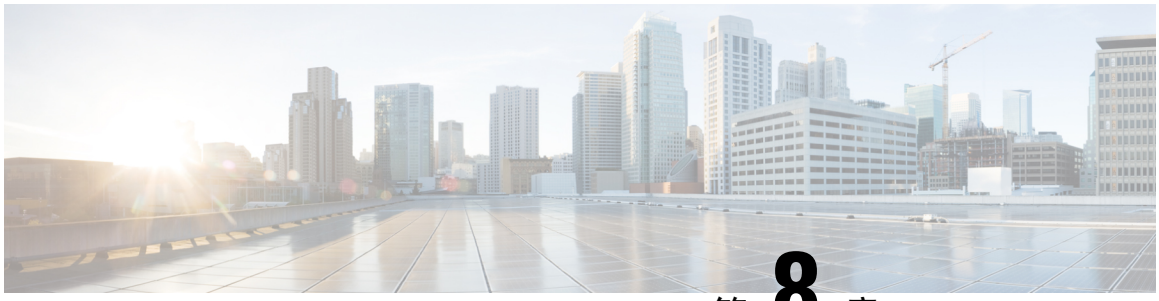
```
firepower-3140(local-mgmt)# show portmanager counters ecmp 1541
PKT_CNT: 430
```

多实例模式的历史记录

表 16:

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Cisco Secure Firewall 4225 的实例数从 15 个增加到 21 个	10.0.0	10.0.0	Cisco Secure Firewall 4225 的最大实例数从 15 个增加到 21 个。
防火墙管理中心中的多实例模式转换	7.6.0	7.6.0	现在，您可以将应用模式设备注册到防火墙管理中心，然后将其转换为多实例模式，而无需使用 CLI。 新增/修改的屏幕： • **设备** > **设备管理**，然后对于某个设备，点击 **更多** (⋮) > **转换为多实例** • **设备** > **设备管理**，然后选择多个设备并选择**选择批量操作** > **转换为多实例**
Cisco Secure Firewall 4200 的多实例模式	7.6.0	7.6.0	Cisco Secure Firewall 4200 现已支持多实例模式。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Cisco Secure Firewall 3100 的多实例模式。	7.4.1	7.4.1	您可以将 Cisco Secure Firewall 3100 作为单个设备（设备模式）或多个容器实例（多实例模式）进行部署。在多实例模式下，您可以在单个机箱上部署多个容器实例充当完全独立设备。请注意在多实例模式下，您可从容器实例（*Firewall Threat Defense*升级）单独升级操作系统和固件（机箱升级）。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **机箱 (Chassis)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **机箱管理器 (Chassis Manager)** • **设备 (Devices)** > **平台设置 (Platform Settings)** > **新建策略 (New Policy)** > **机箱平台设置 (Chassis Platform Settings)** • **设备 (Devices)** > **机箱升级 (Chassis Upgrade)** 新/修改的 Firewall Threat Defense CLI 命令：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新增/修改的 FXOS 命令：**create device-manager**、**set deploymode** 平台限制：Cisco Secure Firewall 3105 上不支持。



第 8 章

Firepower 4100/9300 上的逻辑设备

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。在可将 Firewall Threat Defense 添加到防火墙管理中心 之前，必须配置机箱接口，添加逻辑设备，并使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 将接口分配到 Firepower 4100/9300机箱上的设备。本章介绍基本的接口配置以及如何使用 Cisco Secure Firewall 机箱管理器添加独立或高可用性逻辑设备。要添加集群逻辑设备，请参阅 集群：Firepower 4100/9300，第 637 页。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

- 关于接口，第 273 页
- 关于逻辑设备，第 291 页
- 容器实例的许可证，第 299 页
- 逻辑设备的要求和前提条件，第 300 页
- 逻辑设备的准则和限制，第 307 页
- 配置接口，第 310 页
- 配置逻辑设备，第 315 页
- 逻辑设备的历史记录，第 326 页

关于接口

Firepower 4100/9300 机箱支持物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 防火墙机箱管理器来管理 FXOS 机箱。此接口在**接口 (Interfaces)** 选项卡顶部显示为 **MGMT**，您只可在**接口 (Interfaces)** 选项卡上启用或禁用此接口。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，或者逻辑设备已离线，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口、容器实例的 VLAN 子接口， 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限Firewall Threat Defense-使用-防火墙管理中心 ）共享。 每个容器实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署容器实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、集群或故障切换链路。
- 管理 - 用于管理应用实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口 ， 第 273 页。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 Firewall Threat Defense-using-防火墙管理中心 设备的辅助管理接口。 要使用此接口，您必须在 Firewall Threat Defense CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。有关详细信息，请参阅《管理中心配置指南》。事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。防火墙设备管理器 和 Security Cloud Control 不支持群集技术。



注释 本章仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 276 页。

有关独立部署和集群部署中Firewall Threat Defense和 ASA 应用的接口类型支持，请参阅下表。

表 *17:* 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	事件	集群（仅 EtherChannel）	集群：子接口
Firewall Threat Defense	独立本地实例	是	—	—	—	是	是	—	—
	独立容器实例	是	是	是	是	是	是	—	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	—
	集群容器实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	是
ASA	独立本地实例	是	—	—	—	是	—	是	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	—	是	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

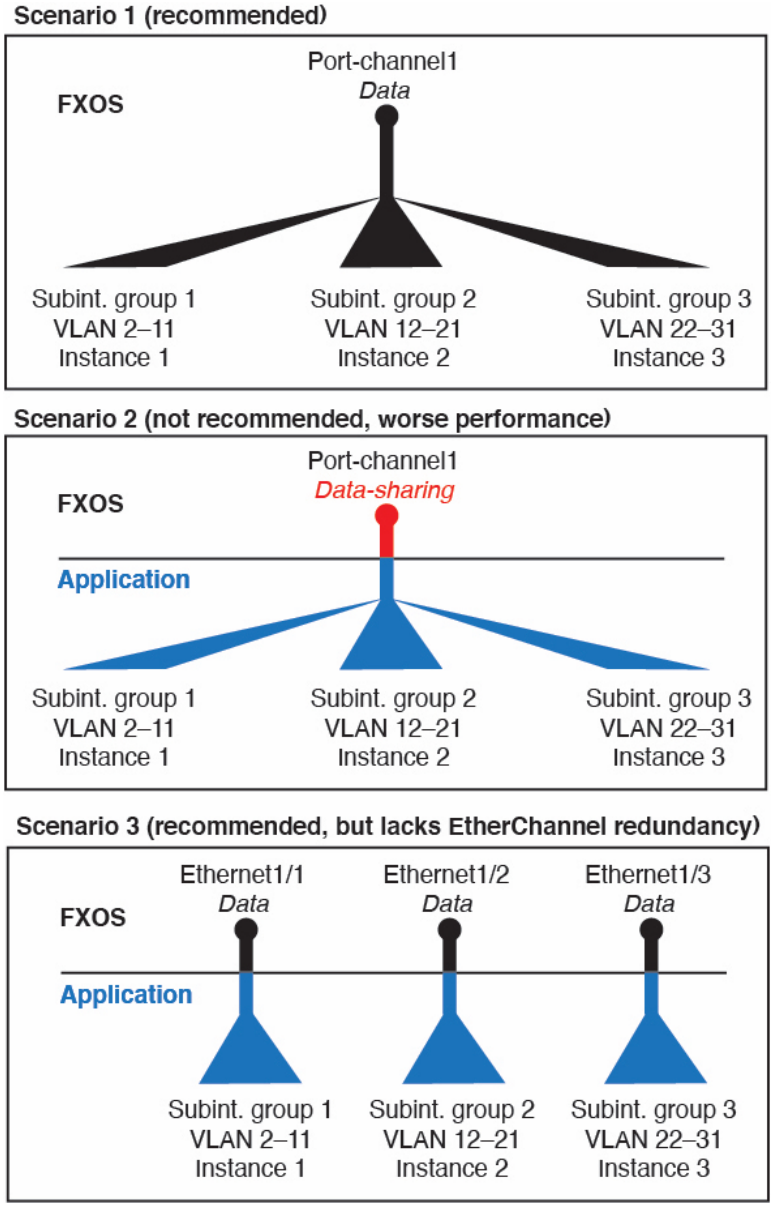
下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

仅对于独立模式下的容器实例，您还可以在 FXOS 中创建 VLAN 子接口。 除集群类型接口外，多实例集群不支持 FXOS 中的子接口。应用定义的子接口不受 FXOS 限值的约束。选择在哪个操作系统创建子接口取决于网络部署和个人偏好。例如，要共享子接口，必须在 FXOS 中创建子接口。偏好 FXOS 子接口的另一种场景包含将单个接口上的单独子接口组分配至多个实例。例如，您想要结合使用端口通道 1 与实例 A 上的 VLAN 2-11、实例 B 上的 VLAN 12-21 和实例 C 上的 VLAN 22-31。如果您在应用内创建这些子接口，则必须在 FXOS 中共享父接口，但这可能并不合适。有关可以用于实现这种场景的三种方法，请参阅下图：

图 *115: FXOS* 中的 *VLAN* 与容器实例的应用



机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

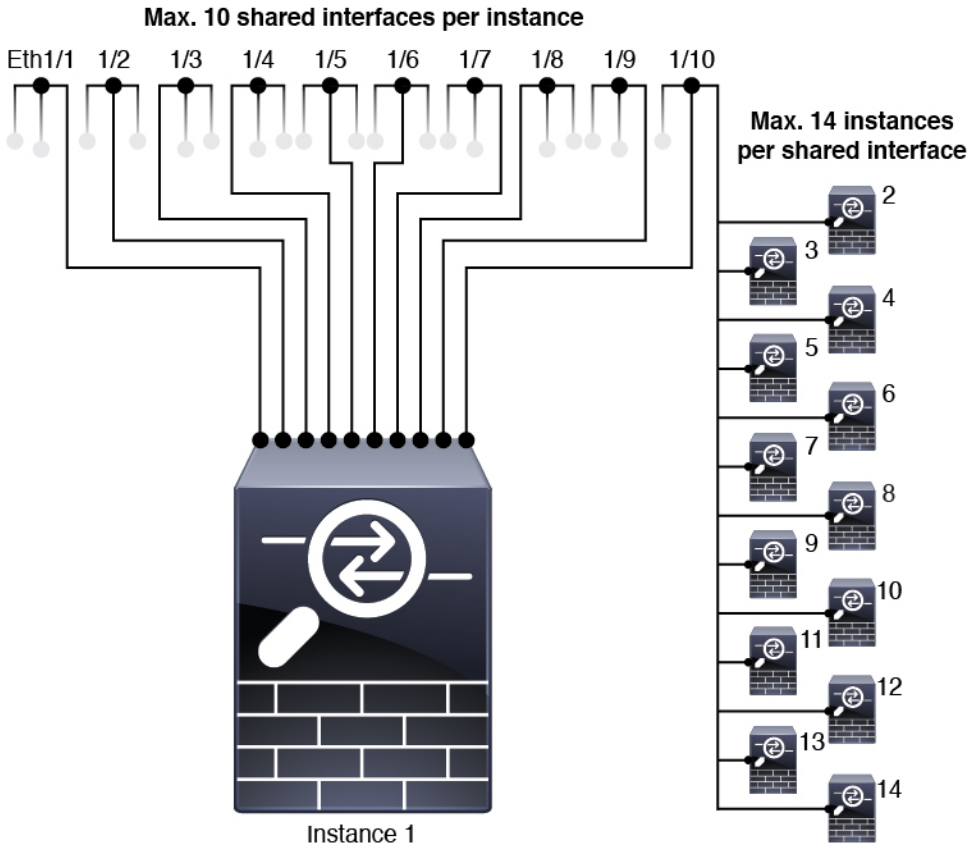
应用内接口的默认状态取决于接口类型。例如，在应用内，默认禁用物理接口或 EtherChannel，但默认启用子接口。

共享接口可扩展性

实例可以共享数据共享型接口。此功能允许您保存物理接口的使用情况，以及支持灵活的网络部署。当您共享接口时，机箱会使用唯一 MAC 地址将流量转发至适当实例。然而，由于需要在机箱内实现全网状拓扑，因此共享接口将导致转发表规模扩大（每个实例都必须能够与共享同一接口的所有其他实例进行通信）。因此，您可以共享的接口存在数量限制。

除转发表外，机箱还维护用于 VLAN 子接口转发的 VLAN 组表。 您最多可以创建 500 个 VLAN 子接口。

请参阅共享接口分配的以下限制：



共享接口最佳实践

为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

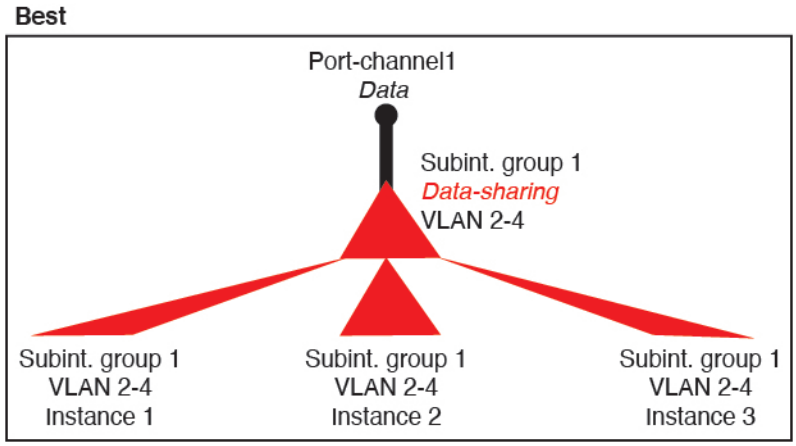
共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

1. 最佳 - 共享单父项下的子接口，并结合使用相同集合的子接口和同组实例。

   例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：Port-Channel1.2, 3 和 4 而不是 Port-Channel2、Port-Channel3 和 Port-Channel4。与跨父项共

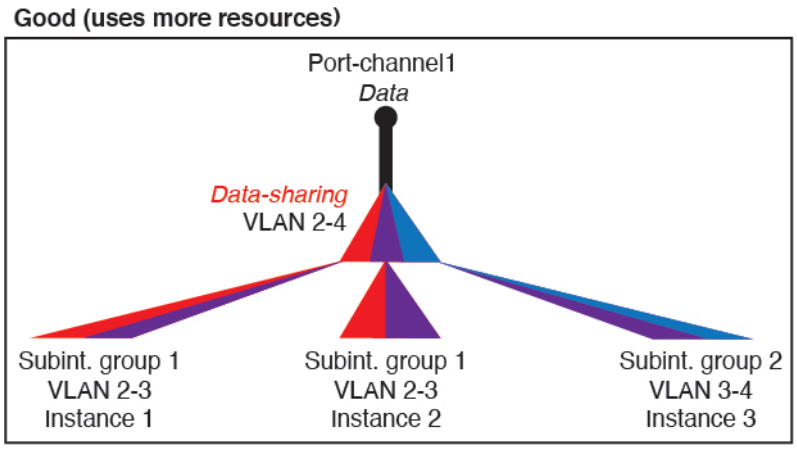
享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

图 *116:* 最佳：一个父项上的共享子接口组



如果未与一组实例共享相同集合的子接口，则配置会提高资源使用率（更多 VLAN 组）。例如，与实例 1、2 和 3（一个 VLAN 组）共享 Port-Channel1.2, 3 和 4 而不是与实例 1 和 2 分享 Port-Channel1.2 和 3，同时与实例 3（两个 VLAN 组）共享 Port-Channel1.3 和 4。

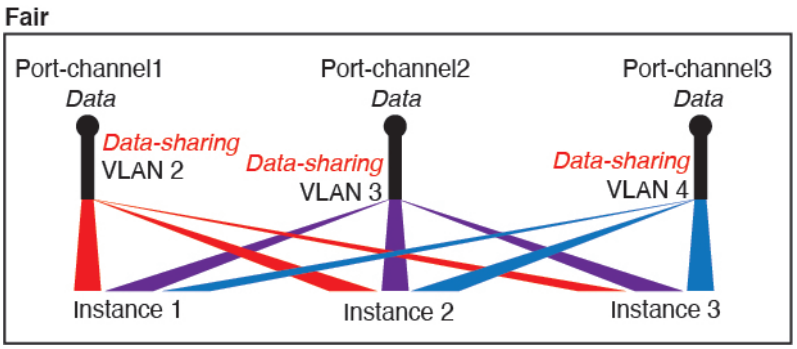
图 *117:* 良好：一个父项上共享多个子接口组



2. 一般 - 跨父项共享子接口。

   例如，共享 Port-Channel1.2、Port-Channel2.3 和 Port-Channel3.4 而不是 Port-Channel2、Port-Channel4 和 Port-Channel4。虽然这种使用方法的效率低于仅共享同一父项上的子接口，但仍可利用 VLAN 组。

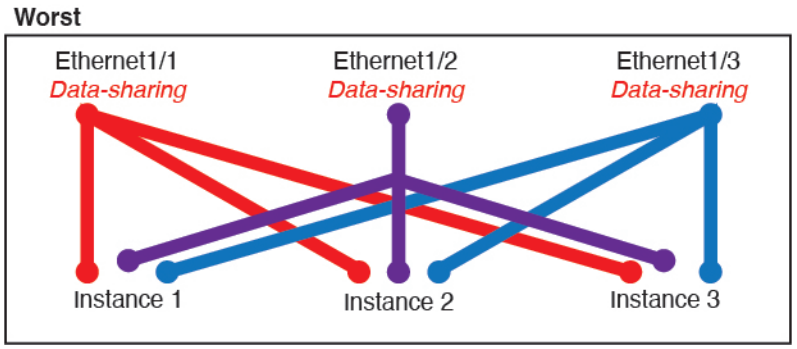
图 *118:* 一般：独立父项上的共享子接口



3. 最差 - 共享单个父接口（物理或 EtherChannel）。

   此方法使用的转发表条目最多。

图 *119:* 最差：共享父接口



共享接口使用示例

有关接口共享示例和可扩展性，请参阅下表。以下情景假设使用一个在所有实例中共享的物理/EtherChannel 接口来实现管理，和另一个设有专用子接口的物理或 EtherChannel 接口，用于实现高可用性。

- 表 18: Firepower 9300（设有三个 SM-44）上的物理/EtherChannel 接口和实例， 第 281 页
- 表 19: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例， 第 283 页
- 表 20: Firepower 9300（设有一个 SM-44）上的物理/EtherChannel 接口和实例， 第 286 页
- 表 21: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例， 第 288 页

Firepower 9300（设有三个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 9300 上的三个 SM-44 安全模块。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 *18: Firepower 9300*（设有三个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用接口	共享接口	实例数	转发表使用百分比
33: • *11*（每个实例 *1* 个专用接口） • *11*（每个实例 *1* 个专用接口） • *12*（每个实例 *1* 个专用接口）	***3:*** • *1* • *1* • *1*	***34:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *34*	*102%* 禁止使用
30: • 30（每个实例 1 个专用接口）	**1**	**6：** • 实例 1 实例 6	25%
30: • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口）	**3:** • 1 • 1 • 1	**6：** • 实例 1 至实例 2 • 实例 2 至实例 4 • 实例 5 至实例 6	23%
30: • 30（每个实例 6 个专用接口）	**2**	**5：** • 实例 1 至实例 5	28%

专用接口	共享接口	实例数	转发表使用百分比
30: • 12（每个实例 6 个专用接口） • 18（每个实例 6 个专用接口）	**4:** • 2 • 2	**5:** • 实例 1 至实例 2 • 实例 2 至实例 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	44%
24: • 12（每个实例 6 个专用接口） • 12（每个实例 6 个专用接口）	**14:** • 7 • 7	**4:** • 实例 1 至实例 2 • 实例 2 至实例 4	41%

下表适用于使用单父项物理接口上子接口的 9300 的三个 SM-44 安全模块。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 ***19: Firepower 9300***（设有三个 ***SM-44***）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
168: • 168（每个实例 4 个专用子接口）	**0**	**42:** • 实例 1 至实例 42	33%

专用子接口	共享子接口	实例数	转发表使用百分比
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	27%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用子接口	共享子接口	实例数	转发表使用百分比
70: • 70（每个实例 5 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**6:** • 2 • 2 • 2	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%
165: • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口）	***30:*** • *10* • *10* • *10*	***33:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *33*	*102%* 禁止使用

Firepower 9300（设有一个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 Firepower 9300（设一个 SM-44）。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 *20: Firepower 9300*（设有一个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
14: • 7（每个实例 1 个专用子接口） • 7（每个实例 1 个专用子接口）	**2:** • **1** • **1**	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
32: • 8 • 8 • 8 • 8	**1**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	21%

专用接口	共享接口	实例数	转发表使用百分比
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**2**	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	25%
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**4:** • 2 • 2	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	24%
24: • 8 • 8 • 8	**8**	**3:** • 实例 1 • 实例 2 • 实例 3	37%
10: • 10（每个实例 2 个专用接口）	**10**	**5:** • 实例 1 至实例 5	69%

专用接口	共享接口	实例数	转发表使用百分比
10: • 6（每个实例2个专用接口） • 4（每个实例2个专用接口）	**20:** • 10 • 10	**5：** • 实例 1 至实例 3 • 实例 4 至实例 5	59%
14: • *12*（每个实例 *2* 个专用接口）	***10***	***7***： • 实例 *1* 至实例 *7*	*109%* 禁止使用

下表适用于使用单父项物理接口上子接口的Firepower 9300（设有一个SM-44）。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 ***21: Firepower 9300***（设有一个 ***SM-44***）上的一个父接口的子接口和实例

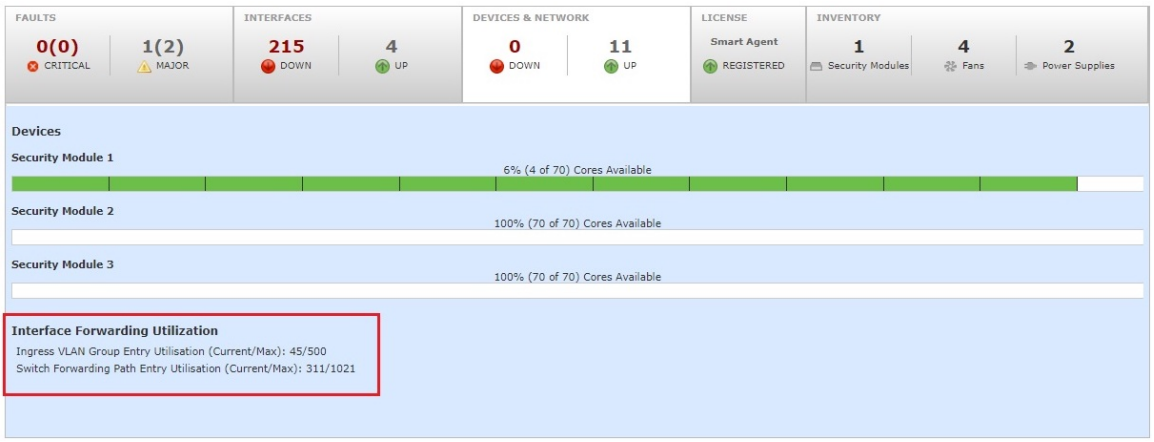
专用子接口	共享子接口	实例数	转发表使用百分比
112： • 112（每个实例 8 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%

专用子接口	共享子接口	实例数	转发表使用百分比
14: • 7（每个实例1个专用子接口） • 7（每个实例1个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**4：** • 2 • 2	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
140: • 140（每个实例 10 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%

专用子接口	共享子接口	实例数	转发表使用百分比
140: • 70（每个实例10个专用子接口） • 70（每个实例10个专用子接口）	**20:** • 10 • 10	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%

查看共享接口资源

要查看转发表和 VLAN 组使用情况，请参阅**设备和网络 (Devices & Network)** > **接口转发利用率 (Interface Forwarding Utilization)** 区域 下输入 **show detail** 命令。例如：



防火墙威胁防御 支持的内联集链路状态传播

内联集类似于导线上的凹凸，用于将两个接口绑定在一起插入到现有网络中。此功能使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

当您在 防火墙威胁防御 应用中配置内联集并启用链路状态传播时，防火墙威胁防御 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，机箱会感知该更改并更新其他接口的链路状态以与其匹配。请注意，机箱最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

注释 请勿为同一内联集启用 硬件旁路 和传播链路状态。

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 防火墙威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。



注释 对于Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和防火墙威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

独立和集群逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。
- 集群 - 集群逻辑设备允许您将多个单元集合在一起，具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。对于Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。防火墙设备管理器不支持集群。

逻辑设备应用实例：容器和本地

应用实例在以下类型部署中运行：

- 本地实例 - 本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此您仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。仅使用 防火墙管理中心 的 防火墙威胁防御 支持多实例功能；ASA 或使用 防火墙设备管理器 的 防火墙威胁防御 不支持。



注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全防火墙威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。防火墙威胁防御 的多情景模式不可用。

对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

容器实例接口

要确保灵活使用容器实例的物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。本地实例不得使用 VLAN 子接口或共享接口。 多实例集群不得使用 VLAN 子接口或共享接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。请参阅共享接口可扩展性，第 278 页和为容器实例添加 VLAN 子接口，第 313 页。

注释 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 276 页。

机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的实例。在应用内配置每个接口时，您也可以手动设置MAC地址。

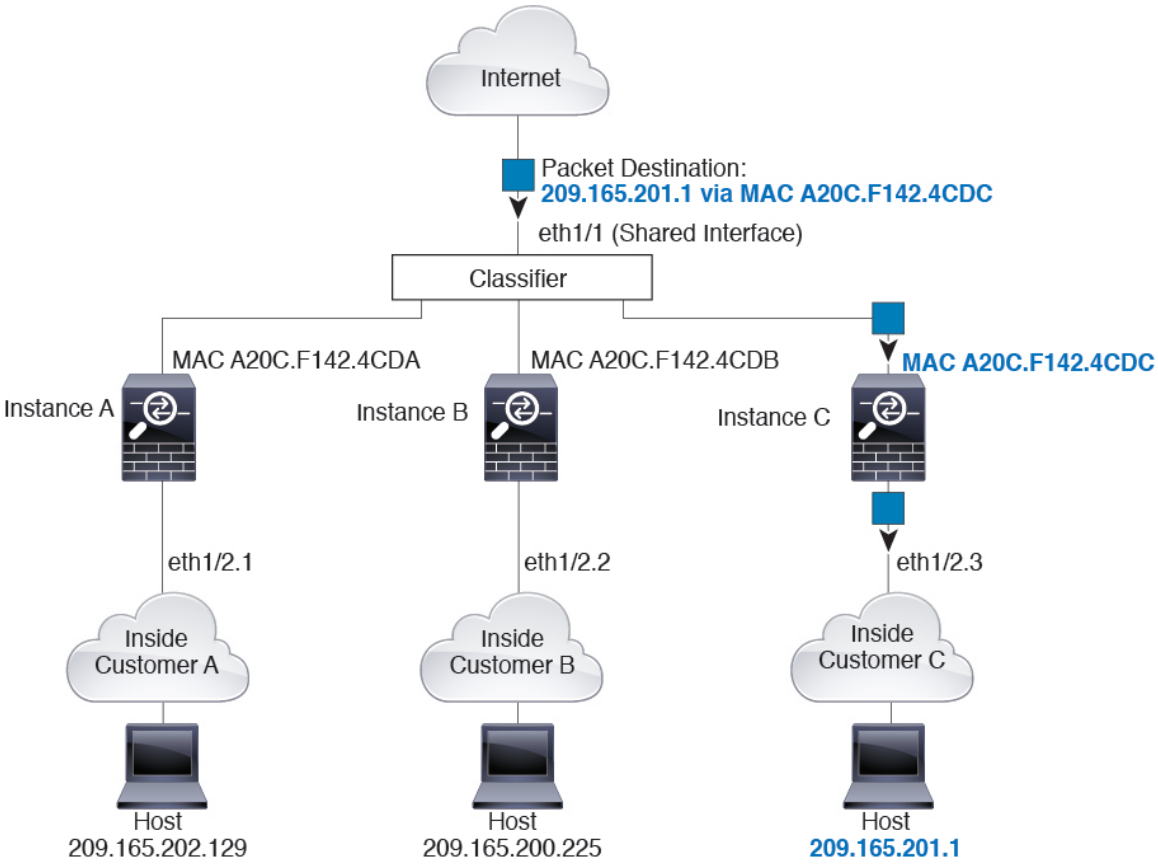
注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

使用 MAC 地址通过共享接口进行数据包分类

下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

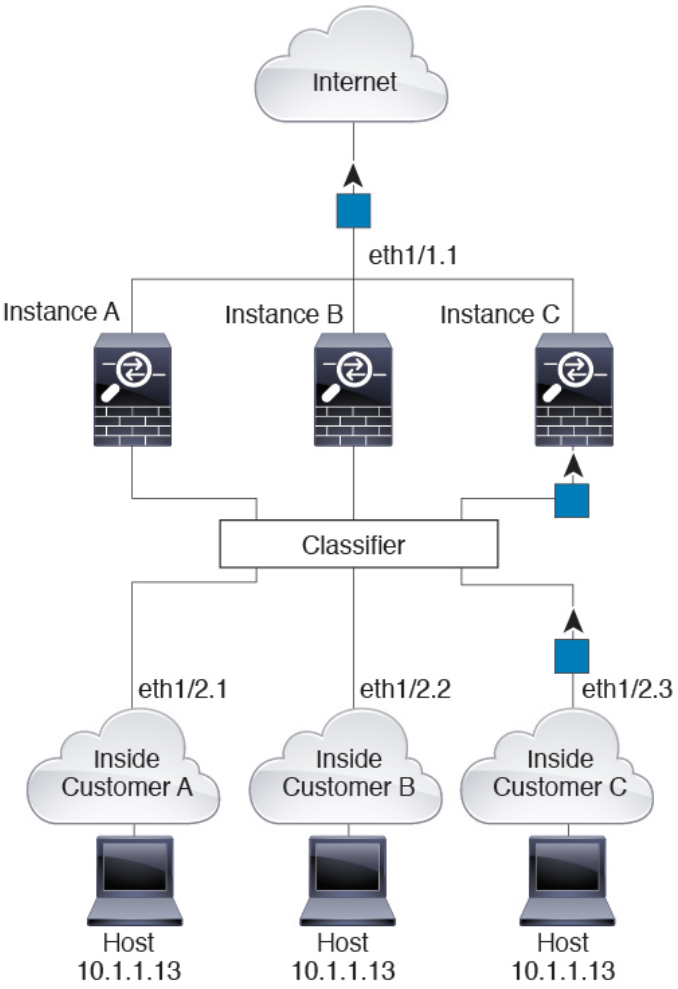
图 *120:* 使用 ***MAC*** 地址通过共享接口进行数据包分类



来自内部网络的传入流量

请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

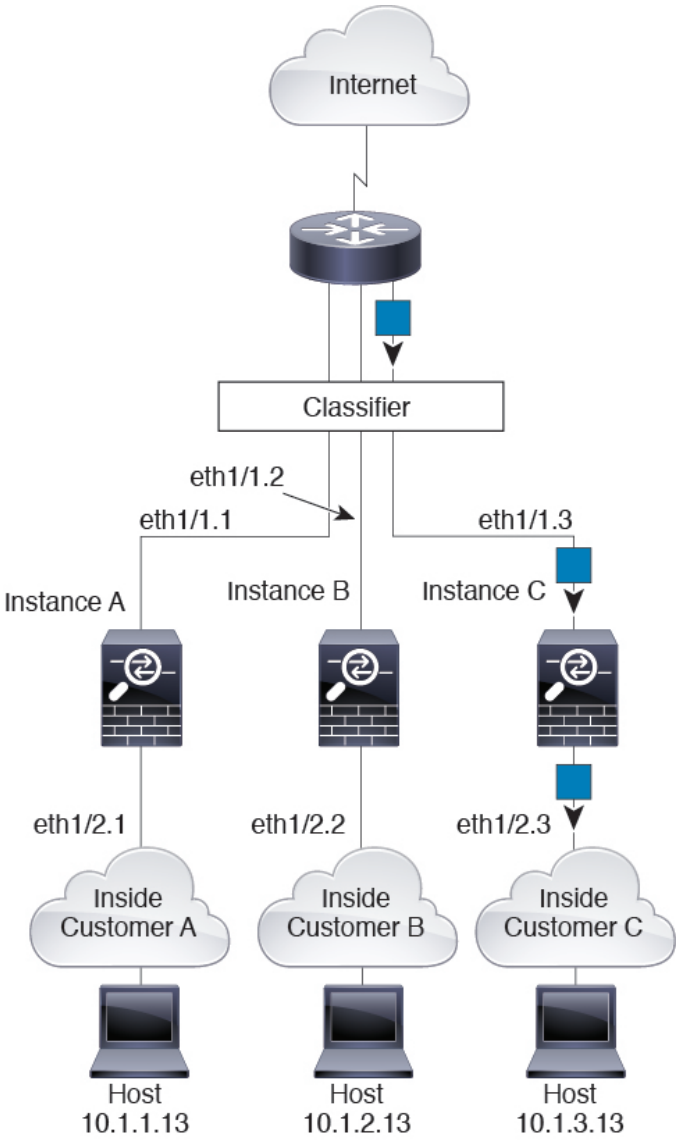
图 *121:* 来自内部网络的传入流量



透明防火墙实例

对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

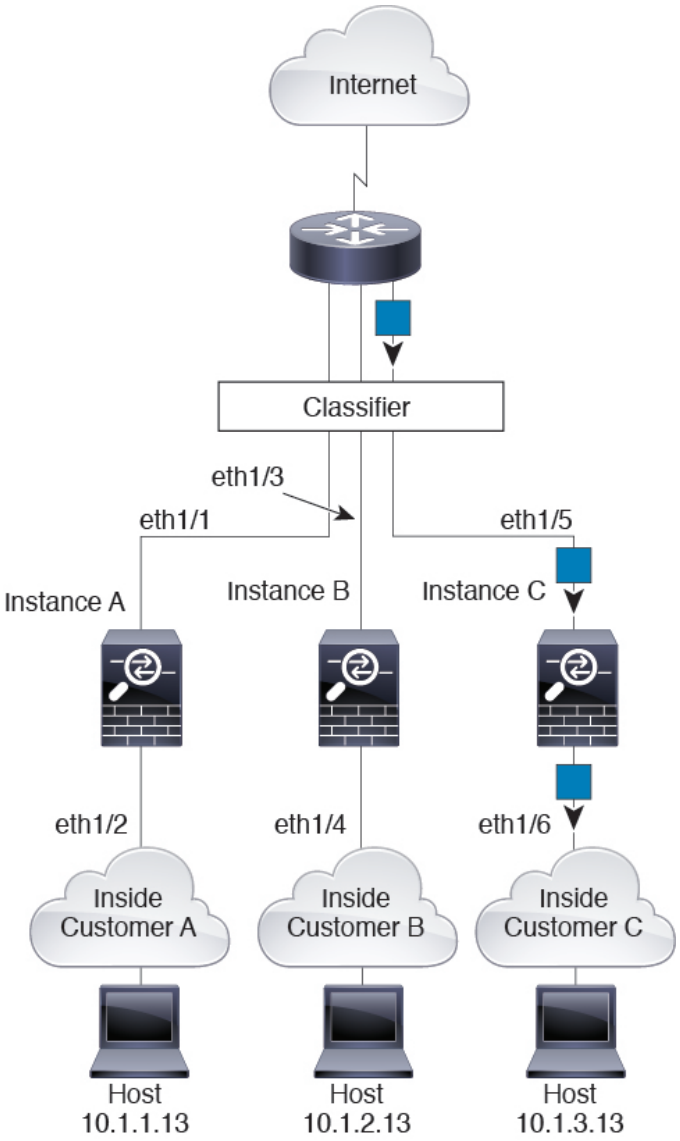
图 *122:* 透明防火墙实例



内联集

对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 *123:* 内联集

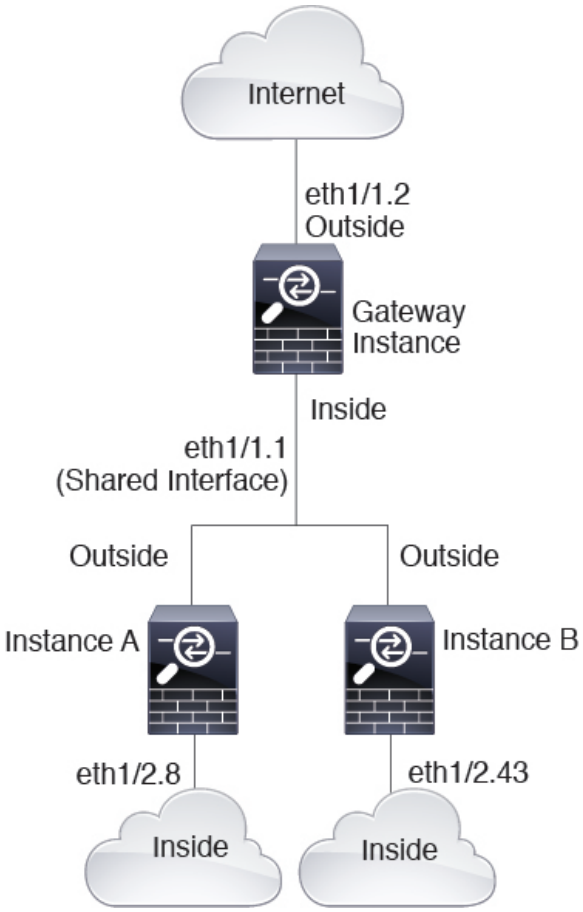


级联容器实例

直接在一个实例前面放置另一个实例的行为称为 级联实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

图 *124:* 级联实例



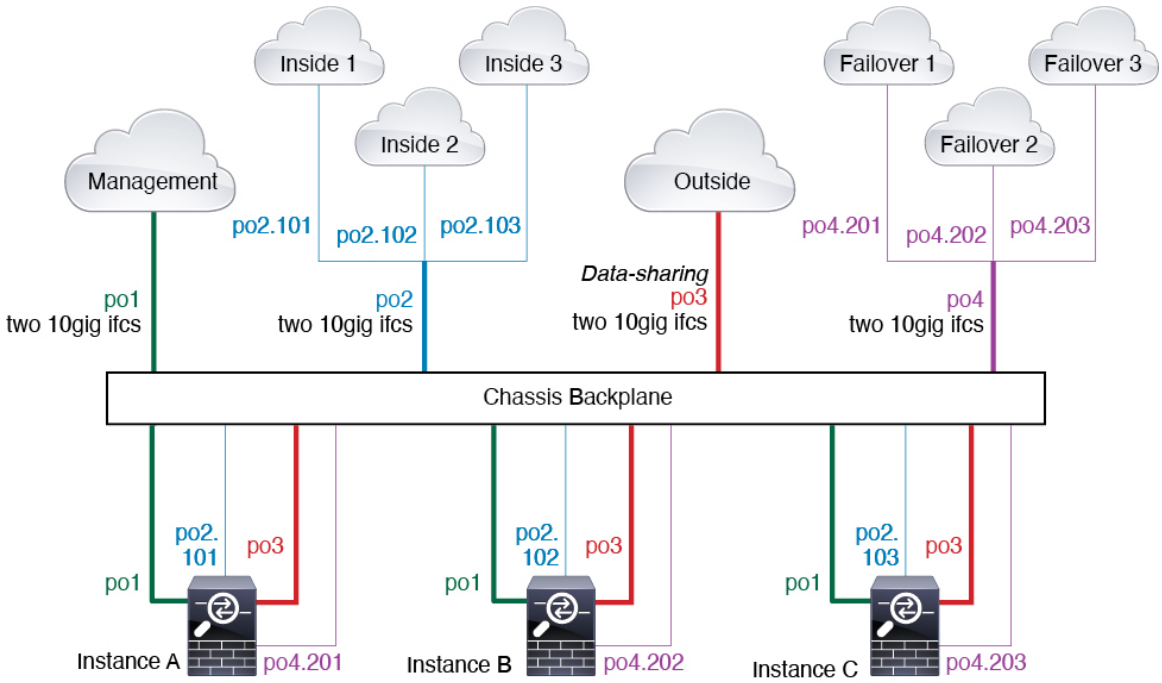
注释 请勿使用具有高可用性的级联实例（使用共享接口）。发生故障转移且备用设备重新加入后，MAC 地址可能会暂时重叠并导致中断。您应改为为网关实例和内部实例使用唯一接口，使用外部交换机在实例之间传递流量。

典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例都使用端口通道 1 接口（管理类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 2 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 3 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一外部网络上的唯一 IP 地址。

- 故障切换 - 每个实例都使用端口通道 4 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。



容器实例接口的自动 MAC 地址

机箱会自动为实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一 MAC 地址。

如果您手动为实例中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在实例中为接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。

机箱使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中， *xx.yy* 是用户定义的前缀或系统定义的前缀，*zz.zzzz* 是由机箱生成的内部计数器。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与机箱的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03**zz.zzzz

容器实例资源管理

要指定每个容器实例的资源使用情况，请在FXOS中创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置CPU核心数量；系统会根据核心数量动态分配RAM，并将每个实例的磁盘空间设为40 GB。要查看每个型号的可用资源，请参阅容器实例的要求和前提条件，第 302 页。要添加资源配置文件，请参阅为容器实例添加资源配置文件，第 315 页。

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数和 TLS 代理会话数）是为了得出本地实例的内存和 CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的容器实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但容器实例可用的吞吐量可能低于本地实例可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html。

容器实例与高可用性

您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建 10 个高可用性对。请注意，不得在FXOS中配置高可用性；在应用管理器中配置每个高可用性对。

有关详细要求，请参阅高可用性的要求和前提条件，第 303 页和添加高可用性对，第 321 页。

容器实例和集群

您可以每个安全模块/引擎各使用一个容器实例创建容器实例集群。有关详细要求，请参阅集群要求和前提条件，第 303 页。

容器实例的许可证

所有许可证按每个引擎/机箱（对于Firepower 4100）或每个安全模块（对于Firepower 9300）予以使用，而不是按每个容器实例使用。请查看以下详细信息：

- 基础版 许可证自动分配：每个 安全模块/引擎一个。
- 功能许可证手动分配到每个实例；但每个 安全模块/引擎每个功能只能使用一个许可证。例如，对于具有 3 个安全模块的 Firepower 9300，每个模块只需要一个 URL 过滤 许可证，总共需要 3 个许可证，而无须考虑正在使用的实例数。

例如：

表 *22: Firepower 9300* 上容器实例的许可证使用情况示例

Firepower 9300	实例	许可证
安全模块 1	实例 1	基础版、 URL 过滤、 恶意软件防御
	实例 2	基础版、 URL 过滤
	实例 3	基础版、 URL 过滤
安全模块 2	实例 4	基础版、 IPS
	实例 5	基础版、 URL 过滤、 恶意软件防御、 IPS
安全模块 3	实例 6	基础版、 恶意软件防御、 IPS
	实例 7	基础版、 IPS

表 *23:* 许可证总数

基础版	URL 过滤	恶意软件防御	IPS
3	2	3	2

逻辑设备的要求和前提条件

有关要求和前提条件，请参阅以下章节。

硬件和软件组合的要求与前提条件

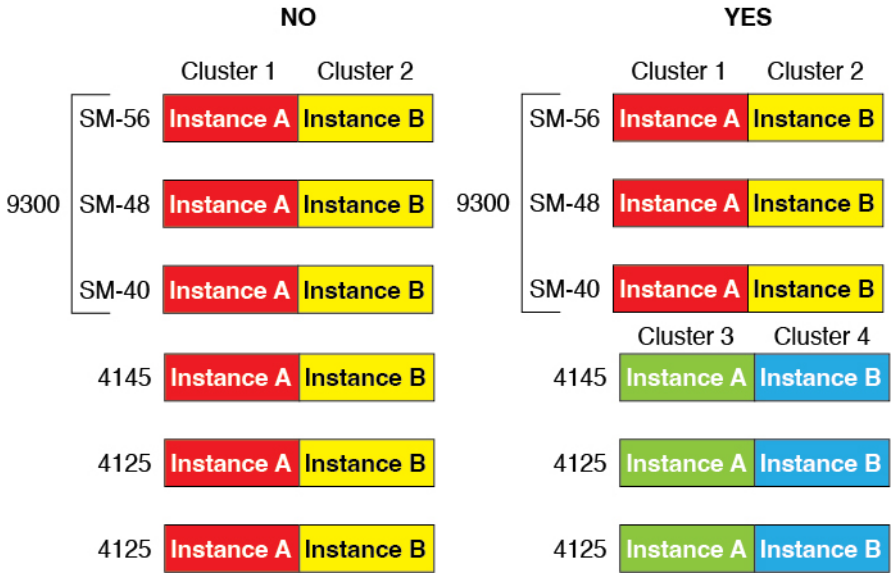
Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地实例 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。例如，您可以在机箱 1 中安装 2 个 SM-40，在机箱 2 中安装 3 个 SM-40。 如果在同一机箱中安装了 1 个 SM-48 和 2 个 SM-40，则无法使用集群。

- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。

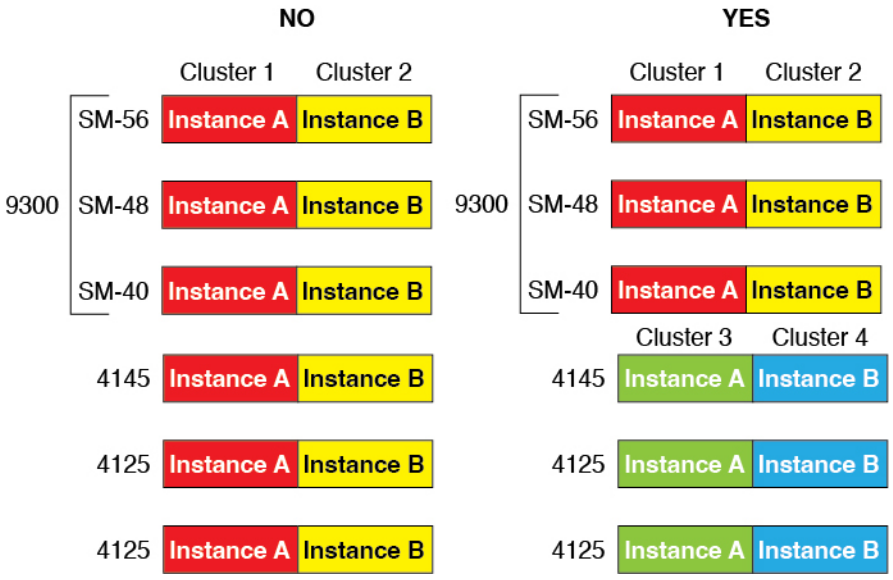


- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 Firewall Threat Defense 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 Firewall Threat Defense 。
- ASA 或 Firewall Threat Defense 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 Firewall Threat Defense 6.3，在模块 2 上安装 Firewall Threat Defense 6.4，在模块 3 上安装 Firewall Threat Defense 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。
- 本地实例 集群 - 集群内的所有机箱都必须为同一型号。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 4145 和 4125 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 Firewall Threat Defense 应用类型 - Firepower 4100 只能运行一种应用类型。
- Firewall Threat Defense 容器实例版本 - 您可以在同一模块上将不同版本的 Firewall Threat Defense 作为单独的容器实例运行。

容器实例的要求和前提条件

有关多实例的高可用性或集群要求的信息，请参阅高可用性的要求和前提条件，第 303 页和集群要求和前提条件，第 303 页。

受支持应用类型

- 使用 防火墙管理中心 的 Firewall Threat Defense

每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的 CPU 核心数量。系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

表 *24:* 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 **CPU** 核心	可用 **RAM**	可用磁盘空间
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4125	10	62	162 GB	644 GB

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 9300 SM-40 安全模块	13	78	334 GB	1359 GB
Firepower 9300 SM-48 安全模块	15	94	334 GB	1341 GB
Firepower 9300 SM-56 安全模块	18	110	334 GB	1314 GB

防火墙管理中心 要求

对于在 Firepower 4100 机箱或 Firepower 9300 模块上的所有情况下，由于许可实施，您必须使用相同 防火墙管理中心 。

高可用性的要求和前提条件

- 高可用性故障转移配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。
- 对于容器实例，每个单元必须使用相同的资源配置文件属性。
- 对于容器实例：请勿使用具有高可用性的级联实例（使用共享接口）。发生故障转移且备用设备重新加入后，MAC 地址可能会暂时重叠并导致中断。您应改为为网关实例和内部实例使用唯一接口，使用外部交换机在实例之间传递流量。
- 有关其他高可用性系统要求，请参阅 系统要求 ， 第 334 页一章。

集群要求和前提条件

集群型号支持

Firewall Threat Defense 在以下型号上支持集群：

- Firepower 9300-您可以在集群中包含最多 16 个节点。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。支持多个机箱的集群，以及与一个机箱内的安全模块隔离的集群。
- Firepower 4100-使用多机箱集群时，最多支持 16 个节点。

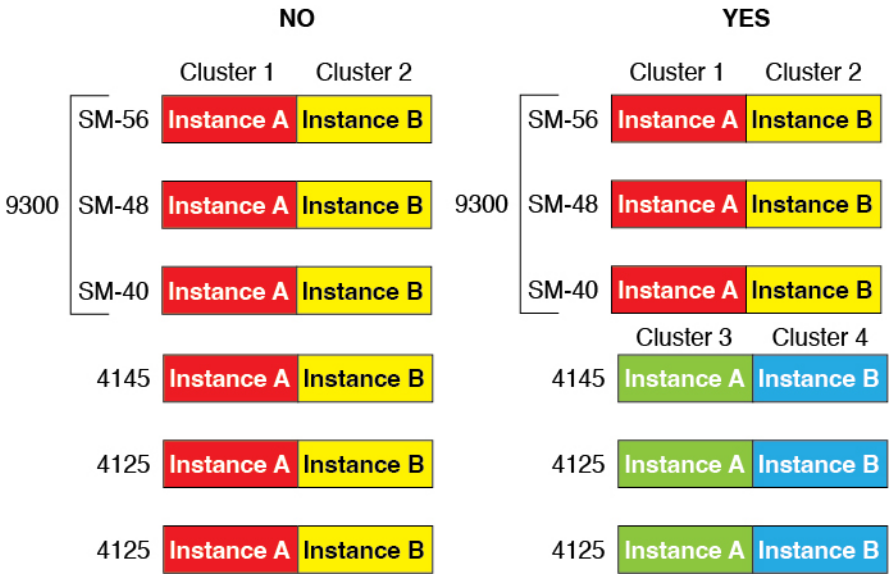
用户角色

- 管理员
- 访问管理员
- 网络管理员

集群硬件和软件要求

集群中的所有机箱：

- 本地实例集群 -对于 Firepower 4100：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 容器实例集群 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



- 除进行映像升级外，必须运行完全相同的 FXOS 和应用软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。

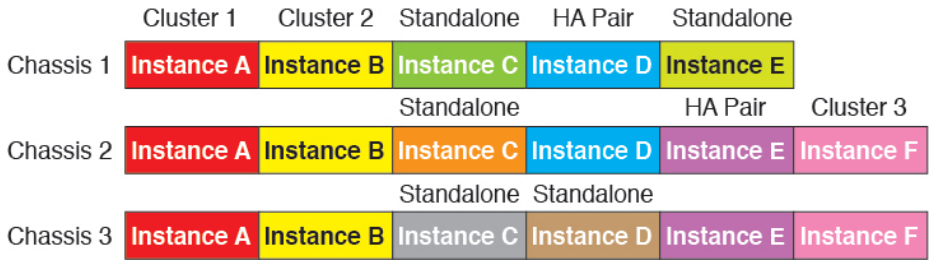
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。 对于 防火墙威胁防御， 防火墙管理中心 必须使用同一台 NTP 服务器。请勿手动设置时间。

多实例集群要求

- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。



- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。

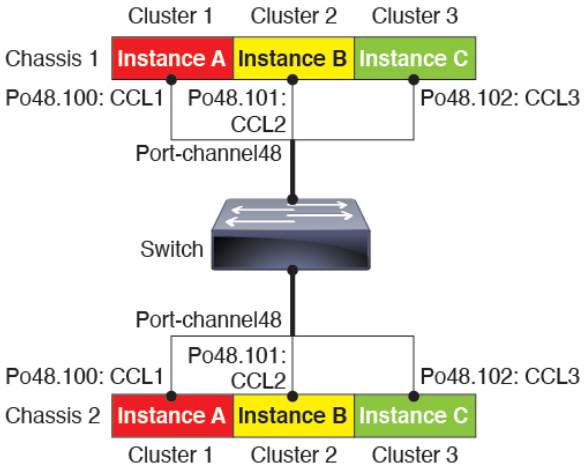


- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。

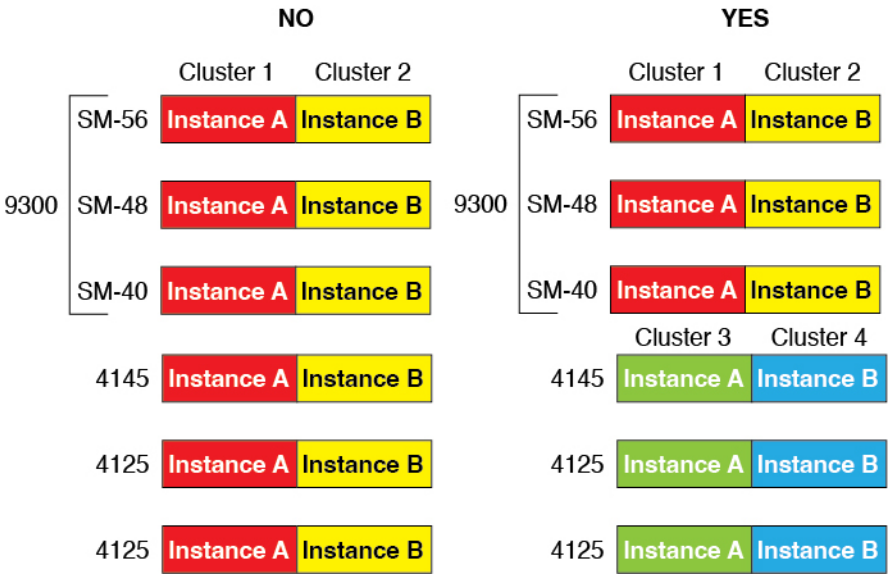


- 匹配资源配置文件 - 建议集群中的每个节点都使用相同的资源配置文件属性；但是，在将集群节点更改为使用其他资源配置文件或使用不同型号时，允许使用不匹配的资源。

- 专用集群控制链路 - 对于具有多个机箱的集群，每个集群都需要专用的集群控制链路。例如，每个集群可以在同一集群类型 EtherChannel 上使用单独的子接口，也可以使用单独的 Etherchannel。



- 无共享接口 - 集群不支持共享类型接口。但是，多个集群可以使用相同的管理接口和事件接口。
- 无子接口 - 多实例集群无法使用 FXOS 定义的 VLAN 子接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。
- 混合机箱型号 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



- 最多 6 个节点 - 在一个集群中最多可以使用六个容器实例。

交换机要求

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机的特性，请参阅思科 FXOS 兼容性。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

VLAN 子接口

- 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 276 页。
- 子接口（和父接口）仅可分配至容器实例。

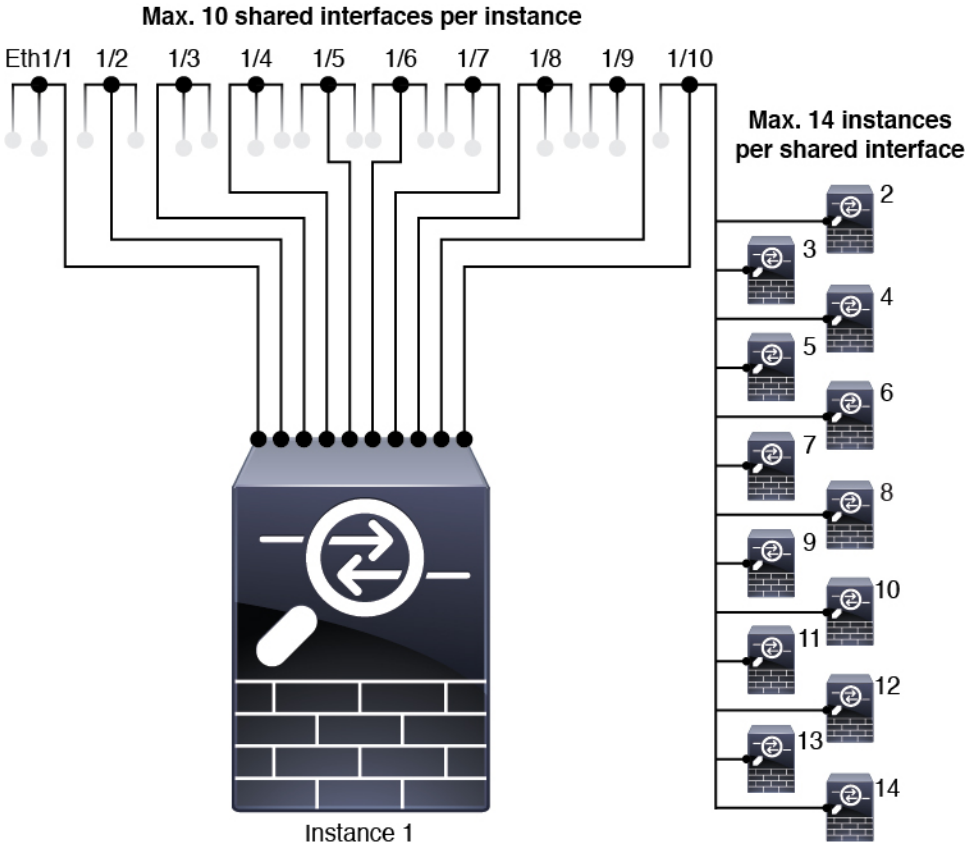
注释 如果将父接口分配至容器实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。对于集群类型接口，不得使用父接口。

- 子接口在数据或数据共享型接口以及集群类型接口上受支持。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。
- 对于多实例集群，数据接口上不支持 FXOS 子接口。但是，集群控制链路支持子接口，因此可以将专用 EtherChannel 或 EtherChannel 子接口用于集群控制链路。请注意，数据接口支持 应用定义的子接口。
- 最多可以创建 500 个 VLAN ID。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得将子接口用于 Firewall Threat Defense 内联集或用作被动接口。
  - 如果将子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。不得将某些子接口用作故障转移链路，而将某些用作常规数据接口。

数据共享接口

- 不得结合使用数据共享接口和本地实例。
- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。

每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。



- 不得在集群中使用数据共享接口。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得结合使用数据共享接口和透明防火墙模式设备。
  - 不得结合数据共享接口和 Firewall Threat Defense 内联集或被动接口。
  - 不得将数据共享接口用于故障转移链路。

FTD 的内联集 Firewall Threat Defense

- 支持物理接口（常规端口和分支端口）和 Etherchannel。 不支持子接口。
- 支持链路状态传播。
- 请勿为同一内联集启用 硬件旁路 和传播链路状态。

硬件旁路

- 支持 Firewall Threat Defense；可以将它们用作 ASA 的常规接口。

- Firewall Threat Defense仅支持包含内联集的 硬件旁路。
- 不可为分支端口配置具有硬件旁路功能的接口。
- 不得包含 EtherChannel 中的硬件旁路接口包含在并将它们用于硬件旁路；可以将它们用作 EtherChannel 中的常规接口。
- 硬件旁路不支持高可用性。
- 请勿为同一内联集启用 硬件旁路 和传播链路状态。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址，第 298 页。

一般准则和限制

防火墙模式

您可以在 防火墙威胁防御 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。 不支持数据共享接口。

多实例

- 包含容器实例的多实例功能仅适用于使用 防火墙管理中心 的 防火墙威胁防御。
- 对于 防火墙威胁防御 容器实例，单个 防火墙管理中心必须管理安全模块/引擎上的所有实例。
- 对于 防火墙威胁防御 容器实例，不支持以下功能：
  - Radware DefensePro 链路修饰器

- 防火墙管理中心 UCAPL/CC 模式
- 到硬件的数据流分流

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，添加 VLAN 子接口，编辑接口属性。

启用或禁用接口

可以将每个接口的**管理状态**更改为启用或禁用。默认情况下，物理接口处于禁用状态。 对于 VLAN 子接口，其管理状态继承自父接口。

过程

步骤 1 选择**接口 (Interfaces)** 打开接口页面。

“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 要启用接口，请点击已禁用**滑块已禁用**（），使其更改为已启用**滑块已启用**（）。

点击**是**，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用**滑块已启用**（），使其更改为已禁用**滑块已禁用**（）。

点击**是**，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。



注释

- 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。
- 如果使用其他 SFP 模块替换端口上的 SFP，则该接口的速度、双工和自动协商不会自动更新。您必须手动重新配置该接口。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 在您要编辑的接口所对应的行中点击**编辑 (Edit)**，可打开**编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中**启用**复选框。要禁用接口，请取消选中**启用**复选框。

步骤 4 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 274 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 Firewall Threat Defense 。
- **集群** - 请勿选择**集群**类型；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 （可选） 从**速度 (Speed)** 下拉列表中选择接口的速度。

步骤 6 （可选） 如果您的接口支持**自动协商**，请点击**是 (Yes)** 或**否 (No)** 单选按钮。

如果通过 50G 电缆连接到端口的对等交换机不支持自动协商，请确保同时在交换机和平台接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持在 50G 电缆上进行自动协商。因此，要连接端口，必须在平台和交换机上禁用默认自动协商。

步骤 7 （可选） 从**双工 (Duplex)** 下拉列表中选择接口双工。

步骤 8 （可选） 明确配置**防反跳时间 (ms)**。输入 0-15000 毫秒之间的值。

注释
不支持在 1G 接口上配置防反跳时间。

步骤 9 点击**确定**。

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是RJ-45或SFP；可以混合使用不同类型（铜缆和光纤）

的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如1GB和10GB接口）。链路聚合控制协议(LACP)将在两个网络设备之间交换链路汇聚控制协议数据单元(LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据或数据共享接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。



注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

非数据接口仅支持主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。 如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

Firepower 4100/9300 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开LACP模式），直到将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除EtherChannel或删除逻辑设备，EtherChannel 将恢复为**挂起**或**关闭**状态。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击接口表上方的**添加端口通道 (Add Port Channel)**，可打开**添加端口通道 (Add Port Channel)** 对话框。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中输入端口通道 ID。有效值介于 1 与 47 之间。

部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，可以将其删除并为集群类型EtherChannel配置不同的ID。您可以添加多个集群类型Etherchannel，

并添加 VLAN 子接口以与多实例集群结合使用。对于机箱内集群，请不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中**启用**复选框。要禁用端口通道，请取消选中**启用**复选框。

步骤 5 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 274 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 Firewall Threat Defense 。
- **集群**

步骤 6 从下拉列表设置成员接口要求的**管理速度**。

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。

步骤 7 对于数据或数据共享接口，选择 LACP 端口通道**模式**、**主用**或**保持**。

对于非数据或数据共享接口，模式始终是主用模式。

步骤 8 为成员接口、**全双工**或**半双工**设置所需的**管理双工**。

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。

步骤 9 要将接口添加到端口通道，请在**可用接口 (Available Interface)** 列表中选择该接口，点击**添加接口 (Add Interface)**，将接口移动至“成员 ID”列表。

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

提示
一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 10 要从端口通道删除接口，请点击“成员 ID”(Member ID) 列表中接口右侧的**删除 (Delete)** 按钮。

步骤 11 点击**确定**。

为容器实例添加 VLAN 子接口

您可以向机箱添加 250 至 500 个 VLAN 子接口，具体取决于网络部署。您最多可以将 500 个子接口连接到您的机箱。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的容器实例，您就可以在单独接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关何时使用 FXOS 子接口与应用子接口的详细信息，请参阅FXOS 接口与应用接口，第 276 页。

过程

步骤 1 选择**接口 (Interfaces)**打开**所有接口 (All Interfaces)**选项卡。

页面顶部的**所有接口 (All Interfaces)** 选项卡显示当前已安装的接口的直观展示图，并在下表中提供已安装接口列表。

步骤 2 点击**添加新 (Add New)** > **子接口 (Subinterface)**打开**添加子接口 (Add Subinterface)** 对话框。

步骤 3 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 274 页。

- **数据**
- **数据共享**
- **集群** - 如果向某个集群接口添加子接口，则不能将此接口用于本地集群。

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

步骤 4 从下拉列表选择父**接口**。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的**子接口 ID**。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 **VLAN ID** 。

步骤 7 点击**确定**。

展开父接口查看其项下所有子接口。

配置逻辑设备

在 Firepower 4100/9300上添加独立逻辑设备或高可用性对。

有关集群，请参阅用于 Firepower 4100/9300 的集群。

为容器实例添加资源配置文件

要指定每个容器实例的资源使用情况，请创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置CPU核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

- 最小核心数量为 6。

注释 与具有较大内核数量的实例相比，具有较小核心数量的实例可能具有相对更高的 CPU 利用率。具有较小核心数量的实例对流量负载变化更敏感。如果出现流量丢弃情况，请尝试分配更多核心。

- 您可以分配偶数（6、8、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于安全模块/机箱型号，请参阅容器实例的要求和前提条件，第 302 页。

机箱包括一个命名为 "Default-Small" 的默认资源配置文件，此文件包括最小核心数。您可以更改此配置文件定义，甚至可在未使用情况下将其删除。请注意，此配置文件在机箱重新加载且系统上不存在任何其他配置文件时创建而成。

在分配资源配置文件后更改资源配置文件会造成中断。请参阅以下准则：

- 如果当前正在使用，则无法更改资源配置文件设置。必须禁用使用此文件的任何实例，然后更改资源配置文件，最后重新启用该实例。
- 如果在将 防火墙威胁防御 实例添加到 防火墙管理中心 后更改资源配置文件设置，稍后应在设备设备管理设备系统清单对话框上更新每个设备的清单。防火墙管理中心选择 **设备** > **设备管理**，点击**编辑** ()实例的，然后点击**刷新** ()**设备** > **清单详细信息**区域。
- 如果将其他配置文件分配给实例，它会重新启动。
- 如果将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：
  1. 中断高可用性。
  2. 将新配置文件分配给两台设备。
  3. 重新建立高可用性。

- 如果将不同的配置文件分配给已建立的集群中的实例，则允许不匹配的配置文件，则首先在数据节点上应用新的配置文件；全部恢复后，您可以将新的配置文件应用到控制节点。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **资源配置文件 (Resource Profiles)**，然后点击**添加 (Add)**。

系统将显示**添加资源配置文件**对话框。

步骤 2 设置以下参数。

- **Name** - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。
- **Description** - 设置最多 510 个字符的配置文件说明。
- **Number of Cores** - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。

步骤 3 点击**确定**。

为 防火墙管理中心

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

可以在某些模块上使用本地实例，在其他模块上使用容器实例。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 Firewall Threat Defense）。还可以在独立模块上运行一种应用实例的不同版本。

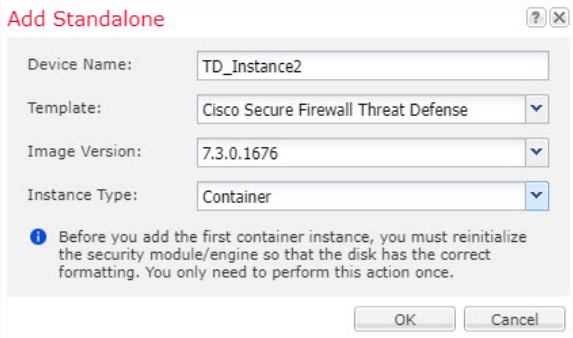
- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口 （并且在**接口**选项卡的顶部显示为 **MGMT**）。
- 您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

- 您还必须至少配置一个数据类型的接口。或者，您也可以创建Firepower事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅接口类型，第 274 页。
- 对于容器实例，如果您不想使用默认配置文件，则请根据为容器实例添加资源配置文件，第315页添加资源配置文件。
- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择**安全模块**或**安全引擎**，然后点击**重新初始化图标**。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的防火墙管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址
  - 防火墙威胁防御 主机名和域名

过程

步骤 1 选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

注释
添加逻辑设备后，无法更改此名称。

b) 对于**模板**，请选择 **Cisco Firepower Threat Defense**。

c) 选择**映像版本**。

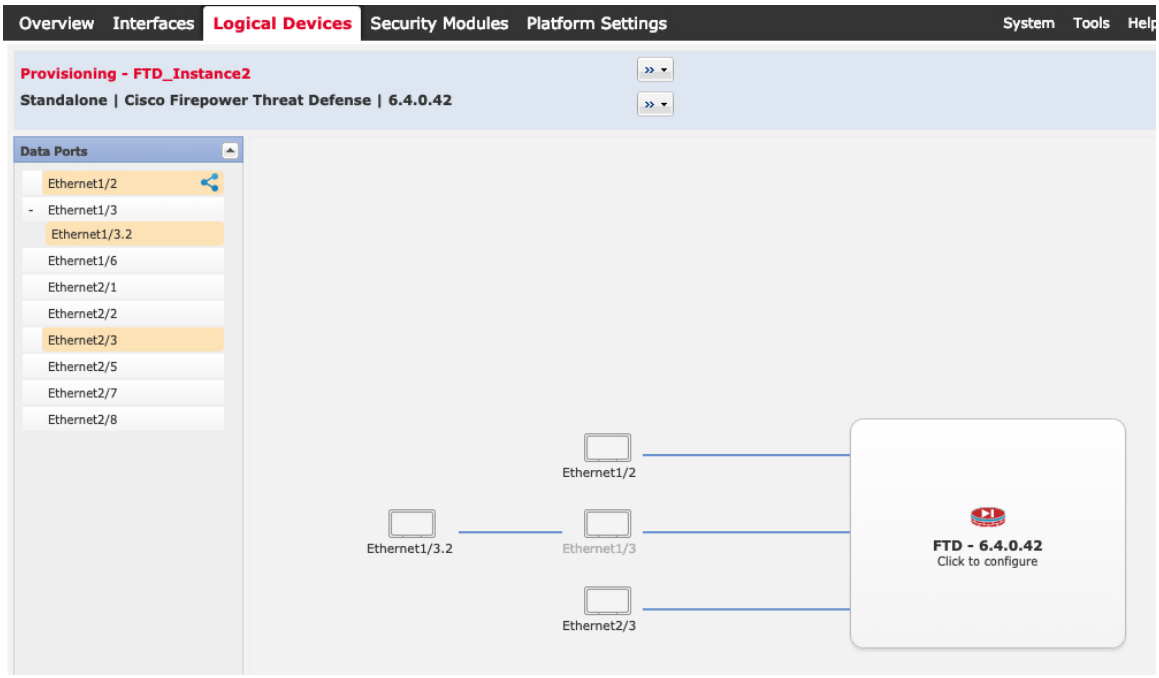
d) 选择**实例类型：容器**或**本地**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此仅可安装一个本地实例。容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。

e) 点击**确定**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个接口。



您仅可分配先前在接口 (Interfaces) 页面上启用的数据**和数据共享**接口。稍后您需要在 防火墙管理中心 中启用和配置这些接口，包括设置 IP 地址。

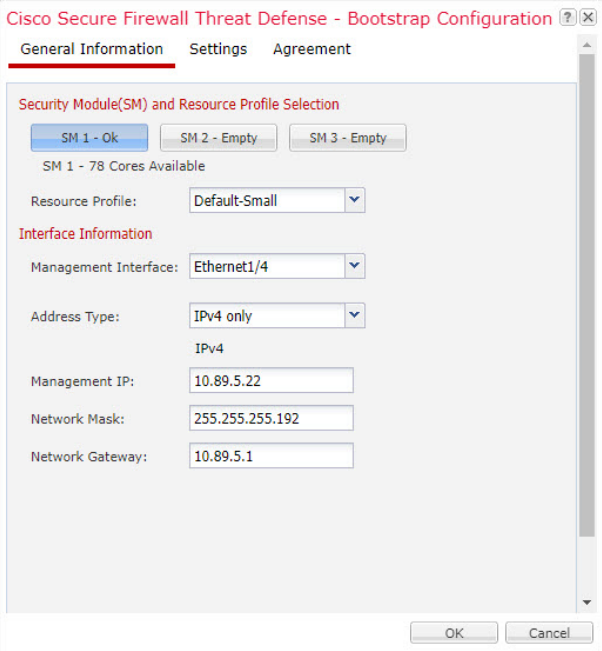
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（ ） 表示。

具有硬件旁路功能的端口使用以下图标显示： 。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能（请参阅 防火墙管理中心配置指南）。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在**一般信息 (General Information)** 页面上，完成下列操作：



a) （对于 Firepower 9300）在**安全模块选择**下，点击您想用于此逻辑设备的安全模块。

b) 对于容器实例，指定**资源配置文件**。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。

注释
如果稍后将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：

1. 中断高可用性。
2. 将新配置文件分配给两台设备。
3. 重新建立高可用性。

c) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

d) 选择管理接口**地址类型**：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。

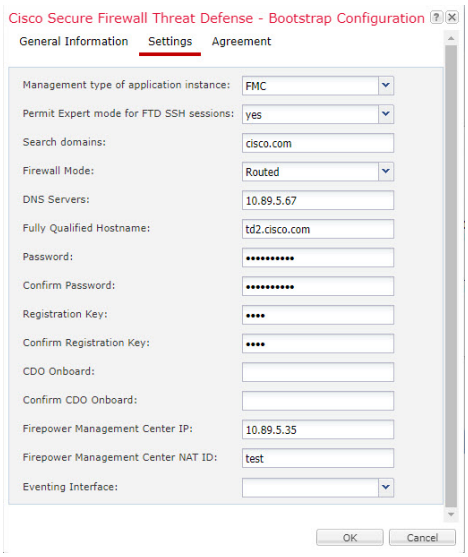
e) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

f) 输入**网络掩码**或**前缀长度**。

g) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



a) 对于本地实例，在**应用实例的管理类型**下拉列表中，选择 **FMC**。

本地实例还支持 防火墙设备管理器 作为管理器。部署逻辑设备后，无法更改管理器类型。

b) 输入管理 防火墙管理中心 的 **Firepower 管理中心 IP**。如果您不知道 防火墙管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中输入口令。

c) 对于容器实例，选择**是否允许 FTD SSH 会话专家模式：是** 或**否**。专家模式提供 防火墙威胁防御 shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择**是**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否**以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 防火墙威胁防御 CLI 中使用 **expert** 命令。

d) 输入逗号分隔列表形式的**搜索域**。

e) 选择**防火墙模式：透明**或**路由式**。

在路由模式中，防火墙威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 防火墙管理中心 主机名，则 防火墙威胁防御 使用 DNS。

g) 输入 防火墙威胁防御 的**完全限定主机名**。

h) 输入注册期间要在防火墙管理中心和设备之间共享的**注册密钥**。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加防火墙威胁防御时，需要在防火墙管理中心上输入相同的密钥。

i) 输入供防火墙威胁防御管理员用户用于 CLI 访问的**密码**。

j) 选择应该发送事件的**事件接口**。如果未指定，系统将使用管理接口。

此接口必须定义为 Firepower 事件接口。

k) 对于容器实例，请将**硬件加密**设置为**已启用**或**已禁用**。

此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。始终为本地实例启用此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

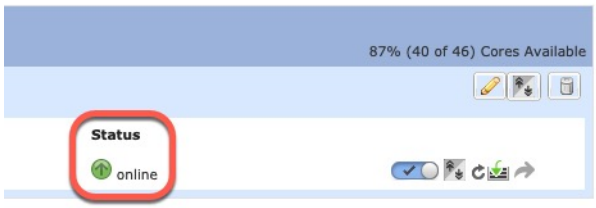
步骤 7 在**协议**选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置安全策略。





步骤 10 请参阅 防火墙管理中心 配置指南，将 防火墙威胁防御 添加为托管设备，并开始配置安全策略。

添加高可用性对

Firewall Threat Defense 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅高可用性的要求和前提条件，第 303 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

对于容器实例，故障转移链路不支持数据共享接口。我们建议您在父接口或 EtherChannel 上创建子接口，并为每个实例分配子接口以用作故障转移链路。请注意，您必须将同一父接口上的所有子接口用作故障转移链路。不得将一个子接口用作故障转移链路，然后将其他子接口（或父接口）用作常规数据接口。

步骤 3 在逻辑设备上启用高可用性。请参阅设备的高可用性，第 333 页。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

更改Firewall Threat Defense逻辑设备上的接口

可以在 Firewall Threat Defense 逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 防火墙管理中心 中同步接口配置。

添加新接口或删除未使用接口对 Firewall Threat Defense 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 Firewall Threat Defense 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 防火墙管理中心 上进行同步。

删除接口将删除与该接口相关的任何配置。

开始之前

- 根据配置物理接口，第 310 页和添加 EtherChannel（端口通道），第 311 页配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到EtherChannel。对于新的EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。Firewall Threat Defense 重新启动（管理接口更改导致重新启动），并且在防火墙管理中心中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在防火墙管理中心中同步配置。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

- 在多实例模式下，要更改具有相同 vlan 标记的另一个子接口的子接口，必须先删除该接口的所有配置（包括 nameif config），然后从 防火墙机箱管理器取消分配该接口。取消分配后，添加新接口，然后使用 防火墙管理中心中的同步接口。

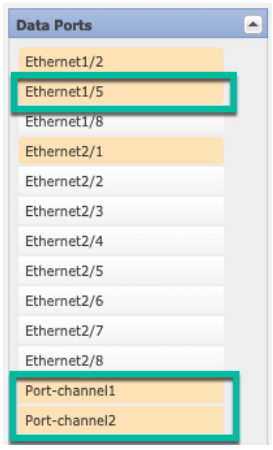
过程

步骤 1 在 防火墙机箱管理器中，选择**逻辑设备**。

步骤 2 点击右上角的**编辑**图标以编辑逻辑设备。

步骤 3 通过在**数据端口**区域中选择新的数据接口来分配该接口。

请勿删除任何接口。



步骤 4 替换管理或事件接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

a) 点击页面中心的设备图标。
b) 在**常规**或**集群信息**选项卡上，从下拉列表中选择新的**管理接口**。
c) 在**设置**选项卡上，从下拉列表中选择新的**事件接口**。
d) 点击**确定**。

如果更改管理接口的 IP 地址，则还必须更改 防火墙管理中心中设备的 IP 地址：转到**设备** > **设备管理** > **设备/集群**。在**管理**区域中，设置 IP 地址以匹配引导程序配置地址。

步骤 5 点击**保存**。

步骤 6 同步 防火墙管理中心 中的接口。

a) 登录至防火墙管理中心。
b) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 Firewall Threat Defense 设备的**编辑**（）。系统默认选择**接口 (Interfaces)** 页面。
c) 点击**接口 (Interfaces)** 页面左上方的**同步设备 (Sync Device)** 按钮。
d) 检测到更改后，可以在**接口 (Interfaces)** 页面上看到红色横幅，表明接口配置已发生更改。点击**点击了解详细信息**链接以查看接口更改。

e) 如果计划删除接口，请手动将任何接口配置从旧接口传输至新接口。

由于尚未删除任何接口，因此可以引用现有配置。在删除旧接口并重新运行验证后，将有额外的机会来修复配置。验证将显示仍在使用旧接口的所有位置。

f) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

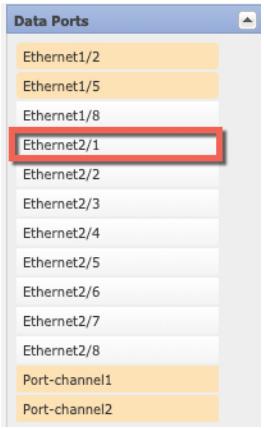
如出现任何错误，则需要更改配置并重新运行验证。

g) 点击**保存 (Save)**。

h) 依次点击**部署** > **部署**。

i) 选择设备然后点击**部署**，以将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 7 在 防火墙机箱管理器 中，通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。



步骤 8 点击**保存**。

步骤 9 再次在 防火墙管理中心 中同步接口。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- Firewall Threat Defense - 输入 **exit**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

逻辑设备的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Firewall Threat Defense运行链路状态与物理链路状态之间的同步	6.7	任意	机箱现在可以将 Firewall Threat Defense 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 Firewall Threat Defense 应用接口管理状态。如果没有从 Firewall Threat Defense同步，数据接口可能在 Firewall Threat Defense 应用完全上线之前处于“Up”物理状态，或者在您启动 Firewall Threat Defense 关闭后的一段时间内保持 “Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 Firewall Threat Defense 可以处理流量之前开始向 Firewall Threat Defense 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 Firewall Threat Defense 不支持此功能。此外，ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail**
对容器实例使用防火墙管理中心 的 Firewall Threat Defense 配置备份和恢复	6.7	任意	您现在可以在 Firewall Threat Defense 容器实例上使用 防火墙管理中心 备份/恢复工具。 新增/修改的 防火墙管理中心 屏幕：**系统** > **工具** > **备份/恢复** > **托管设备备份** 新增/修改的 Firewall Threat Defense CLI 命令：**restore** 支持的平台：Firepower 4100/9300 **注释** 需要 FXOS 2.9。

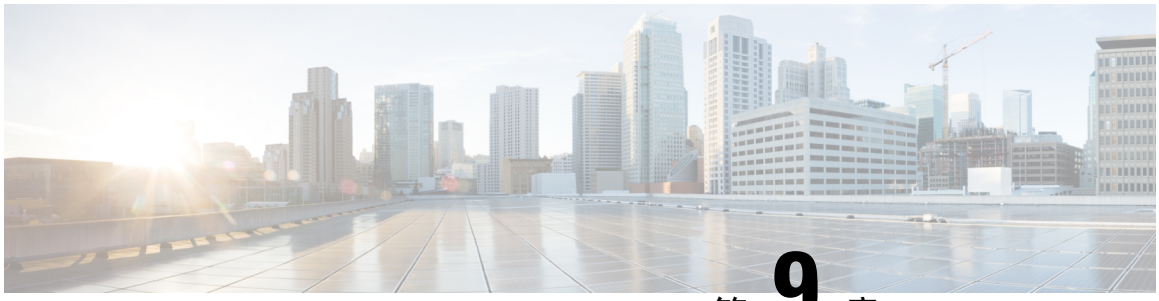
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持集群类型接口上的VLAN子接口（仅限多实例使用）	6.6	任意	要与多实例集群配合使用，您现在可以在集群类型接口上创建VLAN子接口。由于每个集群都需要唯一的集群控制链路，因此VLAN子接口提供了一种可满足此要求的简单方法。您也可以为每个集群分配专用的EtherChannel。现在允许多个集群接口。 新增/修改的 Firepower 机箱管理器菜单项： **接口** > **所有接口** > **新增**下拉菜单**子接口** > **类型**字段 新增/修改的 FXOS 命令：**set port-type cluster** **注释** 需要 FXOS 2.8.1。
Firepower 4112 上的 Firewall Threat Defense	6.6	任意	我们推出了 Firepower 4112。 **注释** 需要 FXOS 2.8.1。
多个容器实例的TLS加密加速	6.5	任意	现在，在Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。 新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，请依次使用 **enter hw-crypto** 和 **set admin-state enabled** FXOS 命令。 新增/修改的 Firepower 机箱管理器菜单项： **逻辑设备** > **添加设备** > **设置** > **硬件加密**下拉菜单 **注释** 需要 FXOS 2.7.1。
Firewall Threat Defense（位于 Firepower 4115、4125 和 4145 上）	6.4	任意	我们推出了 Firepower 4115、4125 和 4145。 **注释** 需要 FXOS 2.6.1.157。
Firepower 9300 SM-40、SM-48 和 SM-56 支持	6.4	任意	引入了以下三个安全模块：SM-40、SM-48 和 SM-56。 **注释** 需要 FXOS 2.6.1.157。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
支持在同一个Firepower 9300 上使用独立的 ASA 和 Firewall Threat Defense 模块	6.4	任意	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 Firewall Threat Defense 逻辑设备。 **注释** 需要 FXOS 2.6.1.157。
支持将SSL硬件加速用于模块/安全引擎上的一个 Firewall Threat Defense 容器实例	6.4	任意	您现在可以启用用于模块/安全引擎上的一个容器实例的SSL硬件加速。SSL 硬件加速禁用于其他容器实例，但启用于本地实例。 新增/修改的 FXOS 命令：**config hwCrypto enable** 未修改任何屏幕。 **注释** 需要 FXOS 2.6.1.157。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 4100/9300 上 Firewall Threat Defense 的多实例功能	6.3	任意	您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 Firewall Threat Defense 容器实例。以前，您仅可部署单个本地应用实例。 要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。资源管理允许您自定义每个实例的性能。 您可以使用在 2 个独立机箱上使用一个容器实例的高可用性。不支持集群。 注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。Firewall Threat Defense 的多情景模式不可用。 新增/修改的 防火墙管理中心菜单项： • **设备** > **设备管理** > **编辑**图标**接口**选项卡 新增/修改的 Firepower 机箱管理器菜单项： • **概述** > **设备** • **接口** > **所有接口** > **新增**下拉菜单**子接口** • **接口** > **所有接口** > **类型** • **逻辑设备** > **添加设备** • **平台设置** > **Mac 池** • **平台设置** > **资源配置文件** 新增/修改的 FXOS 命令：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**create resource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	6.3	任意	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **添加设备** > **集群信息** > **CCL 子网 IP** 字段 新增/修改的 FXOS 命令：**set cluster-control-link network** 支持的平台：Firepower 4100/9300
支持保存模式下的数据 Etherchannel	6.3	任意	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 新增/修改的 Firepower 机箱管理器菜单项： • **接口** > **所有接口** > **编辑端口通道** > **模式** 新增/修改的 FXOS 命令：**set port-channel-mode** 支持的平台：Firepower 4100/9300
支持 Firewall Threat Defense 内联集中的 Etherchannel	6.2	任意	现在可以使用 Firewall Threat Defense 内联集中的 EtherChannel。 支持的平台：Firepower 4100/9300
对 6 个 Firewall Threat Defense模块进行机箱间集群	6.2	任意	现在，您可以对 Firewall Threat Defense启用机箱间集群。在最多 6 个机箱中最多可以包含 6 个模块。 新增/修改的 Firepower 机箱管理器屏幕： • **逻辑设备** > **配置** 支持的平台：Firepower 4100/9300
Firepower 4100/9300 上对所支持网络模块的硬件旁路支持	6.1	任意	硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
内联集链路状态传播支持 Firewall Threat Defense	6.1	任意	当您在 Firewall Threat Defense 应用中配置内联集并启用链路状态传播时，Firewall Threat Defense 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的 FXOS 命令：**show fault |grep link-down**、**show interface detail** 支持的平台：Firepower 4100/9300
支持在 Firepower 9300 上的 Firewall Threat Defense 上执行机箱内集群	6.0.1	任意	Firepower 9300 支持使用 Firewall Threat Defense 应用执行机箱内集群。 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **配置** 新增/修改的 FXOS 命令：**enter mgmt-bootstrap ftd**、**enter bootstrap-key FIREPOWER_MANAGER_IP**、**enter bootstrap-key FIREWALL_MODE**、**enter bootstrap-key-secret REGISTRATION_KEY**、**enter bootstrap-key-secret PASSWORD**、**enter bootstrap-key FQDN**、**enter bootstrap-key DNS_SERVERS**、**enter bootstrap-key SEARCH_DOMAINS**、**enter ipv4 firepower**、**enter ipv6 firepower**、**set value**、**set gateway**、**set ip**、**accept-license-agreement** 支持的平台：Firepower 4100/9300



第 9 章

设备的高可用性

以下主题介绍如何配置主用/备用设备故障转移，以实现 防火墙威胁防御 的高可用性。

- Cisco Secure Firewall Threat Defense 高可用性， 第 333 页
- Config-sync 优化， 第 352 页
- 高可用性的要求和先决条件， 第 353 页
- 准则， 第 354 页
- 添加高可用性对， 第 356 页
- 配置可选高可用性参数， 第 359 页
- 管理， 第 361 页
- 监控 ， 第 368 页
- 配置同步失败故障排除， 第 369 页
- 高可用性历史记录， 第 369 页

Cisco Secure Firewall Threat Defense 高可用性

Cisco Secure Firewall Threat Defense 高可用性是一种故障转移配置，

- 需要两个相同的 Firewall Threat Defense 设备通过专用故障转移链路连接，还可以选择使用状态链路
- 支持主备故障转移，其中一个单元传输流量，而备用单元不主动传输流量，后者会同步配置和状态信息，以及
- 监控活动单元的运行状况（硬件、接口、软件和环境状态），以确定是否满足故障转移条件。

故障转移过程详情

发生故障转移时，主用设备会故障转移到备用设备，后者随即变为主用状态。系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。

注释 在公共云中运行的 Firewall Threat Defense Virtual不支持高可用性。有关配置 Firewall Threat Defense Virtual 设备以实现高可用性的详细信息，请参阅Cisco Secure Firewall Threat Defense Virtual 入门指南。

系统要求

系统要求定义了使 防火墙威胁防御 设备在指定 配置中正常运行所需的硬件、软件和许可证前提条件。

硬件要求

硬件要求是确保 配置中的两台设备可以

- 维护相同的硬件配置，包括型号、接口、模块和 RAM
- 支持适当的同步和故障转移功能，以及
- 确保可靠的高可用性操作。

硬件要求规格

配置中的两台设备必须满足以下要求：

- 型号相同。 此外，对于容器实例，它们必须使用相同的资源配置文件属性。

  对于 Firepower 9300，仅在同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。

  如果在将高可用性对添加到 防火墙管理中心 后更改资源配置文件，则稍后应在**设备** > **设备管理** > **设备** > **系统** > **库存**对话框上更新每个设备的库存。

  如果将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：

  1. 中断高可用性。
  2. 将新配置文件分配给两台设备。
  3. 重新建立高可用性。

- 拥有相同数量和类型的接口。

  对于平台模式下的Firepower 4100/9300 机箱，在启用之前，所有接口都必须在 FXOS 中进行相同的预配置。如果您在启用后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

如果在 配置中使用闪存大小不同的设备，请确保闪存较小的设备具有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

软件要求是 设备为在故障转移配置中正常运行而必须满足的配置规格。

所需软件规格

配置中的两台设备必须满足以下要求：

- 处于相同的防火墙模式（路由或透明）。
- 具有相同的软件版本。
- 位于防火墙管理中心上的同一个域或组中。
- 具有相同的 NTP 配置。请参阅为威胁防御配置 NTP 时间同步。
- 在防火墙管理中心上完全部署且没有未提交的更改。
- 在其任一接口中都未配置 DHCP 或 PPPoE。
- （Firepower 4100/9300）具有相同的流量分流模式，同时启用或禁用。

高可用性对中 Firewall Threat Defense 设备的许可证要求

高可用性对中 Firewall Threat Defense 设备的许可证要求包含以下许可规范

- 需要配置中的两台设备具有相同的许可证
- 为每个许可证类型需要两个许可证授权，以及
- 在高可用性设置期间触发自动许可证同步。

许可证同步过程

高可用性配置中的两台 Firewall Threat Defense 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，防火墙管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基础版 许可证和 IPS 许可证，而备用设备只有 基础版 许可证，防火墙管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 IPS 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

故障转移和状态故障转移链路

故障切换链路和状态同步故障切换链路是专用连接，

- 在采用故障转移配置的两台设备之间建立通信
- 要求在相应设备之间使用相同的接口以实现一致性，并且
- 用于在配对设备之间传输关键的故障转移和状态信息。

配置建议

思科建议在故障转移链路或状态故障转移链路中的两台设备之间使用同一接口。例如，在故障转移链路中，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。

故障切换链路

故障切换链路是一种通信机制，它使故障转移对中的两个单元能够不断通信，以确定每个单元的运行状态。

故障转移链路数据

以下信息通过故障切换链路传输：

- 设备状态（主用或备用）
- Hello 消息 (keep-alives)
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

故障转移链路接口

故障切换链路接口是一个专用的通信通道，

- 仅用于高可用性设备之间的故障转移通信
- 使用未使用的数据接口（物理或 EtherChannel）
- 不能与正常网络接口或用户数据流量共享，并且
- 需要根据设备型号确定特定的接口大小。

要求和限制和要求

您可以使用未使用的数据接口（物理接口 EtherChannel 接口）作为故障转移链路；但不能指定当前已配置名称的接口。您也无法使用子接口，在机箱上定义用于多实例模式的子接口除外。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。

Firewall 威胁防御 用户数据和故障转移链路之间共享接口。 您也不能在同一父接口上使用单独的子接口用于故障转移链路和数据 （仅限多实例机箱子接口）。如果将机箱子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。



注释 使用 EtherChannel 作为故障链路或状态链路时，必须在建立高可用性之前，确认具有相同成员接口的同一 EtherChannel 在两台设备上都存在。

请参阅这些有关故障转移链路的准则：

- Firepower 4100/9300 - 您不能使用管理类型接口作为故障切换链路。
- 请参阅这些有关调整链路大小的准则。

表 *25:* 故障切换链路大小

型号	组合故障转移和状态链路的接口大小
Firewall 200	1 Gbps
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Cisco Secure Firewall 1200	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105—1 Gbps Cisco Secure Firewall 3110—1 Gbps Cisco Secure Firewall 3120—1 Gbps Cisco Secure Firewall 3130—10 Gbps Cisco Secure Firewall 3140—10 Gbps
Firepower 4100	10 Gbps
Cisco Secure Firewall 4200	10 Gbps
Firewall 6100	10 Gbps
Firepower 9300	10 Gbps

交替频率等于设备保持时间。



注释 如果配置较大且设备保持时间较短，则在成员接口之间交替可以防止辅助设备加入/重新加入。这种情况下，请禁用其中一个成员接口，直到辅助设备加入。

对于用作故障转移链路的 EtherChannel，要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障转移链路

故障切换链路可在采用故障转移配置的设备之间启用通信和协调。

您需要在故障转移设备之间建立物理连接，以启用适当的故障转移功能。

过程

使用以下方法之一连接故障切换链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 防火墙威胁防御 设备的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果不在设备之间使用交换机，并且接口发生故障，则两台对等体之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

故障切换链路已物理连接，并为故障转移配置做好准备。

状态故障转移链路

状态同步故障切换链路可以

- 在故障转移设备之间传递连接状态信息，以及
- 必须配置为启用状态故障转移功能。

状态链路配置要求

要使用有状态故障转移，必须配置有状态故障转移链路（也称为有状态链路），以便传送连接状态信息。

共享故障转移链路

共享故障切换链路是一种接口保护方法，可使多个网络功能使用同一故障转移连接，不过大型配置和高流量网络应考虑使用状态和故障转移链路的专用接口。

有状态故障转移链路的专用接口

状态同步故障切换链路的专用接口是一种数据接口配置，该配置使用专门用于故障转移部署中状态链路的物理或 EtherChannel 接口。

性能注意事项

您可以将专用数据接口（如物理或 EtherChannel 接口）用于状态链路。有关专用状态链路的要求，请参阅故障转移链路接口，第 336 页。请参阅有关连接状态链接的的部分了解更多信息连接故障转移链路，第 338 页。

为了实现最佳的长距离故障转移性能，状态链路延迟应小于 10 毫秒，但不超过 250 毫秒。如果延迟超过 10 毫秒，则由于故障转移消息的重新传输，性能可能会下降。

避免故障转移和数据链路中断

避免故障转移和数据链路中断是一种网络设计实践，

- 确保让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。
- 防止故障转移操作在故障切换链路断开时中止，以及
- 通过使用适当的连接场景来保持网络弹性。

连接场景

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路断开，则故障转移操作会被暂停，直到故障转移链路恢复正常。

这些连接情景有助于设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 Firewall Threat Defense设备之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 Firewall Threat Defense设备都将处于主用状态。因此，建议**不要**使用这些图中显示的 2 种连接方法。

图 ***125:*** 使用单交换机连接 - 不推荐

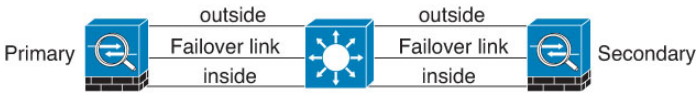
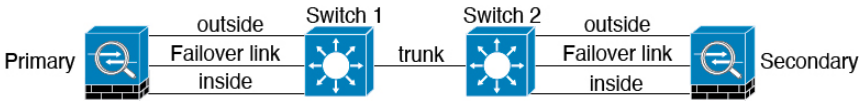


图 ***126:*** 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要让故障转移链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如下图所示。

图 *127:* 使用其他交换机连接

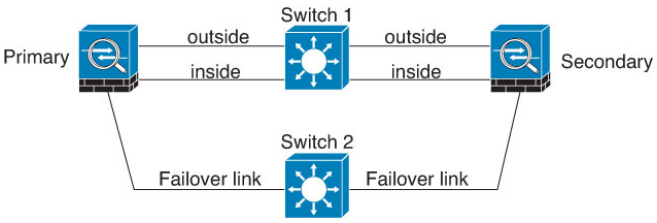
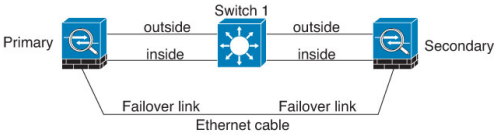


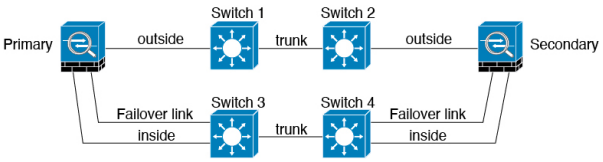
图 *128:* 通过电缆连接



情景 3 - 推荐

如果 Firewall Threat Defense数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 *129:* 使用安全交换机连接



中的 MAC 地址和 IP 地址

中的 MAC 地址和 IP 地址是网络寻址机制，

- 在故障转移场景期间为网络接口提供唯一标识
- 在主设备不可用时保持网络连接，以及
- 确保主用和备用配置之间的无缝流量传输。

地址配置类型

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。通常情况下，当发生故障转移时，新的主用设备会接管主用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注释 虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

在发生故障转移时，状态链路的 IP 地址和 MAC 地址不会更改。

主用/备用配置使用特定地址处理方法：

对于主用/备用，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主用设备始终使用主设备的 IP 地址和 MAC 地址。
2. 当主用设备进行故障转移时，备用设备会使用故障设备的 IP 地址和 MAC 地址，并开始传送流量。
3. 当故障设备恢复在线状态时，它现在处于备用状态，并且接管备用 IP 地址和 MAC 地址。

但如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的MAC 地址。当主设备变为可用时，辅助（主用）设备会将MAC 地址更改为主设备的 MAC，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

如果禁用高可用性并将故障转移配置设置为禁用状态，则需要手动恢复高可用性，或者重新启动设备。建议使用命令 **configure high-availability resume** 并恢复高可用性，而不是重新启动设备。如果在禁用故障转移配置的情况下重新加载备用设备，则备用设备将作为主用设备启动，并使用主设备的 IP 地址和 MAC 地址。这会导致 IP 地址重复并导致网络流量中断。使用命令 **configure high-availability resume** 启用故障转移并恢复流量。



注释 如果在独立设备上启用故障转移，数据接口将在故障转移协商状态下关闭，从而中断流量。

使用虚拟MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用MAC 地址是已知的，并在采用新的主设备硬件时保持不变。建议您在主设备和辅助设备上配置虚拟 MAC 地址，以确保辅助设备在作为主用设备时使用正确的MAC地址，即使它在主设备之前上线。如果您没有配置虚拟MAC 地址，则可能需要清除连接的路由器上的ARP表，以便恢复流量。当MAC地址发生变化时，Firewall Threat Defense不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

对于主用/主用故障转移，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主设备为故障转移组 1 和 2 个情景中的所有接口自动生成主用和备用 MAC 地址。如有必要，例如 MAC 地址发生冲突时，您也可以手动配置 MAC 地址。
2. 每台设备将主用 IP 地址和 MAC 地址用于其主用故障转移组，并将备用地址用于其备用故障转移组。例如，主设备是故障转移组 1 的主用设备，因此它使用故障转移组 1 中情景的主用地址。它是故障转移组 2 中情景的备用设备，因此在其中使用备用地址。
3. 当设备进行故障转移时，另一个设备将会承担出现故障的故障转移组的主用 IP 地址和 MAC 地址，并开始传送流量。
4. 当故障设备恢复在线状态，并且您已启用抢占选项时，它将恢复故障转移组。

虚拟 MAC 地址提供专用功能：

Firewall Threat Defense 有多种方法配置虚拟 MAC 地址。我们建议仅使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

对于多实例功能，FXOS 机箱仅为所有接口自动生成主 MAC 地址。如果同时具有主 MAC 地址和辅助 MAC 地址，则可以使用虚拟 MAC 地址覆盖生成的 MAC 地址，但预定义辅助 MAC 地址并非不可或缺；设置辅助 MAC 地址可确保在使用新的辅助设备硬件的情况下发送到设备的管理流量不会中断。

故障转移事件期间会发生 MAC 地址表更新：

在故障转移期间，被指定为新活动设备的设备会为 MAC 表中的每个 MAC 地址条目生成组播数据包，并将其发送到所有桥接组接口。此操作会提示网桥组中的上游交换机使用新活动设备的接口更新路由表，以确保准确的流量转发。

生成组播数据包和更新上游交换机路由表所需的时间取决于 MAC 地址表的条目数量和桥接组接口的数量。使用 **show failover statistics state-switch-delay** 命令可显示与故障转移事件期间遇到的延迟相关的统计信息。

状态故障转移

状态故障转移是一种高可用性机制，

- 不断将每个连接的状态信息从主用设备传递到备用设备
- 发生故障转移后，维护连接信息，以及
- 允许受支持的最终用户应用继续进行通信会话，而无需重新连接。

状态故障转移操作

状态故障转移期间，主用设备会不断将每个连接的状态信息发送至备用设备。发生故障转移之后，相同的连接信息在新主用设备上可用。支持的最终用户应用不需要通过重新连接来保持同一通信会话。

支持的功能

支持的功能指高可用性功能中

- 能使状态信息在状态故障转移期间传递到备用 Firewall Threat Defense 设备
- 能维护连接状态及关键信息以确保流量无缝传输；以及
- 能确保故障转移期间最大限度减少中断。

状态信息类型

对于状态故障转移，这些状态信息将传至备用设备：

- NAT 转换表。

- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表
- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。



注释 路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障转移期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障转移时评估的连接，有以下注意事项：
  - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障转移之前完成同步，即可实现正确的同步。
  - 入侵检测状态 - 进行故障转移时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
  - 文件恶意软件阻止 - 文件处置必须在故障转移之前变为可用。
  - 文件类型检测和阻止 - 文件类型必须在故障转移之前加以识别。如果在原始主用设备识别文件时发生故障转移，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。

- 身份策略中的用户身份决策，包括通过 ISE 会话目录被动收集的用户到 IP 地址映射以及通过强制网络门户进行的主动身份验证。发生故障转移时进行主动身份验证的用户，可能会被提示再次进行身份验证。
- 网络 AMP - 云查找独立于每台设备，因此故障转移通常不会影响此功能。具体包括：
  - 签名查找 - 如果在文件传输过程中发生故障转移，则不生成文件事件，也不进行检测。
  - 文件存储 - 如果在存储文件时发生故障转移，则文件将存储在原始主用设备上。如果在存储文件时原始主用设备关闭，则不存储文件。
  - 文件预分类（本地分析）- 如果在预分类期间发生故障转移，则检测失败。
  - 文件动态分析（连接至云）- 如果发生故障转移，则系统可能会将文件提交至云。
  - 存档文件支持 - 如果在分析期间发生故障转移，则系统可能会丢失对文件/存档的可视性。
  - 自定义阻止操作 - 如果发生故障转移，系统将不生成事件。
- 安全智能决策。但是，不会完成故障转移过程中发生的基于 DNS 的决策。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在VPN连接上运行的应用，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。
- 在所有连接中，只有已建立的连接会在备用设备上复制。

不支持的功能

不支持的功能指无法满足以下条件的设备功能

- 不会在状态故障转移中同步至备用 Firewall Threat Defense 设备
- 在故障转移事件期间不维护状态信息，以及
- 可能需要在故障转移发生后重新建立。

状态信息限制

对于状态故障转移，以下状态信息不会传送至备用 Firewall Threat Defense：

- 明文隧道（例如 GRE 或 IP-in-IP）中的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 已解密的 TLS/SSL 连接 - 解密状态不同步，如果主用设备发生故障，则系统会重置已解密的连接。需要与新的主用设备建立新连接。未解密的连接（也就是匹配TLS/SSL“不解密”规则操作的连接）不受影响，并且可以正确复制。
- 组播路由。

高可用性的网桥组要求

网桥组对高可用性的要求是需要特别考虑的因素

- 解决了故障转移期间网桥组成员接口上的流量丢失问题
- 防止交换机端口进入阻塞状态 30 到 50 秒，以及
- 提供在拓扑更改期间保持连接的变通方法。

高可用性解决方法

使用网桥组时，高可用性存在特殊的注意事项。

当主用设备故障切换到备用设备时，运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，系统会进入阻塞状态30秒至50秒。当端口处于阻塞状态时，为避免桥接组成员接口上出现流量丢失，您可以配置以下任一变通方案：

- 交换机端口处于接入模式 - 在交换机上启用 STP PortFast 功能：

  ```
  interface interface_id
    spanning-tree portfast
  ```

  链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，它最终会转换为 STP 阻塞模式。

- 如果交换机端口处于中继模式，或无法启用STP PortFast，则您可以使用以下一种会影响故障切换功能或 STP 稳定性的不太理想的变通方案：
  - 对桥接组和成员接口禁用接口监控。
  - 将故障切换条件中的接口保持时间增加到较高的值，以使 STP 在设备进行故障切换之前融合。
  - 减小交换机上的 STP 计时器，以使 STP 比接口保持时间更快地融合。

故障转移运行状态监控

故障转移运行状况监控是一项系统功能，可监控每个设备的整体运行状况和接口运行状况。

健康监控测试

防火墙威胁防御 设备可以执行测试以确定每台设备状态的信息。此部分包括有关 防火墙威胁防御 设备如何执行测试以确定每台设备状态的信息。

设备运行状况监控

设备运行状况监控是一种故障转移机制，

- 通过向故障切换链路发送 Hello 消息来确定对等体单元的运行状况

- 当连续三个 Hello 消息丢失时，在每个数据接口上发送 LANTEST 消息，并且
- 会根据对等设备的响应能力启动适当的故障转移操作。

设备运行状况监控行为

Firewall Threat Defense 设备会通过 Hello 消息监控故障转移链路，进而确定其他设备的运行状况。如果设备在故障转移链路上没有收到三条连续的hello消息，则设备会在每个数据接口（包括故障转移链路）上发送 LANTEST 消息，以验证对等体是否响应。Firewall Threat Defense 设备采取的操作取决于来自其他设备的响应。可能的操作如下：

- 如果 Firewall Threat Defense 设备在故障转移链路上收到响应，则不会进行故障转移。
- 如果 Firewall Threat Defense 设备在故障转移链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障转移。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果 Firewall Threat Defense 设备未在任何接口上收到响应，则备用设备会切换至主用模式，并会将另一台设备分类为故障设备。



注释 在高可用性故障转移事件期间， Firewall Threat Defense 设备 的运行状况监控控制面板中可能会短暂显示为 **离线 (Offline)** 。发生这种情况是因为运行状况警报会在此过程中被清除，并且仅在该过程完成后才会更新。等待故障切换操作完成。

心跳模块冗余

心跳模块冗余是一种高可用性功能，可以

- 使用数据平面传输基础设施发送心跳消息，以补充控制平面心跳数据包
- 在对等体在数据平面中收到心跳数据包时递增计数器
- 在控制平面因流量拥堵时防止虚假故障转移或裂脑场景。

心跳模块冗余行为

HA 中的每个单元定期通过故障转移链路发送广播保活心跳数据包。如果控制平面忙于处理流量，有时心跳数据包无法到达对等体，或者对等体由于 CPU 过载而无法处理心跳数据包。当对等体无法在可配置的超时期限内传达保持连接状态时，会发生错误的故障转移或裂脑场景。

数据平面中的心跳模块有助于避免由于控制平面中的流量拥塞而发生错误的故障转移或裂脑。

- 附加心跳模块的工作原理与控制平面模块类似，但使用数据平面传输基础设施发送和接收心跳消息。
- 当对等体在数据平面中收到心跳数据包时，计数器会递增。

- 如果控制平面中的心跳传输失败，则节点会检查数据平面中的心跳计数器。如果计数器递增，则表示对等体处于活动状态，并且集群在这种情况下不会执行故障转移。



注释

- 每当启用 HA 时，都会默认启用额外的心跳模块。您不必为数据平面中的其他心跳模块设置轮询间隔。此模块使用您为控制平面设置的相同心跳间隔。

接口监控

接口监控是一种故障转移功能，

- 跟踪最多 1025 个接口的运行状况，以检测接口故障
- 当在 15 秒内未收到 hello 消息时执行接口测试，并且
- 当故障接口数达到定义的阈值时，会触发故障转移。

接口监控操作

当设备在 15 个秒，未在受监控的接口上收到 hello 消息时，将运行接口测试。如果对于某个接口，其中一个接口测试失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障，设备停止运行测试。

如果满足您为故障接口数量定义的阈值 （请参阅 **设备** > **设备管理**，然后 **高可用性** > **故障转移触发条件**），并且主用设备的故障接口数量多于备用设备，则会发生故障转移。 如果某个接口在两个单元上都失败，则这两个接口会进入“Unknown”状态，并且不会计入由故障转移接口政策制定的故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的 设备会回到备用模式。

如果接口上配置了 IPv4 和 IPv6 地址， 设备会使用 IPv4 地址执行运行状况监控。如果接口上仅配置了 IPv6 地址，则 设备会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试， 设备会使用所有的 IPv6 节点地址 (FE02::1)。

接口测试

接口测试属于以下监控机制：

- 在故障转移场景期间评估接口的运行状态
- 默认情况下按顺序运行，每个测试的持续时间约为1.5秒，并且
- 确定 防火墙威胁防御 设备单元上的接口故障状态。

接口测试顺序

防火墙威胁防御 设备会按顺序使用这些接口测试：

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则 设备视为测试失败，然后测试停止。如果状态为打开，则 设备执行 Network Activity 测试。
2. 网络活动测试 - 接收的网络活动测试。测试开始时，每台设备会清除其接口收到的数据包计数。在测试期间，一旦设备收到符合条件的数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行 ARP 测试。
3. ARP 测试 - 用于测试成功的 ARP 回复。每台设备都向其 ARP 表中最新条目中的 IP 地址发送一个 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果设备未收到 ARP 回复，则 设备会向 ARP 表中的下一个条目中的 IP 地址发送一次 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 设备开始进行广播 Ping 测试。
4. 广播 Ping 测试 - 测试成功的 Ping 回复。每台设备发送一个广播 Ping，然后对收到的所有数据包进行计数。在测试期间，当设备收到任何数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果未收到任何流量，则测试将通过 ARP 测试再次开始。如果两台设备继续没有收到来自 ARP 和广播 Ping 测试的流量，则测试将会一直运行下去。

接口状态

接口状态是一种监控指示器，

- 显示故障转移配置中受监控接口的当前运行状态
- 跟踪对等设备之间的流量接收和 hello 数据包通信，以及
- 确定故障转移进程是否主动监控接口。

接口状态类型

受监控的接口可以具有以下状态类型：

- **未知**：初始状态。此状态也可能意味着状态无法确定。
- **正常**：接口正在接收流量。
- **正常（正在等待）**：接口已打开，但尚未从对等体设备上的对应接口接收欢迎数据包。
- **正常（未受监控）**：接口已打开，但未受故障转移进程监控。
- **正在测试**：接口上有 5 个轮询时间未收听到 Hello 消息。
- **链路断开**：接口或 VLAN 通过管理方式关闭。
- **链路断开（正在等待）**：接口或 VLAN 已通过管理方式关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- **链路断开（未受监控）**：接口或 VLAN 已通过管理方式关闭，但未受故障转移进程监控。

- **无链接**：接口的物理链路关闭。
- **无链接（正在等待）**：接口的物理链路已关闭，并且尚未从对等体设备上的对应接口接收欢迎数据包。
- **无链接（未受监控）**：接口的物理链路已关闭，但未受故障转移进程监控。
- **失败**：在接口上没有收到流量，但在对等体接口上收听到流量。

故障转移触发器和检测计时

故障转移触发器和检测计时是高可用性机制，具有以下功能：

- 当主用设备上发生特定故障条件时，启动自动切换，
- 通过可配置的检测阈值和计时参数监控系统运行状况，以及
- 当故障超过定义的限制时，通过将控制转移到备用设备来确保服务的连续性。

故障转移触发事件和时间参数

这些事件会在 Firepower 高可用性对中触发故障转移：

- 主用设备上超过 50% 的 Snort 实例已关闭。
- 主用设备上使用的磁盘空间已超过 90%。
- 主用设备上运行的是 **no failover active** 命令，而备用设备上运行的是 **failover active** 命令。
- 主用设备的故障接口比备用设备更多。
- 主用设备上的接口故障超过配置的阈值。

  默认情况下，单个接口发生故障会导致故障转换。您可以通过配置接口数量的阈值或为发生故障转移而必须发生故障的受监控接口的百分比来更改默认值。如果主用设备上的阈值被超过，则会发生故障转移。如果备用设备上的阈值被超过，则设备将进入**故障**状态。

  要更改默认故障转移条件，在全局配置模式下输入此命令：

表 *26:* 接口策略命令

命令	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	更改默认故障转移条件。 指定特定接口数时，*num* 参数可以介于 1 和 250 之间。 指定接口百分比时，*num* 参数可以介于 1 和 100 之间。

此表列出了故障转移触发事件及关联的故障检测时间。如果出现故障转移，您可以在消息中心中查看故障转移的原因，以及有关高可用性对的各种操作。您可以将这些阈值配置为指定的最小-最大范围内的值。

表 *27:* 防火墙威胁防御 故障转移次数

故障转移触发事件	最小	默认	最大
主用设备断电，硬件关闭或软件重新加载或崩溃。当出现这些情况时，受监控接口或故障转移链路不会收到任何 Hello 消息。	800 毫秒	15 秒	45 秒
主用设备接口物理链路发生故障。	500 毫秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

主用/备用故障转移

主用/备用故障转移是一种高可用性配置

- 允许使用备用 Firewall Threat Defense 设备接管故障设备的功能，
- 当主用设备故障，备用设备将变为主用设备，以及
- 若故障为暂时性，故障设备恢复后可重新作为备用设备上线。

若故障非暂时性，必须更换故障设备。更换故障设备前，须先将备用设备设为主设备，以保留辅助设备的配置。

对于多情景模式，ASA 可以在整个设备（包括所有情景）上进行故障转移，但不能在单个情景上单独进行故障转移。

主/辅角色与主/备状态

主/辅角色和主/备状态是故障转移配置概念，

- 定义设备层级结构，在同时启动时主设备优先，
- 确定故障转移操作期间的 IP 地址和 MAC 地址使用模式，以及
- 在主/备故障转移配置中的配对设备之间确立流量传输职责。

主设备与辅设备的差异

当设置主用/备用故障转移时，需要将一台设备配置为主设备，将另一台配置为辅助设备。配置过程中，主设备的策略将同步到辅助设备。此时，两台设备将作为单台设备进行设备和策略配置。但对于事件、控制面板、报告和运行状况监控，它们仍显示为单独的设备。

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

但是，设备之间还存在一些取决于哪一设备为主设备（在配置中指定），哪一设备为辅助设备的差别：

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

启动时主用设备判定是高可用性过程

- 若设备启动时检测到对等体已运行为主用，则该设备置为备用，
- 若设备启动未检测到对等体，则置为主用；
- 若两台设备同时启动，主设备置为主用，辅助设备置为备用。

故障转移事件

故障转移事件是指

- 触发主用/备用故障转移配置中的主用设备将控制权移交给备用设备
- 按设备级别发生，，以及
- 遵循特定故障转移策略以确定是否发生故障转移及各设备应采取的操作。

故障转移事件策略和操作

此表显示各故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *28:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。

故障事件	策略	主用设备操作	备用设备操作	说明
备用设备发生故障（电源或硬件）	禁用故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行过程中发生故障	禁用故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

Config-sync 优化

配置同步优化是一种配置同步增强功能，

- 比较主用设备和加入设备之间的配置散列值，以确定是否需要完全同步
- 通过在散列值匹配时跳过完全配置同步，实现更快的设备重新加入，以及
- 缩短了高可用性操作期间的维护窗口和升级时间。

配置同步优化的准则和局限性

当设备在暂停或恢复高可用性后重启或重新加入时，加入的设备会清除其运行配置。然后，主用设备将其整个配置发送到加入设备，以实现完全的配置同步。如果主用设备配置较大，则此过程可能需要几分钟时间。

配置同步优化功能可通过交换配置散列值来比较加入设备和主用设备的配置。如果主用设备和加入设备上计算的散列值匹配，加入设备就会跳过完全配置同步，重新加入高可用性配置。此功能可确保更快的对等互连，并缩短维护窗口和升级时间。

准则和限制：

- 配置同步优化功能默认已启用。

- Firewall Threat Defense 多情景模式通过在完全配置同步期间共享情景顺序来支持配置同步优化，从而允许在后续节点重新加入期间比较情景顺序。
- 如果配置密码和故障转移 IPsec 密钥，则配置同步优化无效，因为主用设备和备用设备中计算的散列值不同。
- 如果使用动态 ACL 或 SNMPv3 配置设备，则配置同步优化无效。
- 主用设备将 LAN 链路摆动的完整配置作为默认行为进行同步。在主用设备和备用设备之间的故障转移摆动期间，不会触发配置同步优化，设备会执行完整的配置同步。
- 当高可用性配置从主用设备和备用设备之间的网络通信中断或丢失中恢复时，会触发配置同步优化。

监控配置同步优化：

- 系统会生成系统日志消息，显示在主用设备和加入设备上计算的散列值是否匹配，或者操作超时是否已到期。
- 系统日志消息还会显示从发送散列请求到获取并比较散列响应所经过的时间。



注释 **show failover state** 命令中的配置状态会在加入 HA 期间显示配置同步状态。直到启动重新同步之前，此状态不会反映以后的配置部署或更改和设备上的复制。

高可用性的要求和先决条件

本参考介绍了实施高可用性功能所需的要求和前提条件。

型号支持

Cisco Secure Firewall Threat Defense

支持的域

任意

用户角色

管理员

网络管理员

准则

型号支持

- 200/1010/1210/1220:
  - 使用时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。虽然 防火墙管理中心 允许您在高可用性中配置交换机端口/VLAN 接口，但在连接到外部交换机时，可能会因网络环路而导致配置错误。
  - 仅可使用防火墙接口作为故障转移链路。
- Firepower 9300 - 不支持机箱内高可用性。
- 由于需要第 2 层的连接，因此不支持在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 Firewall Threat Defense Virtual。

其他准则

- 当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。
- 发生故障转移事件时，在连接到Firewall威胁防御设备故障转移对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 对于主用/备用 和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往 NMS 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。
- 两个对等设备都进入未知状态，如果在创建高可用性对时在任何对等设备中运行 clish，高可用性配置会失败。
- 故障转移后，系统日志消息的源地址将立即成为故障转移接口地址几秒钟。
- 为了更好地融合（在故障转移期间），您必须关闭 HA 对上未与任何配置或实例关联的接口。

- 在具有共享故障转移和状态接口的高可用性部署中，如果连接转移故障转移接口在备用设备处于“同步配置”状态时发生故障，以及最终在备用设备切换到主用状态时，会导致裂脑。即使有受监控接口，也会出现这种情况。

  连接转移故障转移接口可能在以下情况下发生故障：

  - 备用设备重新启动后，当备用设备处于同步配置状态时，连接切换故障转移接口会发生故障。
  - 启用备用设备上先前禁用的故障转移后，当备用设备处于同步配置状态时，连接故障转移接口会发生故障。

  要避免裂脑，请使用故障转移和状态接口。如果故障转移接口上的连接故障仍然存在，则从网络中隔离新的主用（之前是备用）设备。

- 如果您在评估模式下配置故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。

- 当使用具有故障转移功能的 SNMPv3 时，如果更换故障转移设备，则 SNMPv3 用户不会复制到新设备。 您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。

- 设备不再与其对等体共享 SNMP 客户端引擎数据。

- 如果您有大量访问控制和 NAT 规则，则配置的大小可能会阻止有效的配置复制，导致备用设备需要过长的时间才能达到备用就绪状态。这也会影响您在通过控制台或 SSH 会话进行复制期间连接到备用设备的能力。要提高配置复制性能，请使用 **asp rule-engine transactional-commit access-group** 和 **asp rule-engine transactional-commit nat** 命令为访问规则和 NAT 启用事务提交。

- 转换为备用角色的 对中的设备可将其时钟与主用设备同步。

  示例：

  ```
  firepower#show clock
  01:00:52 UTC Mar 1 2022

  ...
  01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
  Cold Standby               Sync Config               Detected an Active mate

  19:38:21 UTC Apr 9 2022 <======= Updated clock
  Sync Config                Sync File System          Detected an Active mate
  ...
  firepower/sec/stby#show clock
  19:38:40 UTC Apr 9 2022
  ```

- 中的设备不会动态同步时钟。以下是进行同步时的一些事件示例：

  - 将创建一个新的 对。
  - 已中断并已重新创建。
  - 故障转移链路上的通信中断并重新建立。

  - 使用 **no failover/failover** 或 **configure high-availability suspend/resume** （Firewall Threat Defense）命令来在 CLI 手动更改故障转移状态。

- 启用 会强制删除所有路由，并会在 进程变为“活动”状态后重新添加这些路由。在此阶段，您可能会遇到连接丢失的情况。
- 如果更换主设备，则在重新创建高可用性时，应将更换设备设置为辅助设备，以便将配置从以前的辅助设备复制到更换设备。如果将替换设备设置为主设备，则会意外覆盖运行设备上的配置。
- 在形成 之前，请在两台 威胁防御 设备上配置相同的强加密。如果二者不同，则高可用性对等体可能会进入裂脑状态。
- 在配置了数百个接口的高可用性中部署 Firepower 1100 设备可能会导致故障转移时间（秒）增加。
- 在 配置中，短期连接（通常使用端口 53）会快速关闭，并且永远不会从主用设备传输或同步到备用设备，因此两个 设备上的连接数量可能存在差异。这是短期连接的预期行为。您可以尝试比较长期（例如，超过 30-60 秒）的连接。
- 在 配置中，初期连接（尚未完成三次握手过程的连接请求）会快速关闭，并且不会在主用设备和备用设备之间同步。此设计可确保高可用性系统的效率和安全性。因此，两台 设备上的连接数可能存在差异，这是预期行为。
- 如果故障转移LAN链路不是背靠背连接，而是通过一台或多台交换机连接，则中间路径内的故障可能会导致主用设备失去与备用设备的连接，从而导致主用/备用状态不一致。虽然这不会影响 功能，但建议检查并恢复主用设备和备用设备之间的故障转移链路路径。

  当故障转移 LAN 链路发生故障时，不建议部署任何配置，因为它可能不会复制到对等设备。
- 请参阅 Cisco Secure Firewall Threat Defense Virtual 入门指南 并查看 Firewall Threat Defense Virtual 设备配置，以实现高可用性。
- 在 OSPF 中，故障转移后，与对等设备的 OSPF 连接将变为无效。终止无效连接，然后建立新的 OSPF 连接。
- 在透明模式下，如果存在主用设备丢失热备路由器 (HSRP) MAC 地址的问题，请为 MAC 地址创建静态映射。
- 如果威胁防御设备处于高可用性状态，则无法更改UCAPL或CC合规性模式。在形成高可用性对前修改合规模式。

添加高可用性对

建立主/备高可用性对，以确保设备故障时网络防护的连续性。

建立主用/备用高可用性对时，请将其中一台设备指定为主设备，将另一台指定为辅助设备。防火墙管理中心 会将合并的配置应用于配对设备。如果存在冲突，则使用主设备设置。在多域部署中，高可用性对中的设备必须属于同一个域。

注释 故障切换链路和状态故障切换链路位于专用 IP 空间中，仅用于高可用性对中的对等体之间的通信。在高可用性对建立后，无法在不破坏高可用性对并重新配置的情况下修改所选接口链路和加密设置。

注意 创建或中断高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

Before you begin

确认两台设备：

- 型号相同。
- 拥有相同数量和类型的接口。
- 位于同一个域和组中。
- 具有正常运行状态且运行相同的软件。
- 处于路由模式或透明模式下。

注释 数据接口上的管理器访问仅支持路由模式。

- 具有相同的 NTP 配置。请参阅时间同步，第 1030 页。
- 完全部署且没有尚未确认的更改。
- 在其任一接口中都未配置 DHCP 或 PPPoE。
- 对于数据接口上的管理器访问：
  - 在两台设备上使用相同的数据接口进行管理器访问。
  - 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。

注释 如果您使用 零接触调配 注册设备，则当您使用外部接口进行管理器访问时，它会默认使用 DHCP。在启用高可用性之前，需要将 IP 地址更改为静态地址。请参阅更改设备 IP 地址，第 879 页。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

- 在同一子网中有不同的静态 IP 地址。

- 使用相同的管理器配置（**configure manager add** 命令）确保连接相同。
- 不能将数据接口用作故障切换链路或状态链路。



注释 如果主设备上可用的证书在辅助设备上不存在，那么两台 Firewall Threat Defense 设备之间可能会形成高可用性。形成高可用性时，证书将在辅助设备上同步。

过程

步骤 1 根据 向管理中心注册，第 32 页将两台设备添加到 防火墙管理中心。

步骤 2 选择**设备** > **设备管理**。

步骤 3 从 **添加** 下拉菜单中，选择 **高可用性**。

步骤 4 为高可用性对输入显示**名称** 。

步骤 5 为高可用性对选择**主对等 (Primary Peer)** 设备。

步骤 6 为高可用性对选择**辅助对等 (Secondary Peer)** 设备。

步骤 7 点击**继续 (Continue)**。

步骤 8 在 **LAN 故障切换链路 (LAN Failover Link)** 下，选择为故障转移通信保留足够带宽的 **接口** 。

注释
只有没有逻辑名称且不属于安全区域的接口将在 **添加高可用性对** 对话框的 **接口** 下列列表中列出。

步骤 9 键入任何识别**逻辑名称 (Logical Name)**。

步骤 10 为主用设备上的故障切换链路键入**主要 IP (Primary IP)** 地址。

此地址应处于未使用的子网上。

注释
169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

步骤 11 或者，选择**使用 IPv6 地址 (Use IPv6 Address)**。

步骤 12 为备用设备上的故障切换链路键入**辅助 IP (Secondary IP)** 地址。此 IP 地址必须与主要地址在同一子网中。

步骤 13 如果使用 IPv4 地址，请键入适用于主要和辅助 IP 地址的**子网掩码 (Subnet Mask)**。

步骤 14 或者，在**状态性故障切换链路 (Stateful Failover Link)** 下，选择同一**接口**，或选择不同的接口并输入高可用性配置信息。

注释
169.254。1.0/24 and fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

步骤 15 （可选） 选择**已启用**并为故障转移链路间的 IPsec 加密选择**密钥生成**方法。

步骤 16 点击**确定**。由于此过程会同步系统数据，因此需要花费几分钟时间。

配置成功后，建立高可用性对，其中一台设备为活动状态，另一台为备用状态。。

下一步做什么

备份设备。您可以使用备份在设备发生故障时快速更换设备，并在不断开与防火墙管理中心的连接的情况下恢复高可用性服务。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南。

配置可选高可用性参数

您可以在 防火墙管理中心上查看初始高可用性配置。您无法在不破坏高可用性对，然后重新建立它的情况下编辑这些设置。要编辑这些设置，必须先中断高可用性对，然后重新建立它。您可以修改故障切换触发条件，以改进故障切换结果。接口监控可帮助您确定哪些接口最适合于故障切换。

配置备用 IP 地址和接口监控

为高可用性接口配置备用 IP 地址，以使主用设备能够执行网络测试并检查备用接口运行状况，而不仅仅是跟踪链路状态。

为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

默认情况下，所有命名物理接口均启用监控，而对于200/10101210/1220，所有VLAN接口也会启用监控。您可能希望排除连接到非关键网络的接口，以免影响故障转移策略。交换机端口无法进行接口监控。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** (✎)。

步骤 3 点击**高可用性 (High Availability)** 选项卡。

步骤 4 在**监控的接口**区域中，点击要编辑的接口旁边的 **编辑** (✎)。

步骤 5 选中**监控此接口的故障情况**复选框。

步骤 6 在 **IPv4** 选项卡上，输入**备用 IP 地址**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。

步骤 7 如果手动配置了 IPv6 地址，请在 **IPv6** 选项卡上，点击活动 IP 地址旁边的 **编辑** (✎)，输入**备用 IP 地址**，然后点击**确定**。

此地址必须是与活动 IP 地址位于同一网络的可用地址。对于自动生成的地址和**强制 EUI 64** 地址，系统会自动生成备用地址。

步骤 8 点击**确定**。

编辑高可用性故障切换条件

此任务允许自定义高可用性设备对的故障转移条件，以匹配特定的网络部署要求。

您可以根据网络部署自定义故障切换条件。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**高可用性**。

步骤 4 在**故障切换触发条件 (Failover Trigger Criteria)** 旁边，点击 **编辑** ()。

步骤 5 在**接口故障阈值 (Interface Failure Threshold)** 下，选择在设备进行故障切换之前必须出现故障的接口数目或百分比。

步骤 6 在**呼叫数据包间隔 (Hello packet Intervals)** 下，选择通过故障切换链路发送呼叫数据包的频率。

步骤 7 点击**确定**。

配置虚拟 MAC 地址

配置主用和备用 MAC 地址，最大限度减少故障转移期间的流量损失，并为故障转移提供针对 IP 地址映射的冗余。

可以在 Secure Firewall Management Center上使用以下方法配置主用和备用 MAC 地址以进行故障切换：

- 配置接口期间在 **编辑接口** 页面的 **高级**选项卡；请参阅 配置 MAC 地址 ，第 820 页。
- 从 **高可用性** 页面访问的 **添加接口 MAC 地址**页面；请参阅此程序。

注释 要在主设备和辅助设备中配置 MAC 地址（以便将 MAC 地址传输到两台高可用性设备的所有子接口），建议使用 **接口** 选项卡在两个设备上复制子接口上的 MAC 地址主用和备用高可用性设备。

如果在两个位置都配置了主用和备用MAC地址，则在配置接口期间定义的地址优先进行故障切换。

通过将主用和备用 MAC 地址指定到物理接口，可以最大限度地减少故障切换期间的流量损失。此功能为故障切换提供了针对 IP 地址映射的冗余。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 点击**高可用性 (High Availability)**。

步骤 4 点击接口 Mac 地址旁边的 **添加** () 图标。

步骤 5 选择**物理接口**。

步骤 6 输入**主用接口 MAC 地址**。

步骤 7 输入**备用接口 MAC 地址**。

步骤 8 点击**确定**。

注释
有关详细信息，请参阅 任务 2， 在 Firepower 设备上配置 FTD 高可用性中的步骤 10 到 14。

管理

本部分介绍您在启用后如何管理，包括如何更改设置以及如何强制从一台设备故障转移到另一台设备。

在 Firewall Threat Defense 高可用性对中切换主用对等体

此任务允许您手动切换高可用性对中的主用和备用设备，从而有效地强制进行故障转移，例如当前主用设备出现持续故障或运行状况事件。

在建立 Firewall Threat Defense 高可用性对以后，可以手动切换主用和备用设备，出于持续性故障或运行状况事件等原因有效执行故障切换。两台设备应该已经完全部署，然后才能完成此程序。

Before you begin

刷新单个 Firewall Threat Defense 高可用性对的节点状态， 第 362 页。这样可以确保 Firewall Threat Defense 高可用性设备对上的状态与 防火墙管理中心 上的状态同步。

请按照以下步骤切换高可用性对中的主用节点：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要更改主用对等体的高可用性对旁边，点击**切换主用对等体 (Switch Active Peer)**。

步骤 3 选择一个选项：

- 点击**是**将使备用设备立即变成高可用性对中的主用设备。
- 点击 **No** 将取消并返回到 Device Management 页面。

刷新单个 Firewall Threat Defense 高可用性对的节点状态

当通信问题导致数据不同步时，刷新高可用性节点状态以获取有关高可用性对中主用设备和备用设备的准确信息。

每当重新引导 Firewall Threat Defense 高可用性对中的主用或备用设备时， 防火墙管理中心 可能不会显示这两种设备的准确高可用性状态。这是因为，当设备重新引导时，高可用性状态会在设备上立即更新，其相应的事件将会发送到 防火墙管理中心。但是，状态可能不会在 防火墙管理中心 上更新，因为设备和 防火墙管理中心 之间的通信尚未建立。

防火墙管理中心 与设备之间出现通信故障或通信隧道信号弱，可能会导致数据不同步。切换高可用性对中的主用设备和备用设备时，即使持续很长时间，这种更改可能也不会反映在 防火墙管理中心 中。

在此类情况下，可以刷新高可用性节点状态以获取有关高可用性对中主用设备和备用设备的准确信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在希望刷新节点状态的高可用性对旁边，点击 **刷新 HA 节点状态**。

步骤 3 点击 **是** 来刷新节点状态。

暂停和恢复高可用性

当有用时，可以暂停高可用性对中的设备：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障转移。

当您暂停高可用性时，当前主用设备保持活动状态，并继续处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障转移到现在的伪备用设备。

使用数据接口进行管理器访问时，管理连接将断开，直到您恢复。

暂停高可用性和中断高可用性之间的主要区别是，在暂停的高可用性设备上将保留高可用性配置。如果中断高可用性，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

要暂停高可用性，请使用 **configure high-availability suspend** 命令。

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。备用设备接口配置也会被清除。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障转移至暂停的设备。

要恢复故障转移，请使用 **configure high-availability resume** 命令。

```
> configure high-availability resume
Successfully resumed high-availablity.
```

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。

注释 暂停高可用性是一种临时状态。如果您重新加载一台设备，它会自动恢复高可用性配置，并与对等体协商主用/备用状态。

更换 Firewall Threat Defense 高可用性对中的设备

本参考介绍在 Firewall Threat Defense 高可用性对中更换故障设备的流程，包括备份恢复和手动更换程序。

要使用备份文件替换 Firewall Threat Defense 高可用性对中的故障设备，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 恢复 防火墙管理中心和托管设备 。

如果没有故障设备的备份，则必须中断高可用性。然后，将替换设备注册到 Secure Firewall Management Center 并重新建立高可用性。该过程会因设备是主设备还是辅助设备而有所不同：

- 将主 Firewall Threat Defense 高可用性设备替换为无备份 ， 第 363 页
- 将辅助 Firewall Threat Defense HA 单元更换为无备份 ， 第 364 页

将主 Firewall Threat Defense 高可用性设备替换为无备份

此任务将替换 Firewall Threat Defense 高可用性对中出现故障的主设备，以恢复冗余并维持网络保护。

按照这些步骤更换 Firewall Threat Defense 高可用性对中出现故障的主设备。如果无法执行这些步骤，系统可能会覆盖现有的高可用性配置。

注意 创建或中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

注意 切勿在未重新映像磁盘的情况下将磁盘从传感器或防火墙管理中心移动到其他设备。这是不受支持的配置，可能会导致功能中断。

过程

步骤 1 选择**强制中断**以分隔高可用性对；请参阅中断高可用性对，第 365 页。

注释
中断操作会从 Firewall Threat Defense 和 防火墙管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 防火墙管理中心取消注册主 Firewall Threat Defense 设备；请参阅从 防火墙管理中心 取消注册设备，第 63 页。

步骤 3 将替换 Firewall Threat Defense 注册到 防火墙管理中心；请参阅向管理中心注册，第 32 页。

步骤 4 配置高可用性，在注册期间使用现有的辅助/主用设备作为主设备，并将更换设备用作辅助/备用设备；请参阅添加高可用性对，第 356 页。

将辅助 Firewall Threat Defense HA 单元更换为无备份

此任务允许您通过更换 Firewall Threat Defense 高可用性对中出现故障的辅助设备来恢复高可用性功能。

当高可用性配置中的辅助设备发生故障时，您需要更换该设备并重新创建 HA 对，以维持网络冗余和保护。

注意 创建或中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。系统会向您发出警告，指明继续创建高可用性对会重启主用和辅助设备上的 Snort 进程，并允许您取消。

过程

步骤 1 选择**强制中断**以分隔高可用性对。

请参阅中断高可用性对，第 365 页。

注释
中断操作会从 Firewall Threat Defense 和 防火墙管理中心删除与 HA 相关的所有配置，您需要稍后手动重新创建。要成功配置同一 HA 对，请确保在执行 HA 中断操作之前保存所有接口/子接口的 IP，MAC 地址和监控配置。

步骤 2 从 防火墙管理中心 取消注册辅助 Firewall Threat Defense 设备。

请参阅从 防火墙管理中心 取消注册设备，第 63 页。

步骤 3 将替换 Firewall Threat Defense 注册到 防火墙管理中心。

请参阅向管理中心注册，第 32 页。

步骤 4 在注册期间使用现有主/主用设备作为主设备并将替换设备作为辅助/备用设备配置高可用性。

请参阅添加高可用性对，第 356 页。

中断高可用性对

中断高可用性对，以从两台设备中删除高可用性配置，同时保持主用设备上的流量。

中断高可用性对时，将从两台设备中删除高可用性配置。

使用管理接口进行管理器访问时： 主用设备保持运行并传递流量。备用设备接口配置被清除。

使用数据接口进行管理器访问时： 请参阅以下详细信息。

- 主用设备保持运行并传递流量。
- 备用设备的数据接口将关闭，但管理器访问接口除外，该接口使用备用 IP 地址保持运行，因此可以维护管理连接。
- 在远程分支机构部署设置中，所有分配了逻辑名称的备用机数据接口都会关闭，但管理器访问接口除外，因为管理器访问接口仍处于运行状态，以保持管理连接。
- 如果主设备处于备用状态：
  - 管理器访问的 IP 地址在 防火墙管理中心 配置中永久交换：主设备使用备用 IP 地址，辅助设备使用主用 IP 地址。
  - 如果 防火墙管理中心 发起了管理连接，并且您为设备指定了主机名，则需要更新 DNS 服务器，以便将交换的 IP 地址与正确的主机名关联。

- 中断高可用性会导致部署到备用设备。如果由于IP地址交换而尚未重新建立管理连接，则部署可能会失败。在这种情况下，您需要稍后（在建立管理连接后）手动触发部署。在将更改部署到主用设备之前，请务必完成备用部署。

在断开操作之前尚未部署到主用设备的策略，在断开操作完成后仍会保持未部署状态。请在断开操作完成后，在独立设备上部署这些策略。



注释

- 在 Firewall Threat Defense 设备上的高可用性接口上启用 IPsec 时，设备无法确定进入高优先级接收队列的加密数据包的优先级。因此，在高数据流量场景下，尝试中断高可用性可能会失败，因为设备无法有效管理大量加密连接并确定其优先级。要查看设备的资源使用情况和最大吞吐量，请使用 显示资源使用 命令。
- 如果无法使用 防火墙管理中心访问高可用性对，请连接到每台设备上的 CLI 并输入 **configure high-availability disable** 以手动中断高可用性。另请参阅取消注册高可用性对和注册新 防火墙管理中心，第 367 页。



注意 中断 Firewall Threat Defense 高可用性对会立即在主设备和辅助设备上重启 Snort 进程，从而暂时中断两个设备上的流量检查。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

Before you begin

- 刷新单个 Firewall Threat Defense 高可用性对的节点状态，第 362 页。这样可以确保高可用性设备对上的状态与 防火墙管理中心上的状态同步。

按照以下步骤中断高可用性对：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要中断的高可用性对旁边，点击 **更多** (⋮) 并选择**中断 (Break)**。

步骤 3 如果备用对等体没有响应，请选中 **强制中断**。

步骤 4 点击 **Yes**。

断开操作将从主用和备用设备中删除高可用性配置。

在主用设备上部署的 FlexConfig 策略可能会在中断高可用性操作后显示部署失败。您必须在主用设备上修改并重新部署 FlexConfig 策略。

下一步做什么

如果在主用设备上使用 FlexConfig 策略，请修改并重新部署 FlexConfig 策略以消除部署错误。



注释 中断高可用性后，作为主用设备运行的 Firewall Threat Defense 设备仍将在其配置中列出备用设备的 IP 地址。要解决此问题，请在以前主用 Firewall Threat Defense 设备上执行其他部署，以从其配置中删除备用设备的 IP 地址。

取消注册高可用性对和注册新 防火墙管理中心

此任务允许您从防火墙管理中心中取消注册高可用性配对，从而保持高可用性配对的完整性。如果要将其注册到新的防火墙管理中心或无法再访问该对，则防火墙管理中心可能需要取消注册该对。

取消注册高可用性对：

- 会切断 防火墙管理中心 和该对之间的所有通信。
- 从 **设备管理** 页面删除对。
- 如果对的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将对返回本地时间管理。
- 保持配置不变，以便设备对继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

再次向相同或不同的 防火墙管理中心 注册该对会导致配置被删除，因此该对将在该点停止处理流量；高可用性配置保持不变，因此您可以将其作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

Before you begin

- 此过程需要 CLI 对主节点 拥有访问权限。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要注销的高可用性对旁边，点击 **更多** (:) 并选择**取消注册 (Unregister)**。

步骤 3 点击**是 (Yes)**。设备高可用性对随即会被注销。

步骤 4 您可以通过将主设备添加为新设备来将该对注册到新的（或相同的） 防火墙管理中心 。

a) 通过连接到一台设备上的 CLI 并输入 **show failover** 命令来确定主设备。

输出的第一行显示此设备是主设备还是辅助设备。

```
> show failover
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On

[...]
```

b) 在主设备的 CLI 中，使用 **configure manager add** 命令识别新 防火墙管理中心 。请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口，第 879 页。

c) 选择 **设备** > **设备管理**，然后点击**添加** > **设备**。

您只需将主设备添加为设备， 防火墙管理中心 即可发现辅助设备。

监控

监控 是一种系统功能，可让您查看 状态。

查看故障切换历史记录

在单个视图中查看高可用性设备的故障转移历史记录，了解故障转移事件的时间顺序及其原因。

您可以在单个视图中查看两个高可用性设备的故障切换历史记录。历史记录按时间顺序显示，并包括任何故障切换的原因。

Before you begin

按照以下步骤查看故障转移历史记录：

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**摘要**。

步骤 4 在“常规”(General) 下，点击 **视图** ()。

查看状态故障切换统计信息

通过此任务，可以通过监控状态故障切换链路统计信息来评估高可用性配置的性能和运行状况。

您可以在高可用性对中查看主设备和辅助设备的状态故障切换链路统计信息。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑的设备高可用性对旁边，点击 **编辑** ()。

步骤 3 选择**高可用性**。

步骤 4 在“状态故障切换链路”(Stateful Failover Link) 下，点击 **视图** ()。

步骤 5 选择一个设备来查看统计信息。

配置同步失败故障排除

形成故障转移对时，加入设备会清除其运行配置并从主用设备复制整个配置。完成完整配置同步后，加入设备将承担备用就绪角色并建立故障切转移。设备加入故障转移对后，主用设备上的任何配置更改也会复制到备用设备上，以保持两台设备同步。

如果备用设备无法复制任何配置更改命令，它会报告配置同步失败并通过禁用故障转移退出高可用性。本节介绍备用设备报告的配置同步失败错误的识别和故障转移步骤。

要查看配置同步错误或统计信息，您可以通过 SSH 会话或威胁防御 CLI 使用这些 CLI 命令：

- **show failover config-sync errors all** 显示与故障转移相关的所有配置同步错误。
- **show failover config-sync stats all** 查看有关故障转移配置同步的统计信息。

要重新启用高可用性，请执行以下操作：

- 通过在主用设备上执行 **failover reset** 命令来重新启用故障转移。
- 如果重新启用故障转移不成功，请删除或更新备用设备无法复制的配置更改，然后重新启用故障转移。



注释 如果达到最大接口限制，主用设备和备用设备上的VPN隧道数可能不一致。这种情况下，在主用设备上运行**write standby**命令以同步配置。

高可用性历史记录

本参考提供了按时间顺序排列的在各种软件版本中实施的高可用性功能、增强功能和改进的历史记录。这些信息有助于您跟踪高可用性功能的发展，并了解各项功能的引入时间。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
改进了故障转移期间的角色切换时间	7.7	7.7	发生故障转移时，新的活动设备会为每个 MAC 地址条目生成组播数据包，并将其发送到所有网桥组接口，从而促使上游交换机更新路由表。生成组播数据包并将其发送到网桥接口的任务现在可以在数据平面中异步运行，从而使控制平面中的关键故障转移任务能够无延迟地进行。此增强功能可缩短故障转移期间的角色切换时间，并减少停机时间。
管理器访问数据接口的高可用性支持	7.4	7.4	您现在可以使用数据接口进行 Firewall Threat Defense 高可用性管理器访问。
取消注册高可用性对现在可以在不中断高可用性对的情况下重新注册	7.3	任意	删除（取消注册）高可用性对时，无需再在 CLI 中手动断开配对并重新注册独立设备。您现在可以将主设备添加到新防火墙管理中心，系统将自动发现备用设备。重新注册该对仍将清除配置，并且您的策略将需要重新应用。
策略支持回滚以实现高可用性	7.2	任意	**configure policy rollback** 命令支持高可用性。
配置同步优化功能可实现更快的高可用性对	7.2	任意	配置同步优化功能通过交换配置散列值来比较加入设备和主用设备的配置。如果在主用设备和加入设备上计算的散列值匹配，则加入设备将跳过完全配置同步并重新加入 HA。此功能可实现更快的 HA 对等，并缩短维护窗口和升级时间。
改进了集群和高可用性设备的升级工作流程。	7.1	任意	我们改进了集群与高可用性设备的升级流程： • 升级向导现在可以将集群和高可用性设备正确显示为组，而不是单个设备。系统可以识别、报告和预先要求修复您可能遇到的组相关问题。例如，如果您在 Firepower 机箱管理器上进行了未同步的更改，则无法升级 Firepower 4100/9300 上的集群。 • 我们提高了将升级包复制到集群和高可用性对的速度和效率。以前，FMC 会按顺序将数据包复制到每个组成员。现在组成员可在正常同步过程中互相获取软件包。 • 您现在可以指定集群中数据设备的升级顺序。控制设备始终最后升级。
清除高可用性组或集群中的路由。	7.1	任意	在以前的版本中， **清除路由** 命令仅清除设备上的路由表。现在，在高可用性组或集群中运行时， 命令仅在主用或控制设备上可用，并清除组或集群中所有设备上的路由表。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
FTD 高可用性加固	6.2.3	任意	版本 6.2.3 为高可用性中的 FTD 设备引入了以下功能： • 每当重启高可用性对中的主用或备用 FTD 设备时， 可能不会显示这两种托管设备的准确高可用性状态。但是，状态可能不会在FMC上更新，因为设备和 FMC 之间的通信尚未建立。通过 **设备** > **设备管理** 页面上的 **刷新节点状态** 选项，可以刷新高可用性设备状态以获取有关高可用性对中主用设备和备用设备的准确信息。 • FMC UI 的 **设备** > **设备管理** 页面上有一个新的 **交换机活动对等体** 图标。 • 版本 6.2.3 包括一个新的 REST API 对象、**设备高可用性对服务**，其中包含四个功能： • 删除 **ftddevicehapairs** • **PUT ftddevicehapairs** • **POST ftddevicehapairs** • **GET ftddevicehapairs**



第 10 章

群集技术： Cisco Secure Firewall 3100/4200/6100

通过集群，您可以将多个 Firewall Threat Defense 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 430 页。

- 关于 Cisco Secure Firewall 3100/4200/6100 的集群，第 373 页
- 集群的许可证，第 375 页
- 集群要求和前提条件，第 375 页
- 面向集群的指导原则，第 376 页
- 配置集群，第 380 页
- 管理集群节点，第 410 页
- 监控集群，第 420 页
- 对集群进行故障排除，第 425 页
- 集群示例，第 428 页
- 集群参考，第 430 页
- 集群的历史记录，第 443 页

关于 Cisco Secure Firewall 3100/4200/6100 的集群

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的高速背板网络（称为集群控制链路）用于集群内的通信。
- 对每台防火墙的管理访问权限，用于进行配置和监控。

将集群接入网络中时，上游和下游路由器需要能够使用 以下方法之一使出入集群的数据实现负载均衡：

- 跨网络 EtherChannel（推荐）- 将多个集群成员上的接口分组为一个 EtherChannel；EtherChannel 在设备之间执行负载均衡。
- 策略型路由（仅适用于路由防火墙模式）- 上游和下游路由器使用路由映射和 ACL 在设备之间执行负载均衡。
- 等价多路径路由（仅适用于路由防火墙模式）- 上游和下游路由器使用等价静态或动态路由在设备之间执行负载均衡。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 首次创建集群时，您可以指定要成为控制节点的节点，因为它是添加到集群的第一个节点，所以它将成为控制节点。

集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

集群接口

您可以将数据接口配置为 或 跨区以太网通道 或独立接口。集群中的所有数据接口只能。有关详细信息，请参阅关于集群接口，第 380 页。

对于跨区以太网通道： 您可以使用常规防火墙接口或仅 IPS 接口（内联集或被动接口）。对于独立接口：不支持仅 IPS 接口。

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。有关详细信息，请参阅集群控制链路，第 380 页。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

管理网络

您必须使用管理接口来管理每个节点；集群不支持从数据接口进行管理。

集群的许可证

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。您可以通过点击 **管理** > **许可证** > **智能许可证** 中的**编辑许可证**或选择 **设备** > **设备管理**、点击集群的 **编辑** (✎)、然后在**许可证**区域中点击 **编辑** (✎) 来修改集群的许可证。



注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

集群要求和前提条件

型号要求

- Cisco Secure Firewall 3100 - 最多 16 台设备
- Cisco Secure Firewall 4200 - 最多 16 台设备
- Cisco Secure Firewall 6100 - 最多 4 个节点

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件和软件要求

集群中的所有设备：

- 必须是相同型号。
- 必须包含相同的接口。
- 必须从管理接口访问 防火墙管理中心；不支持数据接口管理。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。
- 必须处于相同的防火墙模式（路由或透明）。

- 必须在同一域中。
- 必须在同一组中。
- 不得有任何待处理或进行中的部署。
- 控制节点不得配置任何不受支持的功能（请参阅集群不支持的功能，第 430 页）。
- 数据节点不得配置任何 VPN。控制节点可以配置站点间 VPN。

交换机要求

- 请务必完成交换机配置后再配置集群。确保连接到集群控制链路的端口配置了正确（更高）的 MTU。默认情况下，集群控制链路 MTU 会被设置为比数据接口高 100 字节。如果交换机的 MTU 不匹配，则集群形成将失败。

面向集群的指导原则

防火墙模式

所有设备上的防火墙模式必须匹配。

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。

- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **src-dst-mixed-ip-port**（请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

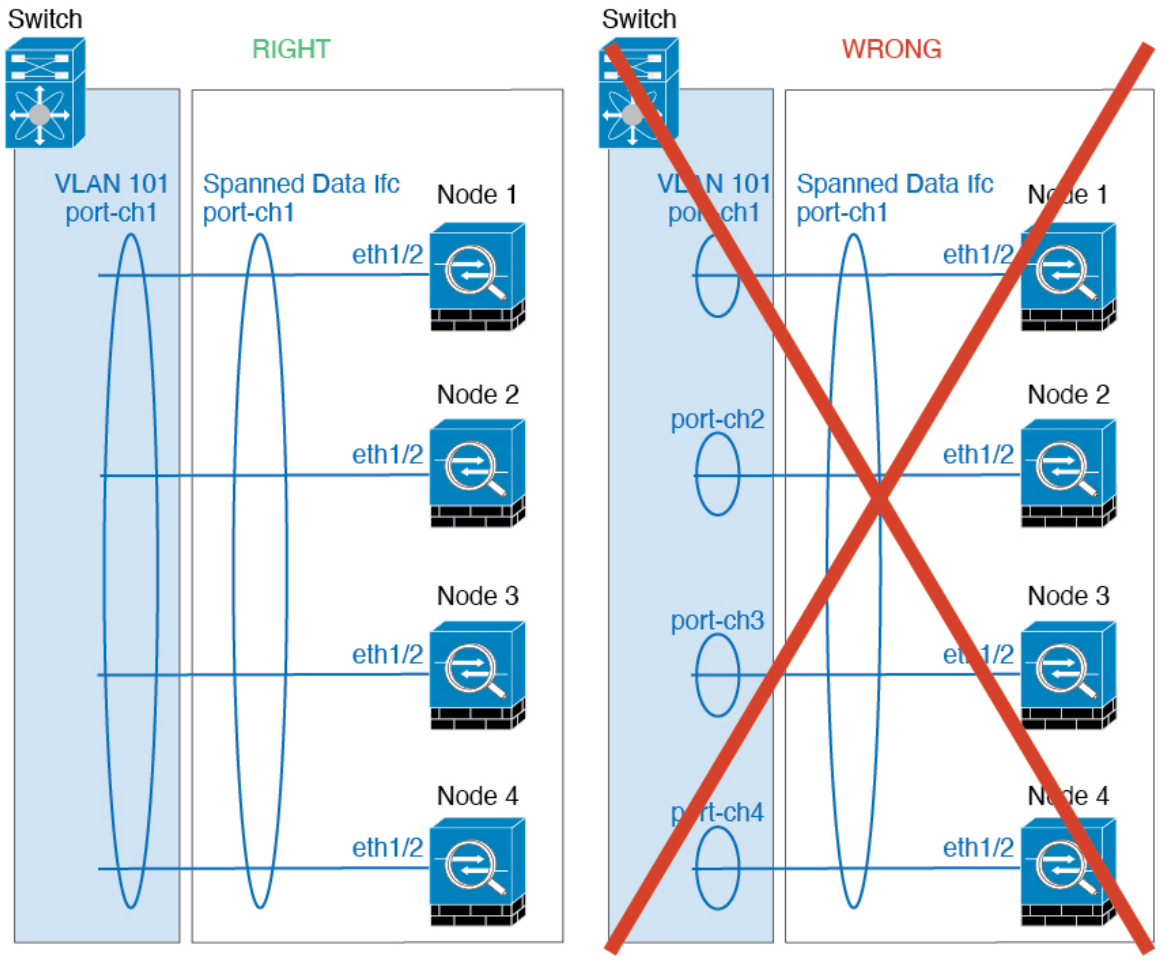
  router(config)# **port-channel** *id* **hash-distribution fixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

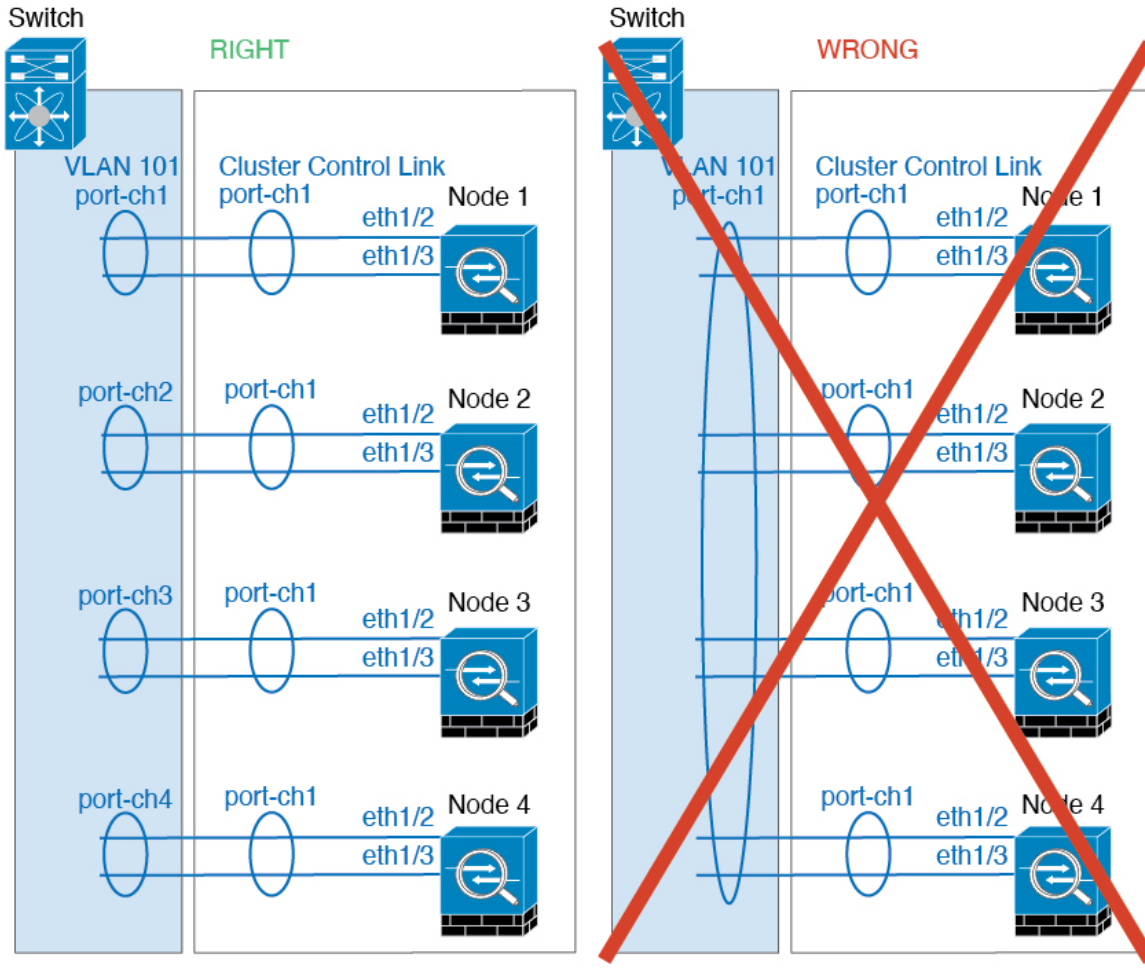
- 您应在所有面向集群的 EtherChannel 接口上为思科 Nexus 交换机禁用 LACP Graceful Convergence 功能。

EtherChannel

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。
  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firewall Threat Defense 或交换机上的接口、添加其他交换机以形成 VSS 或 vPC），应禁用运行状况检查功能，另外还应为禁用的接口禁用接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨网络 EtherChannel 的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器没有限制 ICMP 错误信息时，将会有大量 ICMP 消息被发送回 ASA 集群。这些消息会导致 ASA 集群的某些设备 CPU 使用率极高，进而影响性能。因此，我们建议您限制 ICMP 错误信息。

- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要建立新连接以连通新设备。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。

集群默认设置

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

配置集群

要将集群添加到防火墙管理中心，请将每个节点作为独立设备添加到防火墙管理中心，在要作为控制节点的设备上配置接口，然后即可形成集群。

关于集群接口

您可以将数据接口配置为 或跨区以太网通道或独立接口。集群中的所有数据接口只能是一种类型。不能将以太网 1/1 配置为跨区以太网通道，也不能将以太网 1/2 配置为同一集群内的独立接口，例如。

对于跨区以太网通道： 您可以使用常规防火墙接口或仅 IPS 接口（内联集或被动接口）。对于独立接口：不支持仅 IPS 接口。

每台设备还必须至少将一个硬件接口专门用作集群控制链路。

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。我们建议将 EtherChannel 用于集群控制链路（如果可用）。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

集群控制链路接口和网络

您可以将任何物理接口或 EtherChannel 用于集群控制链路。VLAN 子接口不能用作集群控制链路。您也无法使用管理接口。

每条集群控制链路都有一个属于同一子网的 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。



注释 对于有 2 个成员的集群，请勿将集群控制链路从一个节点直接连接到另一个节点。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。如果需要直接连接设备（例如，出于测试目的），则应在形成集群之前在两个节点上配置并启用集群控制链路接口。

确定集群控制链路规格

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。



注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

集群控制链路 MTU ping 测试

控制节点 ping 测试

当节点加入集群时，控制节点会发送 ping，其负载大小为 MTU 的两倍。此过程测试网络处理数据包分片的能力，因为底层 IP 层会对超过 MTU 限制的数据包进行分片。

Ping 操作成功可确认网络路径支持适当的分片，并且集群控制链路可以按配置的 MTU 大小可靠地处理流量。

如果 ping 失败，请查看以下消息：

- **show cluster history**— 事件：对设备名称的 CCL MTU 测试失败

- 控制台警告 — 警告：在 CCL 巨型帧 ICMP 测试中无法访问设备名称，请检查集群接口和交换机 MTU 配置

即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。

数据节点 ping 测试

当某个节点加入集群时，加入的节点会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。

如果 ping 失败，请查看以下消息：

- **show cluster info trace**— 警告：CCL MTU 配置为 *cfg_mtu_size*。但是，对设备名称的 CCL MTU 测试会失败，大小为 *larger_test_size*（已通过，大小为 *smaller_test_size*）。请检查交换机 MTU 配置。

  要轻松查看此警告，请使用 **show cluster info trace | incl MTU** 过滤 **show** 输出。

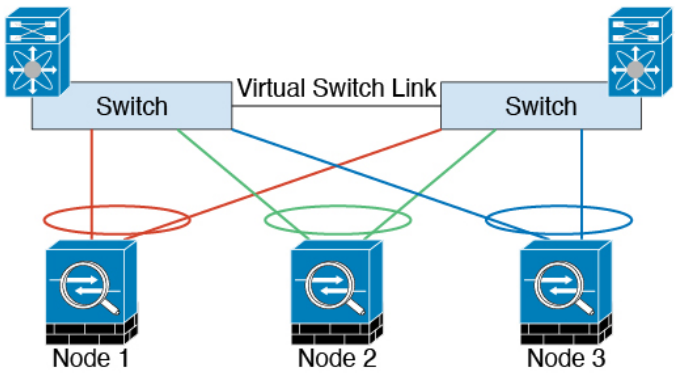
- **show cluster history**、防火墙管理中心 通知 — 警告：在 CCL 接口上检测到 MTU 不匹配。请确保连接的交换机上的 MTU 设置与防火墙的已配置 MTU（*cfg_mtu_size*）相匹配。

- 控制台警告 — 警告：在 CCL 巨型帧 ICMP 测试中无法访问设备名称，请检查集群接口和交换机 MTU 配置

即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。

集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS)、虚拟端口通道 (vPC)、StackWise 或 StackWise Virtual 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是冗余系统的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到冗余系统中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

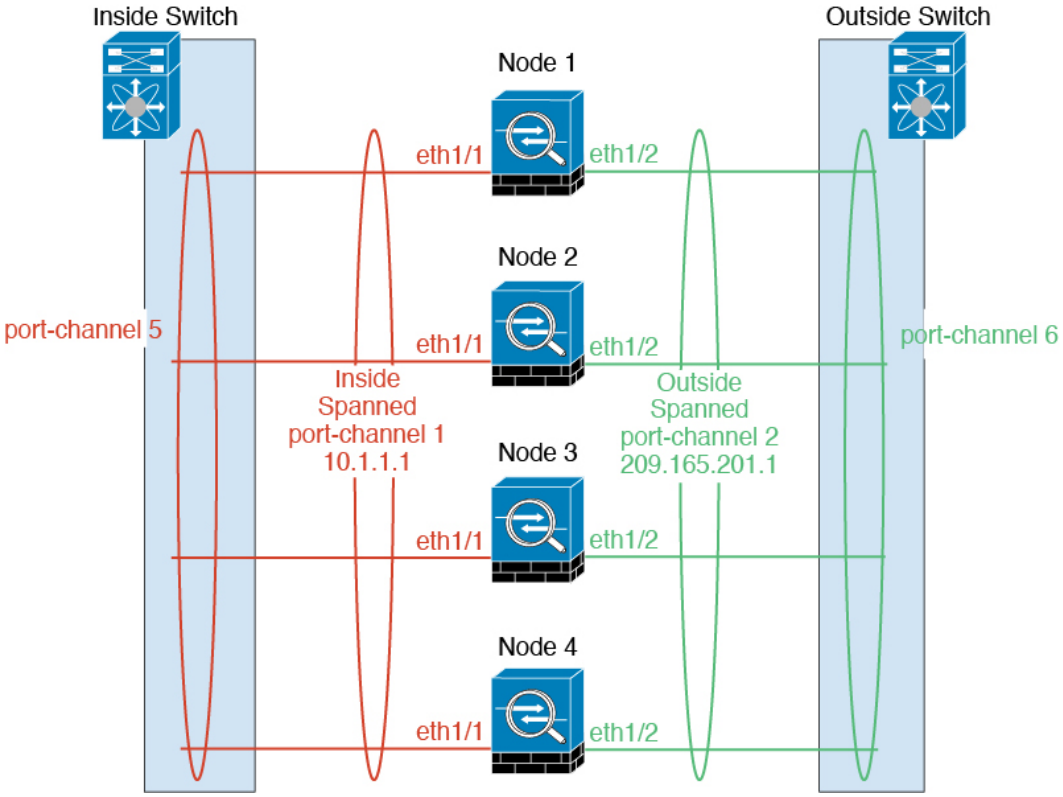
集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

跨网络 EtherChannel（推荐）

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。

对于常规防火墙接口：在路由模式和透明防火墙模式下均可配置跨区以太网通道。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。

负载均衡属于 EtherChannel 固有的基本操作。



跨区以太网通道优势

我们优先推荐 EtherChannel 负载均衡方法，因其具有以下优势：

- 发现故障的速度更快。
- 收敛速度更快。独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。
- 易于配置。

最大吞吐量准则

要实现最大吞吐量，我们建议采取以下措施：

- 使用“对称”的负载均衡散列算法，亦即来自两个方向的数据包具有相同的散列值，并将在跨网络 EtherChannel 中发送到同一台 Firewall Threat Defense。我们建议将源和目标 IP 地址（默认设置）或源和目标端口用作散列算法。
- 将 Firewall Threat Defense 连接到交换机时使用相同类型的线路卡，以使应用于所有数据包的散列算法都相同。

负载均衡

EtherChannel 链路使用专有散列算法并且根据源或目标 IP 地址以及 TCP 和 UDP 端口号进行选择。



注释 在交换机上，我们建议使用以下其中一种算法：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 或思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中 的流量分摊不均。

EtherChannel 中的链路数量会影响负载均衡。

对称的负载均衡有时并不能够实现。如果您配置了 NAT，则转发和返回数据包具有不同的 IP 地址和/或端口。返回流量将根据散列值被发送到不同的设备，因此集群不得不将大部分返回流量重定向到正确的设备。

EtherChannel 冗余

EtherChannel 有内置冗余。它监控所有链路的线路协议状态。如果一条链路发生故障，将在其余链路之间再均衡流量。如果 EtherChannel 中的所有链路在特定设备上发生故障，但其他设备仍然处于活动状态，则会从集群中删除该设备。

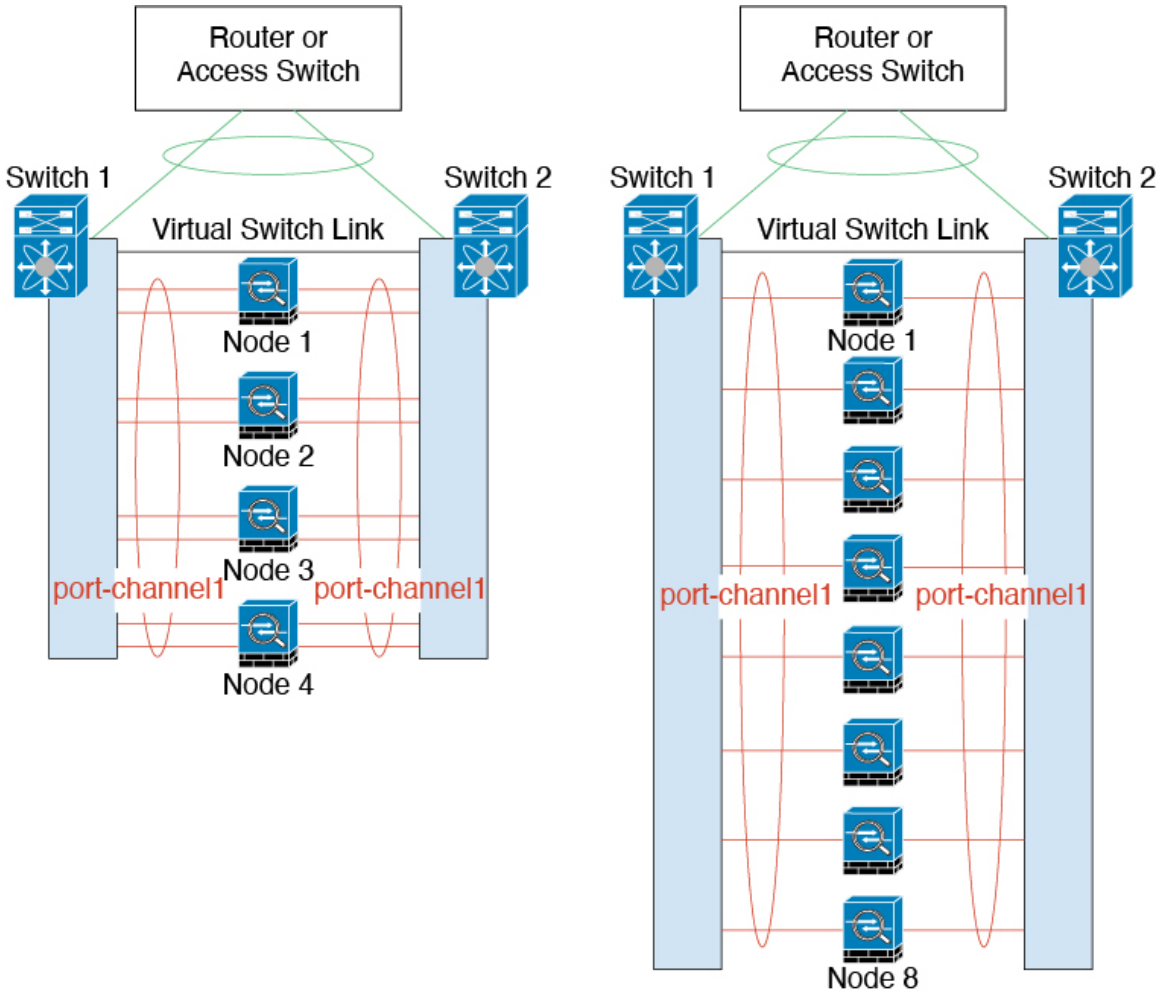
连接到冗余交换机系统

您可以在跨网络 EtherChannel 中包含每台 Firewall Threat Defense 的多个接口。每台 Firewall Threat Defense 有多个接口，对于连接到 VSS、vPC、StackWise 或 StackWise Virtual 中两台交换机的情况特别有用。

根据交换机的不同，最多可在跨网络 EtherChannel 中配置 32 条活动链路。此功能需要 vPC 中的两台交换机都支持各有 16 条活动链路的 EtherChannel（例如带 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。

对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到冗余系统中的两台交换机时，最多可在跨区以太网通道 中配置 16 条活动链路。

下图所示为 4 节点集群和 8 节点集群中有 16 条活动链路的跨区以太网通道。



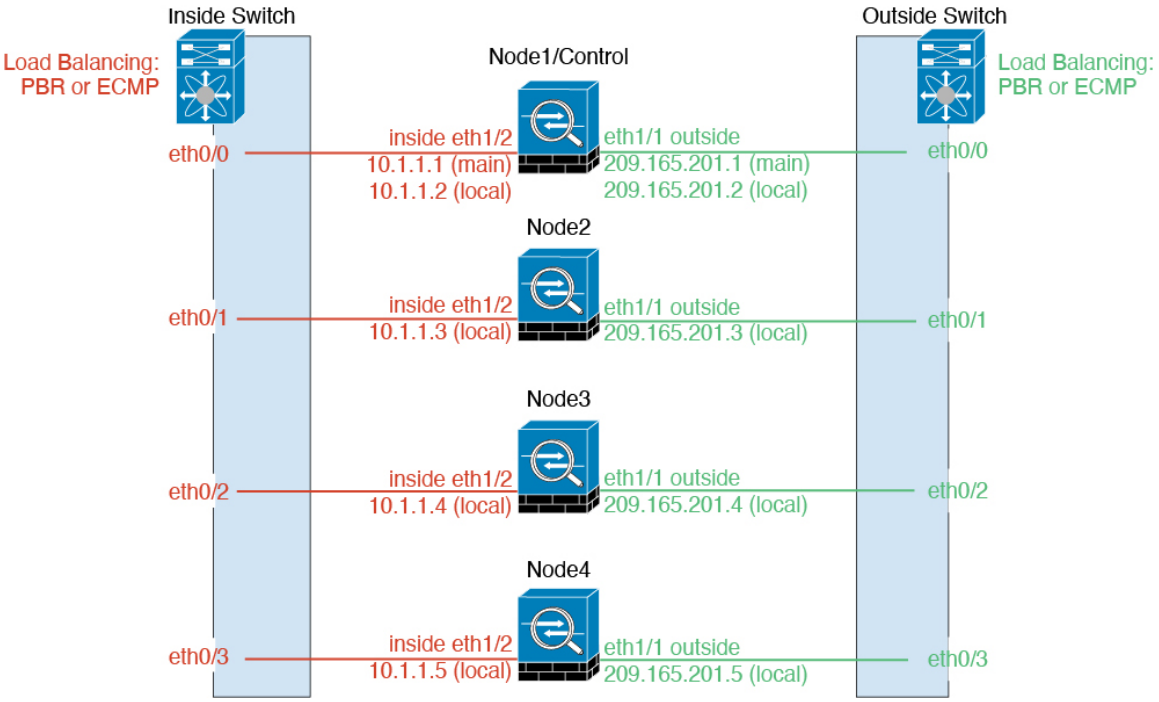
独立接口（仅适用于路由防火墙模式）

独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群IP地址将转移到新的控制节点，使集群的管理得以无缝继续。

不支持仅 IPS 接口（内联集和无源接口）作为独立接口。

由于接口配置只能在控制节点上配置，因此您可以通过接口配置设置一个IP地址池，供集群节点上的给定接口（包括控制节点上的一个接口）使用。

必须在上游交换机上分别配置负载均衡。



策略型路由

使用独立接口时，每个 Firewall 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。策略型路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，我们建议使用此方法。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 Firewall 威胁防御 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。为了获得最佳性能，建议您配置 PBR 策略，以便连接的转发数据包和返回数据包定向到同一个 Firewall 威胁防御。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 Firewall 威胁防御。然后，PBR 可根据特定 Firewall 威胁防御 的可访问性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

同等成本的多路径路由

使用独立接口时，每个 Firewall 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，我们建议使用此方法。

ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 Firewall 威胁防御 故障会导致问题；如果继续使用该路由，发往故障 Firewall 威胁防御 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟

踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 Firewall 威胁防御 使之加入动态路由。

思科智能流量导向器（仅路由防火墙模式）

使用独立接口时，每个 Firewall 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。智能流量导向器 (ITD) 是适用于 Nexus 5000、6000、7000 和 9000 交换机系列的高速硬件负载均衡解决方案。除了完全恢复传统 PBR 的功能以外，它还可以提供简化配置工作流和多种附加功能，以实现更精细的负载分布。

ITD 支持 IP 粘性、面向双向流对称的一致散列处理、虚拟 IP 寻址、运行状态监控、具有 N+M 冗余的复杂故障处理策略、加权负载均衡，以及应用 IP SLA 探测（包括 DNS）。由于负载均衡的动态性质，它可在所有集群节点上实现比 PBR 更均匀的流量分布。为了实现双向流对称，我们建议配置 ITD，以便将连接的数据包转发和返回定向到同一 Firewall 威胁防御。有关详细信息，请参阅以下 URL：

https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd_deployment/ITD_ASA_Deployment_Guide.pdf

连接电缆并将设备添加到防火墙管理中心

在配置集群之前，您需要准备设备。特别是，除非所有节点都可以通过集群控制链路进行通信，否则集群将无法启动。因此，在形成集群之前，集群控制链路必须准备就绪。

过程

步骤 1 使用电缆连接集群控制链路网络、管理网络和数据网络。

步骤 2 配置上游和下游设备。

a) 对于集群控制链路网络，设置 MTU 为比数据接口 MTU 至少高 100 字节。

默认情况下，数据接口 MTU 为 1500 字节，集群节点上的集群控制链路 MTU 会被设置为 1600 字节。如果在数据接口上使用更高的 MTU，请相应地增加连接交换机上的集群控制链路 MTU。

b) 在上游和下游设备上配置集群控制链路接口，包括可选的 EtherChannel。

有关集群控制链路的要求，请参阅集群控制链路接口和网络，第 381 页。

c) 如果选择该集群接口模式，则在上游和下游设备（包括跨区以太网通道）上配置数据接口。

有关如何连接跨区以太网通道的信息，请参阅关于集群接口，第 380 页。

步骤 3 将每个节点作为同一域和组中的独立设备添加到 防火墙管理中心。

请参阅使用注册密钥添加设备 - 基本配置，第 33 页。您可以创建包含单个设备的集群，然后稍后添加更多节点。您在添加设备时设置的初始设置（许可、访问控制策略）将被控制节点的所有集群节点继承。您将在形成集群时选择控制节点。

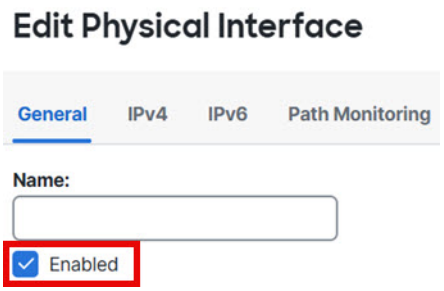
步骤 4 在要作为控制节点的设备上启用集群控制链路。

当您添加其他节点时，它们将继承集群控制链路配置。

注释
请不要为集群控制链路配置名称或 IP 地址。在形成集群时，集群控制链路接口的 MTU 会被自动设置为比最高数据接口 MTU 多 100 个字节，所以现在不需要设置。但是，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。如果在添加集群时 MTU 设置在此范围内，我们建议返回到 **接口** 页面并手动将其增加到 8362 以上。当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。

a) 在要作为控制节点的设备上，选择 **设备** > **设备管理**，然后点击 **编辑** ()。
b) 点击**接口 (Interfaces)**。
c) 启用接口。如果要将 EtherChannel 用于集群控制链路，请启用所有成员。请参阅启用物理接口并配置以太网参数，第 716 页。

图 *130:* 启用集群控制链路接口



d) （可选） 添加 EtherChannel.请参阅配置 EtherChannel，第 724 页。

我们建议对集群控制链路成员接口使用 ON 模式来减少集群控制链路上不必要的流量（默认为主动模式）。由于集群控制链路是单独、稳定的网络，因此无需 LACP 流量开销。**注意：** 我们建议将数据 EtherChannel 设置为 Active 模式。

e) 点击 **保存**，然后点击 **部署**，将接口更改部署到控制节点。

创建集群

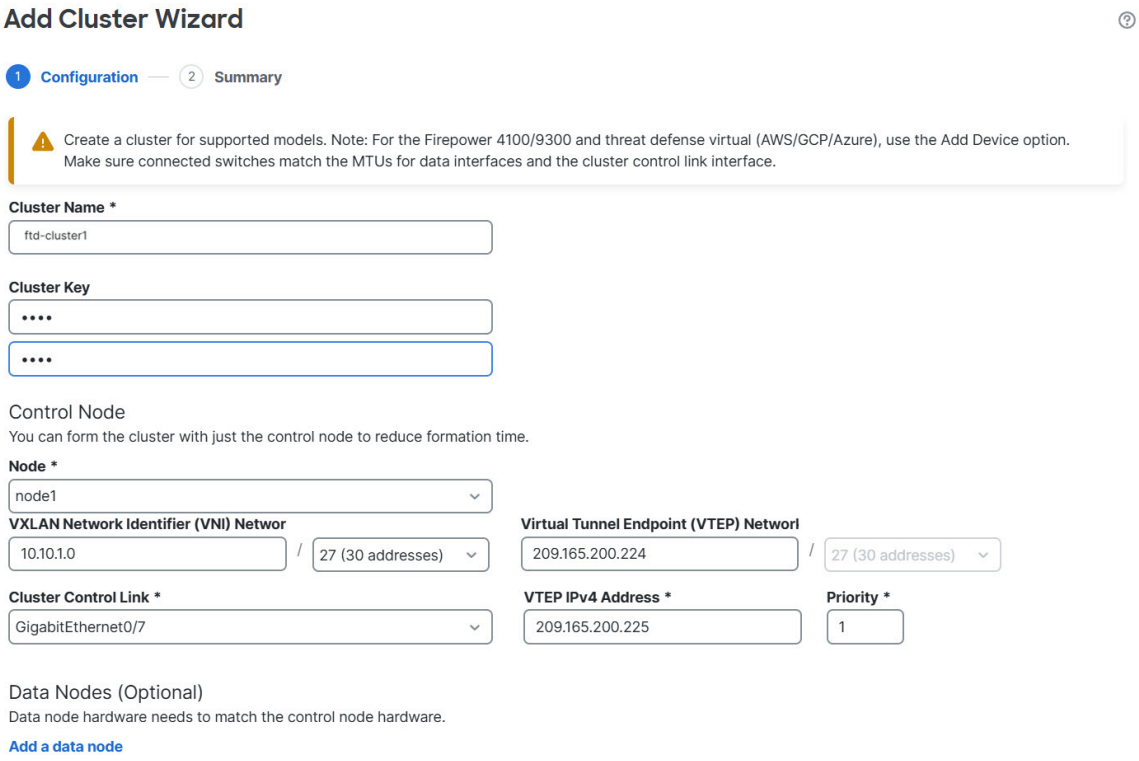
从 防火墙管理中心 中的一个或多个设备组成集群。

过程

步骤 1 选择 **设备** > **设备管理**，然后选择**添加** > **集群**。

出现**添加集群向导 (Add Cluster Wizard)**。

图 *131:* 添加集群向导



步骤 2 为控制流量指定**集群名称 (Cluster Name)** 和身份验证**集群密钥 (Cluster Key)**。

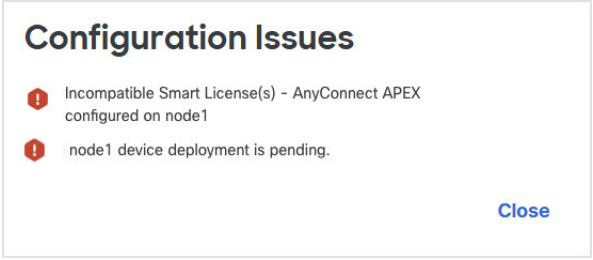
- **集群名称 (Cluster Name)** - 1 到 38 个字符的 ASCII 字符串。
- **集群密钥 (Cluster Key)** - 1 到 63 个字符的 ASCII 字符串。 **集群密钥 (Cluster Key)** 值用于生成加密密钥。此加密不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 3 对于**控制节点**，请进行以下设置：

- **节点 (Node)** - 选择一开始要作为控制节点的设备。当 防火墙管理中心 形成集群时，它会首先将此节点添加到集群，因此它将成为控制节点。

  注释
  如果您在节点名称旁边看到一个 **错误** ( ) 图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。例如：

图 *132:* 配置问题



要解决上述问题，请删除不支持的 VPN 许可证，并将待处理的配置更改部署到设备。

- **集群控制链路网络 (Cluster Control Link Network)** - 指定 IPv4 子网；此接口不支持 IPv6。指定 **24**、**25**、**26** 或 **27** 子网。
- **集群控制链路 (Cluster Control Link)** - 选择要用于集群控制链路的物理接口或 EtherChannel。

  注释
  集群控制链路接口的 MTU 会被自动设置为比最高数据接口 MTU 多 100 个字节；默认情况下，MTU 为 1600 字节。我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。如果在添加集群时 MTU 设置在此范围内，我们建议将 MTU 增加到 8362 以上。选择 **设备** > **设备管理**，然后点击**接口**。

  确保将连接到集群控制链路的交换机配置为正确（更高）的 MTU；否则，建立集群会失败。

- **集群控制链路地址 (Cluster Control Link IPv4 Address)** - 此字段将自动填充集群控制链路网络上的第一个地址。如果需要，您可以编辑主机地址。
- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。即使您将优先级设置为低于其他节点，在首次建立集群时，此节点仍将作为控制节点。
- **站点 ID (Site ID)** -（FlexConfig 功能）输入此节点的站点 ID，范围介于 1 和 8 之间。值 0 表示禁用站点间集群。仅可通过使用 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。

步骤 4 对于 **集群模式**，请选择 **跨区以太网通道模式** 或 **独立接口模式**。

步骤 5 对于**数据节点（可选）**，点击**添加数据节点 (Add a data node)** 以便将节点添加到集群。

您可以仅使用控制节点建立集群，以便加快集群建立的速度，也可以立即添加所有节点。为每个数据节点设置以下内容：

- **节点 (Node)** - 选择要添加的设备。

  注释
  如果您在节点名称旁边看到一个 **错误** ( ) 图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。

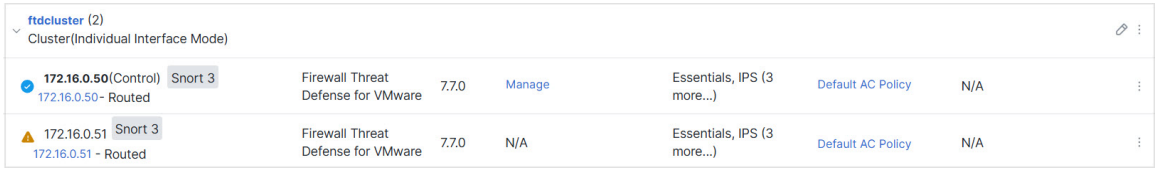
- **集群控制链路地址 (Cluster Control Link IPv4 Address)** - 此字段将自动填充集群控制链路网络上的下一个地址。如果需要，您可以编辑主机地址。

- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。
- **站点 ID (Site ID)** -（FlexConfig 功能）输入此节点的站点 ID，范围介于 1 和 8 之间。值 0 表示禁用站点间集群。仅可通过使用 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。

步骤 6 点击**继续**。查看**摘要**，然后点击**保存**。

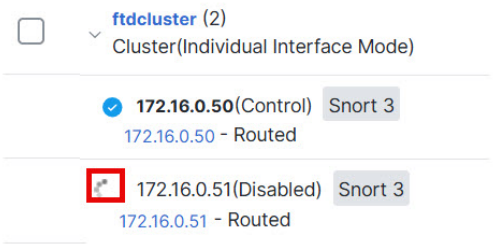
集群名称显示在 **设备** > **设备管理** 页面上；展开集群可查看集群节点。

图 *133:* 集群管理

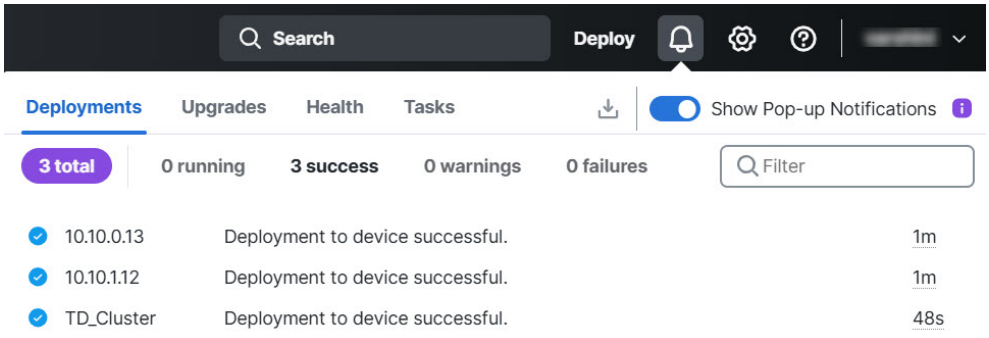


当前正在注册的节点会显示加载图标。

图 *134:* 节点注册



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。防火墙管理中心 会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

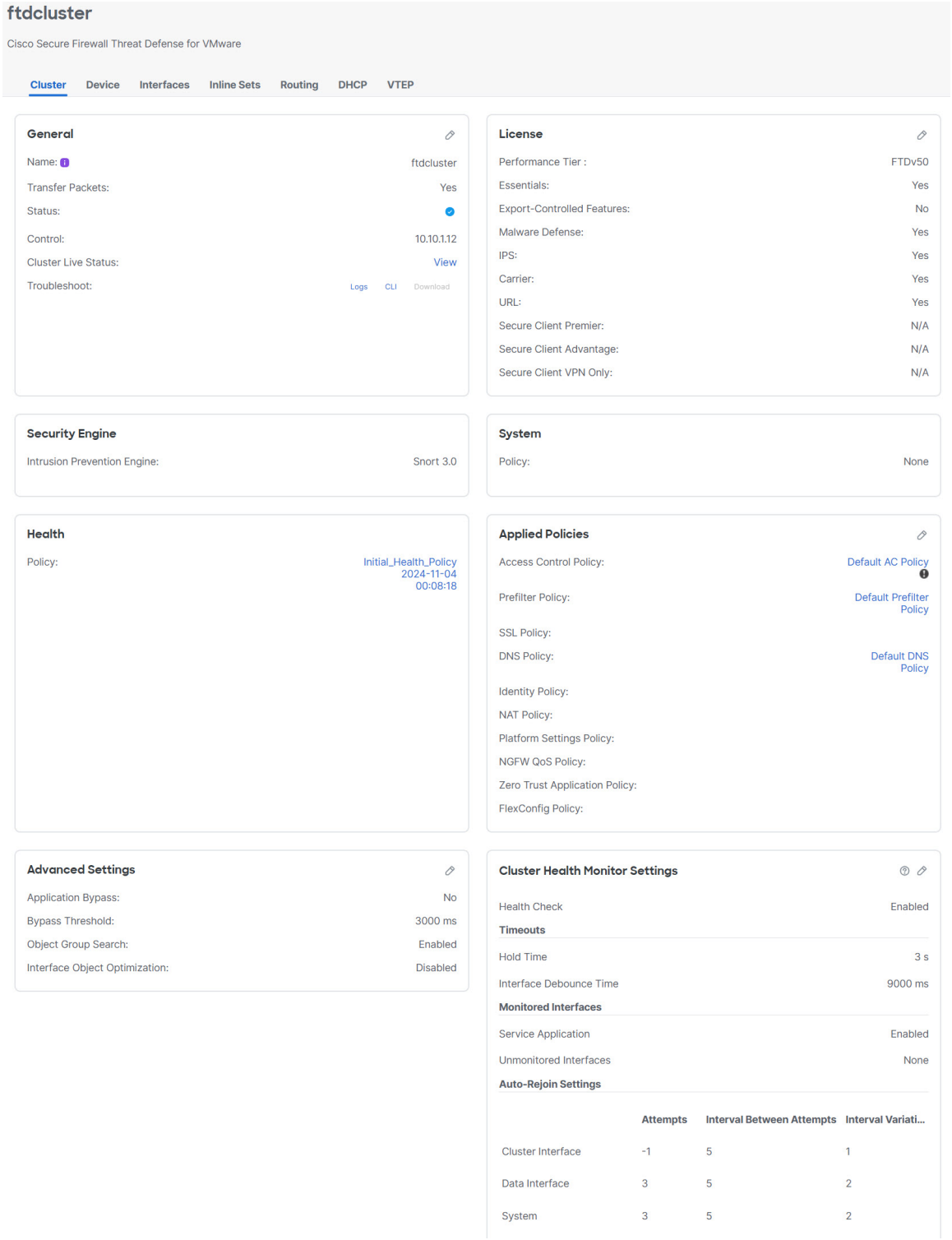


步骤 7 通过点击集群的 **编辑** ()，配置设备特定设置。

大多数配置可以应用于整个集群，而不适用于集群中的节点。例如，可以更改每个节点的显示名称，但只能配置整个集群的接口。

步骤 8 在 **设备** > **设备管理** 上选择**添加**、**集群**屏幕，您可以查看集群的**常规**和其他设置。

图 *135:* 集群设置

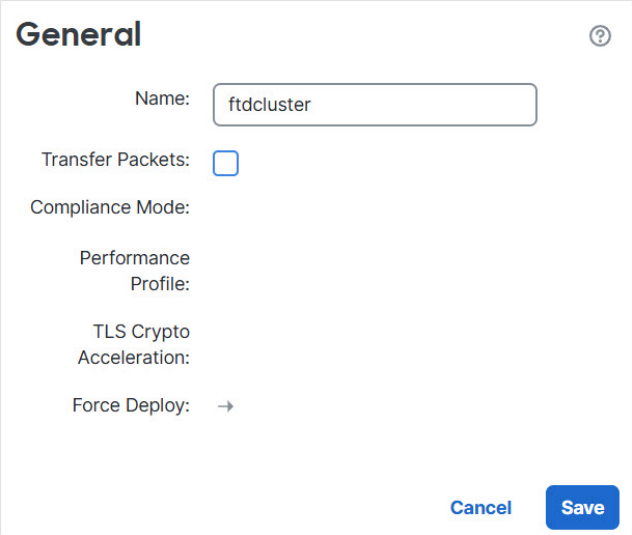


请参阅常规 **(General)** 区域中的以下集群特定项：

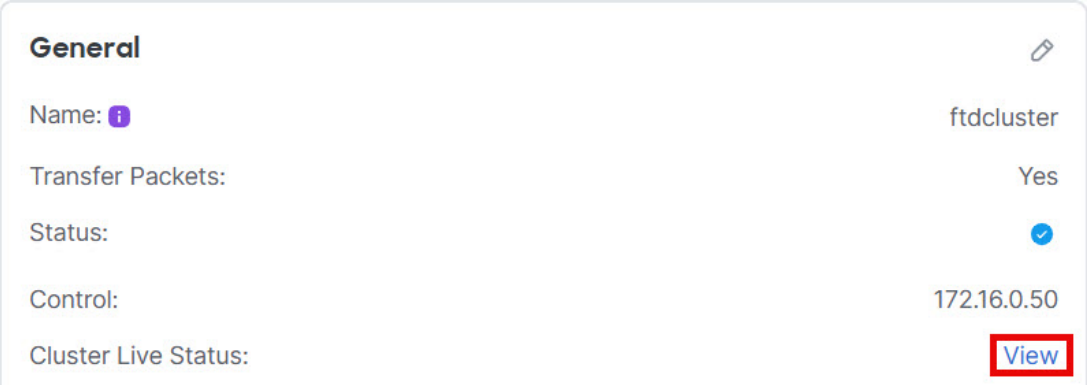
- **常规 (General) > 名称 (Name)** - 通过点击 **编辑** (✎)更改集群显示名称。



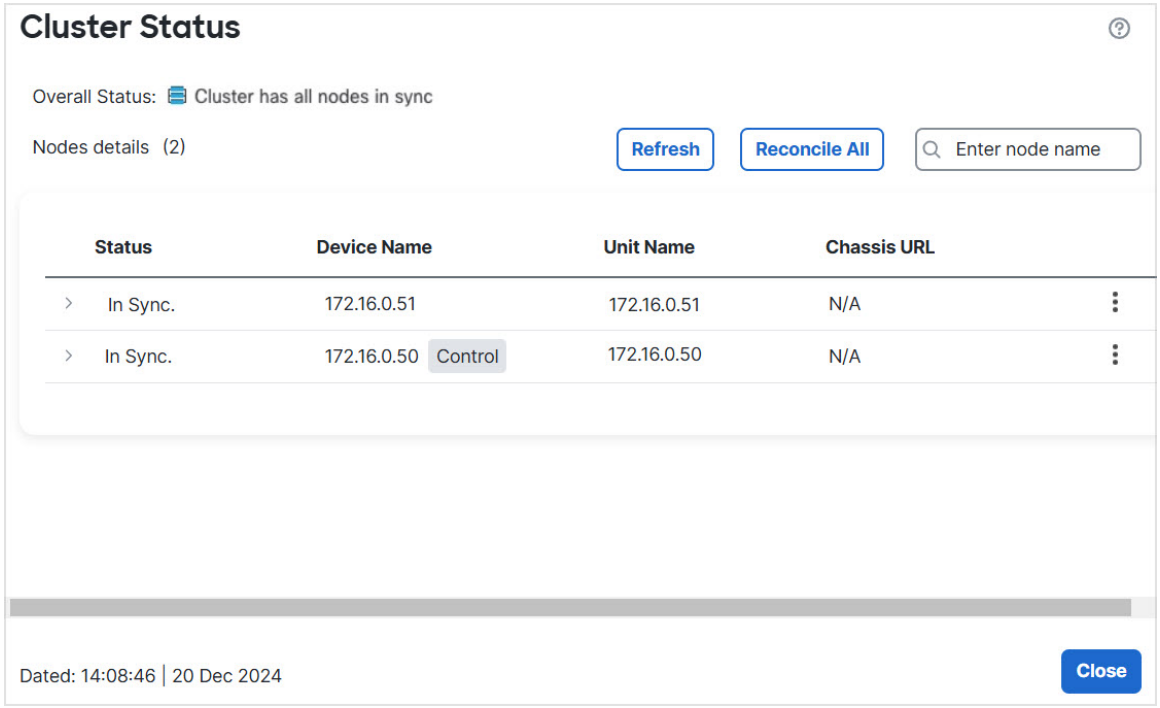
然后设置 **名称** 字段。



- **常规 (General) > 查看集群状态 (View cluster status)** - 点击 **查看 (View)** 链接来打开 **集群状态 (Cluster Status)** 对话框。

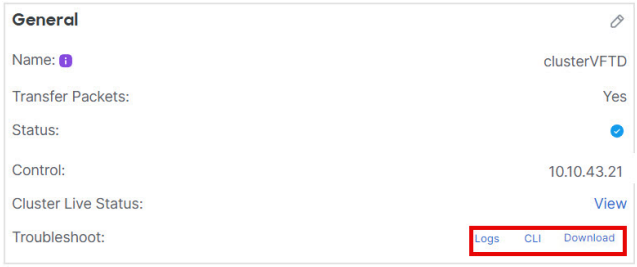


还可在**集群状态 (Cluster Status)** 对话框中点击**协调全部 (Reconcile All)**以重新注册数据单元。您还可以从节点 ping 通集群控制链路。请参阅在集群控制链路上执行 Ping，第 426 页。



- **常规 > 故障排除**- 可以生成和下载故障排除日志，还可以查看集群 CLI。请参阅对集群进行故障排除，第 425 页。

图 *136:* 故障排除



步骤 9 在 **设备 > 设备管理** 上选择**添加**、**设备**，您可从右上方的下拉菜单中选择集群中的每个成员并配置以下设置。

图 *137:* 设备设置

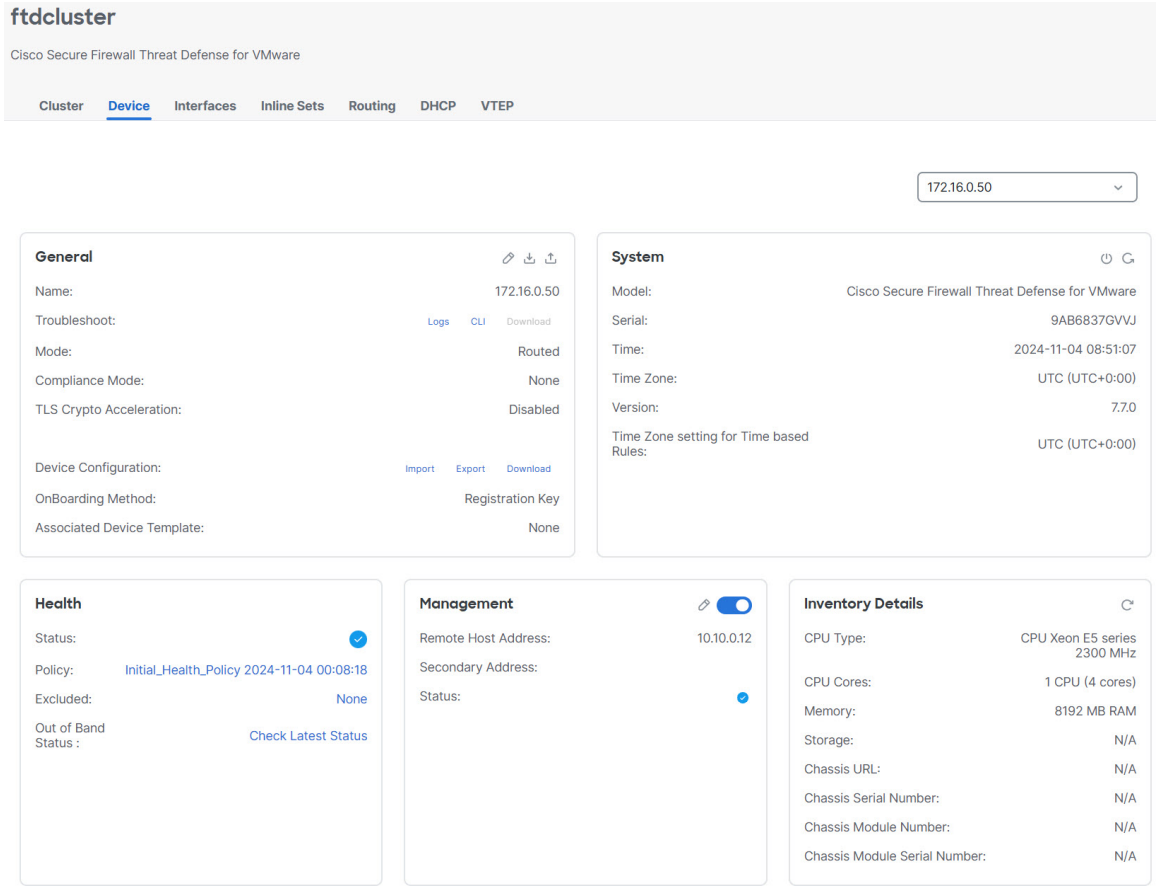
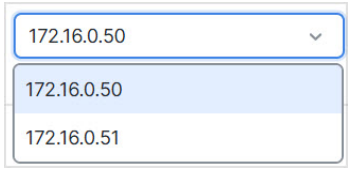
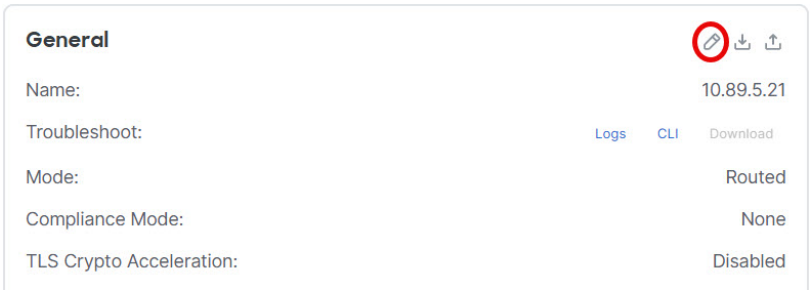


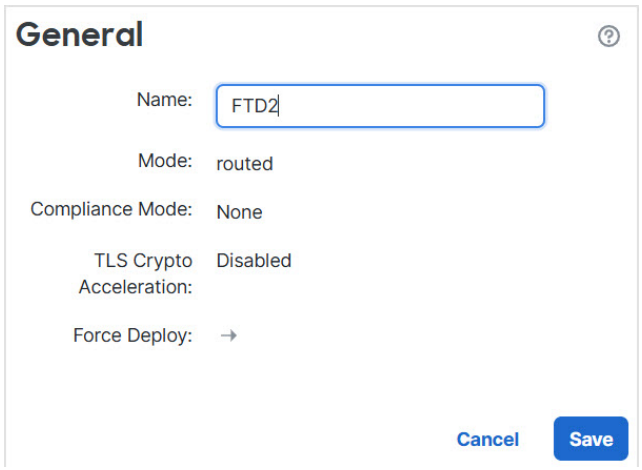
图 *138:* 选择节点



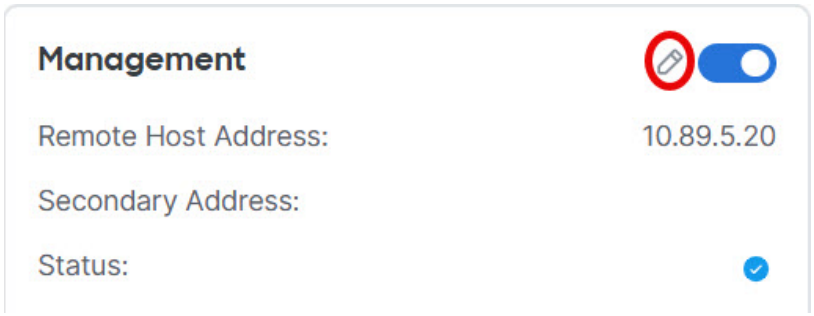
- **常规 (General) > 名称 (Name)** - 通过点击 **编辑** (✎)更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理 (Management) > 主机 (Host)**-如果在设备配置中更改了管理 IP 地址，则必须在 防火墙管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备。首先禁用连接，编辑**管理 (Management)** 区域中的**主机 (Host)** 地址，然后重新启用连接。



配置接口

您可以将数据接口配置为跨区以太网通道或独立接口。每种方法使用的负载均衡机制不同。不能在同一配置中同时配置这两种类型。

配置跨区以太网通道

将数据接口配置为跨区以太网通道。

过程

步骤 1 选择 **设备** > **设备管理**，然后点击集群的 **编辑** (✎)。

步骤 2 点击**接口 (Interfaces)**。

步骤 3 配置跨区以太网通道数据接口。

a) 配置一个或多个 EtherChannel。请参阅配置 EtherChannel，第 724 页。

您可以在 EtherChannel 中包含一个或多个成员接口。由于此 EtherChannel 跨越了所有节点，因此每个节点只需要一个成员接口；但是，为了获得更高的吞吐量和冗余，建议使用多个成员。

b) （可选）对于常规防火墙接口，请在 EtherChannel 上配置 VLAN 子接口。本程序的其余部分适用于子接口。请参阅添加子接口，第 772 页。

c) 点击 EtherChannel 接口的 **编辑** ()。

d) 配置名称和其他参数。对于常规防火墙接口，请参阅配置路由模式接口，第 792 页；对于透明模式，请参阅配置网桥组接口，第 797 页。对于仅 IPS 接口，请参阅内联集和被动接口，第 833 页。

- 如果集群控制链路接口 MTU 不比数据接口 MTU 高出至少 100 个字节，您将看到必须降低数据接口 MTU 的错误。 默认情况下，集群控制链路 MTU 为 1600 字节。如果要增大数据接口的 MTU，请先增大集群控制链路 MTU。请注意，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于路由模式，不支持 DHCP、PPPoE、IPv6 自动配置和手动链路本地地址。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在这种情况下，不会为网络或广播地址预留 IP 地址。

e) 为 EtherChannel 设置唯一的手动全局 MAC 地址。点击 **高级**， 在 **主用 Mac 地址** 字段，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

请勿设置 **备用 Mac 地址**；它会被忽略。

您必须为跨 EtherChannel 配置网络中当前未使用的唯一 MAC 地址，以避免潜在的网络连接问题。如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的 MAC 地址用于该接口，而这可能导致临时网络故障。

f) 点击**确定**。对其他数据接口重复上述步骤。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置独立接口

独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于控制节点。

独立接口可以根据需要直接 SSH 到每台设备，而跨区以太网通道接口则只允许连接到控制节点。

单个接口不支持仅 IPS 接口（内联集或无源接口）。

开始之前

- 必须为独立接口模式。
- 独立接口要求在邻居设备上配置负载均衡。管理接口不需要外部负载均衡。
- （可选）将接口配置为设备本地 EtherChannel 和/或配置子接口。

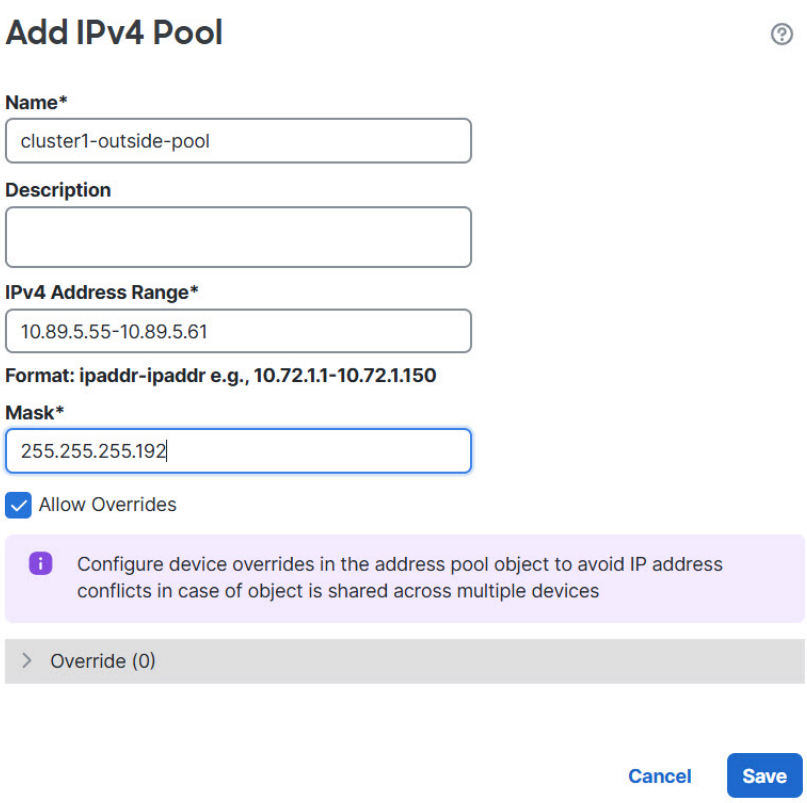
  如果配置为 EtherChannel，则此 EtherChannel 是设备本地的，而非跨区以太网通道。

过程

步骤 1 选择 **对象** > **地址池** 以添加 IPv4 和/或 IPv6 地址池。请参阅地址池，第 2630 页。

至少包含与集群中的设备数量相同的地址。主要 IP 地址不属于此池，但需要位于同一网络中。无法提前确定分配到每台设备的确切本地地址。

图 *139:* 添加地址池



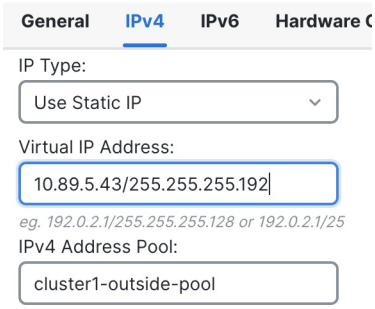
注释
虽然不常见，但如果要手动设置 MAC 地址，还可以添加 MAC 地址池对象。

步骤 2 在 **设备** > **设备管理** 上，选择**接口**，点击您想要配置的接口的 **编辑** ()。

步骤 3 在 **IPv4** 页面上，输入**虚拟 IP 地址** 和掩码。此主要（虚拟）IP 地址是集群的固定地址，始终属于控制节点。

不支持 DHCP 和 PPPoE。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在这种情况下，不会为网络或广播地址预留 IP 地址。

图 *140: IPv4* 页面



步骤 4 从 **IPv4 地址池**下拉列表中，选择您创建的地址池。

步骤 5 在 **IPv6 > 基本**， **IPv6 地址池** 下拉列表中，选择您创建的地址池。

不支持 IPv6 自动配置和手动链路本地地址。

步骤 6 按正常方式配置其他接口设置。

要手动设置 MAC 地址，可以从接口的 **高级** 页面选择 MAC 地址池。

注释
如果集群控制链路接口 MTU 不比数据接口 MTU 高出至少 100 个字节，您将看到必须降低数据接口 MTU 的错误。默认情况下，集群控制链路 MTU 为 1600 字节。如果要增大数据接口的 MTU，请先增大集群控制链路 MTU。请注意，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。

配置集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *141:* 集群运行状况监控设置

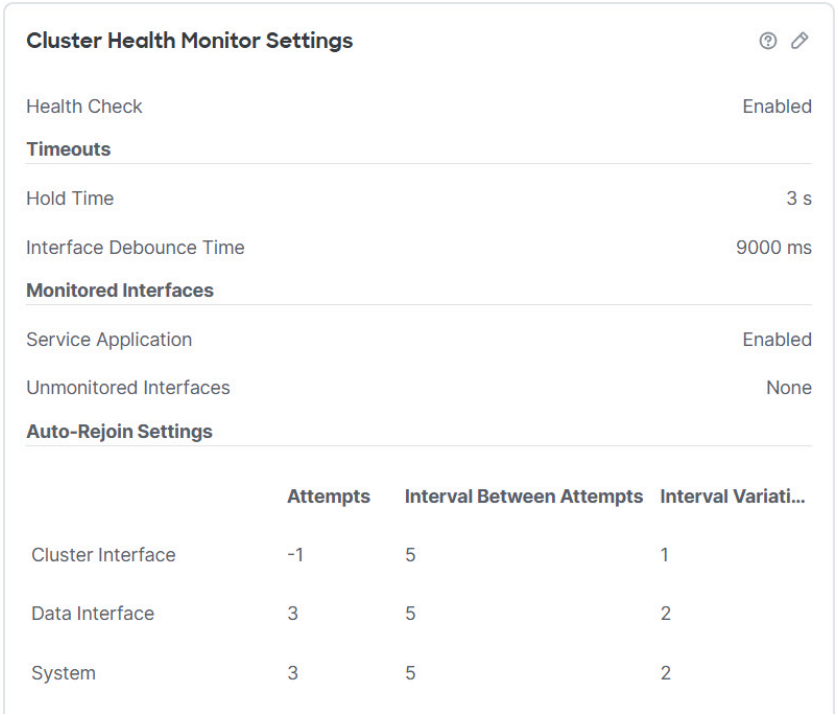


表 *29:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。

字段	说明
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。



注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

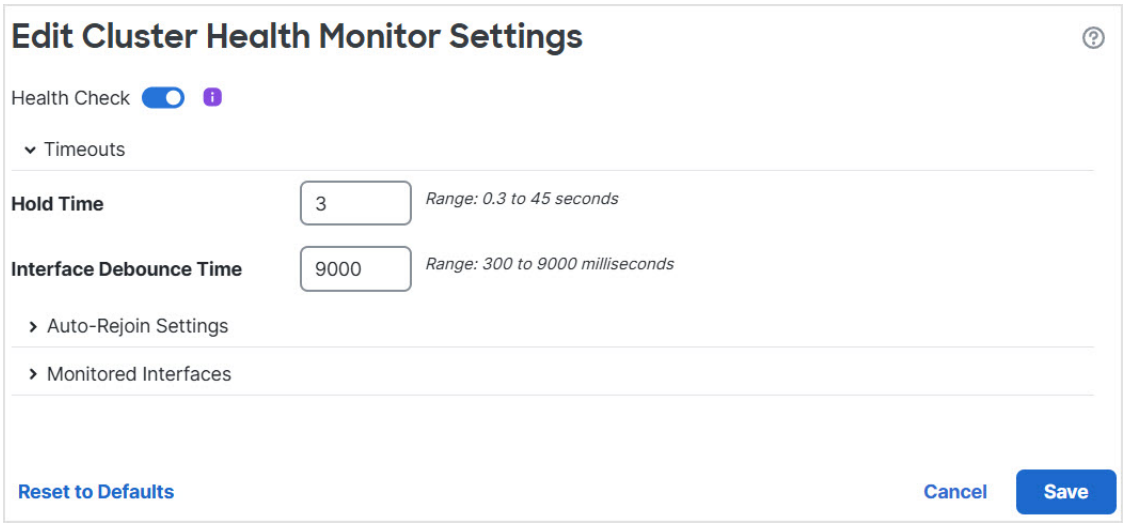
步骤 2 在要修改的集群旁边，点击 **编辑** (✎)。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *142:* 禁用系统运行状况检查



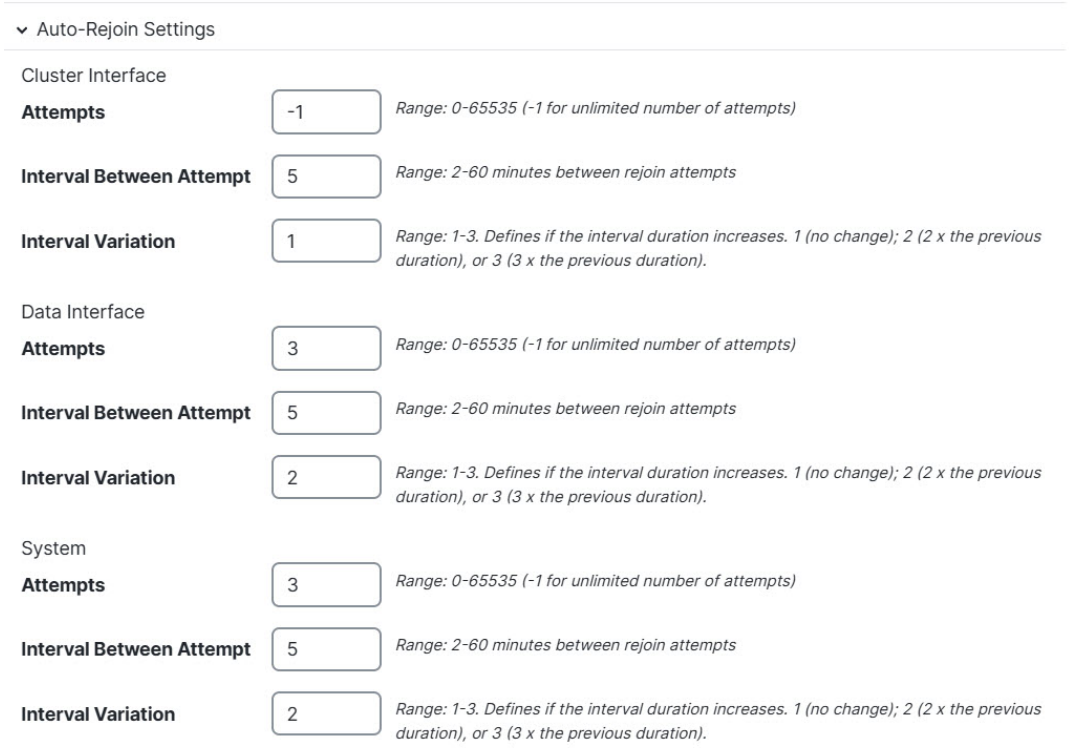
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *143:* 配置自动重新加入设置

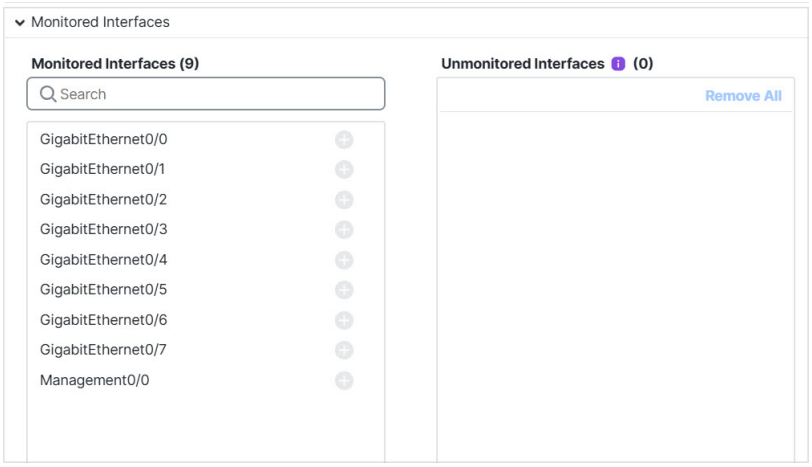


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *144:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改，第 180 页。

配置分布式站点间 VPN

默认情况下，集群使用集中式站点间VPN模式。要利用集群的可扩展性，您可以启用分布式站点间 VPN 模式。

关于分布式站点间 VPN

在分布式模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群节点分发。在集群节点之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

分布式 VPN 连接角色

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。在分布式 VPN 模式下运行时，系统将为集群节点分配以下角色：

- 主用会话所有者 - 最初接收连接的节点，或将备份会话转换为主用会话的设备。所有者为完整的会话维护状态并处理数据包，包括 IKE 和 IPsec 隧道以及所有与之关联的流量。
- 备份会话所有者 - 正在处理现有主用会话的备份会话的节点。如果主用会话所有者发生故障，备份会话所有者将成为主用会话所有者，并在另一个节点上建立新的备份会话。
- 转发器 - 如果与某个 VPN 会话关联的流量被发送至一个未拥有该 VPN 会话的节点，该节点将使用集群控制链路 (CCL) 将流量转发到拥有该 VPN 会话的节点。
- 协调器 - 协调器（始终是集群的控制节点）负责计算将移动哪些会话，在哪里以及何时执行主用会话重新分发 (ASR)。它会向所有者节点 X 发送将 N 个会话移至节点 Y 的请求。成员 X 将在完成操作时向协调器发送回应，指定它已成功移动的会话数量。

分布式 VPN 会话的特征

分布式站点间 VPN 会话具有以下特征。否则，VPN 连接的行为与不在集群上时的行为相同。

- VPN 会话将在会话级别跨集群分布。这意味着同一集群节点将会处理 VPN 连接的 IKE 和 IPsec 隧道及其所有流量。如果 VPN 会话流量被发送至未拥有该 VPN 会话的集群节点，此流量将被转发至拥有该 VPN 会话的集群节点。
- VPN 会话拥有在整个集群内唯一存在的会话 ID。此会话 ID 将用于验证流量，做出转发决策和完成 IKE 协商。
- 在站点间VPN集线器和辐射配置中，当客户端通过集群连接（称为发夹）时，流入的会话流量和流出的会话流量可能在不同的集群节点上。

集群事件的分布式 VPN 处理

事件	分布式 VPN
节点故障	此故障节点上所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并将备份会话重新分配到另一个节点上。
停用集群节点	正在停用的集群节点上的所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并根据备份策略将备份会话重新分配到另一个节点上。
集群节点加入	如果新节点上的VPN集群模式未设置为分布式，则控制节点将请求更改模式。 在与 VPN 模式兼容后，集群节点将被分配正常操作流中的主用和备份会话。

IPsec IKEv2 修改

在分布式站点间 VPN 模式下，IKEv2 进行了以下方面的修改：

- 使用身份取代了 IP/端口元组。这将允许对数据包做出正确的转发决策，以及清理可能位于其他集群成员上的先前连接。
- 标识单个 IKEv2 会话的 (SPI) 标识符是在本地生成的 8 字节随机值，并且在整个集群中是唯一的。SPI 嵌入了时间戳和集群节点 ID。在收到 IKE 协商数据包时，如果时间戳或集群节点 ID 检查失败，则会丢弃数据包并记录一条指示原因的消息。

- IKEv2 处理已修改为通过划分集群成员来预防 NAT-T 协商失败。在接口上启用 IKEv2 后，将添加新的 ASP 分类域 *cluster_isakmp_redirect* 和规则。

CMPv2

系统将跨所有集群节点同步 CMPv2 ID 证书和密钥对。但只有集群中的控制节点会自动续约 CMPv2 证书并重新生成密钥。控制节点会在续约时将这些新的ID证书和密钥同步至所有集群节点。通过这种方式，集群中的所有节点都能使用CMPv2证书进行身份验证，而且任何节点都能接管成为控制节点。

分布式站点间 VPN 的许可

每个集群成员上都需要分布式站点间 VPN 的运营商许可证。

分布式站点间 VPN 的前提条件

型号支持

- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

集群要求

- 跨区以太网通道模式。
- 路由防火墙模式。

最高 VPN 会话数

每个VPN连接需要两个会话，一个用于活动会话，一个用于备份会话。由于每个会话使用两个许可证，集群的最大 VPN 会话容量不能超过列出容量的一半。

表 *30:* 最高 *VPN* 会话数

型号	最高 VPN 会话数
4215	10,000
4225	12500
4245	15,000
6160	280,000
6170	350,000

分布式站点间 VPN 准则

防火墙模式

仅在路由模式下支持分布式站点间 VPN。

其他准则

- 在分布式站点间 VPN 模式下仅支持 IKEv2 IPsec 站点间 VPN。不支持 IKEv1。在集中式 VPN 模式下支持站点间 IKEv1。
- 不支持站点间集群。
- 接口 PAT 在分布式站点间 VPN 模式下不可用。
- 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略，第 1041 页。

启用分布式站点间 VPN

启用分布式站点间 VPN，以充分利用 VPN 会话集群的可扩展性优势。此过程需要对控制节点的 CLI 访问权限。

开始之前

- 按照 站点间 VPN，第 1443 页 配置站点间 VPN。
- 将运营商许可证应用到控制节点。

过程

步骤 1 按照 创建集群，第 388 页 添加 Spanned-EtherChannel-mode 集群，包括所有数据节点。

步骤 2 集群形成并稳定后，按照 禁用集群，第 414 页 移除每个数据节点，然后移除控制节点。

需要禁用集群才能更改 VPN 模式。引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。

步骤 3 连接到控制节点 CLI。请参阅《*Cisco Secure Firewall Management Center* 设备配置指南》中的“登录设备上的命令行界面”部分。

查看 **设备** > **设备管理** 上的集群，确定哪个设备是控制节点。

步骤 4 在每个节点上，在控制节点上启用分布式站点间 VPN。

cluster vpn-mode distributed

要禁用分布式站点间 VPN，请使用 **cluster vpn-mode centralized** 命令。

示例：

```
> cluster vpn-mode distributed
Cryptochecksum: ce4b0bbd 6b9252a5 7e19463d e179067d

5778 bytes copied in 0.70 secs
>
```

步骤 5 在防火墙管理中心中，在控制节点上重新启用集群，然后为每个数据节点重新启用集群。请参阅重新加入集群，第 414 页。

VPN 模式会同步到数据节点。

重新分发分布式站点间 VPN 会话

主用会话重新分发 (ASR) 将在所有集群成员之间重新分发主用 VPN 会话负载。由于开始会话和结束会话的动态性质，ASR 是跨所有集群成员均衡会话的最佳做法。重复进行重新分发操作将会优化均衡。

重新分发可以在任何时间运行，应该在集群中发生任何拓扑更改后运行，并且建议在新成员加入集群后运行。重新分发的目标是创建稳定的 VPN 集群。稳定的 VPN 集群的节点之间具有几乎相等数量的主用和备份会话。

要移动某个会话，备份会话将变为主用会话，并选择另一个节点托管新的备份会话。移动会话依赖于主用会话的备份位置和该特定备份节点上已有的主用会话数量。如果备份会话节点由于某种原因不能托管主用会话，则原始节点继续作为该会话的所有者。

此过程需要对控制节点的 CLI 访问权限。

开始之前

- 如果您想要监控重新分发活动，请启用系统日志。

过程

步骤 1 连接到控制节点 CLI。请参阅《*Cisco Secure Firewall Management Center* 设备配置指南》中的“登录设备上的命令行界面”部分。

查看 **设备** > **设备管理** 上的集群，确定哪个设备是控制节点。

步骤 2 查看活动会话和备份会话在集群中的分布情况。

show cluster vpn-sessiondb distribution

示例：

系统将显示如下分布信息：

```
> show cluster vpn-sessiondb distribution
```

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

每行包含成员 ID、成员名称、主用会话数以及备份会话驻留在哪些成员上。对于以上示例，用户可以读出以下信息：

- 成员 0 上具有 209 个主用会话，成员 1 上备份了 111 个会话，成员 2 上备份了 98 个会话
- 成员 1 上具有 204 个主用会话，成员 0 上备份了 108 个会话，成员 2 上备份了 96 个会话
- 成员 2 没有任何主用会话；因此，没有集群成员正在备份此节点的会话。此成员最近才加入集群。

步骤 3 重新分发会话。

cluster redistribute vpn-sessiondb

示例：

```
> cluster redistribute vpn-sessiondb

Session redistribution initiated.
Use 'show cluster vpn-sessiondb distribution' to view distribution.

>
```

根据需要重新分发的会话数和集群上的负载，这可能需要一些时间。重新分发活动发生时，系统会提供包含以下短语的系统日志（此处未显示其他系统详细信息）：

系统日志短语	说明
已启动 VPN 会话重新分发	仅控制节点
已发送请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅控制节点
未能将会话重新分发消息发送至 *member-name*	仅控制节点
已收到请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅数据节点
已将 *number* 个会话移到 *member-name*	已移至指定集群的活动会话数。
未能收到 *dest-member-name* 的会话移动响应	仅控制节点
已完成 VPN 会话	仅控制节点
检测到集群拓扑更改。已终止 VPN 会话重新分发。	

步骤 4 重新输入 **show cluster vpn-sessiondb distribution** 命令以查看结果。

管理集群节点

部署集群后，您可以更改配置和管理集群节点。

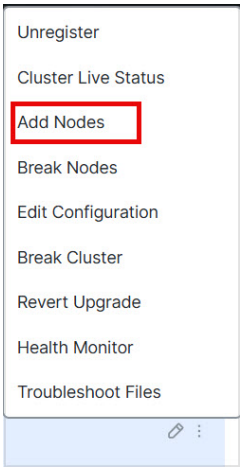
添加新的集群节点

您可以将一个或多个新的集群节点添加到现有的集群。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**添加节点**。

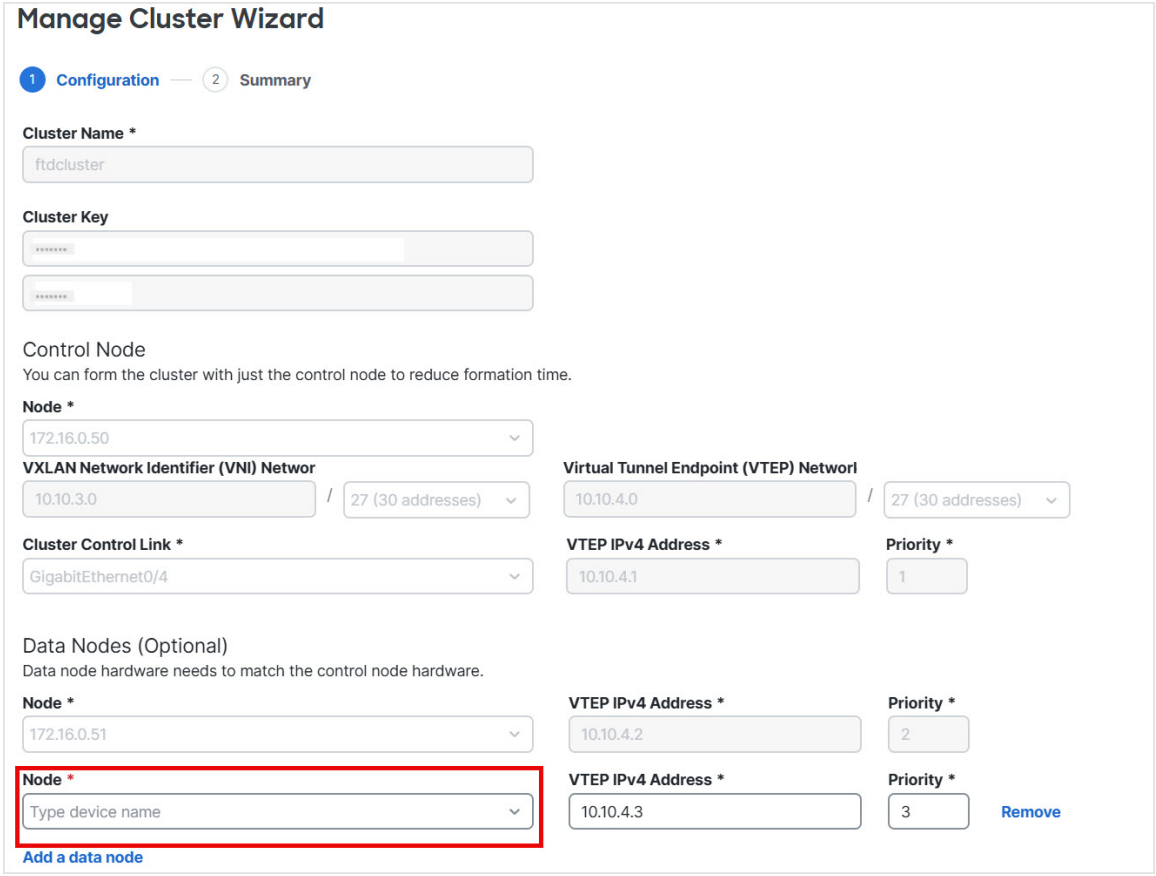
图 *145:* 添加节点



系统将显示**管理集群向导 (Manage Cluster Wizard)**。

步骤 2 从**节点 (Node)** 菜单中选择设备，根据需要调整 IP 地址、优先级和站点 ID。

图 *146:* 管理集群向导

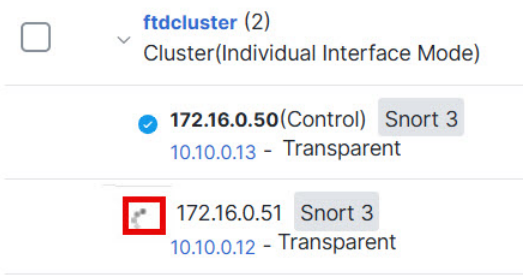


步骤 3 要添加其他节点，请点击**添加数据节点 (Add a data node)**。

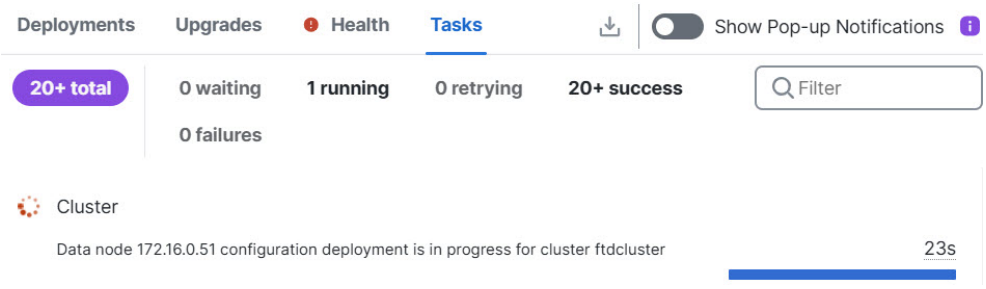
步骤 4 点击**继续**。查看**摘要**，然后点击**保存**

当前正在注册的节点会显示加载图标。

图 *147:* 节点注册



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。



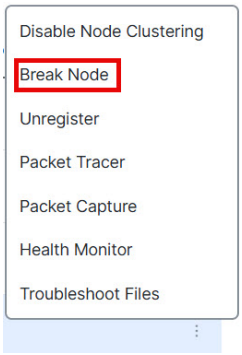
中断节点

您可以从集群中删除节点，使其成为一个独立设备。除非中断整个集群，否则您无法中断控制节点。数据节点的配置已被清除。

过程

步骤 1 选择 **设备** > **设备管理**，点击要中断的节点的 **更多** (⋮)，然后选择**中断节点**。

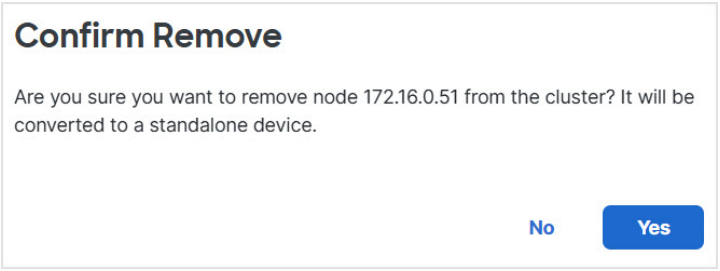
图 ***148:*** 中断节点



您可以选择通过选择**中断节点 (Break Nodes)** 从集群的“更多”(More) 菜单中断一个或多个节点。

步骤 2 系统会提示您确认中断；点击**是**。

图 ***149:*** 确认中断



您可以通过点击**通知 (Notifications)** 图标并选择**任务 (Tasks)** 来监控集群节点中断。

中断集群

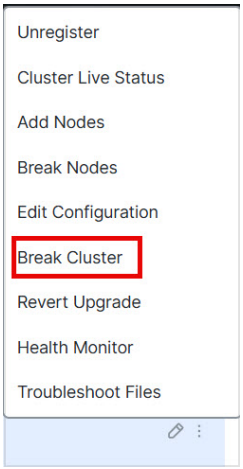
您可以中断集群并将所有节点都转换为独立设备。控制节点会保留接口和安全策略配置，而数据节点则会清除其配置。

过程

步骤 1 确保所有集群节点都由 防火墙管理中心 通过协调节点来管理。请参阅调整集群节点，第 417 页。

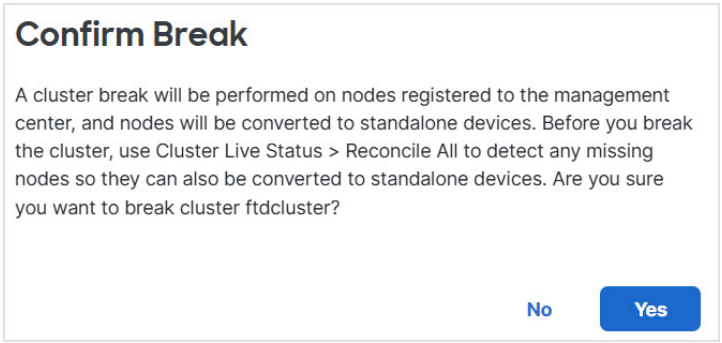
步骤 2 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**中断集群**。

图 ***150:*** 中断集群



步骤 3 系统会提示您断开集群；点击**是**。

图 ***151:*** 确认中断



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群中断。

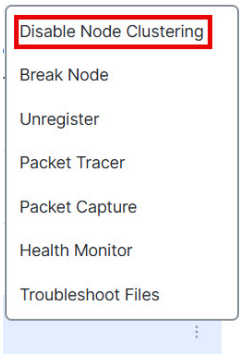
禁用集群

您可能需要停用节点，以准备删除节点，或临时进行维护。此程序旨在暂时停用节点；节点仍将显示在 防火墙管理中心 设备列表中。当节点变为非活动状态时，所有数据接口都将关闭。

过程

步骤 1 对于要禁用的设备，选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**禁用节点集群**。

图 *152:* 禁用集群



如果在控制节点上禁用集群，则其中一个数据节点将成为新的控制节点。请注意，对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。如果控制节点是集群中的唯一节点，则无法在该控制节点上禁用集群。

步骤 2 确认要在节点上禁用集群。

该节点在 **设备** > **设备管理** 列表中其名称旁边会显示（**已禁用**）。

步骤 3 重新启用集群，请参阅 重新加入集群，第 414 页。

重新加入集群

如果从集群中删除了某个节点（例如对于出现故障的接口），或者如果您手动禁用集群，必须手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除节点的原因的更多信息，请参阅重新加入集群，第 438 页。

过程

步骤 1 对于要重新激活的设备，请选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**启用节点集群**。

步骤 2 确认要在设备上启用集群。

更改控制节点

⚠

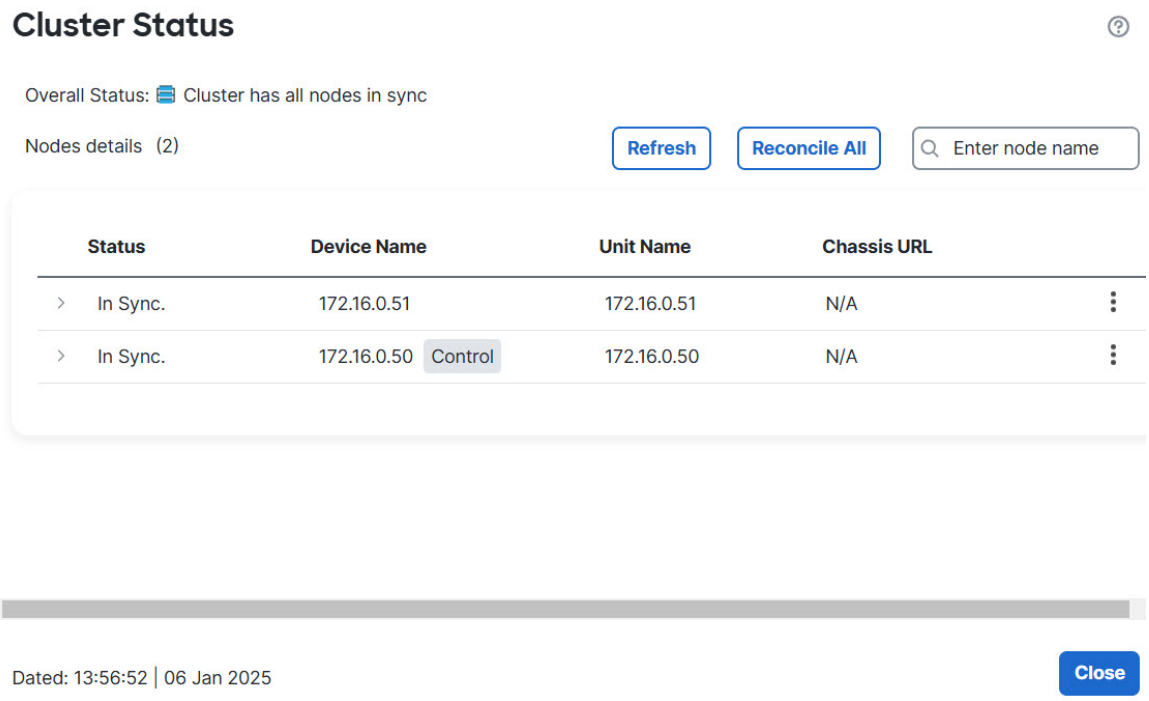
注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体单元，请使用本节中的程序。请注意，对集中功能而言，如果使用任何一种方法来强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

过程

步骤 1 通过选择**设备** > **设备管理** **更多** (⋮) **集群实时状态**打开**集群状态**对话框。

图 *153:* 集群状态



步骤 2 对于要成为控制设备的设备，请选择**更多** (⋮) **将角色更改为控制**。

步骤 3 系统将提示您确认角色更改。选中该复选框，然后点击 **确定**。

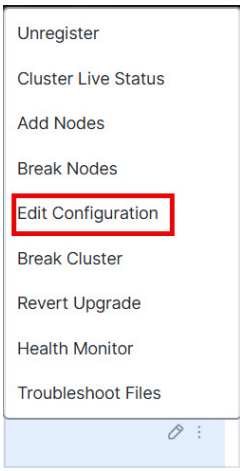
编辑集群配置

您可以编辑集群配置。如果更改集群密钥、集群控制链路接口或集群控制链路网络，则集群会被自动中断并重组。在重组集群之前，您可能会遇到流量中断。如果您更改节点、节点优先级或站点 ID 的集群控制链路 IP 地址，则只有受影响的节点会断开并重新添加到集群。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**编辑配置**。

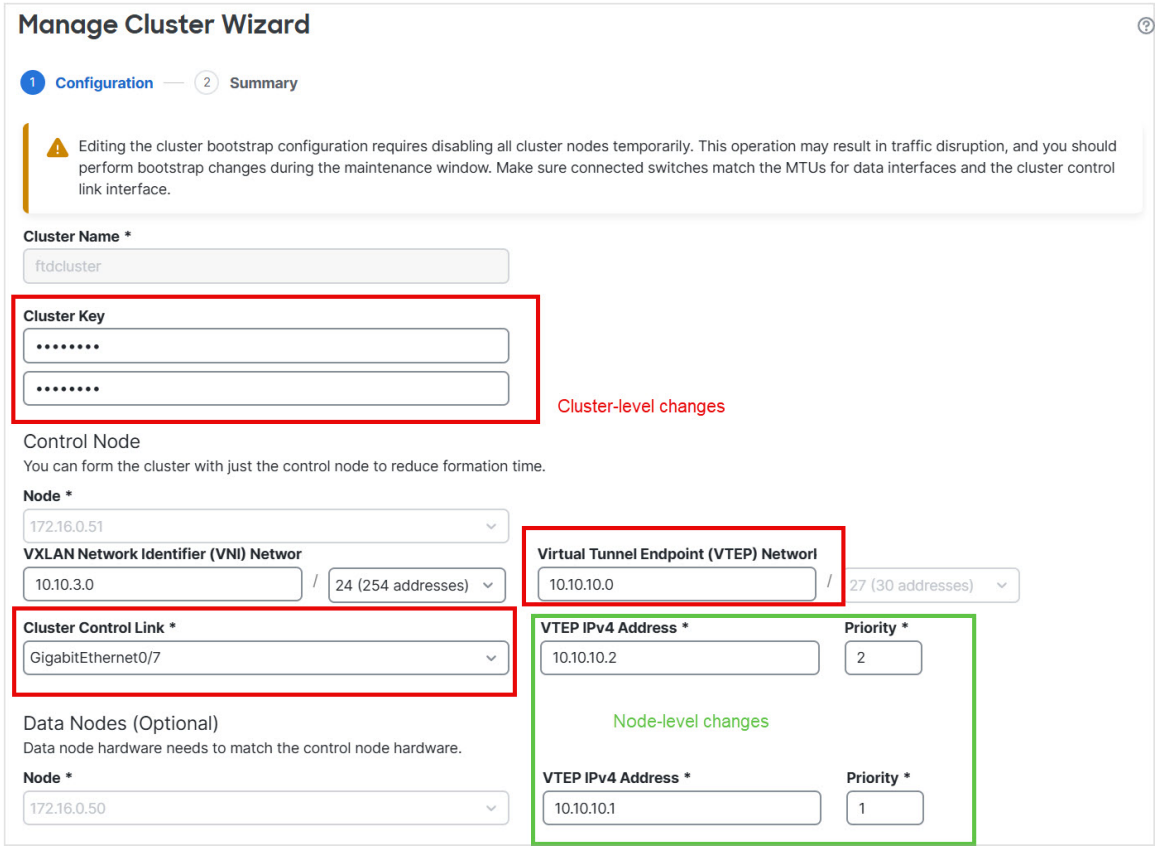
图 *154:* 编辑配置



系统将显示**管理集群向导 (Manage Cluster Wizard)**。

步骤 2 更新集群配置。

图 *155:* 管理集群向导



如果集群控制链路是 EtherChannel，则可以通过点击接口下拉菜单旁边的 **编辑** (✎) 来编辑接口成员身份和 LACP 配置。

步骤 3 点击**继续**。查看**摘要**，然后点击**保存**

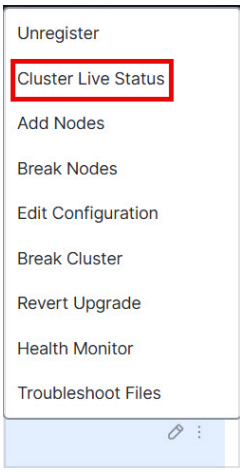
调整集群节点

如果集群节点注册失败，则可将集群成员身份从设备协调至防火墙管理中心。例如，数据节点在防火墙管理中心 被占用或存在网络问题时注册失败的情况下。

过程

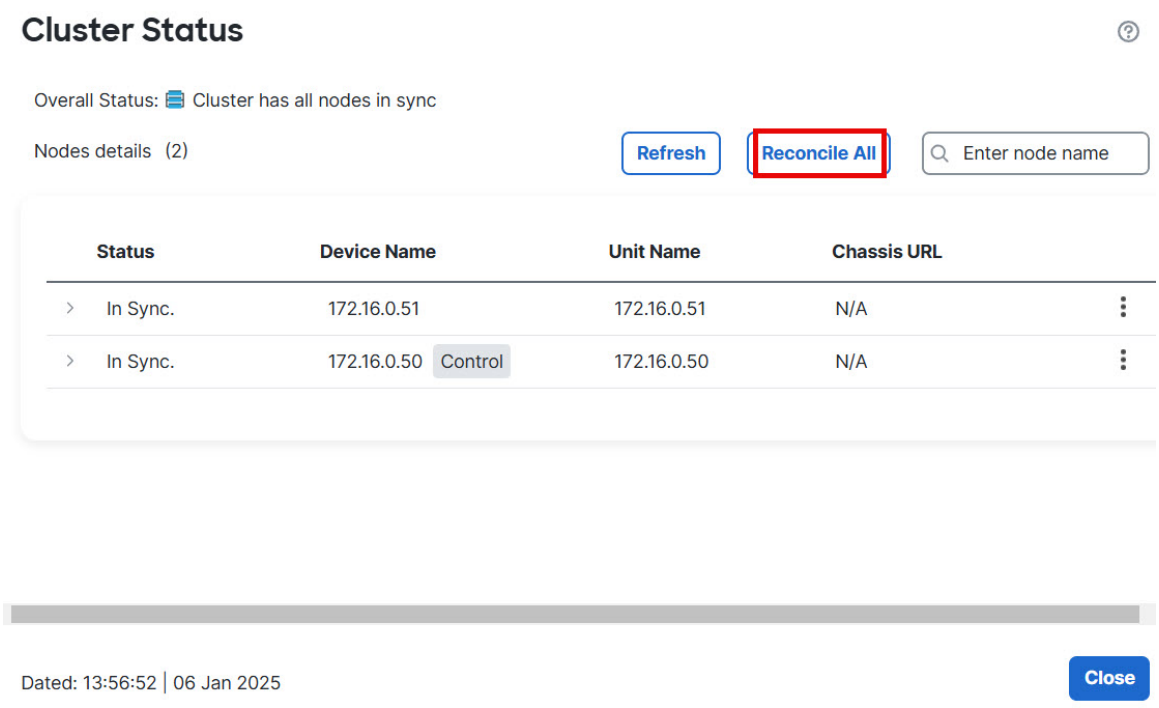
步骤 1 选择集群的 **设备** > **设备管理** **更多** (⋮)，然后选择**集群实时状态**，以打开**集群状态**对话框。

图 *156:* 集群实时状态



步骤 2 点击协调全部 **(Reconcile All)**。

图 *157:* 协调全部



有关集群状态的详细信息，请参阅监控集群，第 420 页。

取消注册集群或节点并注册到新防火墙管理中心

您可以从 防火墙管理中心 中取消注册集群，从而使集群保持不变。如果要将集群添加到新的 防火墙管理中心，则可能需要取消注册该集群。

您还可以从 防火墙管理中心 取消注册节点，而不会中断集群中的节点。虽然该节点不会显示在 防火墙管理中心 中，但它仍然是集群的一部分，并且它会继续传递流量，甚至可能成为控制节点。您无法取消注册当前的控制节点。如果无法再从防火墙管理中心访问该节点，您可能会希望将其取消注册，但在排除管理连接故障时，您仍希望将其作为集群的一部分。

取消注册集群：

- 会切断 防火墙管理中心和该集群之间的所有通信。
- 从 **设备管理** 页面删除集群。
- 如果集群的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将集群返回本地时间管理。
- 保持配置不变，以便集群继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将集群再次注册到相同或不同的防火墙管理中心会导致配置被删除，因此集群将在该点停止处理流量；集群配置保持不变，因此您可以将集群作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

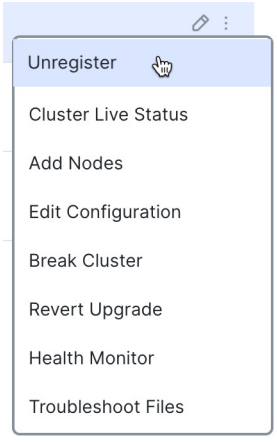
开始之前

此过程需要 CLI 对一个节点拥有访问权限。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群或节点的 **更多** (⋮)，然后选择**取消注册**。

图 *158:* 取消注册集群或节点



步骤 2 系统会提示您取消注册集群或节点；点击**是**。

步骤 3 您可以通过将其中一个集群成员添加为新设备来将集群注册到新的（或相同的）防火墙管理中心集群。

您只用将其中一个集群节点添加为设备，然后便可发现其余集群节点。

a) 连接到一个集群节点的 CLI，并使用 **configure manager add** 命令识别新 防火墙管理中心。请参阅在 CLI 中修改 Firewall Threat Defense 管理接口。

b) 选择 **设备** > **设备管理**，然后点击**添加** > **设备**。

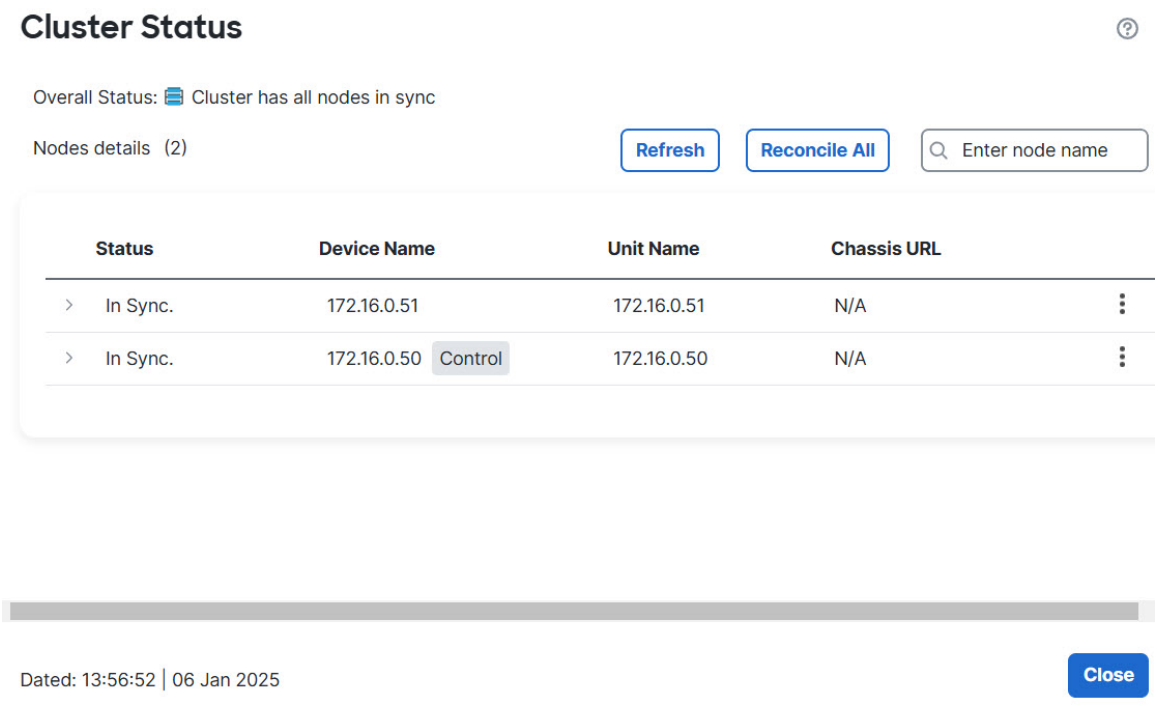
步骤 4 要重新添加未注册的节点，请参阅调整集群节点，第 417 页。

监控集群

您可以在 防火墙管理中心 中和 Firewall Threat Defense CLI 上监控集群。

- **集群状态**对话框（可通过 **设备** > **设备管理** **更多** (⋮) 图标或从**设备** > **设备管理** > **集群**页面**常规**区域**集群实时状态**链接来访问）。

图 *159:* 集群状态



控制节点有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 (In Sync.) - 节点已向 防火墙管理中心 注册。

- 待处理注册 (Pending Registration) - 节点是集群的一部分，但尚未向 防火墙管理中心 注册。如果节点注册失败，则可点击**协调所有 (Reconcile All)** 以重试注册。
- 集群已禁用 (Clustering is disabled) - 节点已向 防火墙管理中心 注册，但它是集群的非活动成员。如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除节点。
- “正在加入集群...”(Joining cluster...) - 节点正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 防火墙管理中心 注册。

对于每个节点，您可以查看**摘要 (Summary)** 或**历史记录 (History)**。

图 *160:* 节点摘要

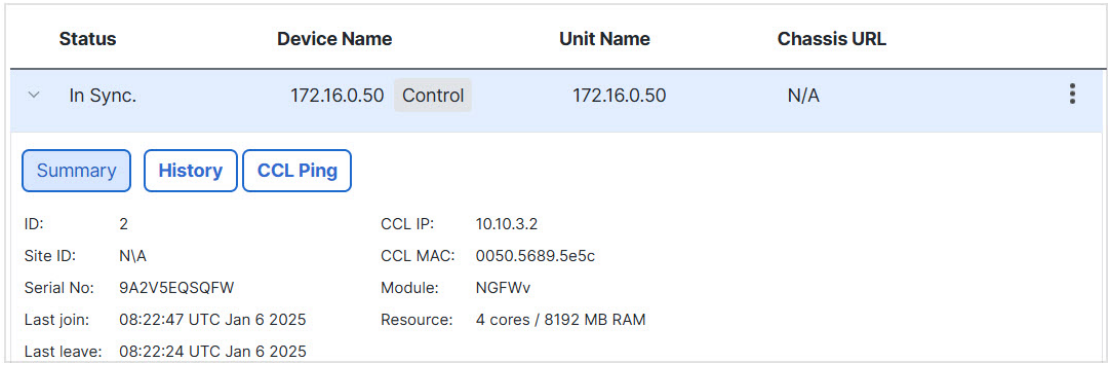
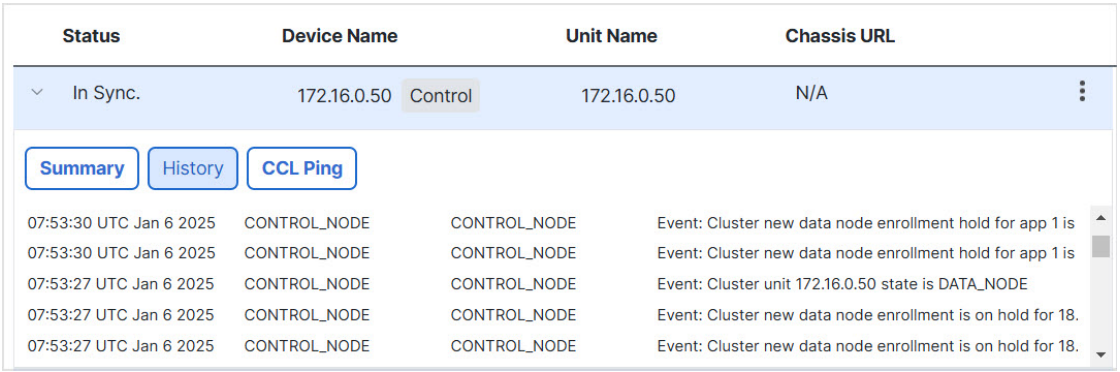


图 *161:* 节点历史记录



- **系统 (⚙) > 任务** 页面。

  任务 (Tasks) 页面会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

- **设备 > 设备管理***cluster_name*。

  展开设备列表页面上的集群时，您可以看到所有成员节点，包括 IP 地址旁显示其角色的控制节点。对于仍在注册的节点，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

集群运行状况监控器控制面板

集群运行状况监控器

当 Firewall Threat Defense 是集群的控制节点时， 防火墙管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加（在公共云集群中，不属于 防火墙管理中心的其他节点）或 正常（节点的理想状态）。
  - 集群统计信息部分显示集群的当前指标，包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和 NAT 转换。

  注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

  - 指标图表（即 CPU 使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。
- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。
  - “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU 使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT 转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。
- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和NAT 转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从防火墙管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（∨） 以展开和折叠托管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 **添加新的控制面板**（＋），通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

集群指标

集群运行状况监控器跟踪与集群及其节点相关的统计信息，以及负载分布、性能和CCL流量统计信息的汇总。

表 *31:* 集群指标

指标	说明	格式
CPU	集群节点上的CPU指标平均值（分别针对数据平面和 snort）。	percentage
Memory	集群节点上的平均内存指标（分别用于数据平面和 snort）。	percentage
数据吞吐量	集群的传入和传出数据流量统计信息。	bytes
CCL 吞吐量	集群的传入和传出 CCL 流量统计信息。	bytes
连接	集群中的活动连接计数。	数字
NAT 转换	集群的 NAT 转换计数。	数字
分布	集群中每秒的连接分布计数。	数字

指标	说明	格式
数据包数	集群中每秒的数据包分发计数。	数字

监控分布式站点间 VPN

使用以下命令监控 VPN 会话的状态和分布：

- 使用 **show cluster vpn-sessiondb distribution** 提供会话的总体分布。如果在多情景环境中运行，则必须在系统执行空间中运行此命令。

  利用此 **show** 命令可以快速查看会话，而无需在每个节点上执行 **show vpn-sessiondb summary**。

- 也可使用 **show cluster vpn-sessiondb summary** 命令提供集群上的 VPN 连接的统一视图。
- 使用 **show vpn-sessiondb** 命令的单独设备监控除了显示常见的 VPN 信息以外，还显示设备上的主用和备份会话数量。

对集群进行故障排除

您可以使用 **CCL Ping** 工具确保集群控制链路正常运行。 您还可以使用以下适用于设备和集群的工具：

- 故障排除文件-如果节点未能加入集群，系统将自动生成故障排除文件。您还可以从 **设备** > **设备管理** 生成和下载故障排除文件，然后选择**添加**、**集群常规**区域。请参阅生成故障排除文件。

  您还可以通过点击 **更多** (⋮) 并选择 **文件故障排除** ，从 **设备管理**页面生成文件。

- CLI 输出 — 在 **设备** > **设备管理** 中选择**添加**、**集群常规**区域，您可以查看一组预定义的 CLI 输出，帮助您排除集群的故障。系统会自动为集群运行以下命令：
  - **show running-config cluster**
  - **show cluster info**
  - **show cluster info health**
  - **show cluster info transport cp**
  - **show version**
  - **show asp drop**
  - **show counters**
  - **show arp**
  - **show int ip brief**
  - **show blocks**

- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

您还可以在命令字段中输入任何 **show** 命令。有关详细信息，请参阅查看 CLI 输出。

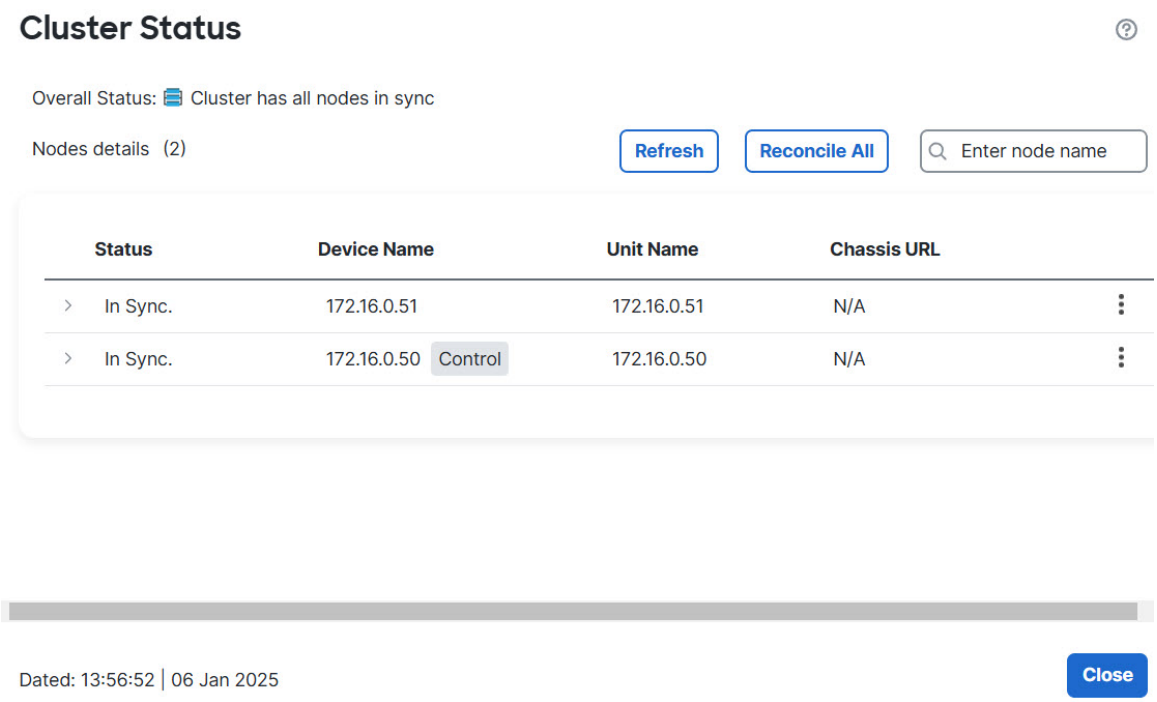
在集群控制链路上执行 Ping

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。如果您遇到集群控制链路连接问题，此工具允许您手动 ping 所有已加入集群的节点。

过程

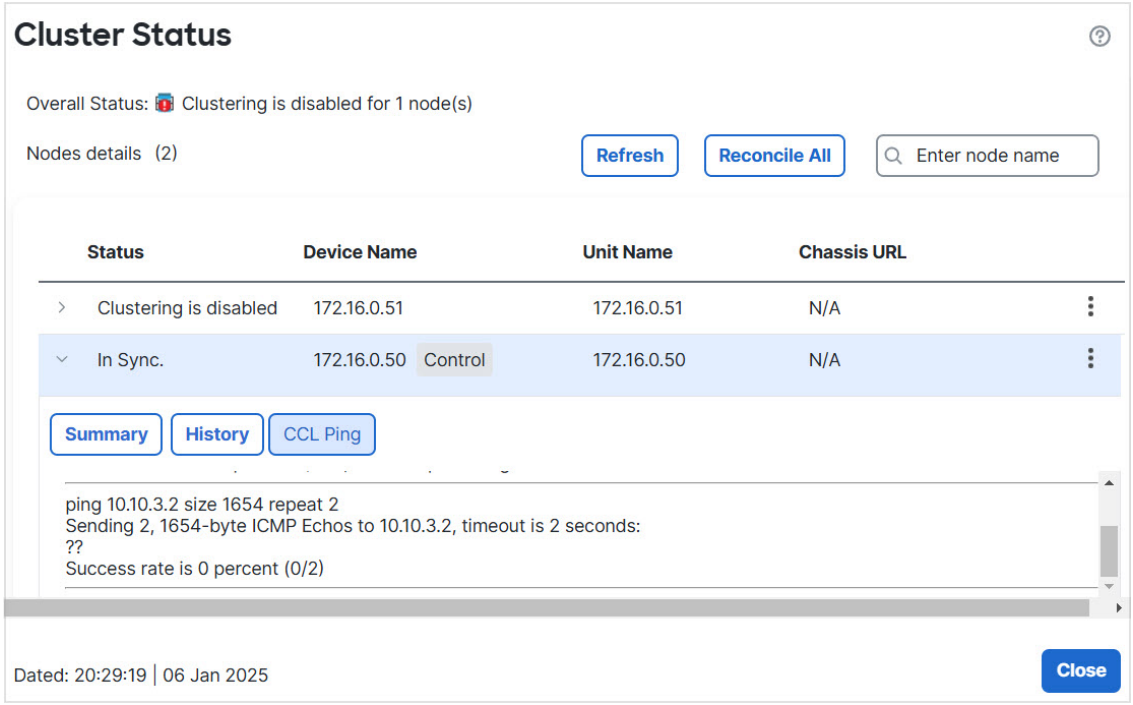
步骤 1 选择 **设备** > **设备管理**，点击集群旁边的 **更多** (⋮) 图标，然后选择**集群实时状态**。

图 *162:* 集群状态



步骤 2 展开其中一个节点，然后点击 **CCL Ping**。

图 *163: CCL Ping*



节点使用与最大 MTU 匹配的数据包大小在集群控制链路上向每个其他节点发送 ping 命令。

分布式站点间 VPN 故障排除

分布式 VPN 通知

当运行分布式 VPN 的集群上发生以下错误情况时，您将收到包含确定短语的通知消息：

情况	通知
如果在尝试加入集群时，某个现有或正在加入集群的数据节点未处在分布式 VPN 模式下：	新集群成员 (*member-name*) 由于 vpn 模式不匹配而被拒绝。 和 主(*control-name*) 拒绝来自设备 (unit-name) 的注册请求，原因是：vpn 模式功能与主配置不兼容
如果分布式 VPN 的集群成员上未正确地配置许可：	错误：主机请求集群的 VPN 模式更改为分布式。由于缺少运营商许可证，无法更改模式。

情况	通知
如果接收的 IKEv2 数据包的 SPI 中的时间戳或成员 ID 无效：	收到已到期的 SPI 或 检测到损坏的 SPI
如果集群无法创建备份会话：	未能创建 IKEv2 会话的备份。
IKEv2 初始联系 (IC) 处理错误：	IKEv2 协商因错误而终止：备份上找到过时的备份会话
重新分发问题：	未能将会话重新分发消息发送至 *member-name* 未能收到 *member-name* 的会话移动响应（仅限主）
如果在重新分发会话期间拓扑发生更改：	检测到集群拓扑更改。已终止 VPN 会话重新分发。

您可能遇到以下情况之一：

- 当使用 **port-channel load-balance src-dst l4port**命令为 N7K 交换机配置 L4port 作为负载均衡算法时，站点间 VPN 会话仅被分发到集群中的一个机箱。集群会话分配的示例如下所示：

```
SSP-Cluster/slave(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

  由于站点间 IKEv2 VPN 使用端口 500 作为源和目标端口，因此 IKE 数据包仅发送至 Nexus 7K 与机箱之间连接的端口通道中的其中一个链路。

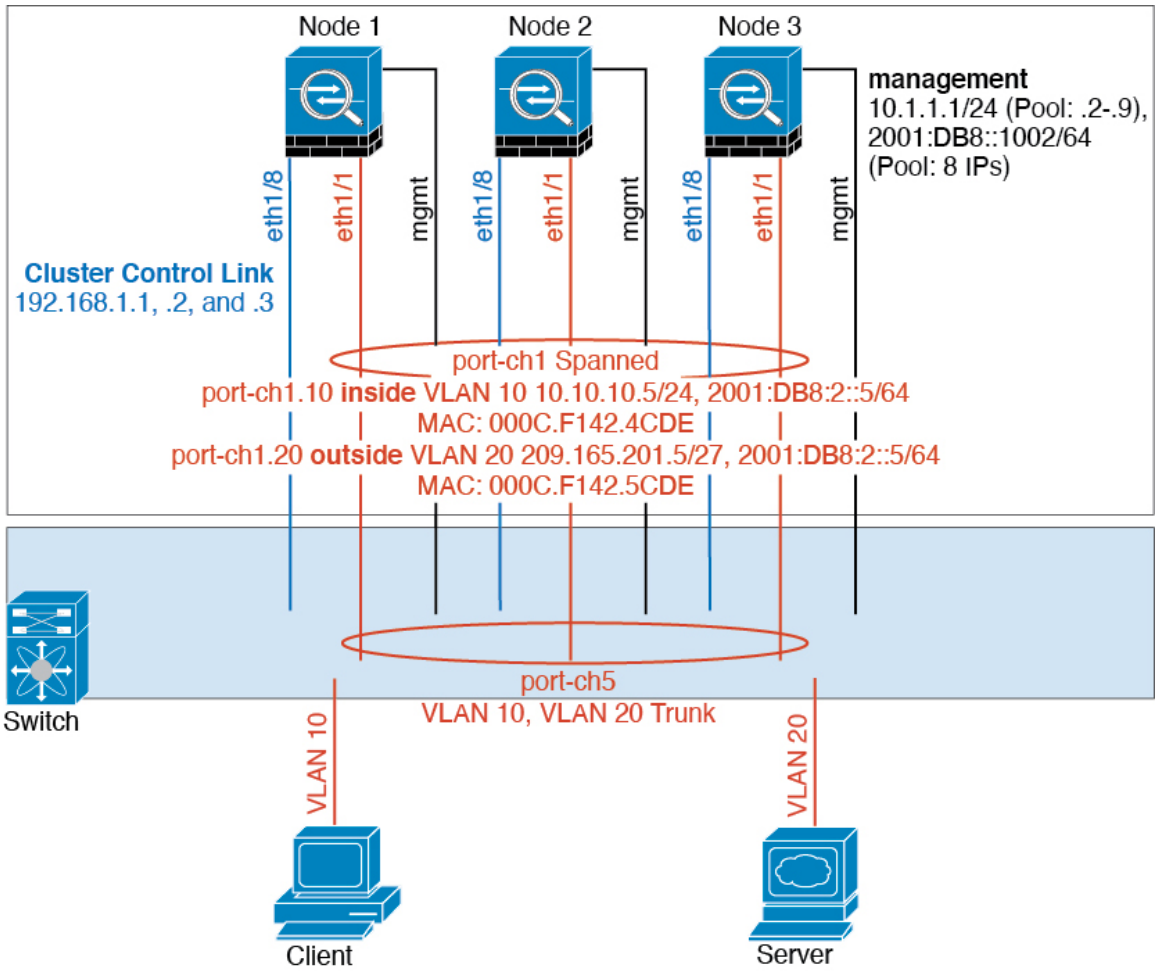
  使用 **port-channel load-balance src-dst ip-l4port** 将 Nexus 7K 负载均衡算法更改为 IP 和 L4 端口。然后，IKE 数据包将被发送至所有链路，进而发送至所有节点。

  要进行更即时的调整，请在集群的控制节点上执行： **cluster redistribute vpn-sessiondb** ，将主用 VPN 会话重新分发至另一机箱的集群节点。

集群示例

这些示例包含典型部署。

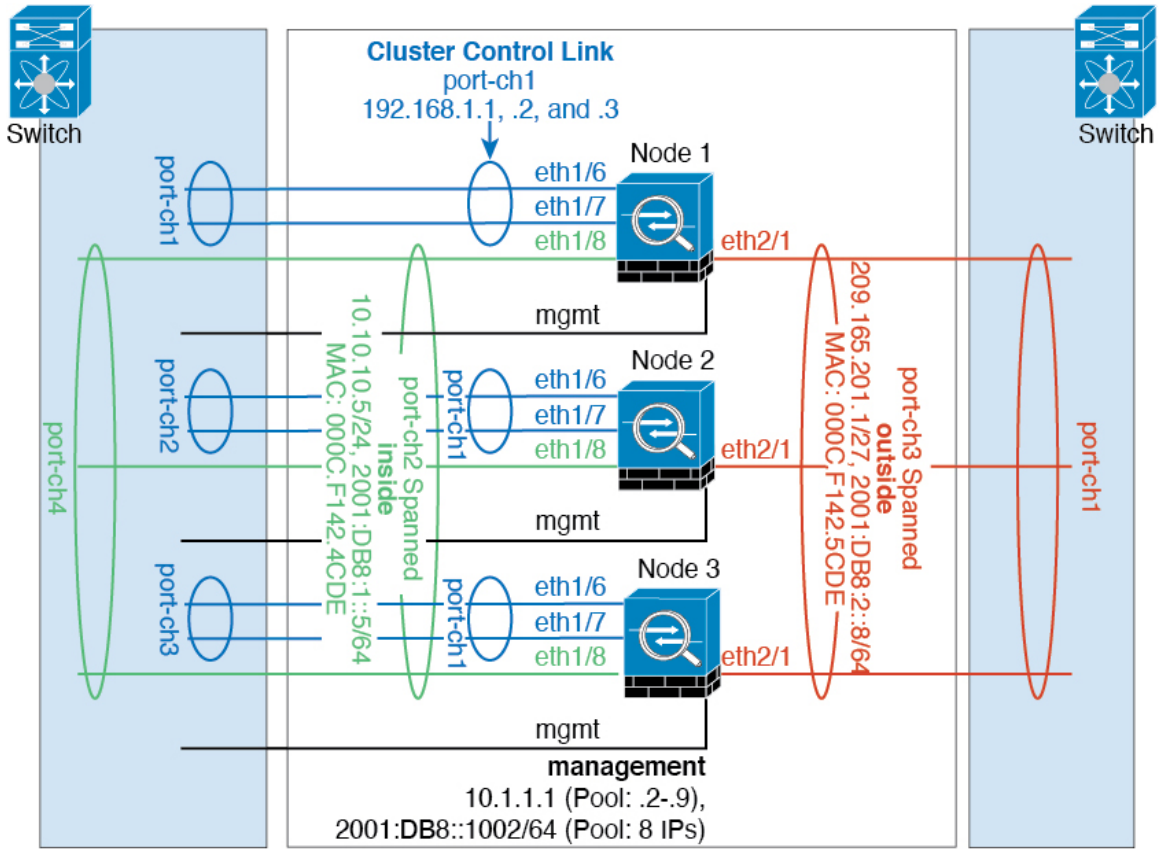
单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如，VLAN 10 用于内部网络，而 VLAN 20 用于外部网络。每台 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机侧分组为一个 EtherChannel。如果一台 变得不可用，交换机将在其余设备之间再均衡流量。

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

集群参考

本部分包括有关集群工作原理的详细信息。

Firewall Threat Defense功能和集群

部分 Firewall Threat Defense 功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略，第 1041 页。

- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 在公共云中不支持站点间 VPN（基于策略和路由）。
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- 防火墙管理中心 UCAPL/CC 模式
- DHCP 客户端、服务器和代理。支持 DHCP 中继。

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略，第 1041 页。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP

- RSH
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 站点间 VPN
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由（仅适用于跨网络 EtherChannel 模式）

连接设置和集群

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

独立接口模式下的组播路由

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

独立接口模式下的组播路由

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 Firewall 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 Firewall 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可防止相邻路由器与可能已不在集群中的节点维持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。
- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP

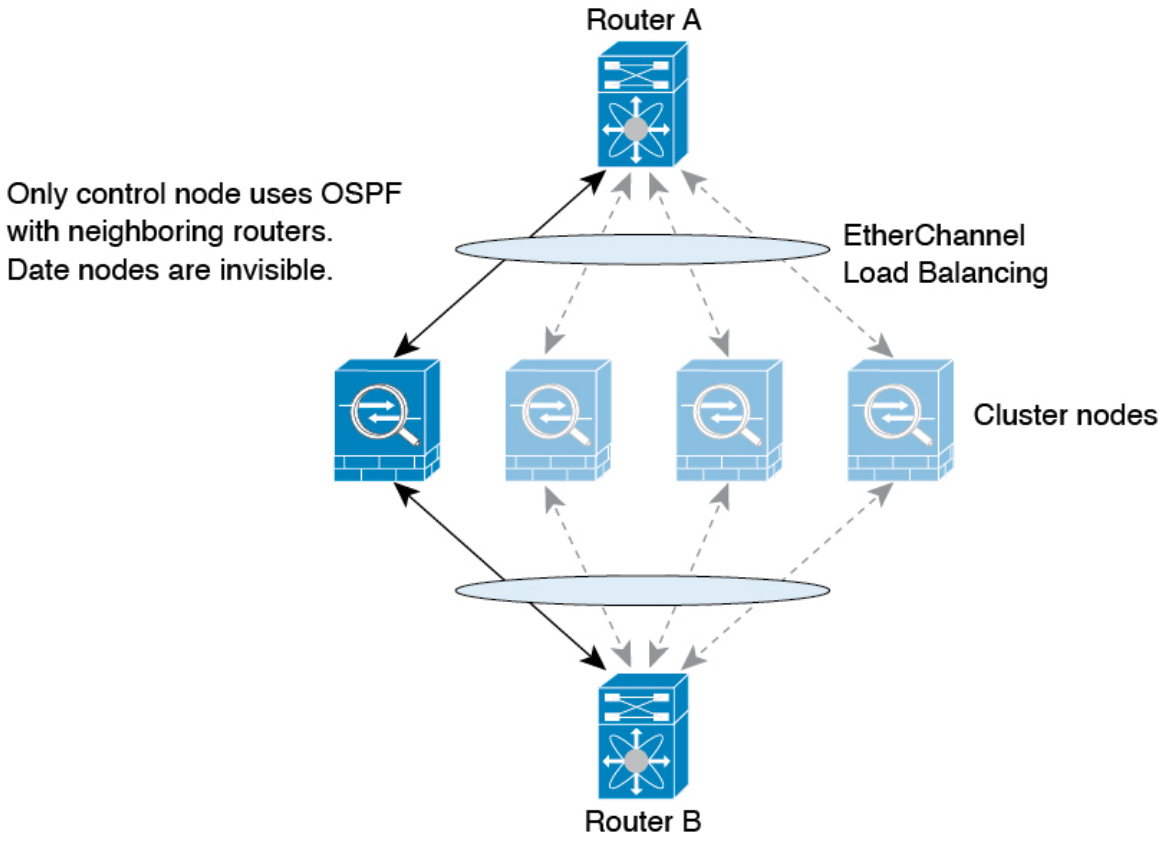
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

动态路由

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *164:* 跨区以太网通道模式下的动态路由



在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

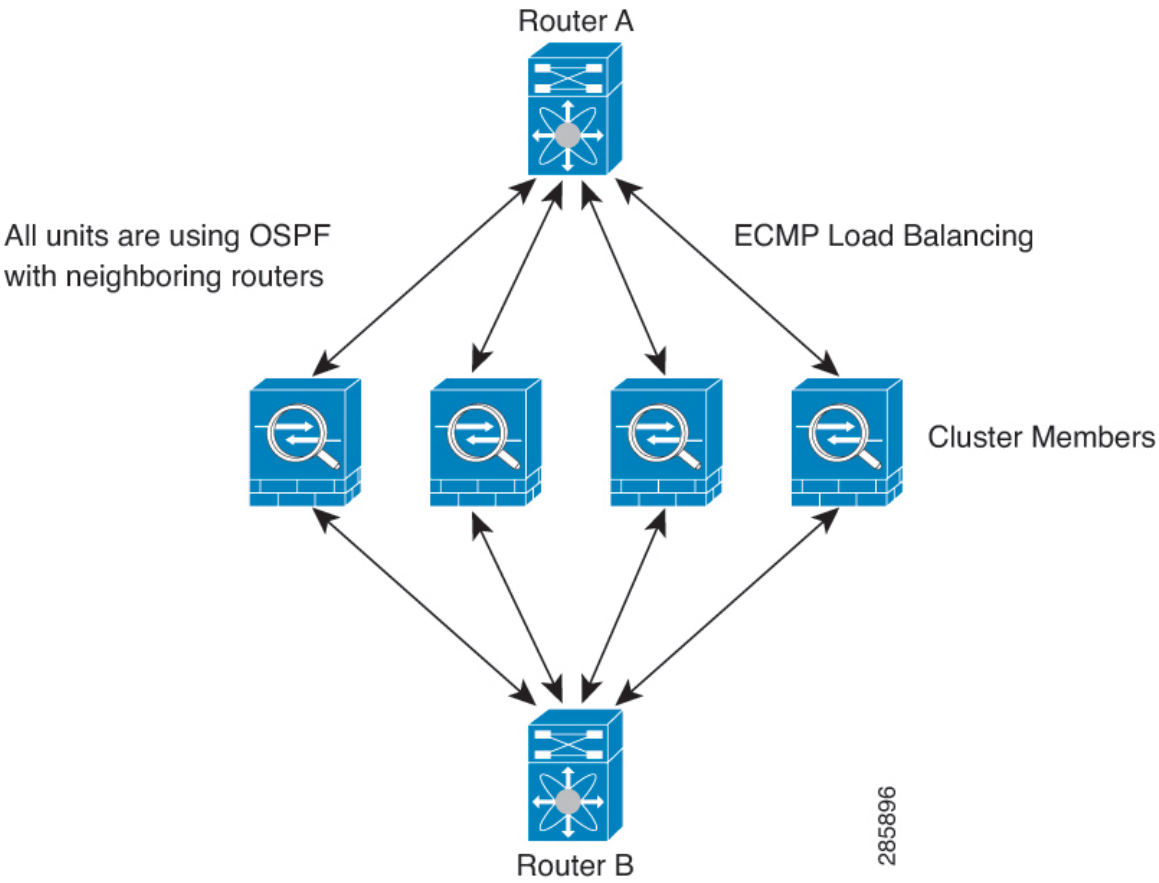
OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路

由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *165:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅创建 ECMP 区域，第 1161 页。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

站点间 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程访问 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨网络 EtherChannel 地址时，连接会自动转移到控制节点。 对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。



注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。



注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

有关详细信息，请参阅控制节点选择，第 437 页。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

- 跨网络 EtherChannel - 使用集群链路聚合控制协议 (cLACP)。每个节点都会监控链路状态和 cLACP 协议消息，以便确定 EtherChannel 中的端口是否仍处于活动状态。状态会报告给控制节点。
- 独立接口（仅适用于路由模式）- 每个节点都会监控自己的接口并向控制节点报告接口状态。

当您启用运行状况监控时，默认情况下会监控有物理接口（包括主要的 EtherChannel）；您可以选择按接口禁用监控。只能监控已命名接口。例如，已命名的 EtherChannel 必须发生故障，才能将其视为发生故障，这意味着 EtherChannel 的所有成员端口必须发生故障才能触发集群删除。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。Firewall Threat Defense 在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定成员还是正在加入集群的设备。对于 EtherChannel（无论是否跨网络）：如果既定成员上的接口关闭，Firewall Threat Defense 将在 9 秒后删除该成员。Firewall Threat Defense 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 Firewall Threat Defense从集群中删除。如果是非 EtherChannel，则无论节点的成员状态如何，都会在 500 毫秒后删除设备。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

Firewall 威胁防御将自动尝试重新加入集群，具体取决于故障事件。



注释 当 Firewall 威胁防御 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - Firewall Threat Defense 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 Firewall Threat Defense应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。Firewall Threat Defense应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。

- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *32:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	支持	—
动态路由	支持	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。



注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

端口地址转换连接

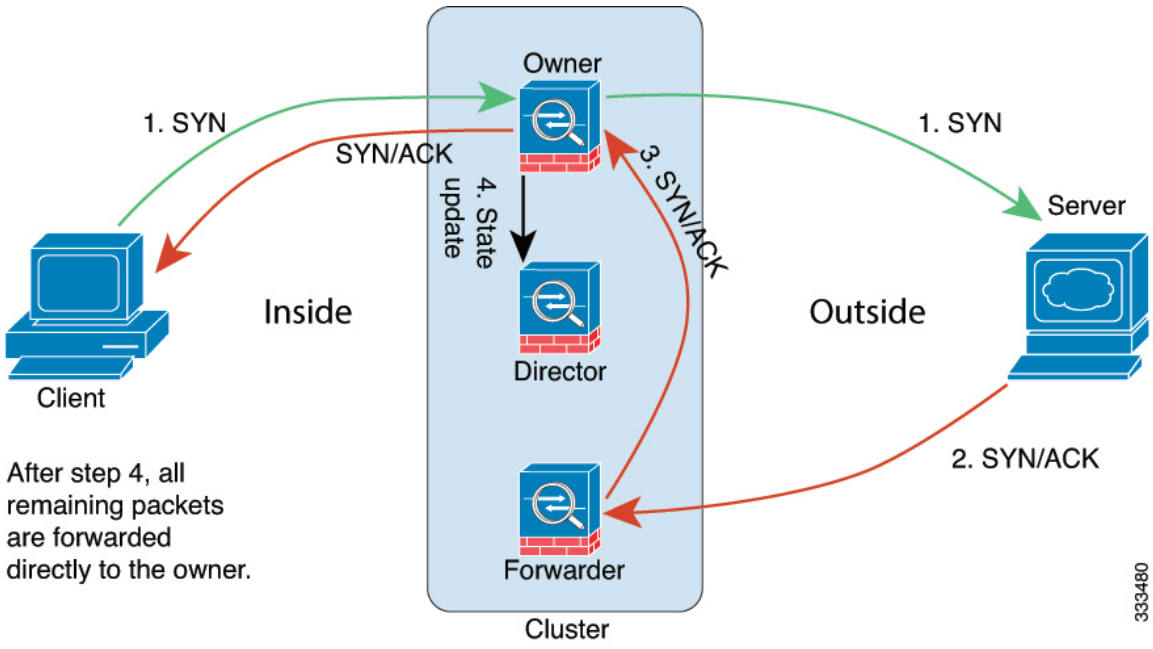
新连接所有权

此版本不支持流量重定向。通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。同一连接的所有后续数据包都应到达同一节点。如果任何连接数据包到达其他节点，它们将被丢弃。如果反向流量到达其他节点，也将被丢弃。对于集中功能，如果连接不到达控制节点，则它们会被丢弃。

默认情况下，AWS GWLB 使用 5 元组来保持流粘性。建议在 AWS GWLB 上启用 2 元组或 3 元组粘性，以确保将相同的流发送到同一节点。

TCP 的数据流示例

以下图例显示了新连接的建立。



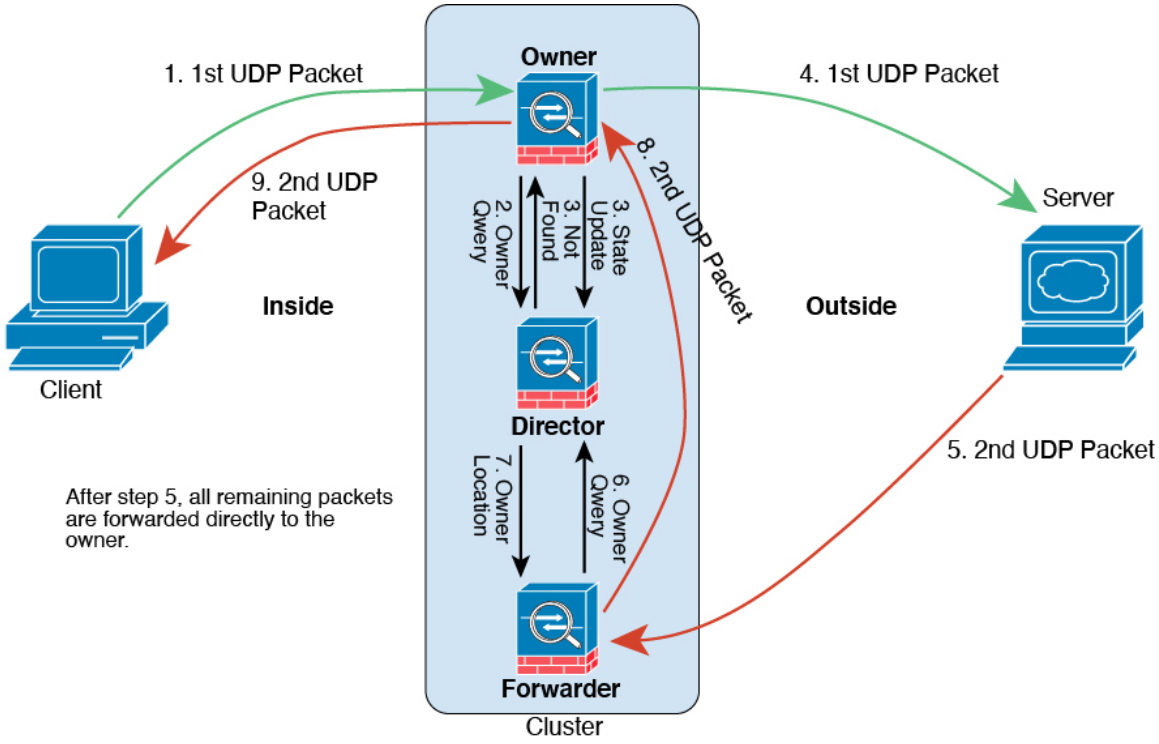
1. SYN 数据包从客户端发出，被传送到一台 Firewall 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 Firewall 威胁防御（基于负载均衡方法）。此 Firewall 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。

7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *166: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个Firewall 威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

集群的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Cisco Secure Firewall 6100 的集群	10.0.0	10.0.0	Cisco Secure Firewall 6100 支持最多 4 个节点的跨区以太网通道集群。
通过 Cisco Secure Firewall 4200 上的集群支持分布式站点间VPN	10.0.0	10.0.0	Cisco Secure Firewall 4200 上的 ASA 集群在分布式模式下支持站点间 VPN。使用分布式模式能够在集群的成员之间分布多个站点间 IPsec IKEv2 VPN 连接，而不仅分布在控制节点上（如集中模式一样）。这将在集中式 VPN 功能的基础上大幅扩展 VPN 支持，并提供高可用性。 新增或修改的命令：**cluster redistribute vpn-sessiondb**、 **show cluster vpn-sessiondb**、**cluster vpn-mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show conn detail**、**show crypto ikev2 stats**
集群重定向：支持 Cisco Secure Firewall 4200非对称集群流量的流卸载	10.0.0	10.0.0	对于不对称流，集群重定向允许转发节点将流量分流到硬件上。此功能默认启用，但可以使用 FlexConfig 配置。 当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。 新增/经修改的命令：**flow-offload cluster-redirect** (FlexConfig)、**show conn**、**show flow-offload flow**、**show flow-offload info**。
在分布式站点间 VPN 模式下，对防火墙管理中心上的集群控制链路上的流量进行 IPsec 流分流	10.0.0	10.0.0	对于分布式站点间 VPN 模式中的不对称流量，IPsec 流分流现在可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，且在启用 IPsec 流卸载时始终可用。 添加/修改的命令：**show crypto ipsec sa detail**。
集群节点加入时的 MTU ping 测试通过尝试较小的 MTU 来提供更多信息	10.0.0	10.0.0	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，它将尝试除以 MTU，并继续除以 2，直到 MTU ping 成功。成功的 ping 值会显示在 **show cluster info trace** 中，因此您可以将 MTU 调整为可用值，然后重试。 即使ping失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。 我们建议将交换机 MTU 的大小增加到建议的值，但如果您无法更改交换机配置，则可以使用集群控制链路的工作值来形成集群。 添加/修改的命令：**show cluster info trace**、**show cluster history**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
改进了高 CPU 情况下的集群控制链路运行状况检查	10.0.0	10.0.0	当集群节点 CPU 使用率较高时，系统将暂停运行状况检查，但不会将节点标记为运行状况不正常。此功能默认启用，但可以使用 FlexConfig 配置。 新增/经修改的命令：**cpu-healthcheck-threshold** (FlexConfig)、、、。
用于 Cisco Secure Firewall 3100/4200 的 16 节点集群。	7.6.0	7.6.0	对于 Cisco Secure Firewall 3100 和 4200，最大节点数从 8 增加到 16。
用于 Cisco Secure Firewall 3100/4200 集群的独立接口模式。	7.6.0	7.6.0	独立接口是正常的路由接口，每个接口都有自己的本地 IP 地址用于路由。每个接口的主集群 IP 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。必须在上游交换机上分别配置负载均衡。 限制：不支持容器实例。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **接口 / EIGRP / OSPF / OSPFv3 / BGP (Interfaces / EIGRP / OSPF / OSPFv3 / BGP)** • **对象** > **对象管理** > **地址池** > **MAC 地址池**
关于节点加入时时间节点的 MTU ping 测试	7.6.0	7.6.0	节点加入集群时，会向控制节点发送数据包大小为集群控制链路 MTU 两倍的 Ping 请求，以检查 MTU 兼容性。此前，仅控制节点发送 Ping。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。 添加/修改的命令：**show cluster history**。
集群控制链路 ping 工具。	7.2.6 7.4.1	任意	您可以通过执行 ping 来检查是否所有集群节点都能通过集群控制链路相互连接。节点无法加入集群的一个主要原因是集群控制链路配置不正确，例如，集群控制链路 MTU 设置可能高于连接交换机的 MTU。 新增/修改的屏幕：**设备** > **设备管理** > **更多** > **集群实时状态**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
当节点未能加入集群时，自动在该节点上生成故障排除文件。	7.4.1	7.4.1	如果节点未能加入集群，系统将自动为该节点生成故障排除文件。您可以从**任务 (Tasks)** 或**集群 (Cluster)** 页面下载该文件。
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
Cisco Secure Firewall 4200 的集群	7.4.0	7.4.0	Cisco Secure Firewall 4200 支持最多 8 个节点的跨区以太网通道集群。
集群运行状况监控设置	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
集群运行状况监控器控制面板	7.3.0	任意	您现在可以在集群运行状况监控控制面板上查看集群运行状况。 新增/修改的屏幕：**系统 (System)** > **运行状况 (Health)** > **监控器 (Monitor)**
集群控制链路 MTU 的自动配置	7.2.0	7.2.0	集群控制链路接口的 MTU 现在会被自动设置为比最高数据接口 MTU 多 100 个字节；默认情况下，MTU 为 1600 字节。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Cisco Secure Firewall 3100 的集群	7.1.0	7.1.0	Cisco Secure Firewall 3100 支持最多 8 个节点的跨区以太网通道集群。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：Cisco Secure Firewall 3100



第 11 章

群集技术：私有云

通过集群，您可以将多台 Firewall Threat Defense Virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。您可以使用 VMware 和 KVM 在私有云中部署 Firewall Threat Defense Virtual 集群。仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅不支持的功能和集群，第 486 页。

- 关于群集技术：私有云，第 447 页
- 群集技术许可证：私有云，第 451 页
- 集群的先决条件：私有云，第 451 页
- 集群的准则：私有云，第 453 页
- 配置群集技术：私有云，第 454 页
- 管理集群节点，第 468 页
- 监控集群：私有云，第 478 页
- 群集技术故障排除：私有云，第 484 页
- 群集技术参考：私有云，第 486 页
- 集群的准则：私有云，第 497 页

关于群集技术：私有云

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 Firewall Threat Defense Virtual 能够通过集群控制链路发送广播/组播消息。

- 对每台防火墙的管理访问权限，用于进行配置和监控。Firewall Threat Defense Virtual 部署包括用于管理集群节点的 Management 0/0 接口。

将集群接入网络中时，上游和下游路由器需要能够使用第 3 层单独接口和以下方法之一使出入集群的数据实现负载均衡：

- 策略型路由 - 上游和下游路由器使用路由映射和 ACL 在节点之间执行负载均衡。
- 等价多路径路由 - 上游和下游路由器使用等价静态或动态路由在节点之间执行负载均衡。



注释 不支持第 2 层跨区以太网通道。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 首次创建集群时，您可以指定要成为控制节点的节点，因为它是添加到集群的第一个节点，所以它将成为控制节点。

集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

独立接口

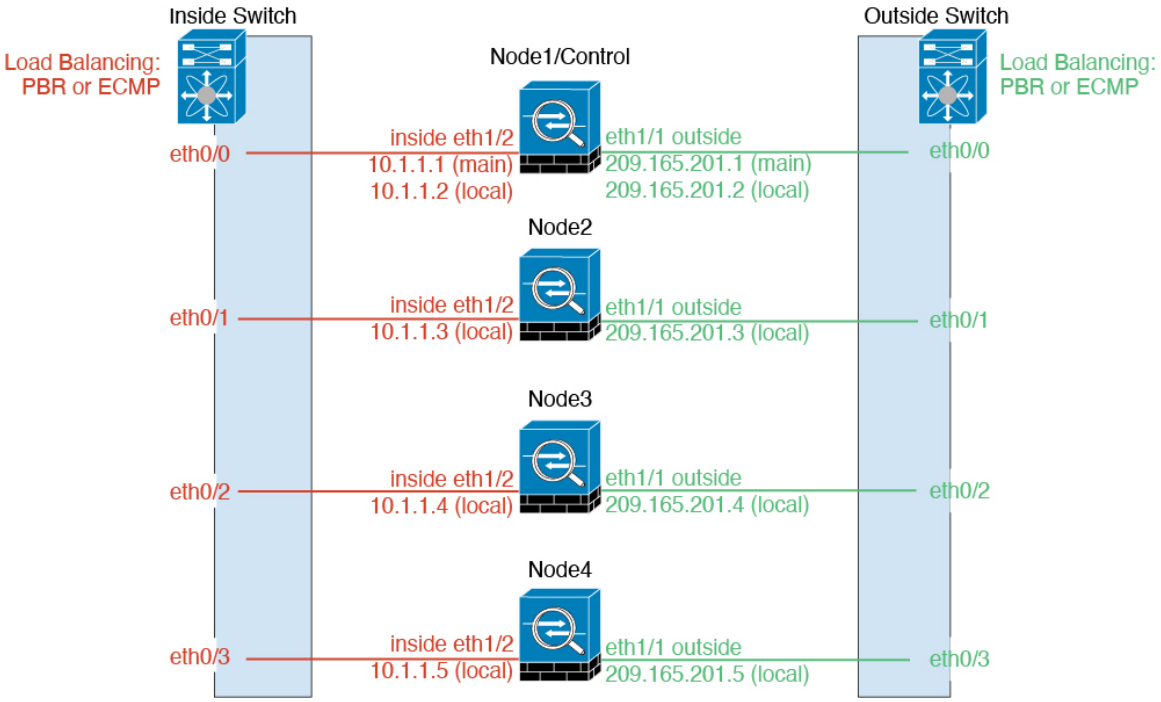
您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群IP地址将转移到新的控制节点，使集群的管理得以无缝继续。

不支持仅 IPS 接口（内联集和无源接口）作为独立接口。

由于接口配置只能在控制节点上配置，因此您可以通过接口配置设置一个 IP 地址池，供集群节点上的给定接口（包括控制节点上的一个接口）使用。

必须在上游交换机上分别配置负载均衡。



注释 不支持第 2 层跨区以太网通道。

策略型路由

使用独立接口时，每个 Firewall 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。策略型路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，我们建议使用此方法。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 Firewall 威胁防御 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。为了获得最佳性能，建议您配置 PBR 策略，以便连接的转发数据包和返回数据包定向到同一个 Firewall 威胁防御。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 Firewall 威胁防御。然后，PBR 可根据特定 Firewall 威胁防御 的可访问性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

同等成本的多路径路由

使用独立接口时，每个 Firewall 威胁防御 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，我们建议使用此方法。

ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 Firewall 威胁防御 故障会导致问题；如果继续使用该路由，发往故障 Firewall 威胁防御 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 Firewall 威胁防御 使之加入动态路由。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅配置 VXLAN 接口，第 783 页。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规Firewall Threat Defense Virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，Firewall Threat Defense Virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。

- 连接所有权查询和数据包转发。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

管理网络

您必须使用管理接口来管理每个节点；集群不支持从数据接口进行管理。

群集技术许可证：私有云

每个 Firewall Threat Defense Virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。您可以通过点击 **管理** > **许可证** > **智能许可证** 中的**编辑许可证**或选择 **设备** > **设备管理**、点击集群的 **编辑** (✎)、然后在**许可证**区域中点击 **编辑** (✎) 来修改集群的许可证。

注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

集群的先决条件：私有云

型号要求

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100
- VMware 或 KVM
- 4x4 配置的集群最多支持 16 个节点。您最多可以设置四个主机，每个主机中最多有四个 Threat Defense Virtual 实例。

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件和软件要求

集群中的所有设备：

- 必须为集群控制链路启用巨帧预留。部署 Firewall Threat Defense Virtual 时，可以通过设置 `"DeploymentType": "Cluster"`在 Day 0 配置中执行此操作。否则，在集群形成且运行状况正常后，您必须重新启动每个节点才能启用巨帧。
- （仅限 KVM）必须对 KVM 主机上的所有 VM 使用 CPU 硬分区（CPU 固定）。
- 必须在同一个性能层。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 必须使用用于 防火墙管理中心 通信的管理接口。不支持数据接口管理。
- 必须运行相同的版本，升级期间除外。支持无中断升级。
- 必须在同一域中。
- 必须在同一组中。
- 不得有任何待处理或进行中的部署。
- 控制节点不得配置任何不受支持的功能：不支持的功能和集群，第 486 页。
- 数据节点不得配置任何 VPN。控制节点可以配置站点间 VPN。

防火墙管理中心 要求

确保 防火墙管理中心NTP服务器设置为所有集群节点均可访问的可靠服务器，来保证正确的同步。默认情况下， 防火墙管理中心 使用与设备相同的 NTP 服务器。如果未将所有集群节点上的时间设置为相同，则可以自动将其从集群中删除。

交换机要求

请务必完成交换机配置后再配置集群。确保连接到集群控制链路的端口配置了正确（更高）的MTU。默认情况下，集群控制链路 MTU 会被设置为比数据接口高 154 字节。如果交换机的 MTU 不匹配，则集群形成将失败。当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路MTU匹配，从而检查MTU兼容性。如果初始ping失败，节点将使用较小的数据包大小（MTU除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。

集群的准则：私有云

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

其他准则

- 当发生重大拓扑更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firewall Threat Defense Virtual 上的接口、添加附加交换机以形成 VSS 或 vPC、在集群上配置 IP 地址或接口抖动），您应禁用运行状况检查功能，并禁用受拓扑更改影响的接口的接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要建立新连接以连通新设备。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。
- 我们不支持数据接口的 VXLAN；只有集群控制链路支持 VXLAN。

集群的默认值

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

升级准则

如果用户想要将新创建的节点添加到现有集群，请在 Day 0 配置中使用 "IfNamingConvention": "Old" 键值对。

配置群集技术：私有云

要在部署 Firewall Threat Defense Virtual 后配置集群，请执行以下任务。

向管理中心添加节点

在配置集群之前部署每个集群节点，然后将设备添加为 防火墙管理中心 上的独立设备。

过程

步骤 1 根据 Cisco Secure Firewall Threat Defense Virtual 入门指南部署每个集群节点。

集群中的所有设备：

- 必须为集群控制链路启用巨帧预留。部署 Firewall Threat Defense Virtual 时，可以通过设置 `"DeploymentType": "Cluster"`在 Day 0 配置中执行此操作。否则，在集群形成且运行状况正常后，您必须重新启动每个节点才能启用巨帧。
- （仅限 KVM）必须对 KVM 主机上的所有 VM 使用 CPU 硬分区（CPU 固定）。

步骤 2 将每个节点作为同一域和组中的独立设备添加到 防火墙管理中心。

请参阅使用注册密钥添加设备 - 基本配置，第 33 页。您可以创建包含单个设备的集群，然后稍后添加更多节点。您在添加设备时设置的初始设置（许可、访问控制策略）将被控制节点的所有集群节点继承。您将在形成集群时选择控制节点。

创建集群

从 防火墙管理中心 中的一个或多个设备组成集群。

开始之前

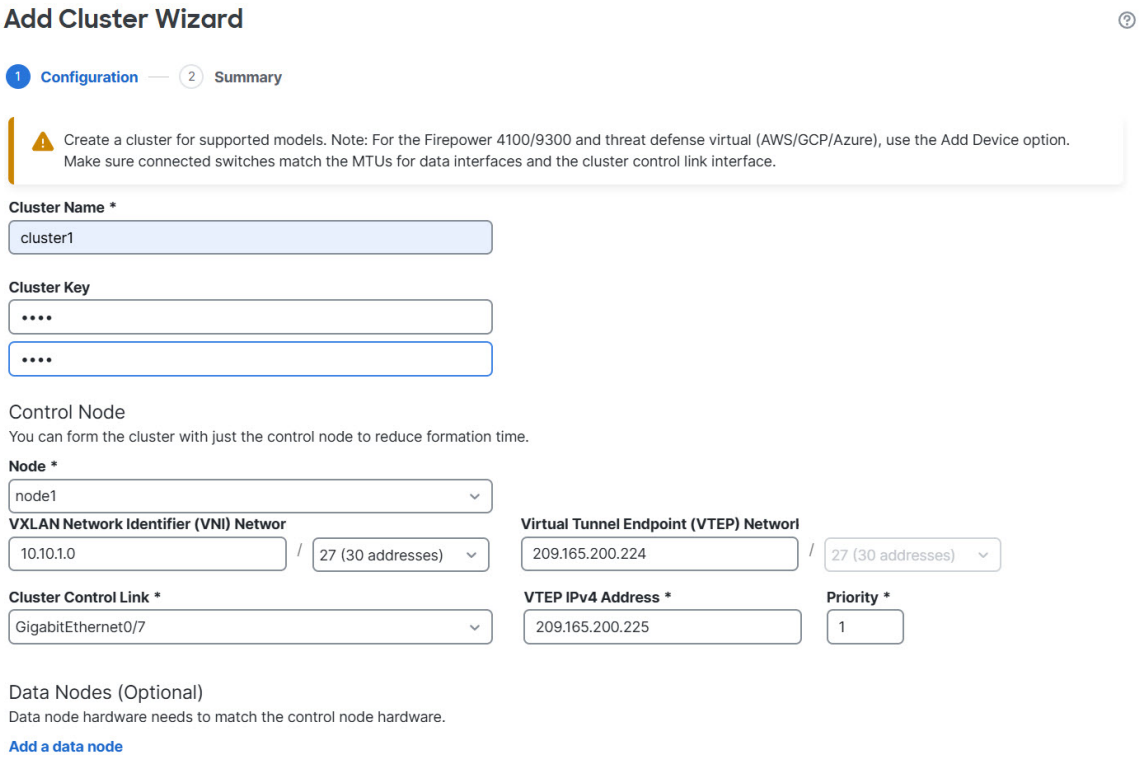
某些功能与集群不兼容，因此应等到启用集群后再执行配置。如果已配置某些功能，则会阻止集群的创建。例如，不要在接口或不支持的接口类型（例如 BVI）上配置任何 IP 地址。

过程

步骤 1 选择 **设备** > **设备管理**，然后选择**添加** > **集群**。

出现**添加集群向导 (Add Cluster Wizard)**。

图 *167:* 添加集群向导



步骤 2 为控制流量指定**集群名称 (Cluster Name)** 和身份验证**集群密钥 (Cluster Key)**。

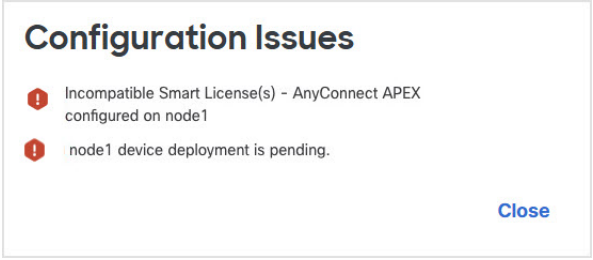
- **集群名称 (Cluster Name)** - 1 到 38 个字符的 ASCII 字符串。
- **集群密钥 (Cluster Key)** - 1 到 63 个字符的 ASCII 字符串。 **集群密钥 (Cluster Key)** 值用于生成加密密钥。此加密不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 3 对于**控制节点**，请进行以下设置：

- **节点 (Node)** - 选择一开始要作为控制节点的设备。当 防火墙管理中心 形成集群时，它会首先将此节点添加到集群，因此它将成为控制节点。

  注释
  如果您在节点名称旁边看到一个 **错误** ( ) 图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。例如：

图 *168:* 配置问题



要解决上述问题，请删除不支持的 VPN 许可证，并将待处理的配置更改部署到设备。

- **VXLAN 网络标识符 (VNI) 网络 (VXLAN Network Identifier [VNI] Network)** - 为 VNI 网络指定 IPv4 子网；该网络不支持 IPv6。指定 **24**、**25**、**26** 或 **27** 子网。IP 地址将被自动分配给此网络上的每个节点。VNI 网络是在物理 VTEP 网络上运行的加密虚拟网络。
- **集群控制链路 (Cluster Control Link)** - 选择要用于集群控制链路的物理接口。
- **虚拟隧道终端 (VTEP) 网络 (Virtual Tunnel Endpoint [VTEP] Network)** - 为物理接口网络指定 IPv4 子网；该网络不支持 IPv6。VTEP 网络与 VNI 网络不同，它被用于物理集群控制链路。
- **VTEP IPv4 地址 (VTEP IPv4 Address)** - 此字段将自动填充 VTEP 网络上的第一个地址。
- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。即使您将优先级设置为低于其他节点，在首次建立集群时，此节点仍将作为控制节点。

步骤 4 对于**数据节点**（**可选**），点击**添加数据节点 (Add a data node)** 以便将节点添加到集群。

您可以仅使用控制节点建立集群，以便加快集群建立的速度，也可以立即添加所有节点。为每个数据节点设置以下内容：

- **节点 (Node)** - 选择要添加的设备。

  注释
  如果您在节点名称旁边看到一个 **错误** ( ) 图标，请点击该图标以查看配置问题。您必须取消建立集群，解决问题，然后再返回到建立集群。

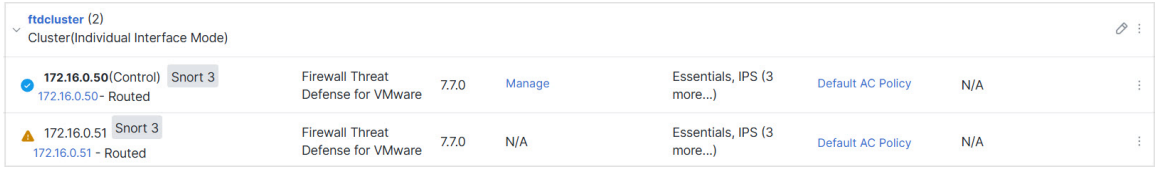
- **VTEP IPv4 地址 (VTEP IPv4 Address)** - 此字段将自动填充 VTEP 网络上的下一个地址。
- **优先级 (Priority)** - 设置控制节点选择的此节点的优先级。优先级的值为 1 到 100，其中 1 为最高优先级。

步骤 5 点击**继续**。查看**摘要**，然后点击**保存**。

集群引导程序配置会被保存到集群节点。引导程序配置包括用于集群控制链路的 VXLAN 接口。

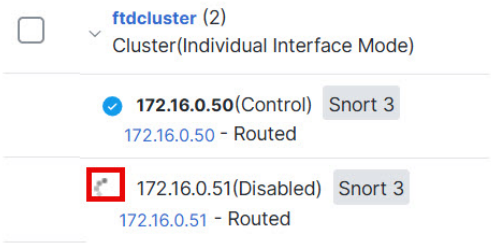
集群名称显示在 **设备** > **设备管理** 页面上；展开集群可查看集群节点。

图 *169:* 集群管理

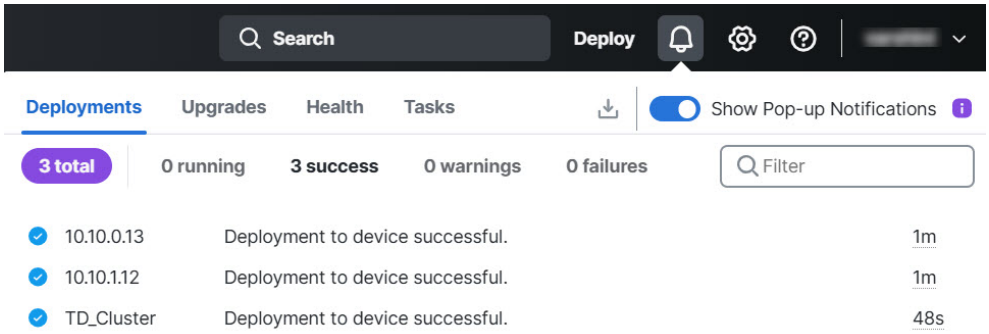


当前正在注册的节点会显示加载图标。

图 *170:* 节点注册



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。防火墙管理中心 会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

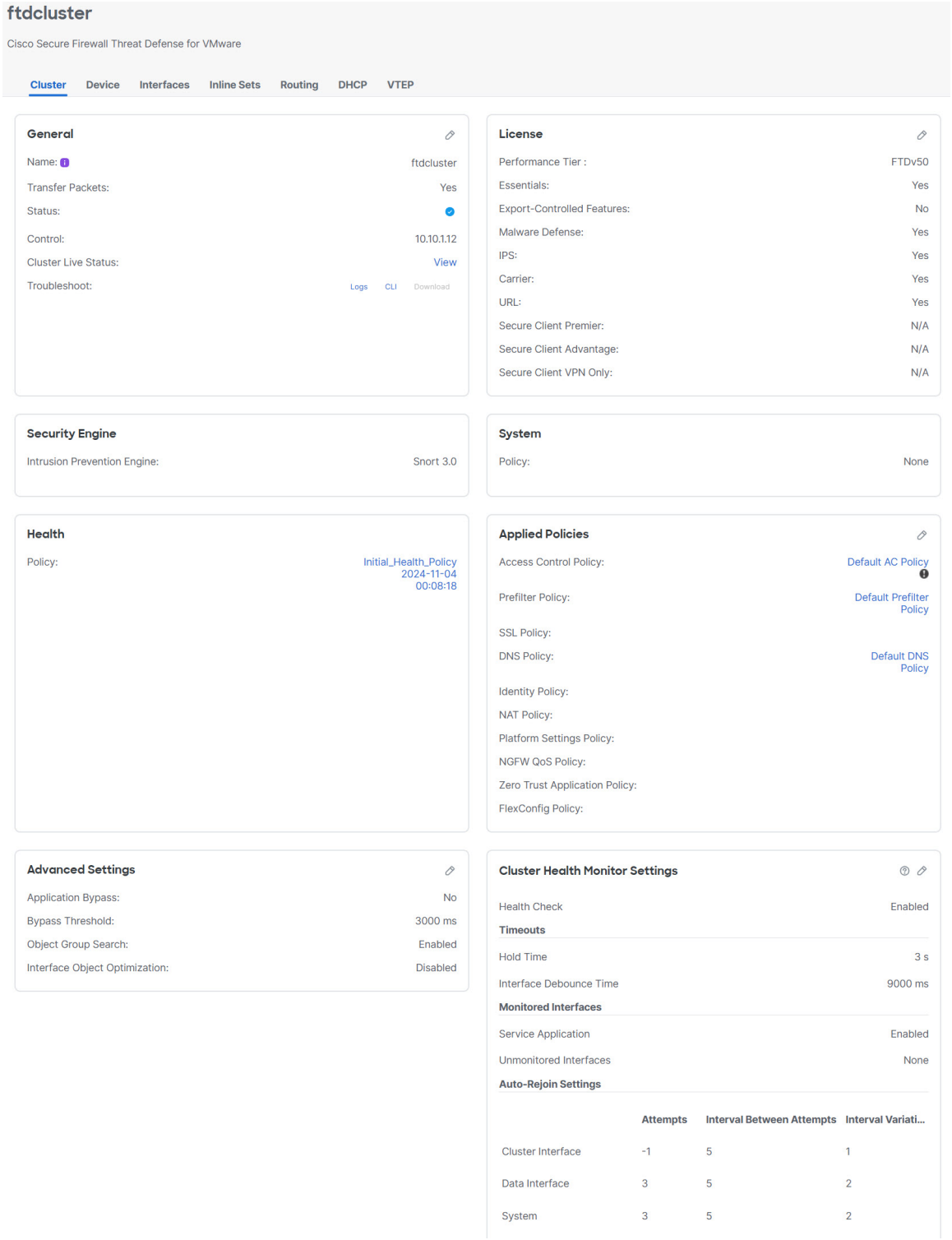


步骤 6 通过点击集群的 **编辑** (✎)，配置设备特定设置。

大多数配置可以应用于整个集群，而不适用于集群中的节点。例如，可以更改每个节点的显示名称，但只能配置整个集群的接口。

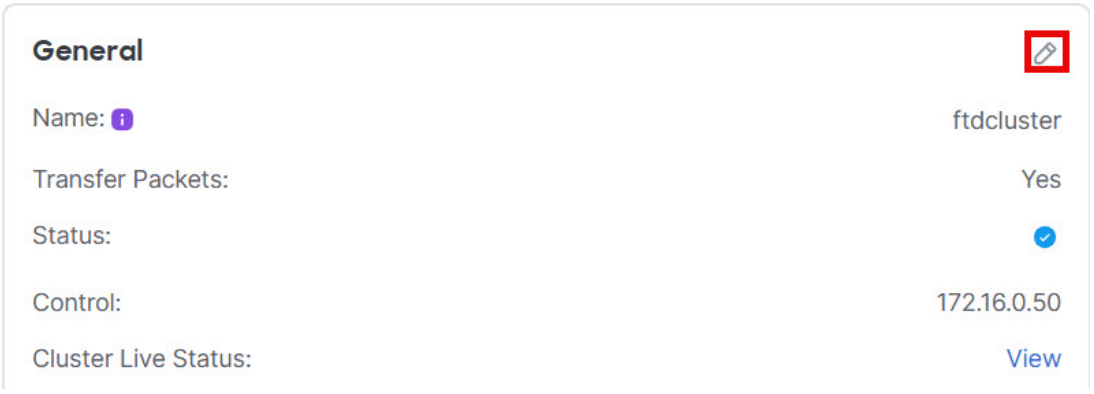
步骤 7 在 **设备** > **设备管理** 的**集群**屏幕上，您可以看到集群的**常规**和其他设置。

图 *171:* 集群设置

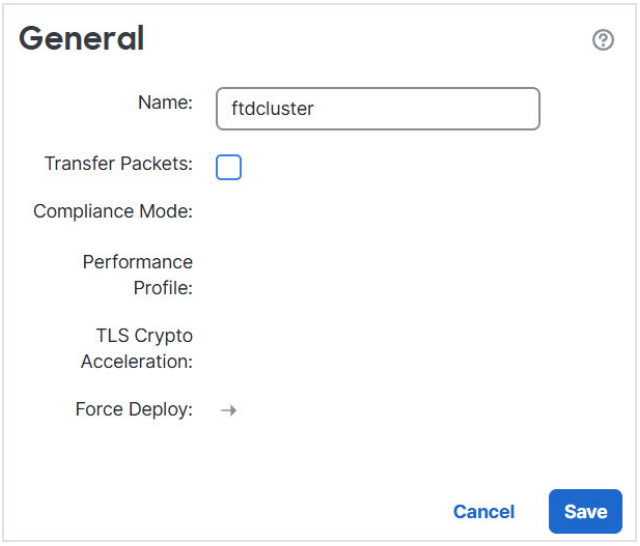


请参阅常规 **(General)** 区域中的以下集群特定项：

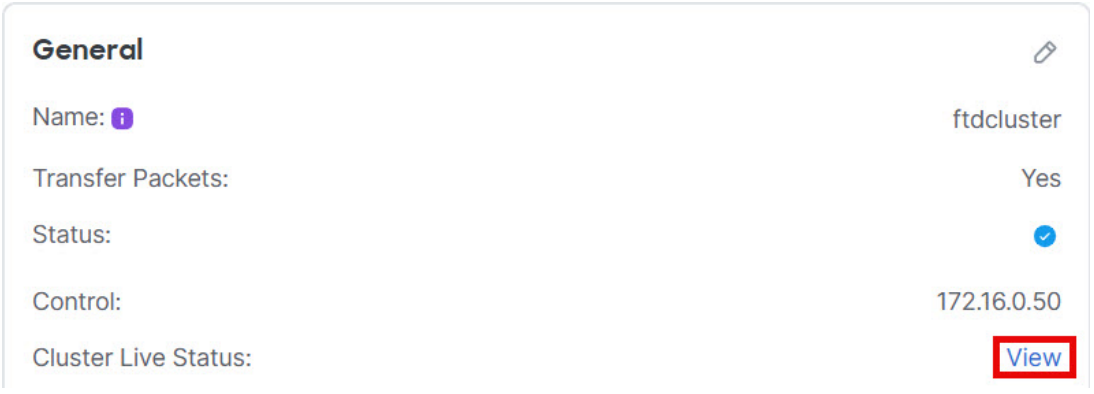
- **常规 (General) > 名称 (Name)** - 通过点击 **编辑** (✎)更改集群显示名称。



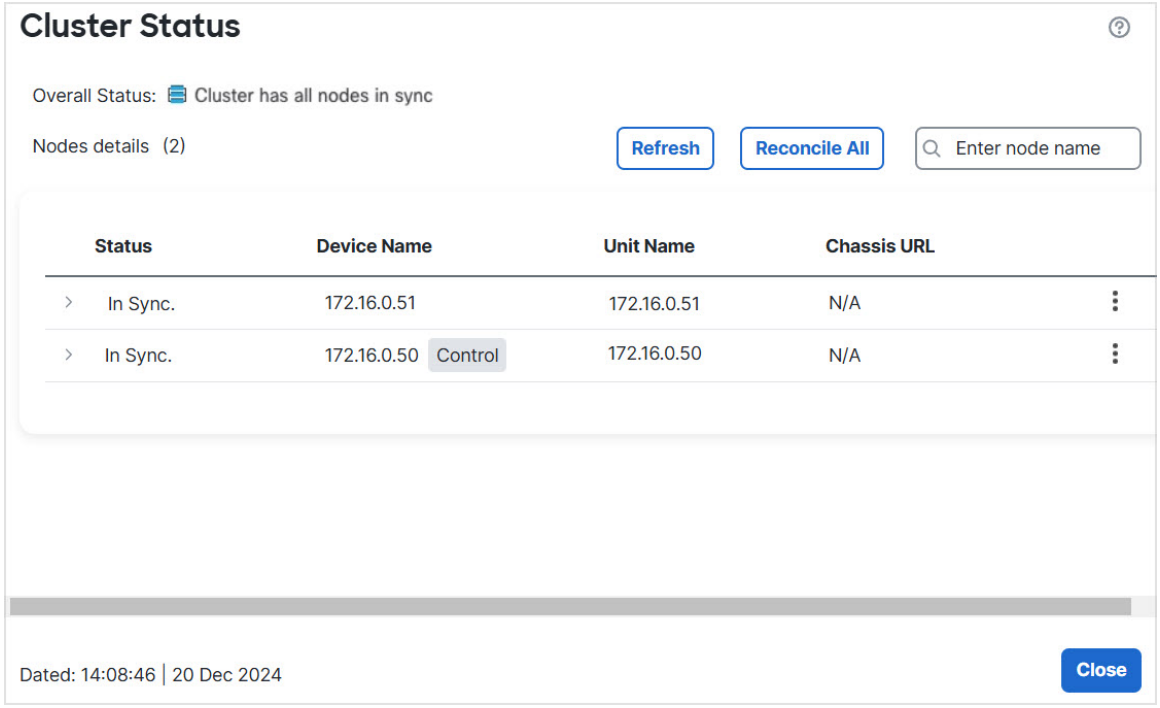
然后设置 **名称** 字段。



- **常规 (General) > 查看 (View)** - 点击**查看 (View)** 链接以打开**集群状态 (Cluster Status)** 对话框。

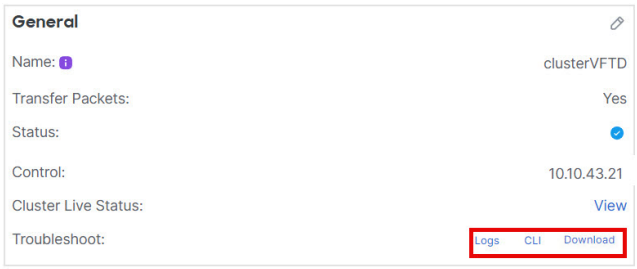


还可在**集群状态 (Cluster Status)** 对话框中点击**协调全部 (Reconcile All)**以重新注册数据单元。您还可以从节点 ping 通集群控制链路。请参阅在集群控制链路上执行 Ping，第 484 页。



- **常规 > 故障排除**- 可以生成和下载故障排除日志，还可以查看集群 CLI。请参阅群集技术故障排除：私有云，第 484 页。

图 *172:* 故障排除



步骤 8 在 **设备 > 设备管理** 上，然后点击**添加 > 设备**，您可以从右上角的下拉菜单中选择集群中的每个成员并配置以下设置。

图 *173:* 设备设置

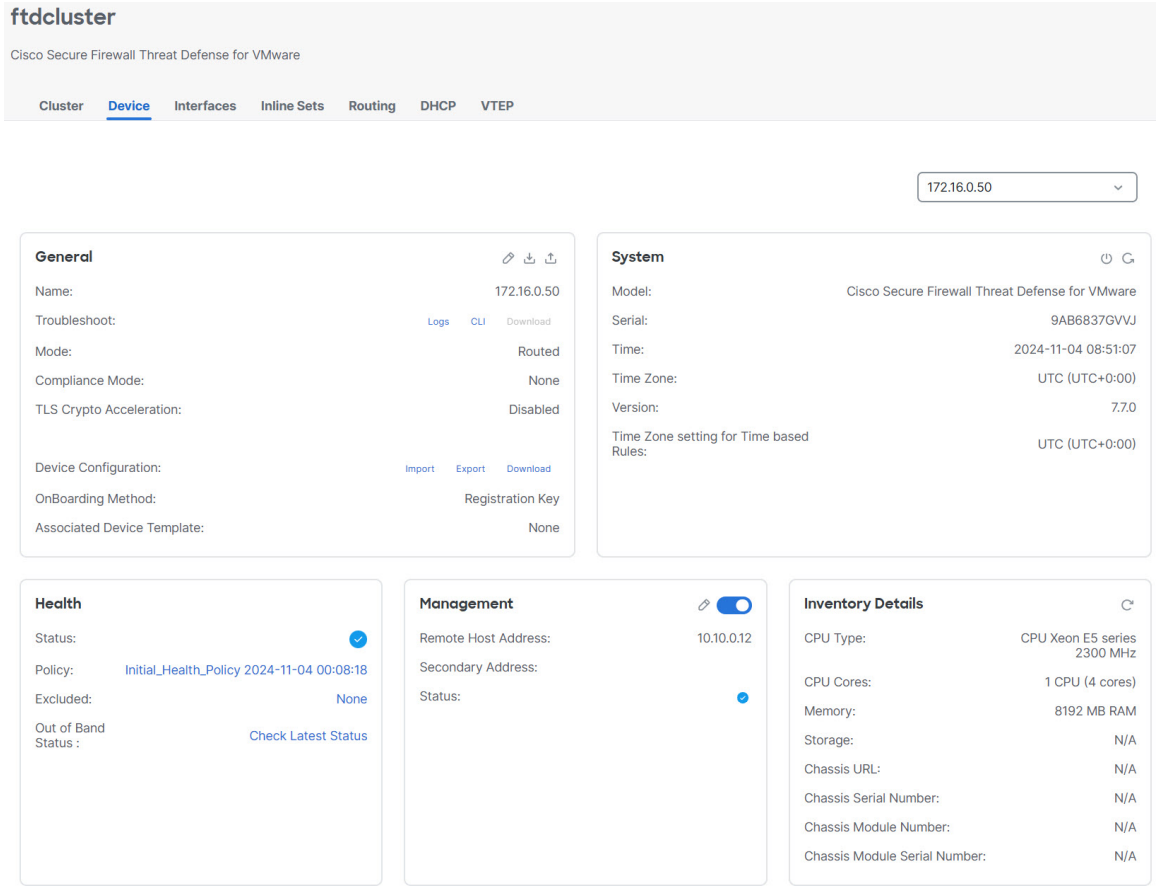
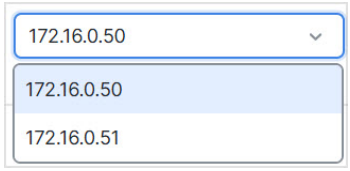
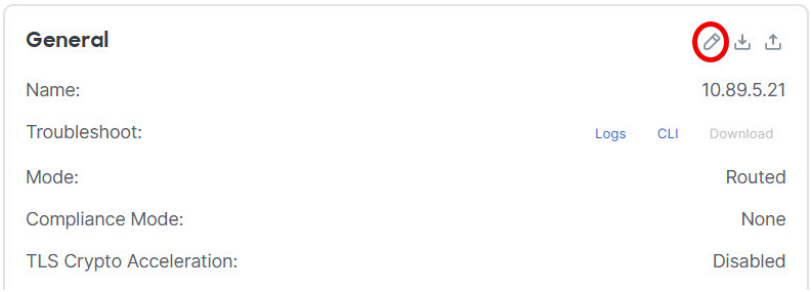


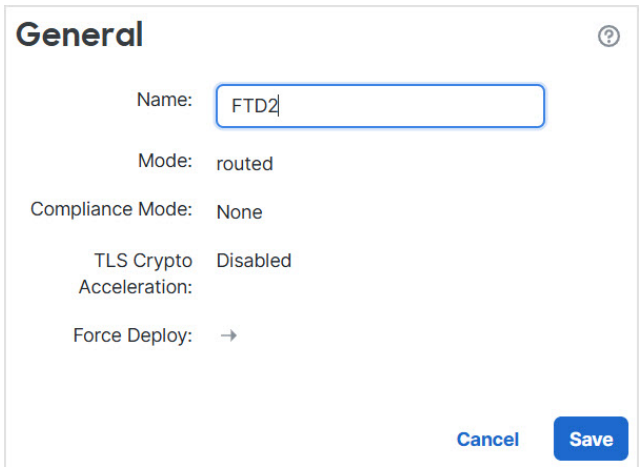
图 *174:* 选择节点



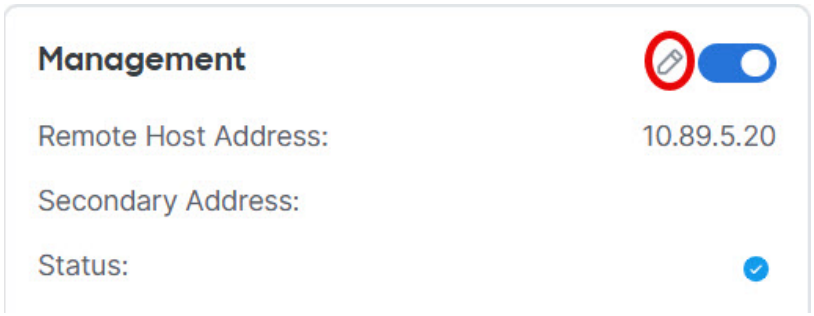
- **常规 (General) > 名称 (Name)** - 通过点击 **编辑** (✎)更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理 (Management) > 主机 (Host)**-如果在设备配置中更改了管理 IP 地址，则必须在 防火墙管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备。首先禁用连接，编辑**管理 (Management)** 区域中的**主机 (Host)** 地址，然后重新启用连接。



步骤 9 如果在未启用极大帧预留的情况下部署集群节点，则重新启动所有集群节点，以便启用集群控制链路所需的极大帧。请参阅关闭或重新启动设备，第 64 页。

如果您之前启用了极大帧预留，则可以跳过这一步。

由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）和 VXLAN 开销（54 字节）。创建集群时，MTU 会被设置为比最高数据接口 MTU（默认为 1654）高 154 个字节。如果后来增加数据接口 MTU，请务必同时增大集群控制链路 MTU。例如，由于最大 MTU 为 9198 字节，因此最高的数据接口 MTU 可以是 9044，而集群控制链路则可以设置为 9198。请参阅配置 MTU，第 819 页。

确保将连接到集群控制链路的交换机配置为正确的（更高的）MTU；否则，集群形成可能会失败。

配置接口

本节介绍如何将接口配置为与集群兼容的独立接口。独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于当前的控制节点。所有数据接口都必须是独立接口。

注释 您不能使用子接口。

过程

步骤 1 选择 **对象** > **地址池** 以添加 IPv4 和/或 IPv6 地址池。请参阅地址池，第 2630 页。

至少包含与集群中的设备数量相同的地址。虚拟 IP 地址不属于此池，但需要位于同一网络中。无法提前确定分配到每台设备的确切本地地址。

步骤 2 选择 **设备** > **设备管理**，然后点击集群的 **编辑** (✎)。

步骤 3 点击**接口 (Interfaces)**，然后点击一个数据接口的 **编辑** (✎)。

步骤 4 在 **IPv4**上，输入 **IP 地址** 和掩码。此 IP 地址是集群的固定地址，始终属于当前的控制设备。

步骤 5 从 **IPv4 地址池 (IPv4 Address Pool)** 下拉列表中，选择您创建的地址池。

注释
如果要手动将 MAC 地址分配给此接口，则需要使用 FlexConfig 来创建一个 **mac-address pool**。

步骤 6 在 **IPv6** > **基本**的 **IPv6 地址池**下拉列表中，选择您创建的地址池。

步骤 7 按正常方式配置其他接口设置。

步骤 8 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *175:* 集群运行状况监控设置

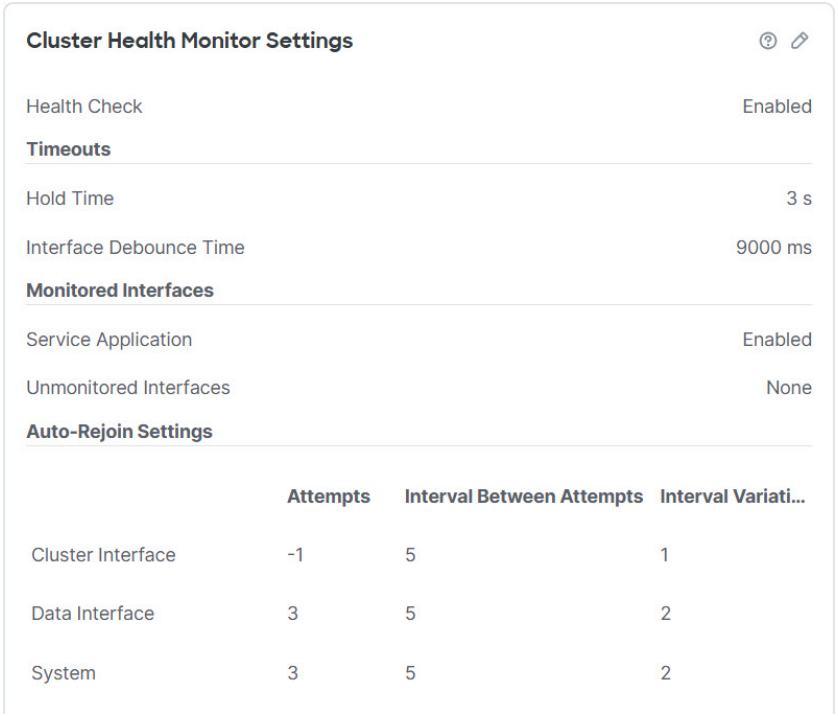


表 *33:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。

字段	说明
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。



注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

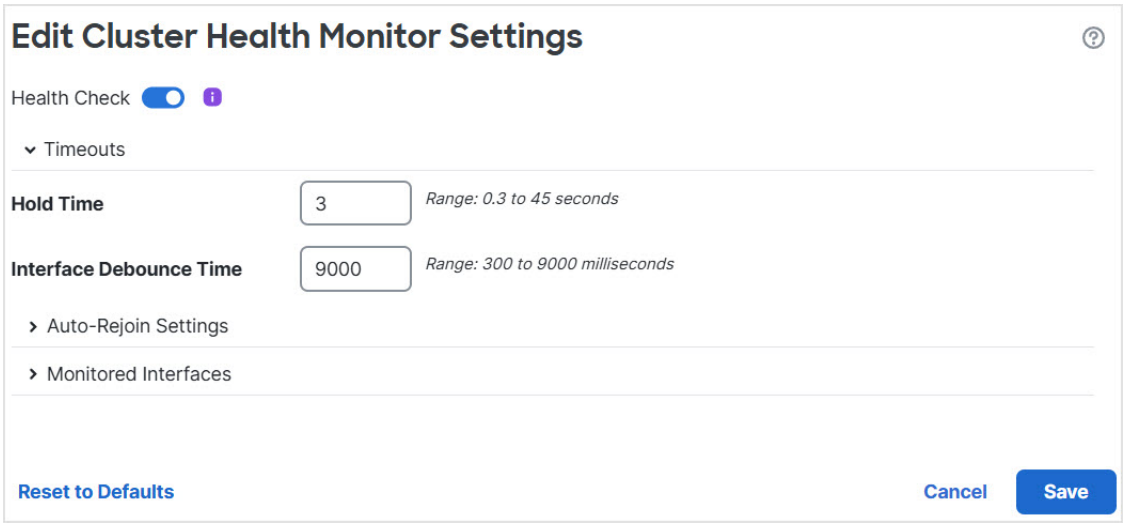
步骤 2 在要修改的集群旁边，点击 **编辑** (✎)。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *176:* 禁用系统运行状况检查



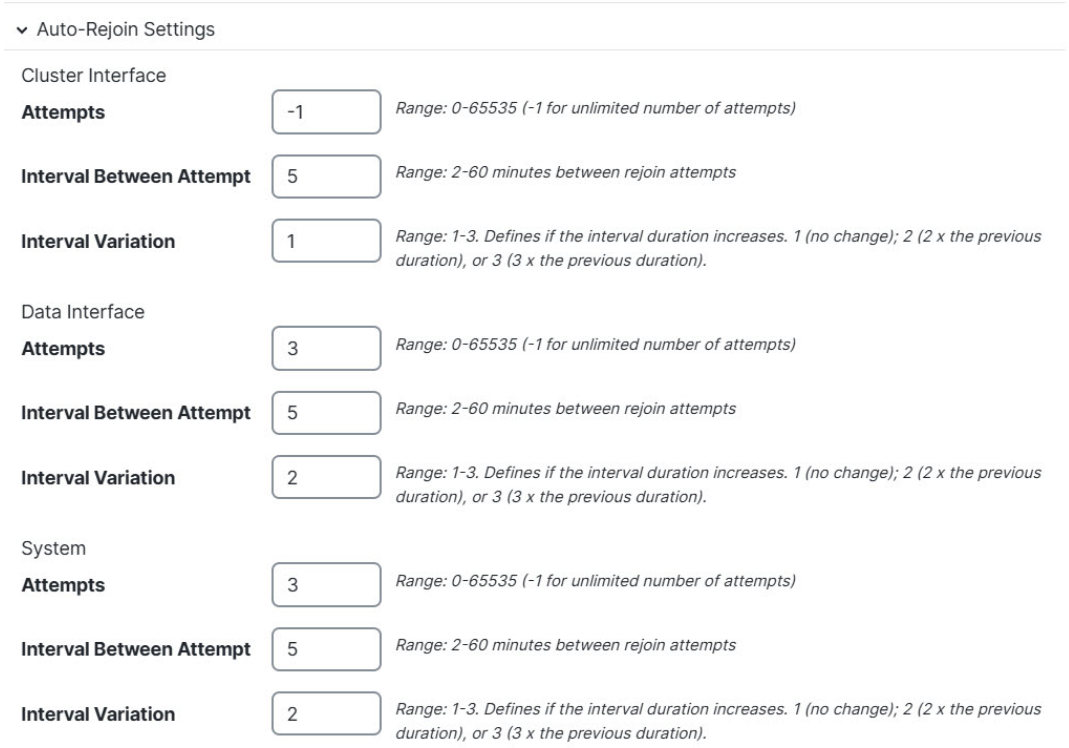
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *177:* 配置自动重新加入设置

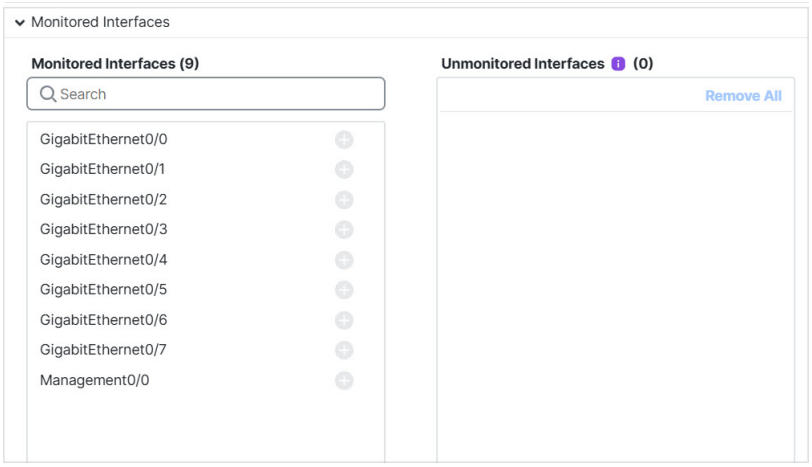


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *178:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改，第 180 页。

管理集群节点

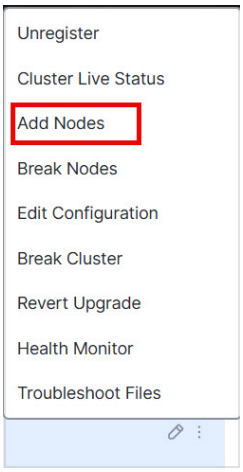
添加新的集群节点

您可以将一个或多个新的集群节点添加到现有的集群。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**添加节点**。

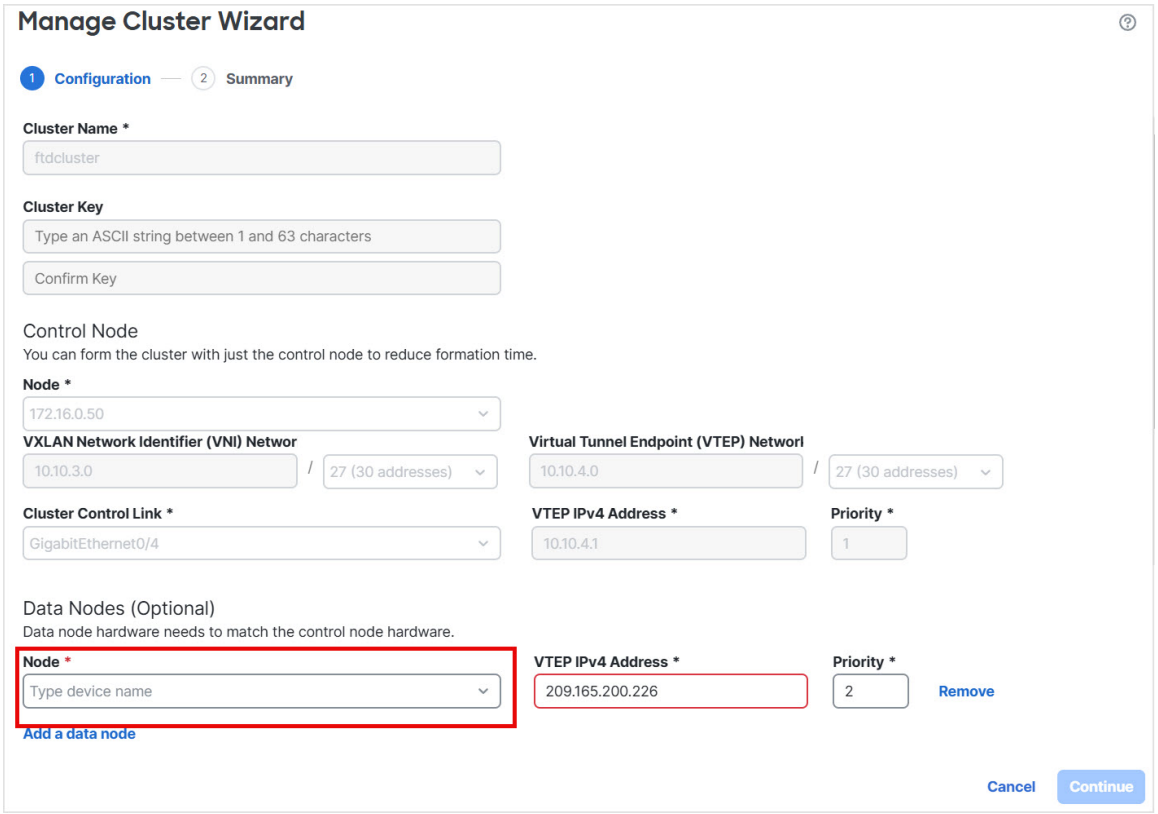
图 *179:* 添加节点



系统将显示**管理集群向导 (Manage Cluster Wizard)**。

步骤 2 从**节点 (Node)** 菜单中选择设备，然后根据需要调整 IP 地址和优先级。

图 *180:* 管理集群向导

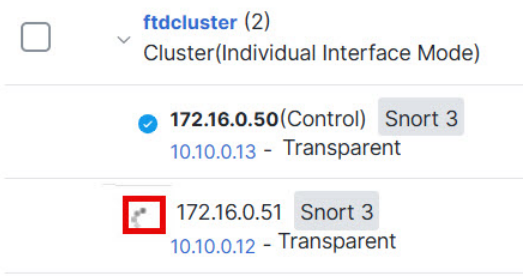


步骤 3 要添加其他节点，请点击**添加数据节点 (Add a data node)**。

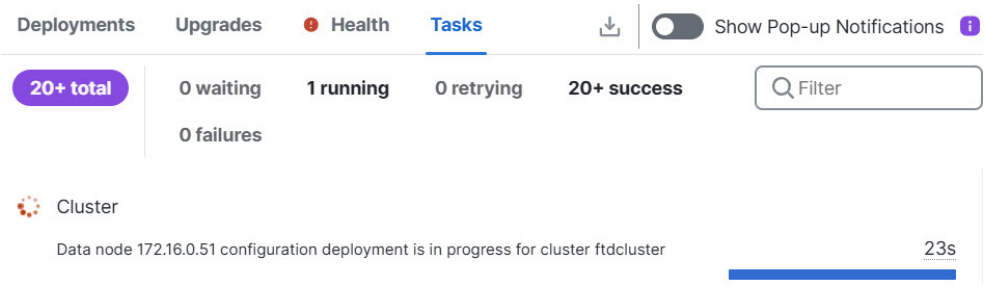
步骤 4 点击**继续**。查看**摘要**，然后点击**保存**

当前正在注册的节点会显示加载图标。

图 *181:* 节点注册



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群节点的注册情况。



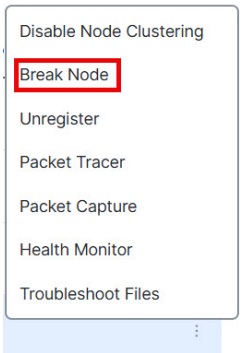
中断节点

您可以从集群中删除节点，使其成为一个独立设备。除非中断整个集群，否则您无法中断控制节点。数据节点的配置已被清除。

过程

步骤 1 选择 **设备 > 设备管理**，点击要中断的节点的 **更多** (⋮)，然后选择**中断节点**。

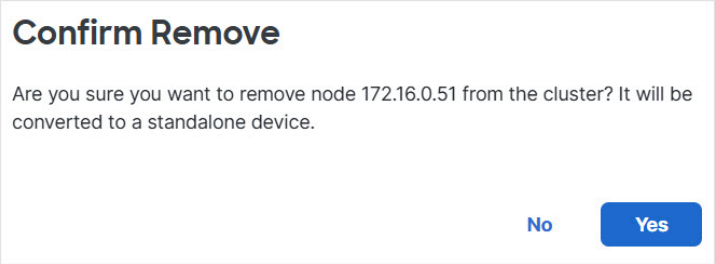
图 *182:* 中断节点



您可以选择通过选择**中断节点 (Break Nodes)** 从集群的“更多”(More) 菜单中断一个或多个节点。

步骤 2 系统会提示您确认中断；点击**是**。

图 ***183:*** 确认中断



您可以通过点击**通知 (Notifications)** 图标并选择**任务 (Tasks)** 来监控集群节点中断。

中断集群

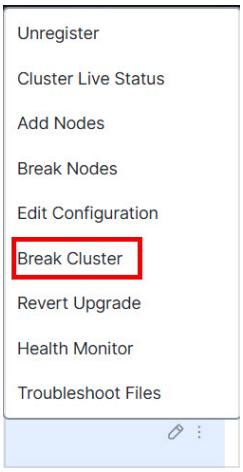
您可以中断集群并将所有节点都转换为独立设备。控制节点会保留接口和安全策略配置，而数据节点则会清除其配置。

过程

步骤 1 确保所有集群节点都由 防火墙管理中心 通过协调节点来管理。请参阅调整集群节点，第 476 页。

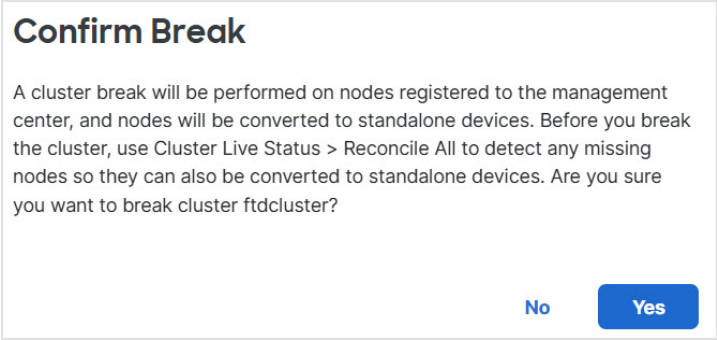
步骤 2 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**中断集群**。

图 ***184:*** 中断集群



步骤 3 系统会提示您断开集群；点击**是**。

图 *185:* 确认中断



您可以通过点击 **通知 (Notifications)** 图标并选择 **任务 (Tasks)** 来监控集群中断。

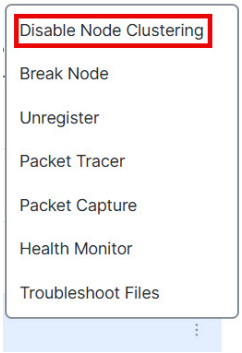
禁用集群

您可能需要停用节点，以准备删除节点，或临时进行维护。此程序旨在暂时停用节点；节点仍将显示在 防火墙管理中心 设备列表中。当节点变为非活动状态时，所有数据接口都将关闭。

过程

步骤 1 对于要禁用的设备，请选择**设备 (Devices)** > **设备管理 (Device Management)**，点击 **更多** (⋮)，然后选择**禁用节点集群 (Disable Node Clustering)**。

图 *186:* 禁用集群



如果在控制节点上禁用集群，则其中一个数据节点将成为新的控制节点。请注意，对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。如果控制节点是集群中的唯一节点，则无法在该控制节点上禁用集群。

步骤 2 确认要在节点上禁用集群。

该节点在 **设备** > **设备管理** 列表中其名称旁边会显示（**已禁用**）。

步骤 3 重新启用集群，请参阅 重新加入集群，第 473 页。

重新加入集群

如果从集群中删除了某个节点（例如对于出现故障的接口），或者如果您手动禁用集群，必须手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除节点的原因的更多信息，请参阅重新加入集群，第 492 页。

过程

步骤 1 对于要重新激活的设备，请选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**启用节点集群**。

步骤 2 确认要在节点上启用集群。

更改控制节点

⚠

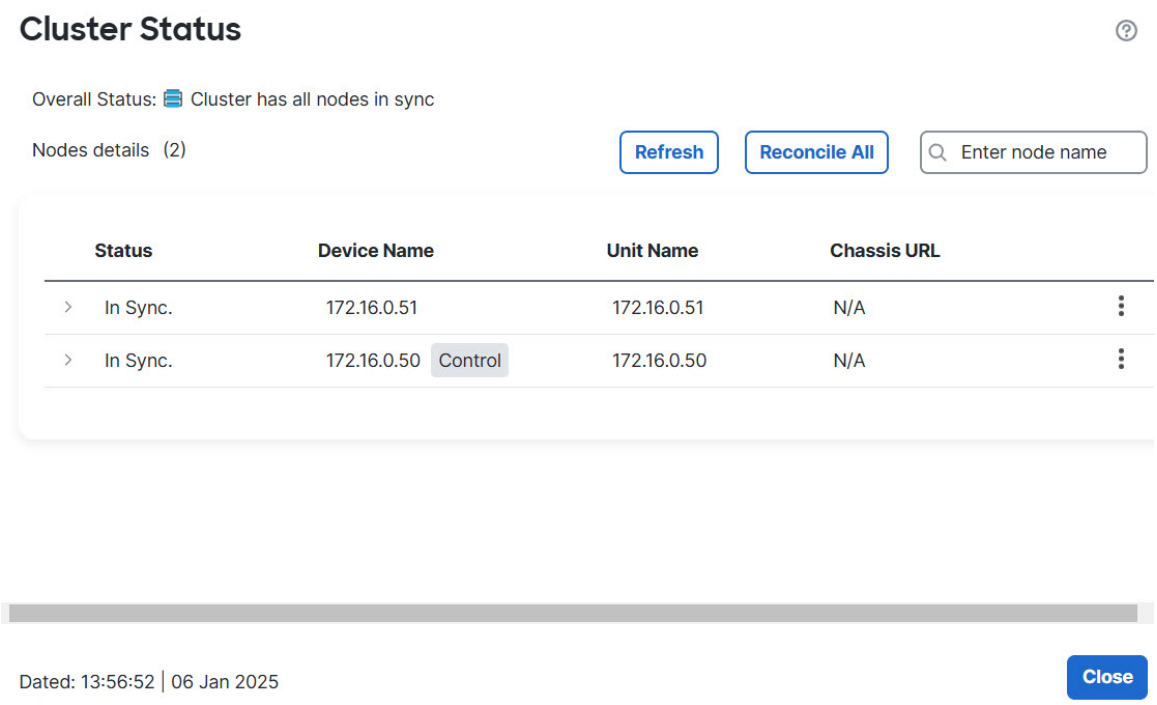
注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体单元，请使用本节中的程序。请注意，对集中功能而言，如果使用任何一种方法来强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

过程

步骤 1 通过选择 **设备** > **设备管理**、**更多** (⋮) > **集群实时状态**打开**集群状态**对话框。

图 *187:* 集群状态



步骤 2 对于要成为控制设备的设备，请选择 **更多** (⋮) > **将角色更改为控制**。

步骤 3 系统将提示您确认角色更改。选中该复选框，然后点击 **确定**。

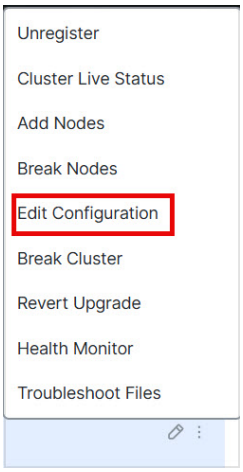
编辑集群配置

您可以编辑集群配置。如果您更改节点或节点优先级的 VTEP IP 地址之外的任何值，则集群将被自动中断和重组。在重组集群之前，您可能会遇到流量中断。如果您更改节点或节点优先级的 VTEP IP 地址，则只有受影响的节点会中断并重新添加到集群。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群的 **更多** (⋮)，然后选择**编辑配置**。

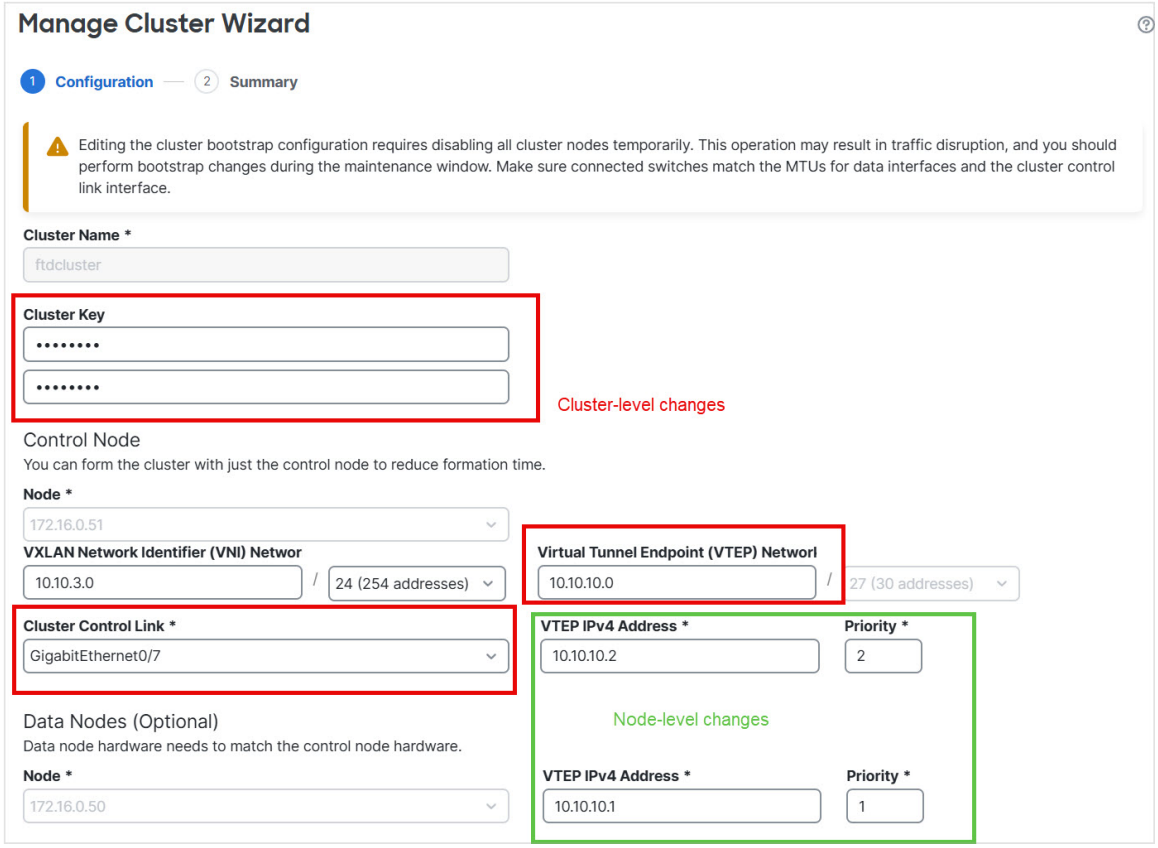
图 *188:* 编辑配置



系统将显示管理集群向导 **(Manage Cluster Wizard)**。

步骤 2 更新集群配置。

图 *189:* 管理集群向导



步骤 3 点击**继续**。查看**摘要**，然后点击**保存**

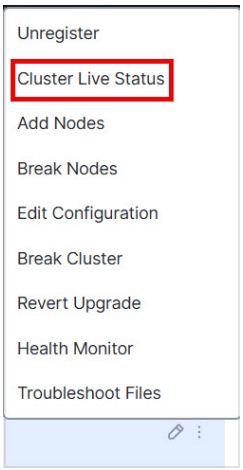
调整集群节点

如果集群节点注册失败，则可将集群成员身份从设备协调至防火墙管理中心。例如，数据节点在防火墙管理中心 被占用或存在网络问题时注册失败的情况下。

过程

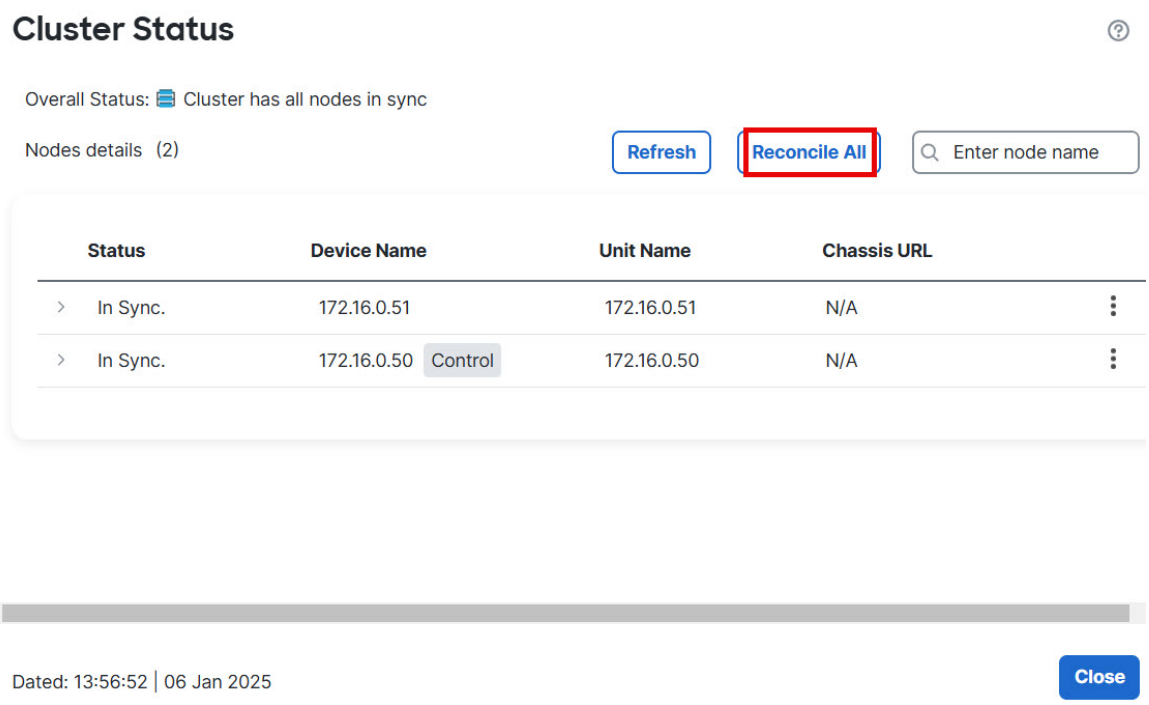
步骤 1 选择集群的 **设备** > **设备管理** **更多** (⋮)，然后选择**集群实时状态**，以打开**集群状态**对话框。

图 ***190:*** 集群实时状态



步骤 2 点击**协调全部 (Reconcile All)**。

图 *191:* 协调全部



有关集群状态的详细信息，请参阅监控集群：私有云 ，第 478 页。

删除（注销）集群或节点并注册到新集群 防火墙管理中心

您可以从 防火墙管理中心 中取消注册集群，从而使集群保持不变。如果要将集群添加到新的 防火墙管理中心，则可能需要取消注册该集群。

您还可以从 防火墙管理中心 取消注册节点，而不会中断集群中的节点。虽然该节点不会显示在 防火墙管理中心 中，但它仍然是集群的一部分，并且它会继续传递流量，甚至可能成为控制节点。您无法取消注册当前的控制节点。如果无法再从防火墙管理中心访问该节点，您可能会希望将其取消注册，但在排除管理连接故障时，您仍希望将其作为集群的一部分。

取消注册集群：

- 会切断 防火墙管理中心和该集群之间的所有通信。
- 从 **设备管理** 页面删除集群。
- 如果集群的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将集群返回本地时间管理。
- 保持配置不变，以便集群继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将集群再次注册到相同或不同的防火墙管理中心会导致配置被删除，因此集群将在该点停止处理流量；集群配置保持不变，因此您可以将集群作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

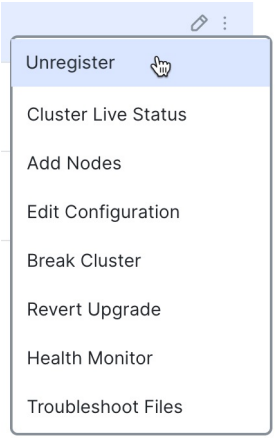
开始之前

此过程需要 CLI 对一个节点拥有访问权限。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群或节点的 **更多** (⋮)，然后选择**取消注册**。

图 *192:* 取消注册集群或节点



步骤 2 系统会提示您取消注册集群或节点；点击**是**。

步骤 3 您可以通过将其中一个集群成员添加为新设备来将集群注册到新的（或相同的）防火墙管理中心集群。

a) 连接到一个集群节点的 CLI，并使用 **configure manager add** 命令识别新 防火墙管理中心。请参阅 在 CLI 中修改威胁防御管理接口。

b) 选择 **设备** > **设备管理**，然后点击**添加设备**。

您只用将其中一个集群节点添加为设备，然后便可发现其余集群节点。

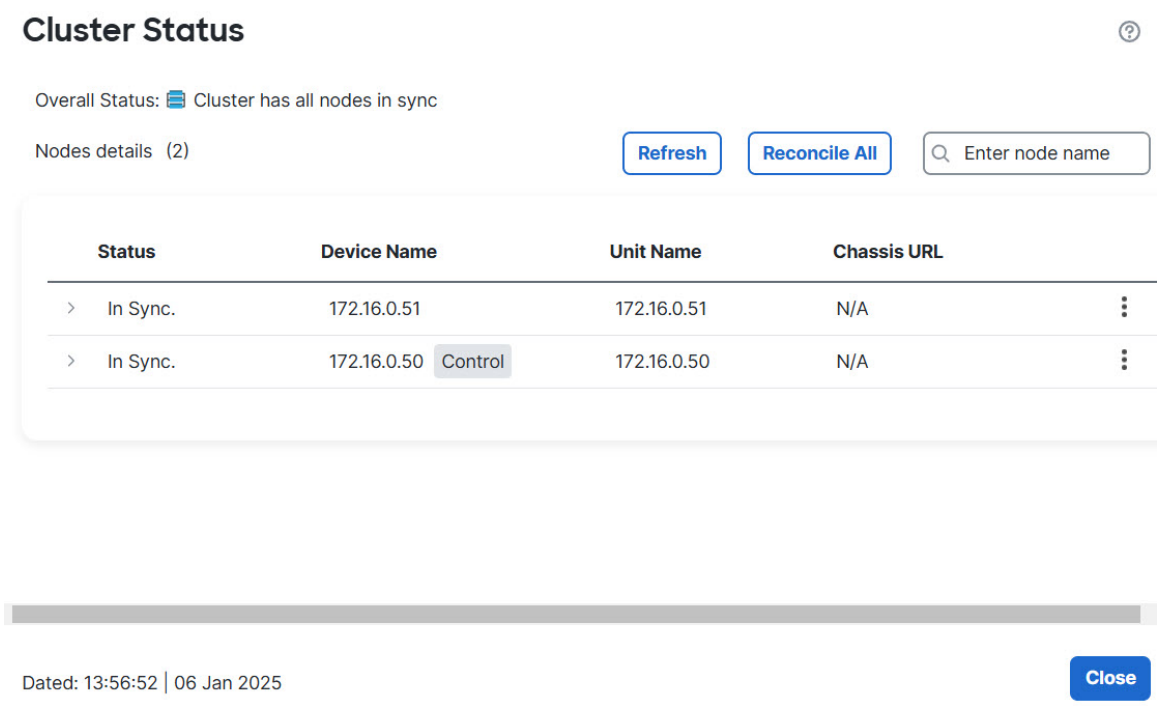
步骤 4 要重新添加已删除的节点，请参阅调整集群节点，第 476 页。

监控集群：私有云

您可以在 防火墙管理中心 中和 Firewall Threat Defense CLI 上监控集群。

- **集群状态**对话框，可从 **设备** > **设备管理**、**更多** (⋮) 图标或 **设备** > **设备管理** 访问，或点击**添加**，选择**集群**页面**常规**区域**集群实时状态**链接。

图 ***193:*** 集群状态



控制节点有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 (In Sync.) - 节点已向 防火墙管理中心 注册。
- 待处理注册 (Pending Registration) - 节点是集群的一部分，但尚未向 防火墙管理中心 注册。如果节点注册失败，则可点击**协调所有 (Reconcile All)** 以重试注册。
- 集群已禁用 (Clustering is disabled) - 节点已向 防火墙管理中心 注册，但它是集群的非活动成员。如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除节点。
- “正在加入集群...”(Joining cluster...) - 节点正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 防火墙管理中心 注册。

对于每个节点，您可以查看**摘要 (Summary)** 或**历史记录 (History)**。

图 *194:* 节点摘要

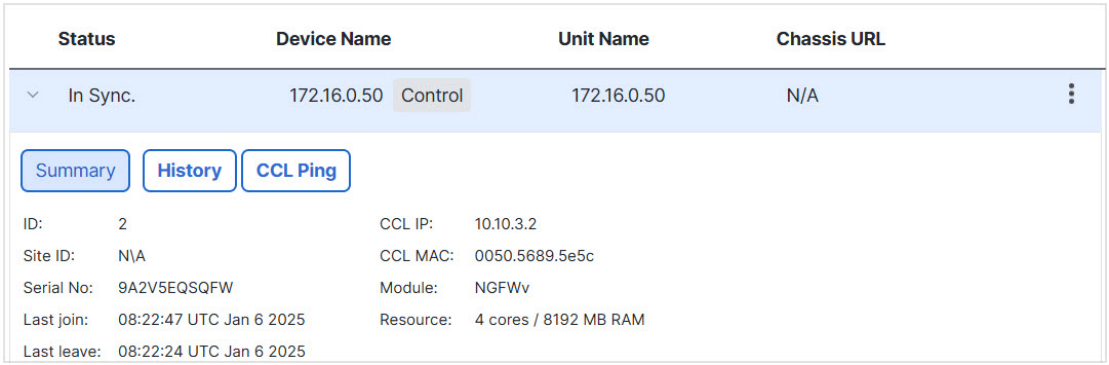
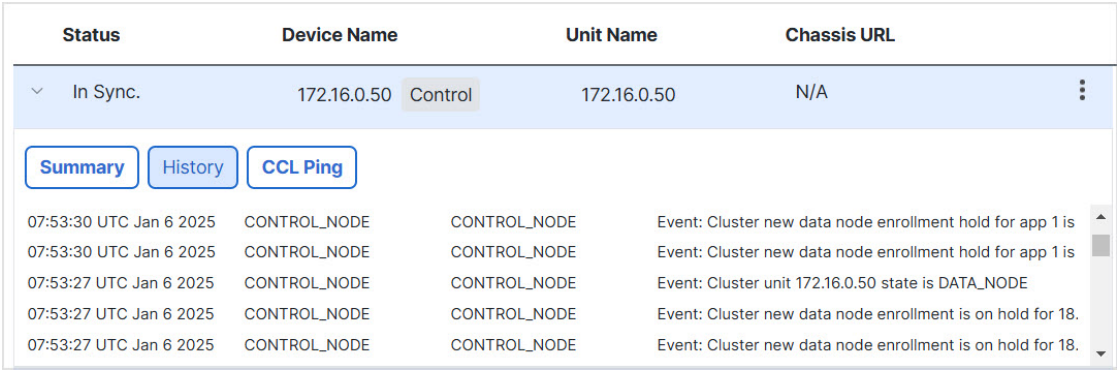


图 *195:* 节点历史记录



- 系统 (⚙) > 任务 页面。

  任务 **(Tasks)** 页面会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

- 设备 > 设备管理 然后点击添加 > 设备 *cluster_name*。

  展开设备列表页面上的集群时，您可以看到所有成员节点，包括 IP 地址旁显示其角色的控制节点。对于仍在注册的节点，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

集群运行状况监控器控制面板

集群运行状况监控器

当 Firewall Threat Defense 是集群的控制节点时， 防火墙管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加（在公共云集群中，不属于防火墙管理中心的其他节点）或 正常（节点的理想状态）。
  - 集群统计信息部分显示集群的当前指标，包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和 NAT 转换。

注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

  - 指标图表（即 CPU 使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。

- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。
  - “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU 使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT 转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。

- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和NAT 转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从防火墙管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（∨） 以展开和折叠托管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 **添加新的控制面板**（+），通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

集群指标

集群运行状况监控器跟踪与集群及其节点相关的统计信息，以及负载分布、性能和CCL流量统计信息的汇总。

表 *34:* 集群指标

指标	说明	格式
CPU	集群节点上的CPU指标平均值（分别针对数据平面和 snort）。	percentage
Memory	集群节点上的平均内存指标（分别用于数据平面和 snort）。	percentage
数据吞吐量	集群的传入和传出数据流量统计信息。	bytes
CCL 吞吐量	集群的传入和传出 CCL 流量统计信息。	bytes
连接	集群中的活动连接计数。	数字
NAT 转换	集群的 NAT 转换计数。	数字
分布	集群中每秒的连接分布计数。	数字
数据包数	集群中每秒的数据包分发计数。	数字

群集技术故障排除：私有云

您可以使用 **CCL Ping** 工具确保集群控制链路正常运行。 您还可以使用以下适用于设备和集群的工具：

- 故障排除文件-如果节点未能加入集群，系统将自动生成故障排除文件。您还可以从 **设备**>**设备管理** > **集群** > **常规** 区域生成和下载故障排除文件。请参阅生成故障排除文件。

  您还可以通过点击 **更多** (⋮) 并选择 **文件故障排除** ，从 **设备管理**页面生成文件。

- CLI 输出-从 **设备** > **设备管理** > **集群** > **常规**区域，您可以查看一组预定义的 CLI 输出，帮助您排除集群的故障。系统会自动为集群运行以下命令：
  - **show running-config cluster**
  - **show cluster info**
  - **show cluster info health**
  - **show cluster info transport cp**
  - **show version**
  - **show asp drop**
  - **show counters**
  - **show arp**
  - **show int ip brief**
  - **show blocks**
  - **show cpu detailed**
  - **show interface** *ccl_interface*
  - **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

  您还可以在命令字段中输入任何 **show** 命令。有关详细信息，请参阅查看 CLI 输出。

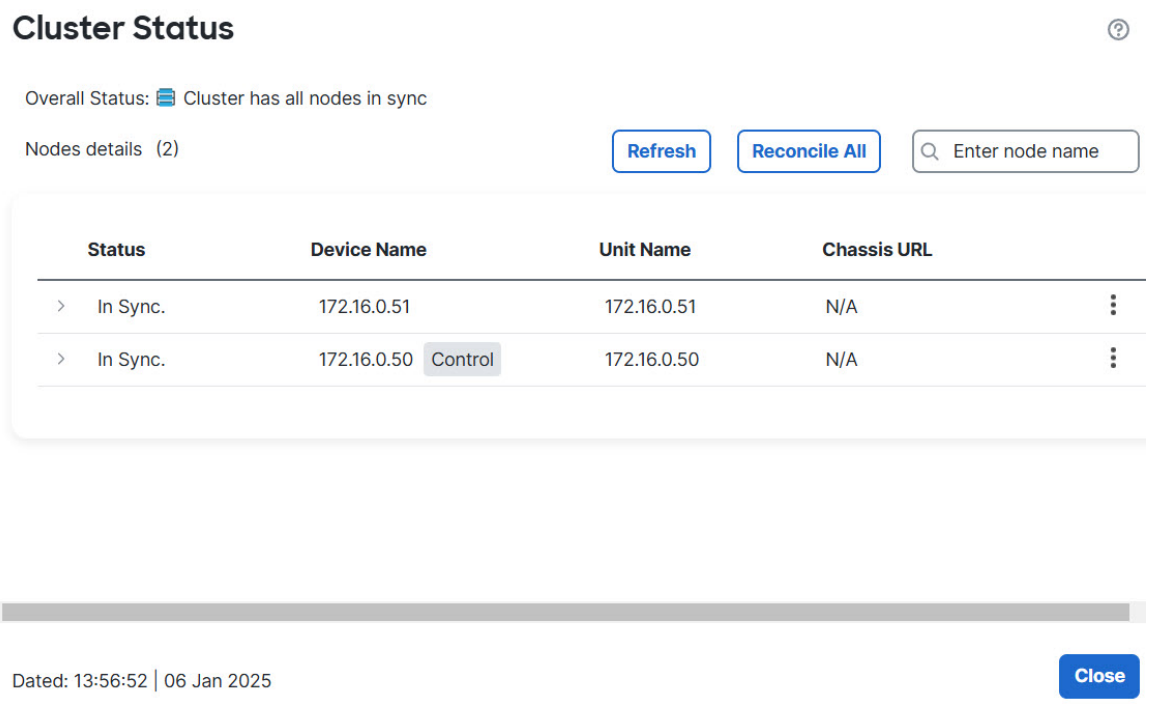
在集群控制链路上执行 Ping

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。如果您遇到集群控制链路连接问题，此工具允许您手动 ping 所有已加入集群的节点。

过程

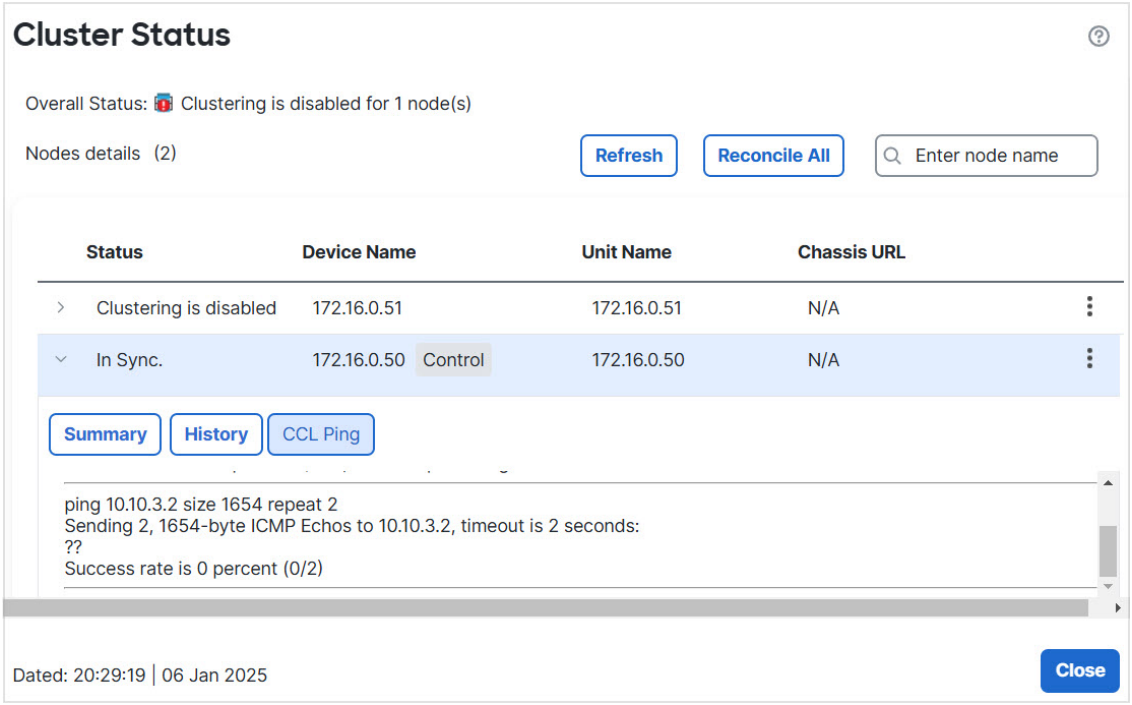
步骤 1 选择 **设备** > **设备管理**，点击集群旁边的 **更多** (⋮) 图标，然后选择**集群实时状态**。

图 ***196:*** 集群状态



步骤 2 展开其中一个节点，然后点击 **CCL Ping**。

图 *197: CCL Ping*



节点使用与最大 MTU 匹配的数据包大小在集群控制链路上向每个其他节点发送 ping 命令。

群集技术参考：私有云

本部分包括有关集群工作原理的详细信息。

威胁防御功能和集群

部分 Firewall Threat Defense 功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

不支持的功能和集群

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略。

- 远程访问 VPN（SSL VPN 和 IPsec VPN）

- 在公共云中不支持站点间 VPN（基于策略和路由）。
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- 防火墙管理中心 UCAPL/CC 模式
- DHCP 客户端、服务器和代理。支持 DHCP 中继。

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。



注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。



注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅 FlexConfig 策略，第 1041 页。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP

- 静态路由监控

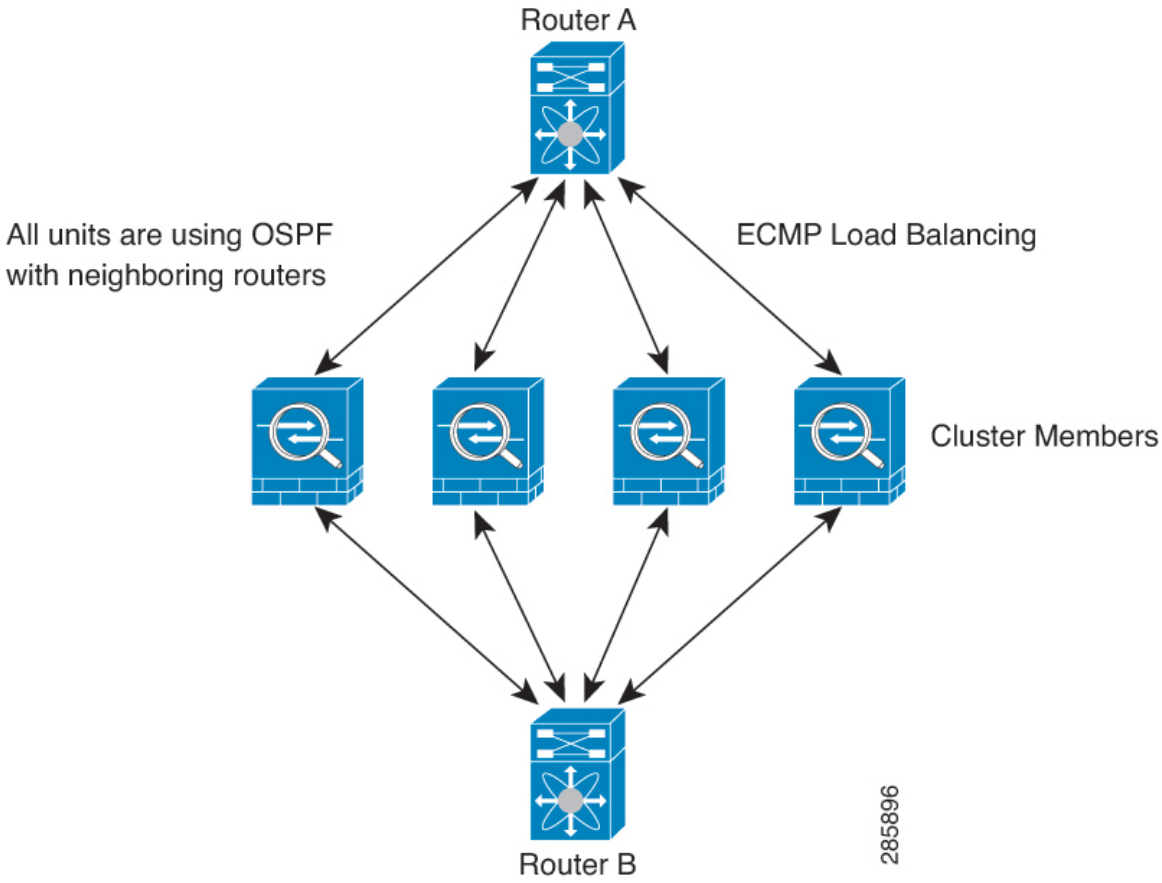
连接设置和集群

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *198:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 Firewall 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 Firewall 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。
- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混

合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。

- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。



注释 集群不支持远程接入 VPN。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。



注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

监控所有物理接口；只能监控已命名的接口。 可以选择性地禁用对每个接口的监控。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。节点将在 500 毫秒后删除。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

Firewall 威胁防御将自动尝试重新加入集群，具体取决于故障事件。

注释 当 Firewall 威胁防御 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。

- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - Firewall Threat Defense 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 Firewall Threat Defense应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。Firewall Threat Defense应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。
- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *35:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	支持	—
动态路由	支持	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。
- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。
- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

端口地址转换连接

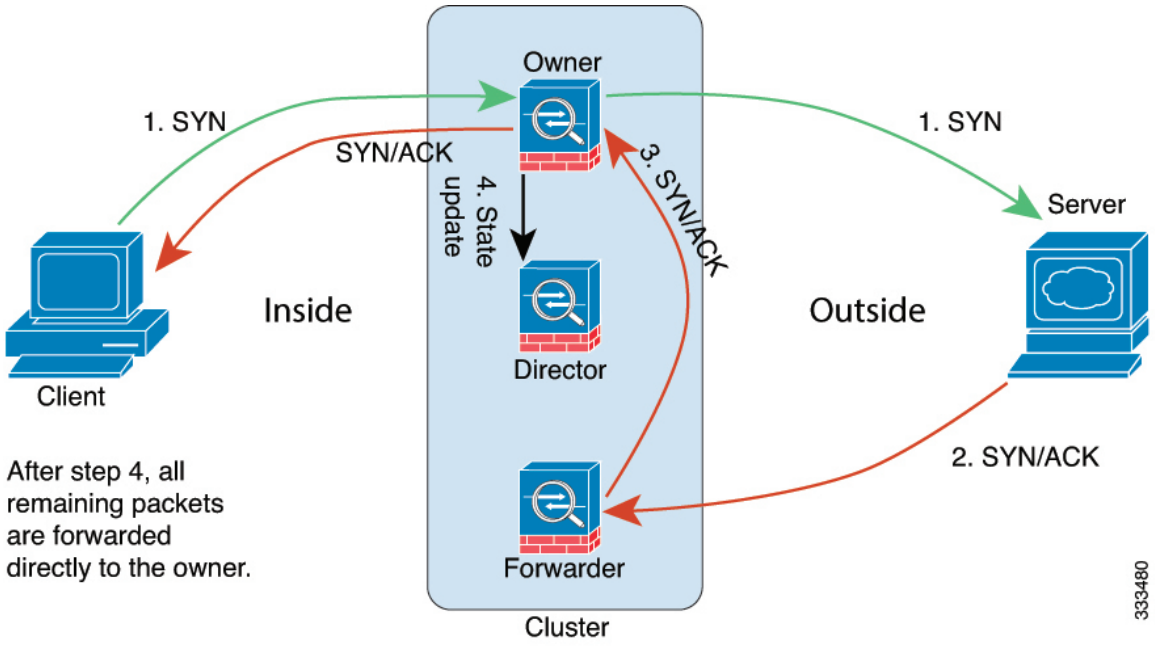
新连接所有权

此版本不支持流量重定向。通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。同一连接的所有后续数据包都应到达同一节点。如果任何连接数据包到达其他节点，它们将被丢弃。如果反向流量到达其他节点，也将被丢弃。对于集中功能，如果连接不到达控制节点，则它们会被丢弃。

默认情况下，AWS GWLB 使用 5 元组来保持流粘性。建议在 AWS GWLB 上启用 2 元组或 3 元组粘性，以确保将相同的流发送到同一节点。

TCP 的数据流示例

以下图例显示了新连接的建立。



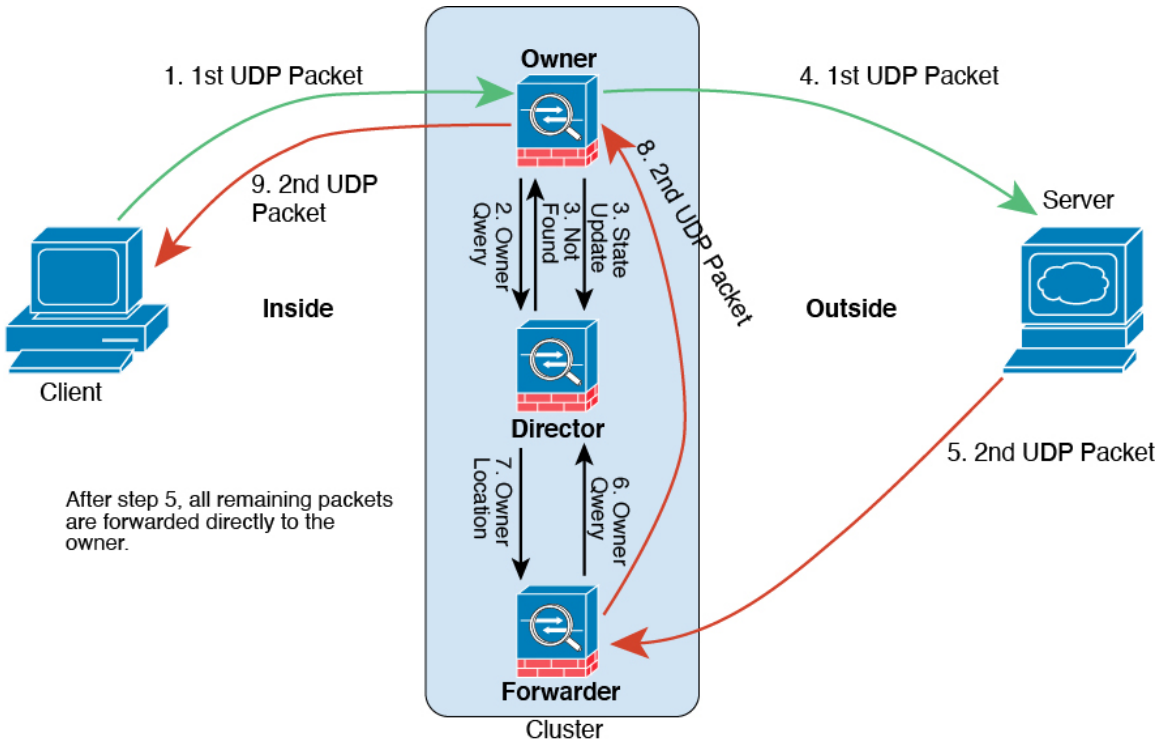
1. SYN 数据包从客户端发出，被传送到一台 Firewall 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。

2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 Firewall 威胁防御（基于负载均衡方法）。此 Firewall 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *199: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个Firewall 威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。

3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

集群的准则：私有云

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群节点加入时的 MTU ping 测试通过尝试较小的 MTU 来提供更多信息	10.0.0	10.0.0	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，它将尝试除以 MTU，并继续除以 2，直到 MTU ping 成功。成功的 ping 值会显示在 **show cluster info trace** 中，因此您可以将 MTU 调整为可用值，然后重试。 即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。 我们建议将交换机 MTU 的大小增加到建议的值，但如果您无法更改交换机配置，则可以使用集群控制链路的工作值来形成集群。 添加/修改的命令：**show cluster info trace**、**show cluster history**。
改进了高 CPU 情况下的集群控制链路运行状况检查	10.0.0	10.0.0	当集群节点 CPU 使用率较高时，系统将暂停运行状况检查，但不会将节点标记为运行状况不正常。此功能默认启用，但可以使用 FlexConfig 配置。 新增/经修改的命令：**cpu-healthcheck-threshold** (FlexConfig)、、、。
关于节点加入时时间节点的 MTU ping 测试	7.6.0	7.6.0	节点加入集群时，会向控制节点发送数据包大小为集群控制链路 MTU 两倍的 Ping 请求，以检查 MTU 兼容性。此前，仅控制节点发送 Ping。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。 添加/修改的命令：**show cluster history**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
VMware 和 KVM 上 Firewall Threat Defense Virtual 的集群	7.4.1	7.4.1	Firewall Threat Defense Virtual 现在支持 VMware 和 KVM 上最多 16 个节点的单个接口集群。
集群控制链路 ping 工具。	7.2.67.4.1	任意	您可以通过执行 ping 来检查是否所有集群节点都能通过集群控制链路相互连接。节点无法加入集群的一个主要原因是集群控制链路配置不正确，例如，集群控制链路 MTU 设置可能高于连接交换机的 MTU。 新增/修改的屏幕：**设备** > **设备管理** > **更多** > **集群实时状态**。
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
当节点未能加入集群时，自动在该节点上生成故障排除文件。	7.4.1	7.4.1	如果节点未能加入集群，系统将自动为该节点生成故障排除文件。您可以从**任务 (Tasks)** 或**集群 (Cluster)** 页面下载该文件。
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
集群运行状况监控设置	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
集群运行状况监控器控制面板	7.3.0	任意	您现在可以在集群运行状况监控控制面板上查看集群运行状况。 新增/修改的屏幕：**系统** > **运行状况** > **监控器**

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
VMware 和 KVM 上 Firewall Threat Defense Virtual 的集群	7.2.0	7.2.0	Firewall Threat Defense Virtual 支持 VMware 和 KVM 上最多 4 个节点的单个接口集群。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：VMware 和 KVM 上的 Firewall Threat Defense Virtual



第 12 章

群集技术：公共云

通过集群，您可以将多台 Firewall Threat Defense Virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。使用以下公共云频台，您可以在公共云中部署 Firewall Threat Defense Virtual 集群：

- Amazon Web 服务 (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

目前仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅不支持的功能和集群，第 624 页。

- 关于公共云中的 Threat Defense Virtual 群集，第 502 页
- Threat Defense Virtual 集群的许可证，第 504 页
- Threat Defense Virtual 集群的要求和前提条件，第 504 页
- Threat Defense Virtual 集群的准则，第 506 页
- 在 AWS 中部署集群，第 508 页
- 在 Azure 中部署集群，第 537 页
- Azure 中的 Firewall Threat Defense Virtual 集群 Autoscale 解决方案，第 555 页
- 在 GCP 中部署集群，第 578 页
- GCP 中的 Threat Defense Virtual 集群 Autoscale 解决方案，第 587 页
- 将集群添加到管理中心（手动部署），第 600 页
- 配置集群运行状况监控设置，第 608 页
- 管理集群节点，第 612 页
- 监控集群，第 615 页
- 对集群进行故障排除，第 621 页
- 升级集群，第 623 页
- 集群参考，第 624 页
- 关于公共云中的 Threat Defense Virtual 集群的历史记录，第 635 页

关于公共云中的 Threat Defense Virtual 群集

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 Firewall Threat Defense Virtual 能够通过集群控制链路发送广播/组播消息。
- 负载均衡器 - 对于外部负载均衡，您有以下选择（具体取决于公共云）：
  - AWS 网关负载均衡器

    AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Firewall Threat Defense Virtual 支持使用 Geneve 接口单臂代理且具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。
  - Azure 网关负载均衡器

    在 Azure 服务链中， Firewall Threat Defense Virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。
  - 本地 GCP 负载均衡器，内部和外部
  - 使用内部和外部路由器（例如思科云服务路由器）的等价多路径路由 (ECMP)

    ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 Firewall Threat Defense 故障会导致问题；如果继续使用该路由，发往故障 Firewall Threat Defense 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 Firewall Threat Defense 使之加入动态路由。

注释 负载均衡不支持第 2 层跨区以太网通道。

独立接口

您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的本地 IP 地址。接口的 IP 地址将通过 DHCP 自动配置。不支持静态 IP 配置。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 首次创建集群时，您可以指定要成为控制节点的节点，因为它是添加到集群的第一个节点，所以它将成为控制节点。

集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅配置 VXLAN 接口，第 783 页。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规Firewall Threat Defense Virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，Firewall Threat Defense Virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

管理网络

您必须使用管理接口来管理每个节点；集群不支持从数据接口进行管理。

Threat Defense Virtual 集群的许可证

每个 Firewall Threat Defense Virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。您可以在**设备** > **设备管理** 、**集群** > **许可证**区域中修改集群的许可证。

注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

Threat Defense Virtual 集群的要求和前提条件

型号要求

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100

注释 FTDv5 和 FTDv10 不支持 Amazon Web 服务 (AWS) 网关负载均衡器。

- 以下公共云服务：

- Amazon Web 服务 (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

- 最多 16 个节点

另请参阅 Cisco Secure Firewall Threat Defense Virtual 入门指南中的 Firewall Threat Defense Virtual 一般要求。

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件和软件要求

集群中的所有设备：

- 必须在同一个性能层。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 必须从管理接口访问 防火墙管理中心；不支持数据接口管理。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。
- 所有设备的集群控制链路接口必须位于同一子网中。

MTU

确保连接到集群控制链路的端口配置了正确（更高）的 MTU。如果存在不匹配的 MTU，则集群形成将失败。当某个节点加入集群时，它会向控制节点发送ping，其数据包大小与集群控制链路MTU匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。

默认情况下，集群控制链路 MTU 会被设置为比数据接口高 154 字节。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）加上 VXLAN 开销（54 字节）。

对于具有 GWLB 的 AWS，数据接口使用 Geneve 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将源接口 MTU 设置为网络 MTU + 306 字节。因此，对于标准的 1500 MTU 网络路径，源接口 MTU 应为 1806，而集群控制链路 MTU 应为 +154, 1960。

对于具有 GWLB 的 Azure，数据接口使用 VXLAN 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将集群控制链路 MTU 设置为源接口 MTU + 80 字节。

下表显示了集群控制链路 MTU 和数据接口 MTU 的默认值。

注释 我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。

表 *36:* 默认 *MTU*

公共云	集群控制链路 **MTU**	数据接口 **MTU**
具有 GWLB 的 AWS	1980 年	1826
AWS	1654	1500
具有 GWLB 的 Azure	1454	1374
Azure	1454	1300
GCP	1554	1400

Threat Defense Virtual 集群的准则

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

多区域集群

多区域集群最多支持三个区域。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firewall Threat Defense 或交换机上的接口、添加其他交换机以形成 VSS、vPC 或 VNet），应禁用运行状况检查功能，另外还应为禁用的接口禁用接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。

- 将节点添加到现有集群时或重新加载节点时，会有限地暂时丢弃数据包/断开连接；这是预期的行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 请勿在节点上禁用集群之前关闭该节点。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要与新节点建立新的连接。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。
- 不支持动态扩展。
- 如果您使用的是 Cisco Secure Firewall 版本 7.2 或 7.3，则在 AWS 上部署集群时不支持状态目标故障切换。
- 在每个维护窗口完成后执行全局部署。
- 确保不要一次从自动扩展组 (AWS)/实例组 (GCP) /规模集 (Azure)中删除多个设备。我们还建议您先在设备上运行 **cluster disable** 命令，然后再从组东扩展组 (AWS) / 实例组 (GCP) / 规模集 (Azure)中删除设备。
- 如果要禁用集群中的数据节点和控制节点，我们建议您在禁用控制节点之前先禁用数据节点。如果在集群中有其他数据节点时禁用了某个控制节点，则必须将其中一个数据节点升级为控制节点。请注意，角色更改可能会对集群造成干扰。
- 在本指南中提供的自定义 Day 0 配置脚本中，您可以根据需要更改 IP 地址，提供自定义接口名称，并更改 CCL-Link 接口的顺序。
- 如果在云平台上部署 Threat Defense Virtual 集群后遇到 CCL 不稳定问题（例如间歇性 ping 失败），我们建议您解决导致CCL不稳定的原因。此外，您可以增加保持时间，作为在一定程度上缓解CCL不稳定问题的临时解决方法。有关如何更改保持时间的详细信息，请参阅 编辑集群运行状况监控设置。
- 为 Management Center Virtual 配置安全防火墙规则或安全组时，必须在源 IP 地址范围中包括 Firewall Threat Defense Virtual 的专用和公共 IP 地址。此外，请确保在 Firewall Threat Defense Virtual的安全防火墙规则或安全组中指定 Firewall Management Center Virtual 的专用和公共 IP 地址。这对于确保在集群部署期间正确注册节点非常重要。

集群默认设置

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

在 AWS 中部署集群

要在 AWS 中部署集群，您可以手动部署或使用 CloudFormation 模板来部署堆栈。您可以将集群与 AWS 网关负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

从版本 10.0.0 开始，AWS Geneve 集群解决方案支持单臂和双臂部署模式，为网络架构提供更高的灵活性。

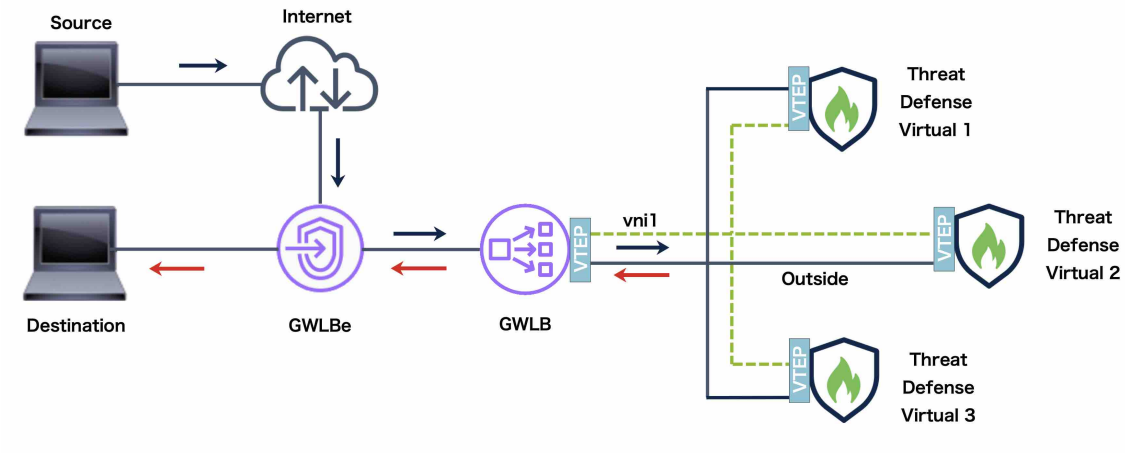
AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Threat Defense Virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个 Threat Defense Virtual 流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

注释 AWS 上的 Geneve 单臂设置不支持传输层安全 (TLS) 服务器身份发现。

图 *200: Geneve* 单臂代理



拓扑示例

Firewall Threat Defense Virtual 在 AWS 区域的单个和多个可用性区域中使用自动扩展进行集群

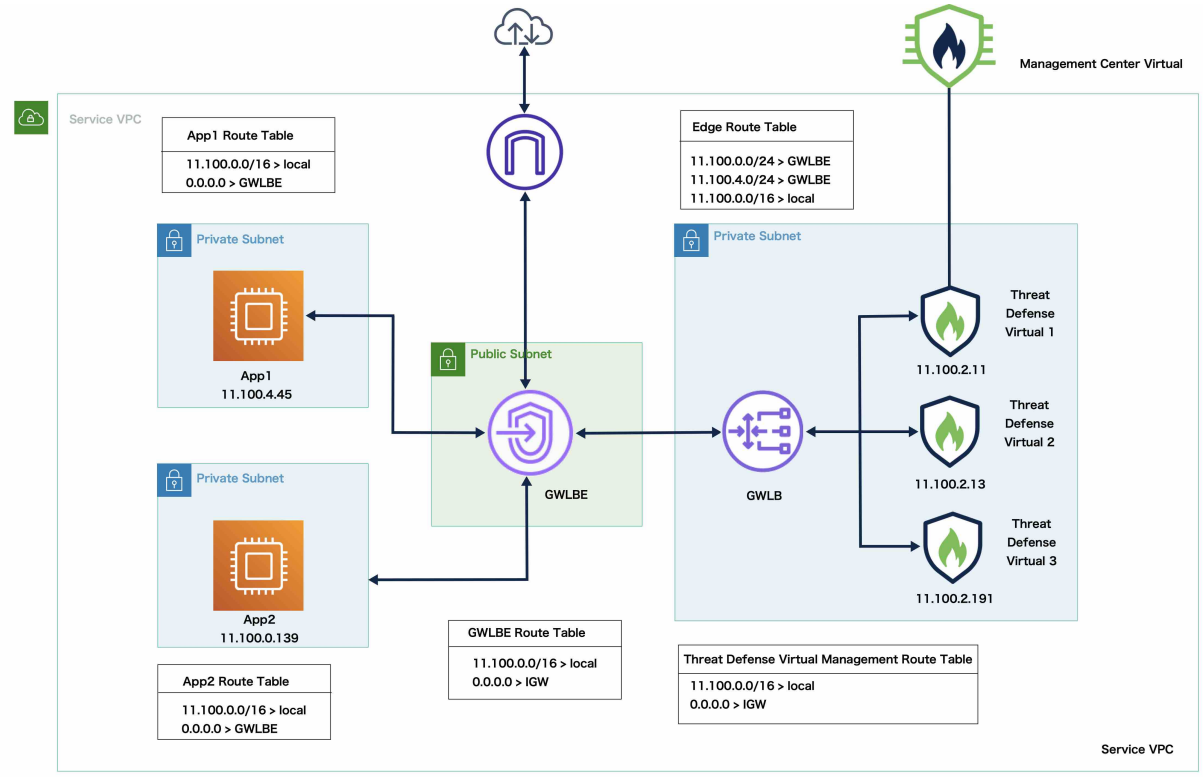
可用性区域是指一个 AWS 区域内独立运行的独立数据中心或一组独立数据中心。每个区域都有自己的网络基础设施、连接和电源，从而确保一个区域的故障不会影响到其他区域。为了提高冗余和可靠性，公司在灾难恢复计划中使用多个可用性区域。

跨多个可用性区域部署 Firewall Threat Defense Virtual 并配置支持动态扩展的集群可以显着增强基础设施的可用性和可扩展性。此外，在同一区域利用多个可用性区域可以提供额外的冗余，并在发生故障时保证高可用性。

您可以修改集群控制链路 (CCL) 的 IP 分配机制，以支持 AWS 上 Firewall Threat Defense Virtual 群集的单可用性区域和多可用性区域部署。下面给出的拓扑结构描述了具有自动扩展能力的单个和多个可用性区域中的入站和出站流量。

Firewall Threat Defense Virtual 在单个可用性区域中使用自动扩展进行集群

集群中有两个连接到 GWLB 的 Firewall Threat Defense Virtual 实例。

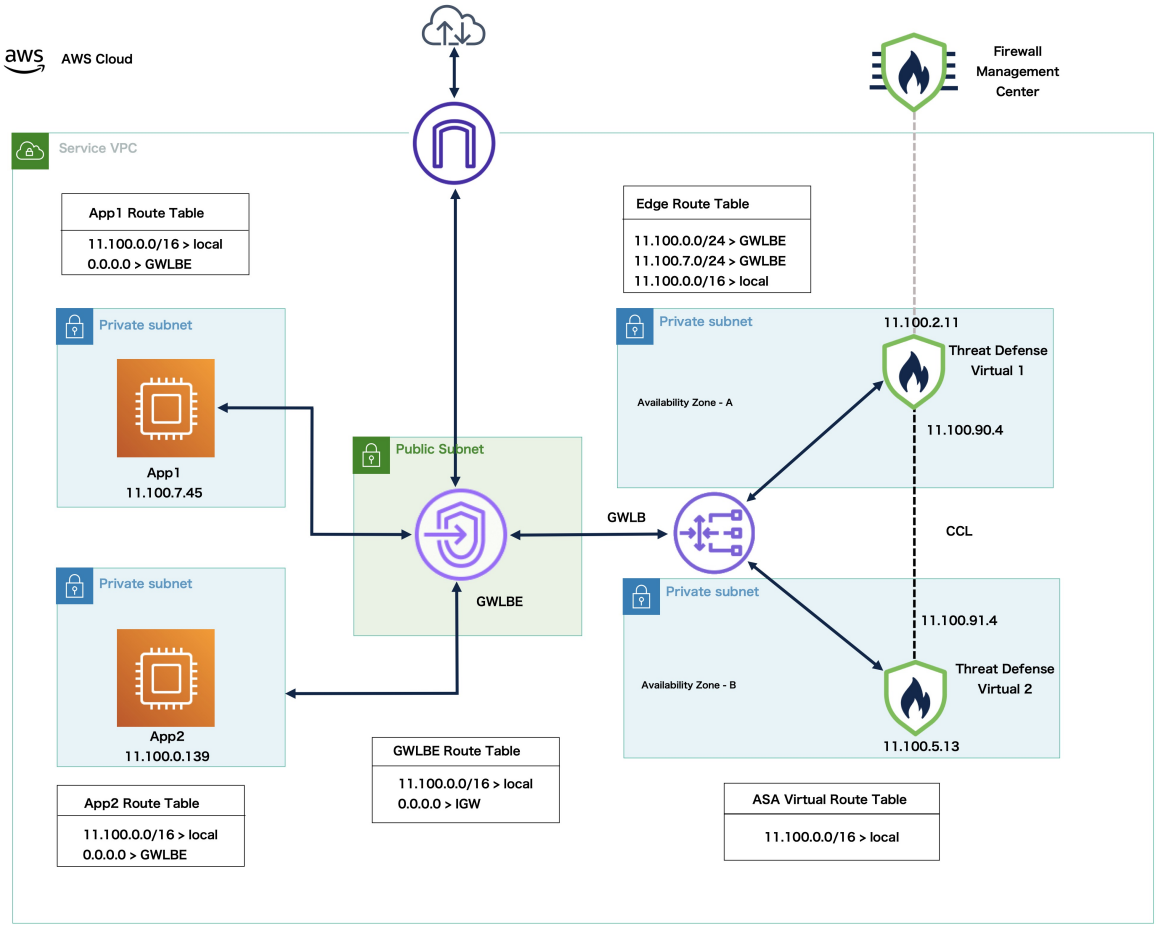


来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，流量被转发到 Firewall Threat Defense Virtual 集群。集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

来自 App1 的出站流量将传输到 GWLB 终端 > GWLB > TDv > GWLB > GWLB 终端，然后由 GWLB 终端发送到互联网。

Firewall Threat Defense Virtual 在多个可用性区域中使用自动扩展进行集群

集群中有两个 Firewall Threat Defense Virtual 实例连接到 GWLB，它们位于不同的可用性区域。

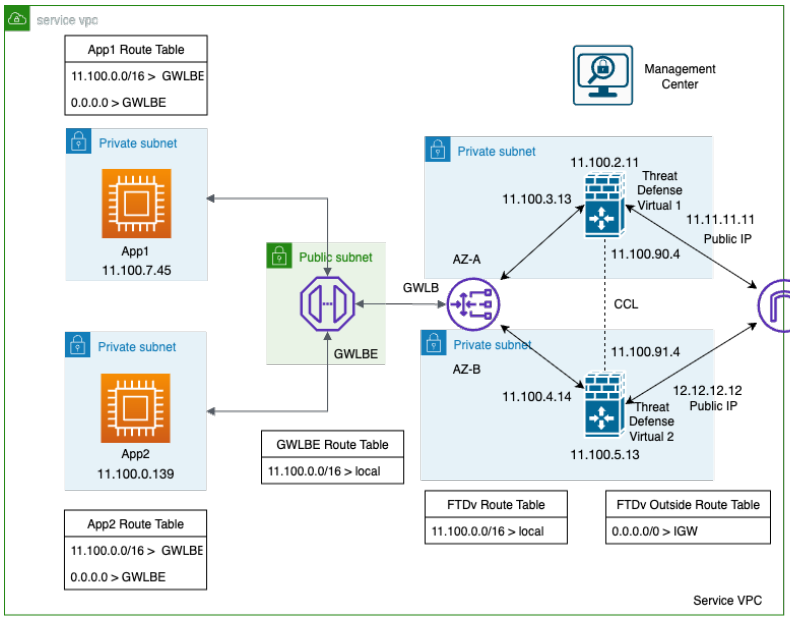


注释 从 Firewall Threat Defense Virtual 版本 7.6.0 及更高版本开始支持多可用性区域部署。

来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，根据可用性区域将流量路由到 Firewall Threat Defense Virtual 集群。集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

AWS 网关负载均衡器和 Geneve 双臂代理

双臂代理是一种网络部署模式，可使 Threat Defense Virtual 检测流量，应用网络地址转换 (NAT)，并通过互联网网关将其从其外部接口直接发送到互联网。此直接出口路径会绕过 GWLB 及其出口终端，从而简化流量以提高效率。此方法在多 VPC 环境中特别有效，其中来自多个 VPC 的出站流量可以共享一个公共出口点。这降低了对基础设施的要求，从而使该解决方案更具成本效益。此外，它还支持集群，以提高流量处理效率。

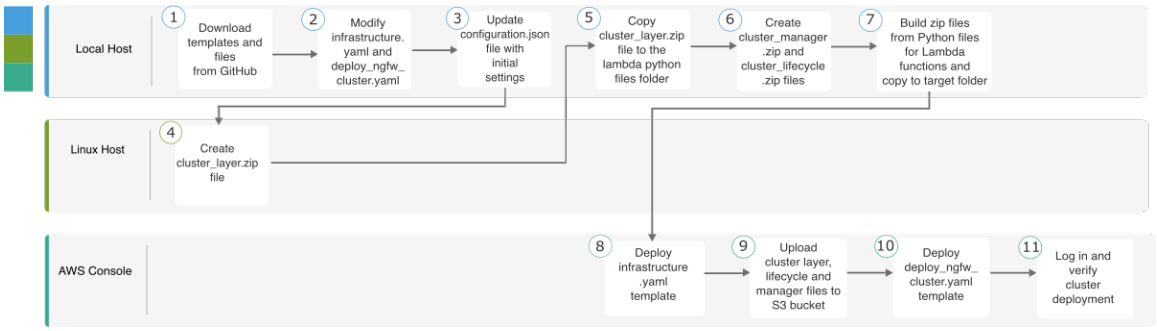


此部署的目的是使用双臂设计中跨单独可用区部署的集群 Threat Defense Virtual 实例，在应用程序将流量发送到互联网之前检查流量，其中内部接口处理入口流量，外部接口处理出口流量。在此流程中，来自 应用的流量将路由到 GWLB，由 GWLB 将流量转发到 Threat Defense Virtual 的内部接口进行检查。应用 NAT 后，Threat Defense Virtual 通过其外部接口将流量直接发送到互联网网关。

在 AWS 上部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

以下流程图说明了在 AWS 上基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 Github 克隆存储库
2	本地主机	修改 *infrastructure.yaml* 和 *deploy_ngfw_cluster.yaml* 模板。

	工作空间	步骤
3	本地主机	使用 FMC 对象名称更新 *Configuration.json* 文件。
4	Linux 主机	创建 *cluster_layer.zip* 文件。
5	本地主机	将 *cluster_layer.zip* 文件复制到 Lambda python files 文件夹。
6	本地主机	创建 *cluster_manager.zip*、*custom_metrics_publisher.zip* 和 *cluster_lifecycle.zip* 文件。
7	本地主机	从 Python 文件为 Lambda 函数构建 zip 文件，并复制到目标文件夹。
8	AWS 控制台	部署 *Infrastructure.yaml* 模板。
9	AWS 控制台	将 *cluster_layer.zip*、*cluster_lifecycle.zip*、*custom_metrics_publisher.zip* 和 *cluster_manager.zip* 上传到 S3 存储桶。
10	AWS 控制台	部署 *deploy_ngfw_cluster.yaml* 模板。
11	AWS 控制台	登录并验证集群部署。

手动部署

以下流程图说明了在 AWS 上手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	创建 Day 0 配置脚本。
2	AWS 控制台	部署 Threat Defense Virtual 实例。

	工作空间	步骤
3	AWS 控制台	将接口连接到实例。
4	AWS 控制台	验证节点是否已加入集群。
5	AWS 控制台	创建目标组和 GWLB；将目标组附加到 GWLB。
6	AWS 控制台	使用数据接口 IP 向目标组注册实例。
7	管理中心	注册控制节点。

模板

以下提供的模板可在GitHub中获取。参数值一目了然，包括模板中给出的参数名称、默认值、允许值和说明。

- Infrastructure.yaml - 基础设施部署模板。
- deploy_ngfw_cluster.yaml - 用于集群部署的模板。

注释 在部署集群节点之前，请确保检查支持的 AWS 实例类型列表。此列表可在 *deploy_ngfw_cluster.yaml* 模板中的参数 InstanceType 的允许值下找到。

使用 CloudFormation 模板在 AWS 中部署堆栈

使用自定义 CloudFormation 模板在 AWS 中部署堆栈。

开始之前

- 您需要安装了 Python 3 的 Amazon Linux 虚拟机。
- 要允许集群自动注册到 防火墙管理中心，您需要在 防火墙管理中心 上创建两个具有管理权限且可以使用 REST API 的用户。请参阅*Cisco Secure Firewall Management Center* 管理指南。
- 在 防火墙管理中心 中添加与您在 `Configuration.json` 中指定的策略名称匹配的访问策略。

过程

步骤 1 准备模板。

a) 将 GitHub 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws。
b) 使用所需的参数修改 **infrastructure.yaml** 和 **deploy_ngfw_cluster.yaml**。
c) 使用初始设置修改 **cluster/aws/lambda-python-files/Configuration.json**。

例如：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- 将 fmcIpforDeviceReg 设置保留为 DONTRESOLVE。
- fmcAccessPolicyName 需要与 防火墙管理中心 上的访问策略匹配。

注释
不支持 FTDv5 和 FTDv10 层。

d) 创建名为 **cluster_layer.zip** 的文件，为 Lambda 函数提供必要的 Python 库。

我们建议使用安装了 Python 3.9 的 Amazon Linux 创建 **cluster_layer.zip** 文件。

注释
如果您需要 Amazon Linux 环境，可以使用 Amazon Linux 2023 AMI 或运行最新版本的 Amazon Linux 的 AWS Cloudshell 创建 EC2 实例。

要创建 cluster-layer.zip 文件，您需要先创建包含 python 库软件包详细信息的 **requirements.txt** 文件，然后运行 shell 脚本。

1. 通过指定 python 软件包详细信息来创建 **requirements.txt** 文件。

   以下是您在 **requirements.txt** 文件中提供的示例软件包详细信息：

   ```
   $ cat requirements.txt
   pycryptodome
   paramiko
   requests
   scp
   jsonschema
   cffi
   zipp
   importlib-metadata
   ```

2. 运行以下 shell 脚本以创建 **cluster_layer.zip**文件。

   ```
   $ pip3 install --platform manylinux2014_x86_64
   --target=./python/lib/python3.9/site-packages
   --implementation cp --python-version 3.9 --only-binary=:all:
   --upgrade -r requirements.txt
   $ zip -r cluster_layer.zip ./python
   ```

注释

如果在安装期间遇到依赖项冲突错误（例如 urllib3 或加密），建议您在 **requirements.txt** 文件中包含冲突软件包及其建议版本。之后，您可以再次运行安装来解决冲突。

e) 将生成的 **cluster_layer.zip** 文件复制到 lambda python files 文件夹 - `cluster/aws/lambda-python-files`。

f) 创建 **cluster_layer.zip**、**custom_metrics_publisher.zip**、 **cluster_manger.zip** 和 **lifecycle_ftdv.zip** 文件。

可以在克隆存储库 (`cluster/aws/make.py`) 中找到 **make.py** 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。

python3 make.py build

注释
如果您使用专用 IP 地址进行 Management Center Virtual 注册，请确保在 `cisco-ftdv/cluster/aws/lambda-python-files/constant.py` 文件中将 USE_PUBLIC_IP_FOR_FMC_CONN 设置为 False 。

步骤 2 部署 **Infrastructure.yaml** 并记下集群部署的输出值。 在部署基础设施堆栈之前，必须确定将使用的 AWS 区域和可用性区域。每个 AWS 区域都有一组不同的可用性区域和 VPC 基础设施，因此必须为部署选择正确的区域和可用性区域。

a) 在 AWS 控制台上，转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **infrastructure.yaml**。

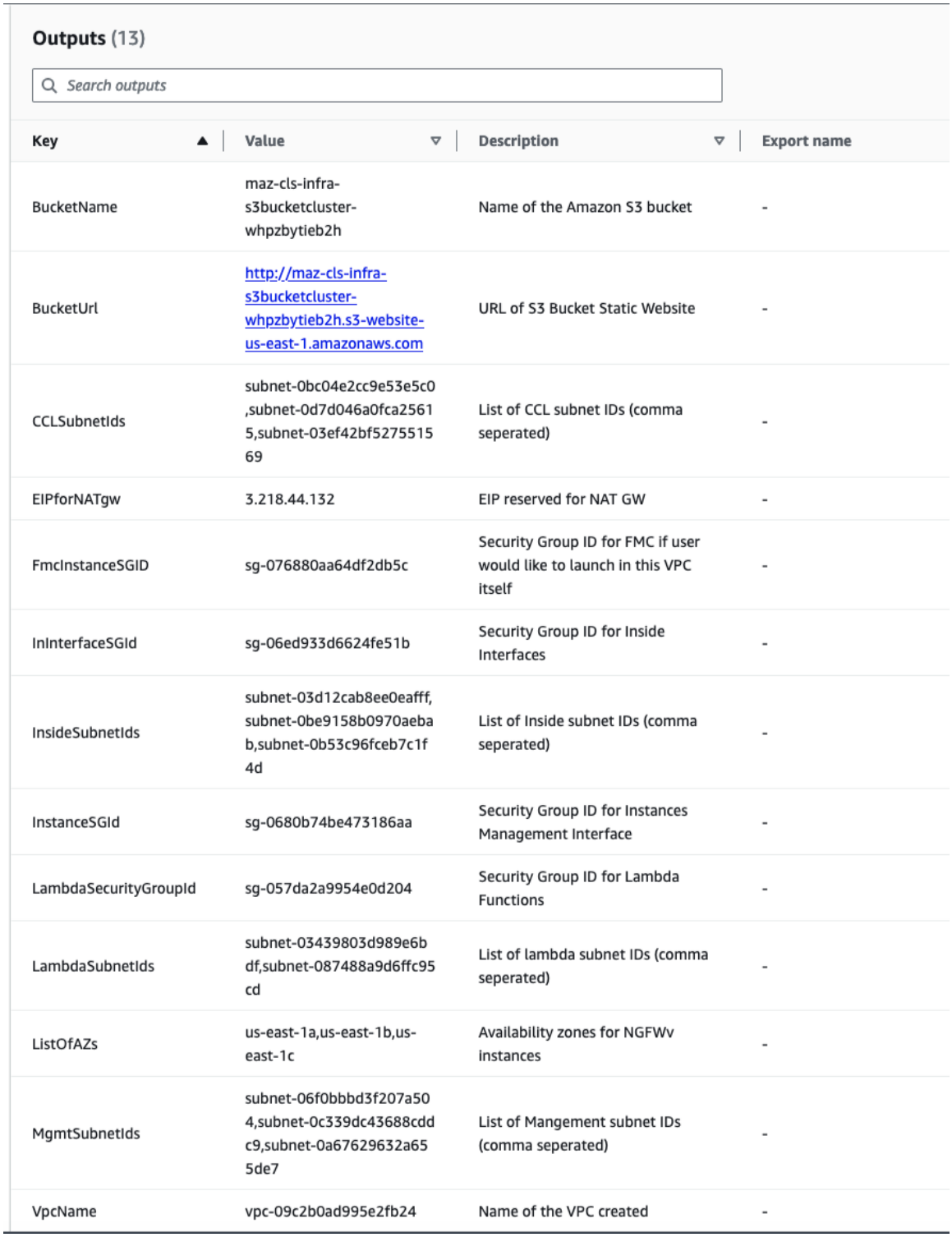
c) 点击**下一步 (Next)** 并提供所需的信息。

参数	允许的值/类型	说明
ClusterName	字符串	输入唯一的集群名称。
ClusterNumber	数字	输入唯一的集群编号。
DeploymentType	字符串	指定是否需要“单臂”或“双臂”部署。 注释 双臂模式支持 10.0.0 及更高版本。
VpcCidr	字符串	为新 VPC 输入 CIDR 块
NoOfAZs	数字	对于 7.6.0 及更高版本，选择 2 或 3 个可用区 (AZ)；对于较低版本，选择 1AZ。 管理、内部、外部和CCL 子网将相应地分布在所选 AZ 中。
ListOfAZs	名单	选择可用区（数量应与可用区数量匹配）
MgmtSubnetNames	CommaDelimitedList	管理子网名称（路由为“互联网 GW”）

参数	允许的值/类型	说明
MgmtSubnetCidrs	CommaDelimitedList	管理子网 Cidr 列表
InsideSubnetNames	CommaDelimitedList	内部子网名称（路由为专用）
InsideSubnetCidrs	CommaDelimitedList	内部子网 Cidr 列表
OutsideSubnetNames	CommaDelimitedList	外部子网名称（路由为“互联网 GW”）（仅双臂模式）
OutsideSubnetCidrs	CommaDelimitedList	输入外部子网 Cidr 列表（仅双臂模式）
CCLSubnetNames	CommaDelimitedList	输入 CCL 子网名称
CCLSubnetCidrs	CommaDelimitedList	输入 CCL 子网 CIDR
LambdaAZs	名单	为 Lambda 选择 2 个可用区
LambdaSubnetNames	CommaDelimitedList	输入 Lambda 子网名称（路由为 NAT GW），用于 Lambda 函数
LambdaSubnetCidrs	CommaDelimitedList	输入 Lambda 子网 CIDR

d) 为集群输入唯一的**集群名称**和**集群编号**。
e) 从**可用性区域 (Availability Zone)** 列表中选择可用性区域。此字段仅列出基于 AWS 区域的可用性区域，您选择该区域是为了使用 ClusterFormation 模板部署基础设施堆栈。
f) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。
g) 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **BucketName**。

图 *201: infrastructure.yaml* 的输出



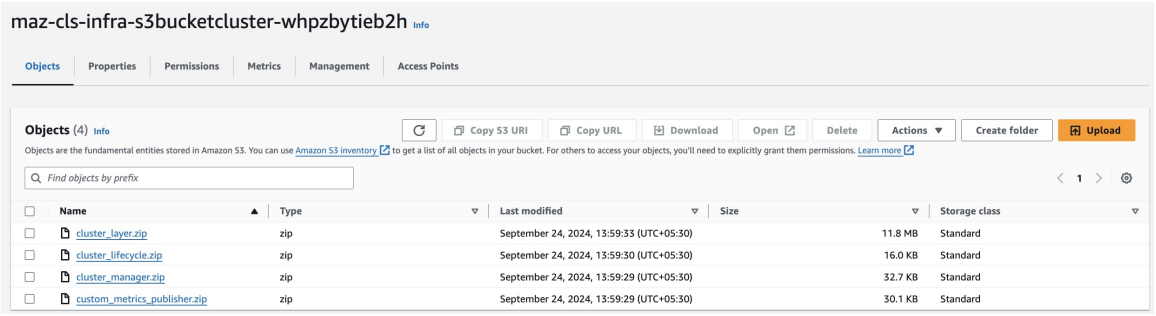
Outputs (13)

Search outputs

Key	Value	Description	Export name
BucketName	maz-cls-infra-s3bucketcluster-whpzbytieb2h	Name of the Amazon S3 bucket	-
BucketUrl	http://maz-cls-infra-s3bucketcluster-whpzbytieb2h.s3-website-us-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetIds	subnet-0bc04e2cc9e53e5c0,subnet-0d7d046a0fca25615,subnet-03ef42bf527551569	List of CCL subnet IDs (comma seperated)	-
EIPforNATgw	3.218.44.132	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-076880aa64df2db5c	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-06ed933d6624fe51b	Security Group ID for Inside Interfaces	-
InsideSubnetIds	subnet-03d12cab8ee0eafff,subnet-0be9158b0970aebab,subnet-0b53c96fceb7c1f4d	List of Inside subnet IDs (comma seperated)	-
InstanceSGId	sg-0680b74be473186aa	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-057da2a9954e0d204	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-03439803d989e6bdf,subnet-087488a9d6ffc95cd	List of lambda subnet IDs (comma seperated)	-
ListOfAZs	us-east-1a,us-east-1b,us-east-1c	Availability zones for NGFWv instances	-
MgmtSubnetIds	subnet-06f0bbbd3f207a504,subnet-0c339dc43688cddc9,subnet-0a67629632a655de7	List of Mangement subnet IDs (comma seperated)	-
VpcName	vpc-09c2b0ad995e2fb24	Name of the VPC created	-

步骤 3 将 **cluster_layer.zip**、**cluster_manager.zip**、**custom_metrics_publisher.zip** 和 **cluster_lifecycle.zip** 上传到由 **infrastructure.yaml** 创建的 S3 存储桶。

图 ***202: S3*** 桶



注释
确保 Lambda NAT 网关的弹性 IP 地址已添加到与 Management Center Virtual 相关联的安全组。

步骤 4 部署 **deploy_ngfw_cluster.yaml**。

a) 转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。
b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **deploy_ngfw_cluster.yaml**。
c) 点击**下一步 (Next)** 并提供所需的信息。
d) 提供以下集群和基础设施配置信息。

参数	允许的值/类型	说明
集群配置		
ClusterGrpNamePrefix	字符串	这是集群名称前缀。集群编号将作为后缀添加。
ClusterNumber	字符串	这是集群编号。这将作为集群名称的后缀 (msa-ftdv-infra)。例如，如果此值为 **1**，则组名称将为 *msa-ftdv-infra-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1。
集群大小	数字	这是集群中 Firewall Threat Defense Virtual 节点的总数。 最小值：1 最大值：16
DeploymentType	字符串	指定是否需要“单臂”或“双臂”部署。 **注释** 双臂模式支持 10.0.0 及更高版本。

参数	允许的值/类型	说明
DiagnosticInterface	字符串	指定是否需要诊断接口。 "ON" - 将附加诊断接口。 “OFF”- 不会附加诊断接口。 注释 “OFF”支持 10.0.0 及更高版本。
基础设施详细信息		
NoOfAZs	字符串	这是部署 Firewall Threat Defense Virtual 的可用性区域总数。（根据地区的不同，可用性区域的数量从最少 1 个到最多 3 个不等）。 子网将在这些可用性区域内创建。 此列表中可用的可用性区域基于为部署集群而选择的区域。 注释 根据此参数在三个可用性区域中创建管理、内部和集群控制链路 (CCL) 子网。
AZ	字符串	可用性区域列表基于您计划部署的区域。 在可用性区域列表中，选择有效的可用性区域（1 个或 2 个可用性区域或 3 个可用性区域）。 计数应与可用性区域数量参数的值匹配。
NotifyEmailID	字符串	集群事件邮件将发送到的邮件地址。您必须接受订用电子邮件请求，才能收到此电子邮件通知。 示例：admin@company.com
VpcId	字符串	集群组的 VPC ID。 类型：AWS::EC2::VPC::Id
S3BktName	字符串	包含已上传的 Lambda zip 文件的 S3 存储桶。您必须指定正确的存储桶名称。
MgmtSubnetIds	名单	每个可用性区域只能输入一个子网。 如果从同一可用性区域选择多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
InsideSubnetIds	名单	为每个可用性区域至少输入一个子网。

参数	允许的值/类型	说明
		如果选择来自同一可用性区域的多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
OutsideSubnetIds	CommaDelimitedList	（仅双臂模式） 每个 AZ 仅提供一个子网。如果选择了来自同一 AZ 的多个子网，错误的子网选择将在部署 NGFWv 实例时导致问题。 确保添加来自所提供 AZ 的子网。
LambdaSubnets	列表	为 Lambda 函数输入至少两个子网。您输入的两个子网必须具有 NAT 网关，以使 Lambda 函数能够与 AWS 服务（即公共 DNS）通信。 类型：List<AWS::EC2::Subnet::Id>
CCLSubnetIds	字符串	为每个可用性区域至少输入一个子网。 如果选择来自同一可用性区域的多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
CCLSubnetRanges	字符串	输入不同可用性区域的 CCL 子网的 IP 地址范围。 排除前 4 个保留的 IP 地址。集群控制链路 (CCL) 的 IP 地址池。 IP 地址从 CCL IP 地址池分配给 Firewall Threat Defense Virtual 实例的 CCL 接口。
MgmtInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例选择安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id>
InsideInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例的内部接口选择安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id>
OutsideInterfaceSG	字符串	（仅双臂模式） 为 NGFWv 实例外部接口提供安全组 ID。
LambdaSG	列表	为 Lambda 函数选择一个安全组。 确保出站连接设置为 **ANYWHERE**。

参数	允许的值/类型	说明
		类型：List<AWS::EC2::SecurityGroup::Id>
CCLInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例的 CCL 接口选择安全组 ID。
DualArmAppCidrList	CommaDelimitedList	（仅双臂模式） 输入用于东西向流量的双臂应用 CIDR。
GWLB 配置		
DeployGWLBE	字符串	点击**是**部署 GWLB 端点。 默认情况下，该值设置为**否**。
VpcIdLBE	字符串	输入 VPC 以部署网关负载均衡器终端。 **注释** 如果不部署GWLB终端，请不要在此字段中输入任何值。
GWLBESubnetId	字符串	仅输入一个子网 ID。 **注释** 如果不部署GWLB终端，请不要在此字段中输入任何值。 确保子网属于正确的 VPC 以及您指定的可用性区域。
TargetFailover	字符串	当目标发生故障或取消注册时，启用目标故障转移支持。（默认情况下，此参数的值设置为 **rebalance**）。 • **no_rebalance**：将现有流量导向故障目标，将新流量导向健康目标，从而确保向后兼容性。 • **rebalance**：重新分配现有流量，同时确保新流量流向正常运行的目标。 从 Firewall Threat Defense Virtual 版本7.4.1 及更高版本开始支持 *rebalance*。
TgHealthPort	字符串	输入 GWLB 的运行状况检查端口。 **注释** 默认情况下，此端口不得用于流量。 确保您提供的值是有效的 TCP 端口。默认值：8080

参数	允许的值/类型	说明
思科 NGFWv 实例配置		
InstanceType	字符串	思科 Firewall Threat Defense Virtual EC2 实例类型。 确保 AWS 区域支持您选择的实例类型。 默认情况下，**c5.xlarge** 处于选中状态。 **注释** 当诊断接口为“ON”时，双臂部署仅支持 _.4xlarge。
LicenseType	字符串	选择思科 Firewall Threat Defense Virtual EC2 实例许可证类型。确保您在 **AMI-ID** 参数中输入的 AMI ID 的许可类型相同。 默认情况下，选择 **BYOL**。
AssignPublicIP	字符串	将该值设置为 **true** 可从 AWS IP 地址池为 Firewall Threat Defense Virtual 分配公共 IP 地址。
AmiID	字符串	根据地区、版本和许可证类型（BYOL 或 PAYG）选择正确的 AMI ID。 Firewall Threat Defense Virtual 7.2 及更高版本支持集群，Firewall Threat Defense Virtual 7.6 及更高版本支持自动扩展和多个可用性区域增强功能。 类型：AWS::EC2::Image::Id
ngfwPassword	字符串	Firewall Threat Defense Virtual 实例密码。 所有 Firewall Threat Defense Virtual 实例都提供一个默认密码，该密码位于启动模板（集群组）的 Userdata 字段中。 密码将在 Firewall Threat Defense Virtual 可访问后激活。 最小长度必须为 8 个字符。密码可以是纯文本密码，也可以是 KMS 加密密码。
KmsArn	字符串	输入现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。 如果在此字段中指定值，则 Firewall Threat Defense Virtual 实例的**管理员**密码必须是加密密码。 生成加密密码示例：*“aws kms encrypt --key-id <KMS ARN> --plaintext <password>”*

参数	允许的值/类型	说明
		密码加密必须仅使用指定的 ARN 进行。
FMC 自动化配置		
fmcDeviceGrpName	字符串	在管理中心中输入集群组的唯一名称。
fmcPublishMetrics	字符串	选择 **true** 以创建 Lambda 函数以轮询管理中心，并将特定设备组指标发布到 AWS CloudWatch。 允许的值： • true • false 默认情况下，该值设置为 **true**。
fmcMetricsUsername	字符串	输入用于从管理中心轮询内存指标的唯一内部用户名。 用户必须具有**网络管理员**和**维护用户**权限或更高权限。
fmcMetricsPassword	字符串	输入密码。 如果您提到了 KMS 主密钥 ARN 参数，请确保提供加密密码。 确保输入正确的密码，因为输入错误的密码可能会导致指标收集失败。
fmcServer	字符串	IP 地址可以是外部 IP 地址，也可以是在 VPC 的 Firewall Threat Defense Virtual 管理子网中可访问的 IP 地址。 最小长度：7 最大长度：15
fmcOperationsUsername	字符串	为 CloudWatch 的 Firewall Management Center Virtual 提供唯一的内部用户名。 用户必须拥有**管理员**权限。
fmcOperationsPassword	字符串	输入密码。 如果您提到了 KMS 主密钥 ARN 参数，请确保提供加密密码。
扩展配置		

参数	允许的值/类型	说明
CpuThresholds	CommaDelimitedList	（可选）指定非零的下阈值和上阈值将创建比例策略。如果选择(0,0)，则不会创建CPU扩展警报或策略。评估点和数据点采用默认值或建议值。 默认情况下，此模板中启用**自动扩展**。部署后可以禁用自动扩展。
MemoryThresholds	CommaDelimitedList	指定非零下限和上限阈值将创建扩展策略。如果选择 (0,0)，则不会创建内存扩展警报或策略。评估点和数据点采用默认值或建议值。

e) 点击**下一步**。
f) 点击以确认所有 AWS CloudFormation 选项。
g) 点击**提交 (Submit)** 以部署集群。
h) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

Lambda 函数将管理该过程的其余部分，并且 Firewall Threat Defense Virtual 将自动注册到 防火墙管理中心。

图 ***203:*** 已部署的资源

状态从 **CREATE_IN_PROGRESS** 更改为 **CREATE COMPLETE**，表示部署成功。

步骤 5 通过登录到任何一个节点并使用 **show cluster info** 命令来验证集群部署。

图 *204:* 集群节点

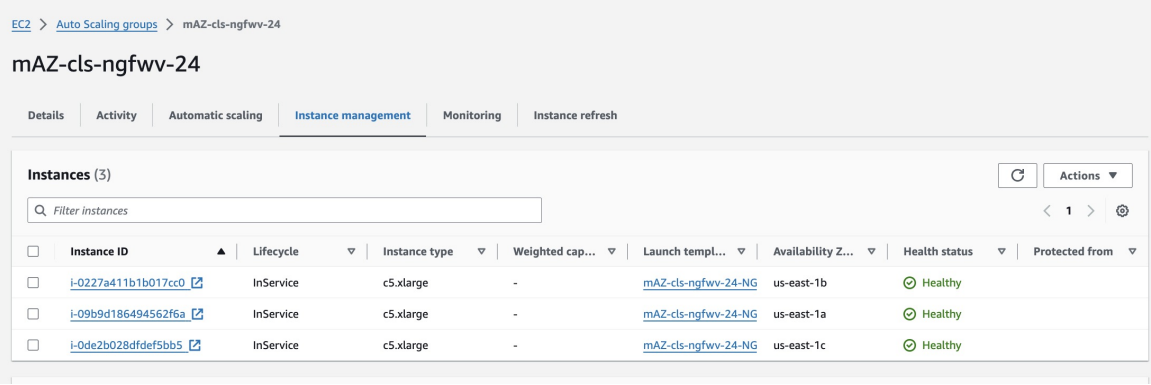
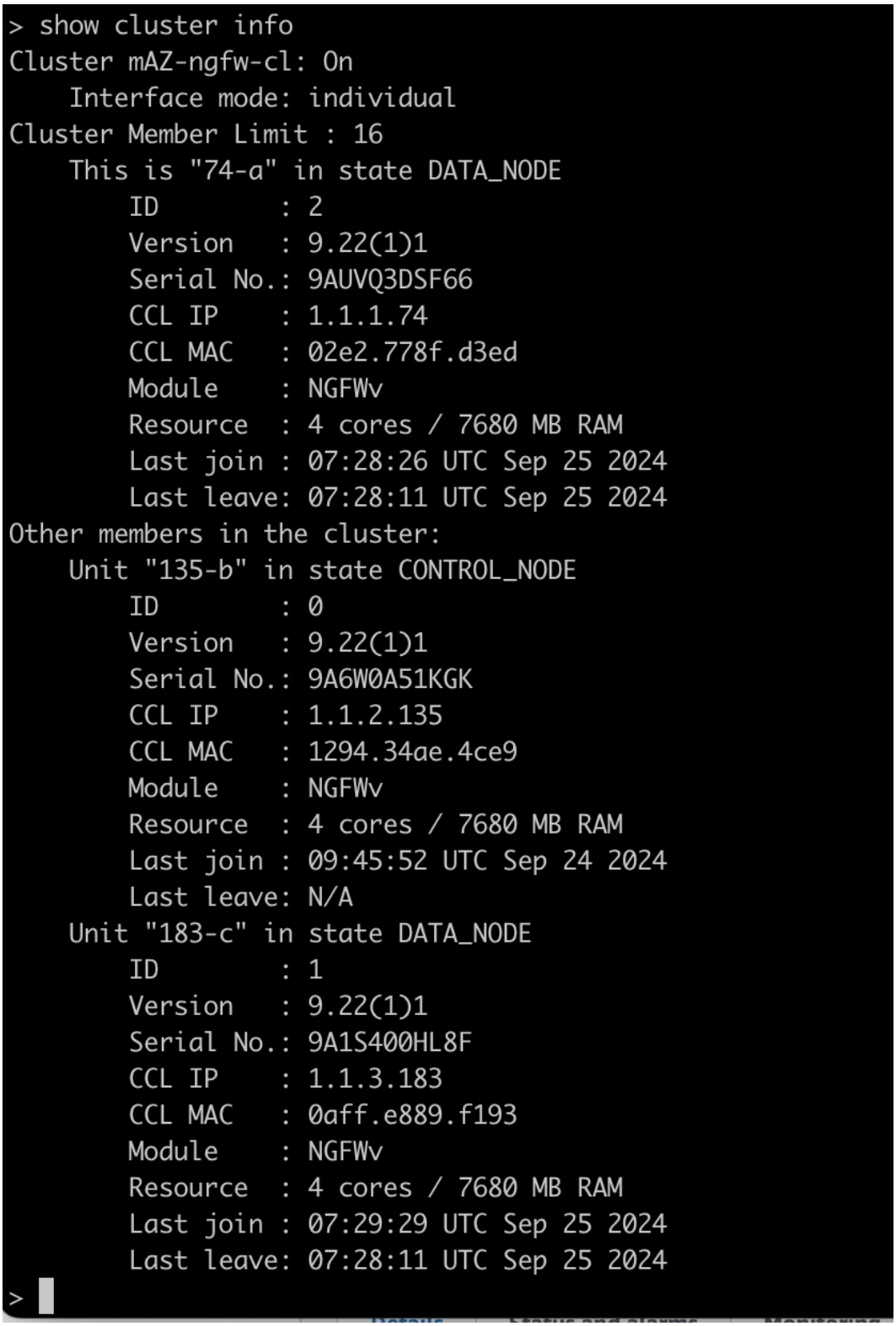


图 *205: show cluster info*



管理中心双臂部署的 NAT 配置

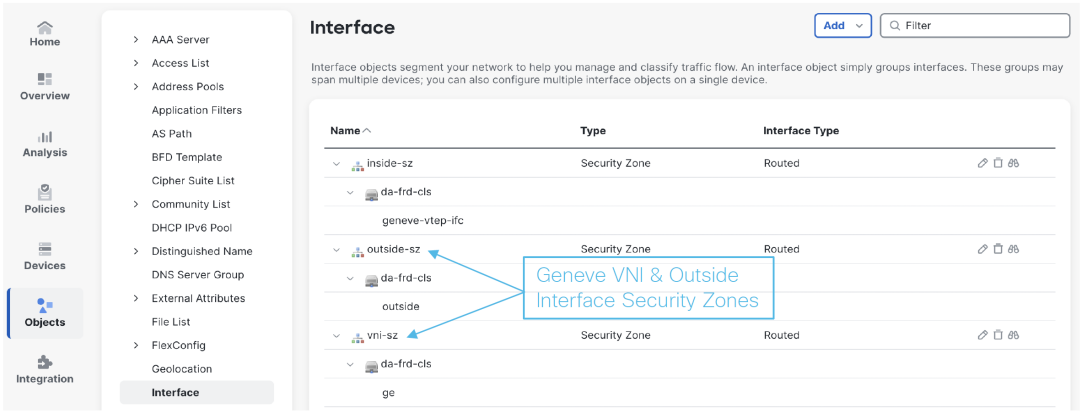
过程

步骤 1 创建安全区域。

安全区域允许您将访问控制、NAT 和检查策略统一应用于一组接口，而无需单独配置它们。

在管理中心中，导航至“对象 > 接口 > 添加 > 安全区域”。

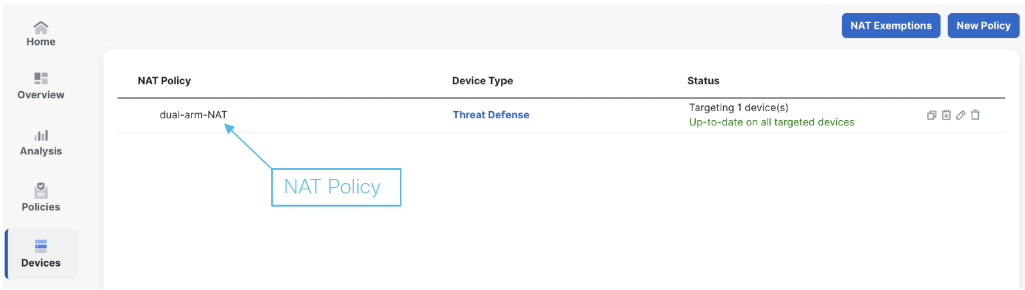
- **内部安全区域** → 用于内部或入口接口（来自应用程序的流量）。
- **VNI 安全区域** → 用于 Geneve VNI 隧道接口（来自 GWLB 的流量）。
- **外部安全区域** → 用于通向互联网网关的出口接口。



步骤 2 配置 NAT 政策。

NAT 政策（双臂 NAT）定义了源和目标地址转换规则，这些规则需要将流量从内部接口（经防火墙检查后）直接转发到外部接口以访问互联网，在出口时绕过 GWLB。

导航至“设备 > NAT > 新建政策”。

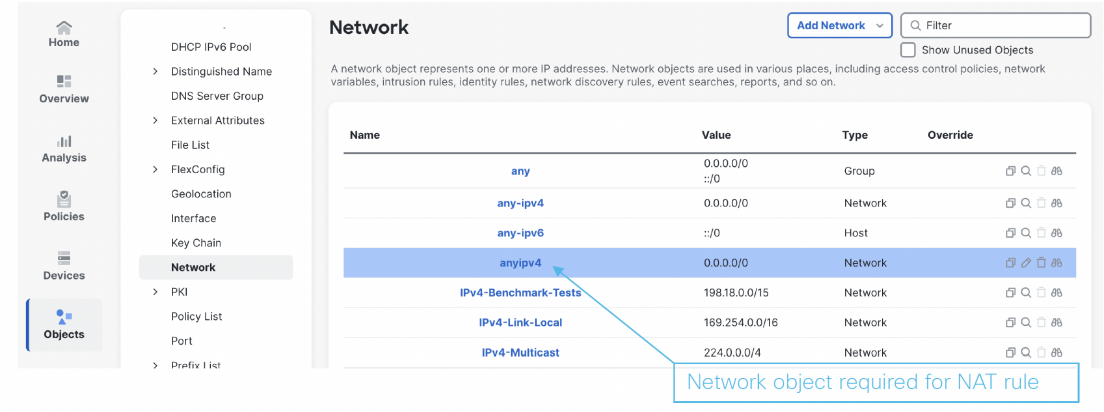


步骤 3 为您的源网络创建一个网络对象。

网络对象代表一个或多个 IP 地址或范围。这些对象用于 NAT 规则、访问控制政策和网络发现规则等多个地方。

导航至“对象 > 网络 > 添加网络”。

- **名称**：赋予网络对象的逻辑名称。
- **值**：实际的 IP 地址范围或 CIDR 格式的网段（例如，`0.0.0.0/0` 代表所有 IPv4 地址）。
- **类型**：指定对象是组、网络还是主机。

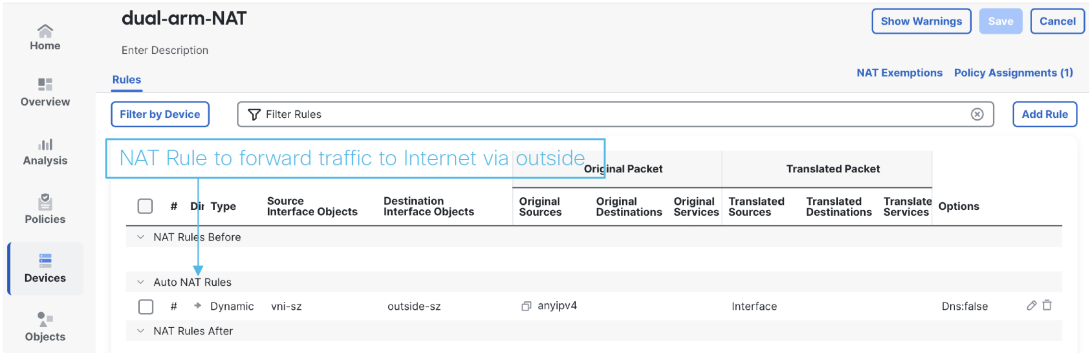


步骤 4 添加 NAT 规则

NAT 策略是为双臂部署配置的，以将流量通过外部接口转发到互联网。

导航至“设备 → NAT → 双臂 NAT → 添加规则”

完成配置后，按照“部署 > 选择集群组 > 全部部署”的路径将策略部署到集群组。

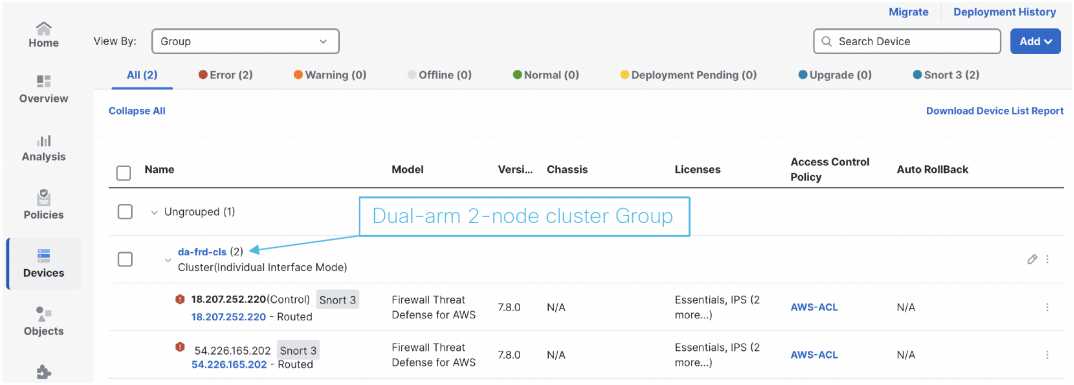


步骤 5 部署后检查

a) 验证双臂 2 节点集群组。

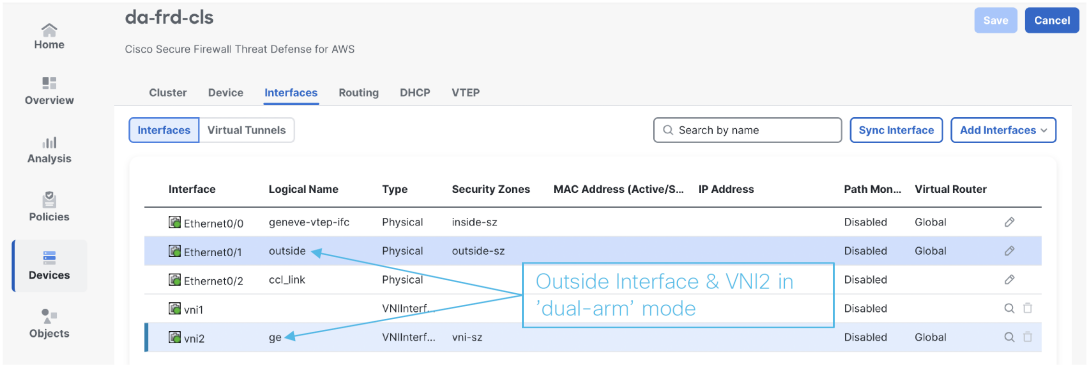
此步骤旨在验证集群是否包含在双臂模式下运行的两个 Threat Defense Virtual 实例,其中每个实例至少使用两个专用网络接口来处理单独的流量路径。

导航到“设备 → 设备管理”，然后验证集群组。



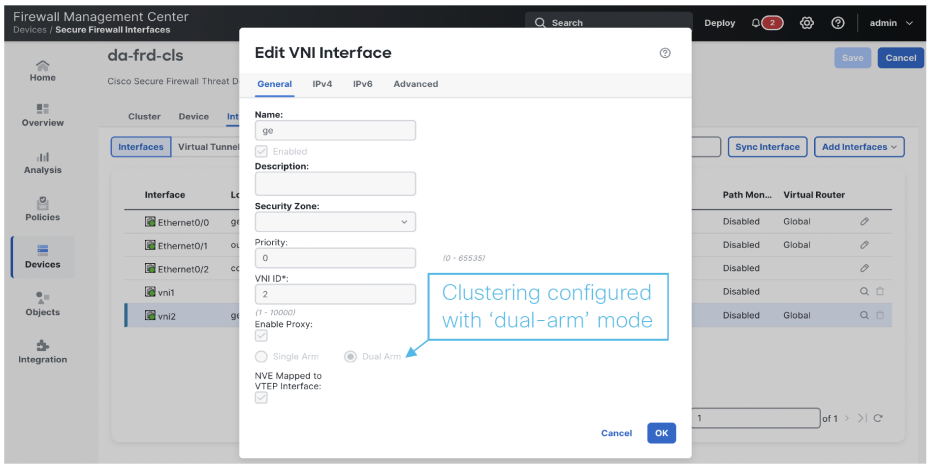
b) 验证 Cisco Secure Firewall Threat Defense Virtual 集群的接口和配置。

导航到“设备 > 设备管理 > 集群组 > 接口”，然后验证双臂部署所用的接口。



c) 确认双臂配置。

导航到“设备 > 设备管理 > 集群组 > 接口 > vni2”。点击“编辑 VNI 接口”以验证双臂配置。

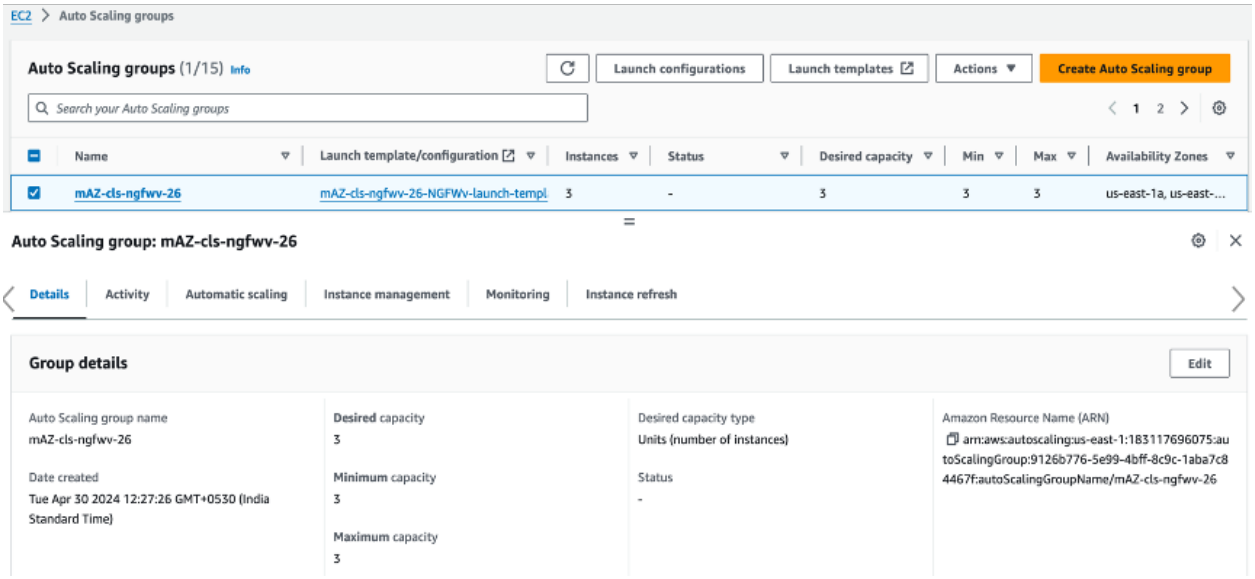


自动扩展参数配置

部署完成后，必须指定 Firewall Threat Defense Virtual Autoscale 组的**最小 (Minimum)**、**最大 (Maximum)** 和**期望 (Desired)** 容量。您必须验证自动扩展功能。

过程

步骤 1 在 AWS 控制台中，依次选择 **服务 (Services)** > **EC2** > **自动扩展组 (Auto Scaling groups)** > **已创建 ClusterAutoscale 组 (Created ClusterAutoscale group)**。



步骤 2 选中自动扩展组复选框。

步骤 3 点击**操作 (Actions)** 以编辑自动扩展组容量。

步骤 4 配置**所需容量 (Desired capacity)**，然后设置**扩展限制 (Scaling limits)** 容量。

步骤 5 在 AWS Cloudwatch 警报中检查 CPU 和内存指标数据是否可用，缩放是否按预期进行。

通过更新堆叠在 Firewall Threat Defense Virtual 集群中配置所需的 IMDSv2 模式

您可以为 AWS 上已部署的 Firewall Threat Defense Virtual 个自动扩展组实例配置 IMDSv2 必需模式。

Before you begin

仅 Firewall Threat Defense Virtual 版本 7.6 及更高版本支持 IMDSv2 必需模式。在为部署配置 IMDSv2 模式之前，您必须确保现有实例版本与 IMDSv2 模式兼容（升级到版本 7.6）。

Procedure

步骤 1 在 AWS 控制台上，转到 **CloudFormation** ，然后点击 **堆栈**。

步骤 2 选择初始部署的集群实例的堆栈。

步骤 3 点击**更新**。

步骤 4 在 **更新堆栈** 页面上，点击 **替换现有模板**。

步骤 5 在 **指定模板** 部分下，点击 **上传模板文件**。

步骤 6 选择并上传支持 IMDSv2 的模板。

步骤 7 为模板中的输入参数提供值。

步骤 8 更新堆栈。

在 AWS 中手动部署集群

要手动部署集群，请准备 day 0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。



注释 从版本 7.6.4-69 和 10.0.0 开始，对于内部集群配置，每个集群节点都需要一个唯一的 AWS 实例标记“cluster-node-id”，其值范围为 1 到 16。请确保在设备启动之前添加标签。

例如：键“cluster-node-id” -> 值“1”

此外，请确保将“在实例元数据中允许标记”设置为“已启用”。

创建 AWS 的 Day0 配置

您可以使用固定配置或自定义配置。我们建议使用固定配置。

使用 AWS 的固定配置创建 Day0 配置

固定配置将自动生成集群引导程序配置。

单个可用性区域 - 第 0 天配置与 AWS 的固定配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
```

```
    }
}
```

例如：

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
              "CclSubnetRange": "10.5.90.4 10.5.90.30",
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

多个可用性区域 - 第 0 天配置与 AWS 的固定配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
    "CclSubnetRange":[
    "ip_address_start_AZ1 ip_address_end_AZ1",
    "ip_address_start_AZ2 ip_address_end_AZ2",
    "ip_address_start_AZ3 ip_address_end_AZ3"
     ],
   "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

例如：两个可用性区域

```
{
 "AdminPassword": "Sup4rnatural",
 "Hostname": "ftdvcluster",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
        "CclSubnetRange": [
            "10.5.90.4  10.5.90.30",
            "10.5.91.4  10.5.91.30"
        ],
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "8080"
 }
}
```

例如：三个可用性区域

```
{
 "AdminPassword": "Sup4rnatural",
 "Hostname": "ftdvcluster",
```

```
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
        "CclSubnetRange": [
            "10.5.90.4  10.5.90.30",
            "10.5.91.4  10.5.91.30",
            "10.5.92.4  10.5.92.30"
        ],
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "8080"
 }
}
```

双臂部署的单个或多个可用性区域 Day0 配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Diagnostic": "OFF",
    "Cluster": {
    "CclSubnetRange":[
    "ip_address_start_AZ1 ip_address_end_AZ1",
    "ip_address_start_AZ2 ip_address_end_AZ2",
    "ip_address_start_AZ3 ip_address_end_AZ3"
     ],
    "ProxyType": "dual-arm"
    "DualArmAppCidrList":[
    "CIDR_BLOCK_1",
    "CIDR_BLOCK_2",
    "CIDR_BLOCK_3"
     ],
   "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

例如：

```
{
"AdminPassword": "FtDv_ClU3TeR44",
"Hostname": "ftdvcluster",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF",
"Cluster": {
"CclSubnetRange": [
"10.5.90.4 10.5.90.30",
"10.5.91.4 10.5.91.30",
"10.5.92.4 10.5.92.30"
],
"ProxyType": "dual-arm",
"DualArmAppCidrList": [
"10.0.0.0/8",
"172.16.0.0/12",
"192.168.0.0/16"
],
"Geneve": "Yes",
"HealthProbePort": "8080",
"ClusterGroupName": "ftdv-cluster"
```

```
}
}
```

对于 **CclSubnetRange** 变量，请指定从 xxx4 开始的 IP 地址范围。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始 (*ip_address_start*) 和结束 (*ip_address_end*) IP 地址的一些示例。

表 *37:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

注释 所有集群基础设施子网都必须使用 /27 CIDR

部署集群节点

部署集群节点，以便它们形成集群。

过程

步骤 1 使用具有所需数量的接口的集群 Day 0 配置部署 Threat Defense Virtual 实例 - 如果使用网关负载均衡器 (GWLB)，则为四个接口；如果使用非本地负载均衡器，则为五个接口。在 **配置实例详细信息** > **高级详细信息** 部分中，粘贴您的 day0 配置。

注释
确保按以下顺序将接口连接到实例。

- AWS 网关负载均衡器 - 四个接口 - 管理、诊断、内部和集群控制链路。
- 非本地负载均衡器 - 五个接口 - 管理、诊断、内部、外部和集群控制链路。

有关在 AWS 上部署 Threat Defense Virtual 的更多信息，请参阅 在 AWS 上部署 Threat Defense Virtual。

步骤 2 重复步骤 1 以部署所需数量的其他节点。

步骤 3 使用 Threat Defense Virtual 控制台上的 **show cluster info** 命令验证是否所有节点都已成功加入集群。

注意
多可用区部署中的集群形成问题 (Threat Defense Virtual 7.6.2)：

在使用由管理中心 7.6.2.1 管理的 Threat Defense Virtual 7.6.2 的 AWS 多可用区部署中，一个已知问题可能会阻止成功形成集群。在这种情况下，无法配置第二个 VTEP，并且 VNI 配置可能缺失。

解决方法：

从管理中心取消注册现有集群，然后在所有集群节点上逐个运行以下 CLI 命令：

```
cluster reset-interface-mode
```

重新注册并重新配置集群。

此操作将解决 VNI 配置缺失的问题，并允许成功建立集群。

步骤 4 配置 AWS 网关负载均衡器。

a) 创建目标组和 GWLB。
b) 将目标组连接到 GWLB。

注释
确保将 GWLB 配置为使用正确的安全组、侦听程序配置和运行状况检查设置。

c) 使用 IP 地址向目标组注册数据接口（内部接口）。

有关详细信息，请参阅创建网关负载均衡器。

步骤 5 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 600 页。

在 AWS 中使用 GWLB 配置 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移

AWS 中的 Threat Defense Virtual 集群利用网关负载均衡器 (GWLB) 来均衡网络数据包并将其转发到指定的 Threat Defense Virtual 节点。GWLB 用于在目标节点发生故障切换或取消注册的情况下，继续向该节点发送网络数据包。

AWS 中的目标故障转移功能使 GWLB 能够在计划维护期间取消注册或目标节点发生故障的情况下将网络数据包重定向到正常运行的目标节点。它利用集群的状态故障切换。

在 AWS 中，您可以通过 AWS 弹性负载均衡 (ELB) API 或 AWS 控制台来配置目标故障转移。

注释 如果目标节点在 GWLB 使用某些协议（例如 SSH、SCP、CURL 等）路由流量时发生故障，则将流量重定向到正常目标可能会出现延迟。此延迟是由于流量的重新平衡和重新路由造成的。

在 AWS 中，您可以通过 AWS ELB API 或 AWS 控制台来配置目标故障转移。

- AWS API - 在 AWS 弹性负载均衡 (ELB) API - *modify-target-group-attributes* 中，您可以通过修改以下两个新参数来定义流量处理行为。
  - target_failover.on_unhealthy - 定义当目标变得运行不正常时 GWLB 如何处理网络流量。
  - target_failover.on_deregistration - 定义当目标取消注册时 GWLB 如何处理网络流量。

  以下命令显示了定义这两个参数的 API 参数配置示例。

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:…/my-targets/73e2d6bc24d8a067 \
--attributes \
Key=target_failover.on_unhealthy, Value=rebalance[no_rebalance] \
Key=target_failover.on_deregistration, Value=rebalance[no_rebalance]
```

  有关详细信息，请参阅 AWS 文档中的 TargetGroupAttribute。

- AWS 控制台 – 在 EC2 控制台中，您可以通过配置以下选项来启用目标组页面上的目标故障转移选项。
  - 编辑目标组属性
  - 启用目标故障转移
  - 验证再平衡流量

  有关如何启用目标故障转移的详细信息，请参阅 在 AWS 中启用 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移，第 536 页。

在 AWS 中启用 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移

Firewall Threat Defense Virtual 的数据接口已注册到 AWS 中的 GWLB 目标组。在 Firewall Threat Defense Virtual 集群中，每个实例都与一个目标组关联。GWLB 进行负载平衡，并将流量发送到该运行状况正常的实例，而该实例已被识别或注册为目标组中目标节点。

开始之前

您必须已通过手动方法或使用 CloudFormation 模板在 AWS 中部署集群。

如果您使用 CloudFormation 模板部署集群，您还可以通过分配集群部署文件 `deploy_ftdv_clustering.yaml` 的 **GWLB 配置**部分下提供的 **rebalance** 属性来启用 **Target Failover** 参数。在模板中，默认情况下，此参数的值设置为 **rebalance**。但在 AWS 控制台上，此参数的默认值设置为 **no_rebalance**。

其中，

- **no_rebalance** - GWLB 继续将网络流量发送到发生故障或已取消注册的目标。
- **rebalance** - 当现有目标发生故障或取消注册时，GWLB 将网络流量发送到另一个正常运行的目标。

有关在 AWS 中部署堆栈的信息，请参阅：

- 在 AWS 中手动部署集群
- 使用 CloudFormation 模板在 AWS 中部署堆栈

过程

步骤 1 在 AWS 控制台上，转到 **服务 > EC2**

步骤 2 点击**目标组 (Target Groups)** 以查看目标组页面。

步骤 3 选择向其注册 Firewall Threat Defense Virtual 数据接口 IP 的目标组。系统将显示目标组详细信息页面，您可以在其中启用目标故障转移属性。

步骤 4 转到**属性 (Attributes)** 菜单。

步骤 5 点击**编辑 (Edit)** 以编辑属性。

步骤 6 将 **重新平衡流量** 滑块按钮切换到右侧，以便启用目标故障转移，从而将 GWLB 配置为在发生故障转移或取消注册时重新平衡现有网络数据包，并将其转发到正常运行的目标节点。

在 Azure 中部署集群

您可以将集群与 Azure 网关负载均衡器 (GWLB) 或非本地负载均衡器配合使用。要在 Azure 中部署集群， 可使用 Azure 资源管理器 (ARM) 模板来部署虚拟机规模集。

基于 GWLB 的集群部署的拓扑示例

图 *206: GWLB* 的入站流量使用案例和拓扑

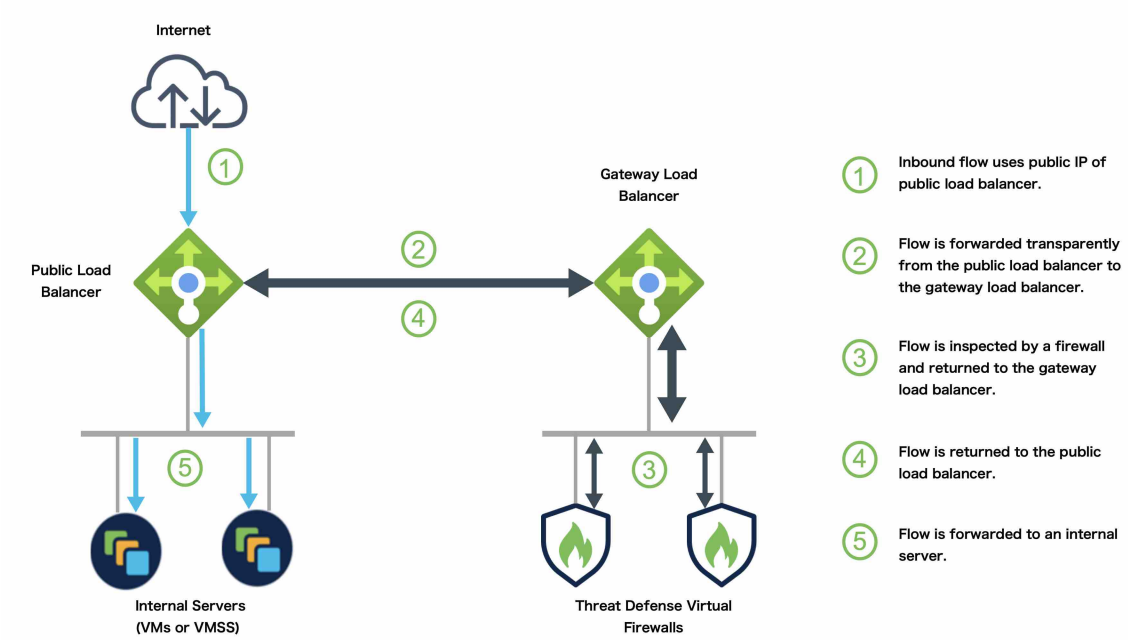
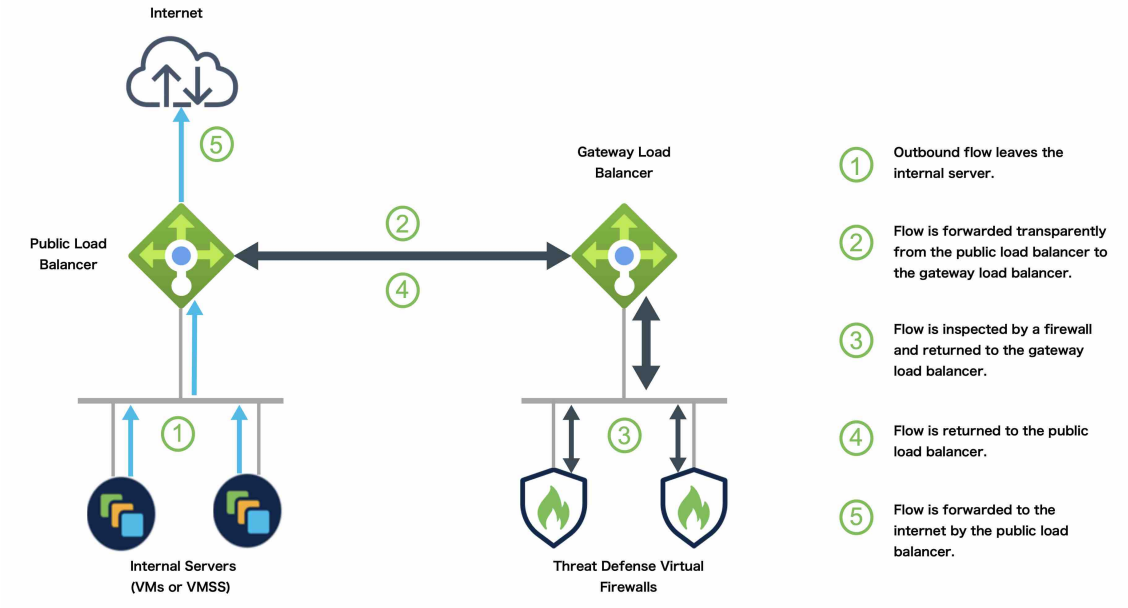


图 *207: GWLB* 的出站流量使用案例和拓扑

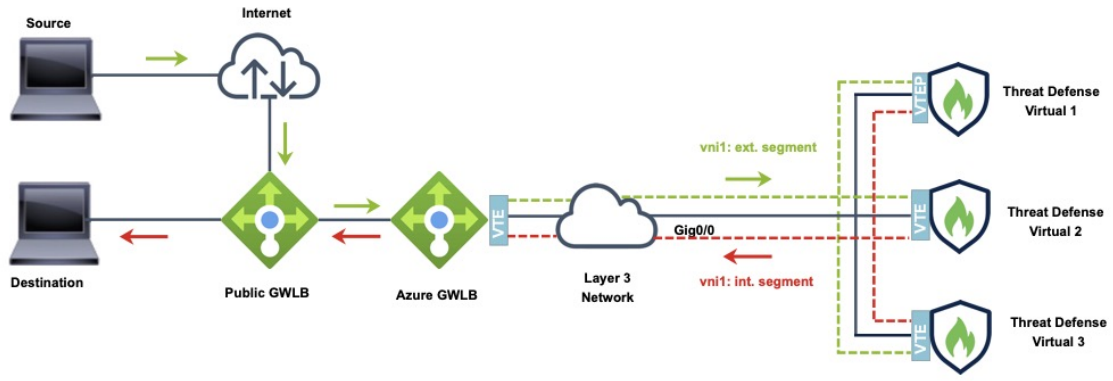


Azure 网关负载均衡器和配对代理

在 Azure 服务链中，Threat Defense Virtual 充当可以拦截互联网和客户服务之间的数据包的透明网关。Threat Defense Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 Threat Defense Virtual 流量之间进行均衡，这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *208: Azure* 网关负载均衡器和配对代理

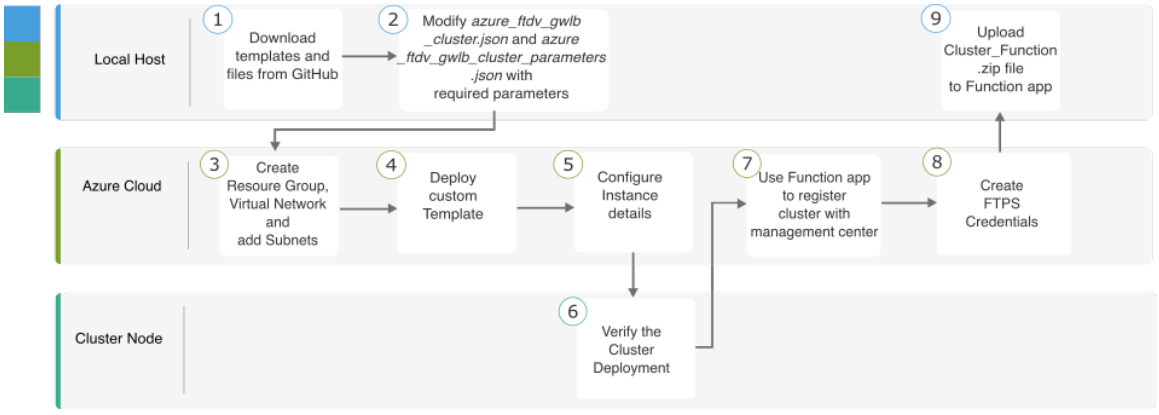


Traffic flow between GWLBe to GWLB (Geneve Single-Arm Proxy) in Azure

使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

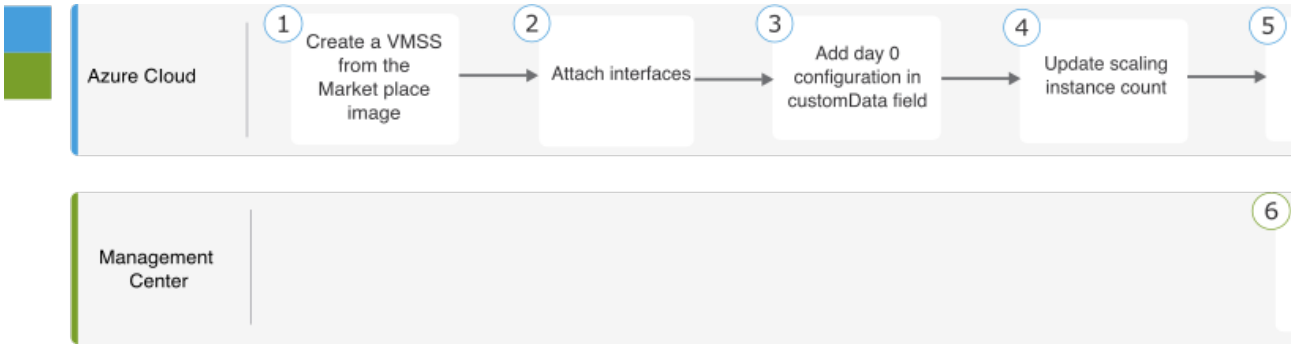
以下流程图说明使用 GWLB 在 Azure 中基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	使用所需的参数来修改 *azure_ftdv_gwlb_cluster.json* 和 *azure_ftdv_gwlb_cluster_parameters.json*。
3	Azure Cloud	创建资源组、虚拟网络和子网。
4	Azure Cloud	部署自定义模板。
5	Azure Cloud	配置实例详细信息。
6	集群节点	验证集群部署。
7	Azure Cloud	使用函数应用向管理中心注册集群。
8	Azure Cloud	创建 FTPS 凭证。
9	本地主机	将 *Cluster_Function.zip* 文件上传到 Function 应用。

手动部署

以下流程图说明了使用 GWLB 在 Azure 中手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从市场映像创建 VMSS。
2	本地主机	连接接口。
3	本地主机	在 customData 字段中添加 Day 0 配置。
4	本地主机	更新扩展实例计数。

	工作空间	步骤
5	本地主机	配置 GWLB。
6	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- azure_ftdv_gwlb_cluster_parameters.json - 用于为 Firewall Threat Defense Virtual 集群输入参数的模板
- azure_ftdv_gwlb_cluster.json - 用于部署 Firewall Threat Defense Virtual 集群的模板。

前提条件

- 要允许集群自动注册到管理中心，请在管理中心创建具有网络管理员和维护用户权限的用户。具有这些权限的用户可以使用 REST API。请参阅 Cisco Secure Firewall Management Center 管理指南。
- 在管理中心添加与您将在模板部署期间指定的策略名称匹配的访问策略。
- 确保 Management Center Virtual 已获得适当许可。
- 将集群添加到 Management Center Virtual 后，执行以下步骤：
  1. 使用管理中心中的运行状况检查端口号配置平台设置。有关配置此功能的详细信息，请参阅平台设置。
  2. 为数据流量创建静态路由。有关创建静态路由的详细信息，请参阅 添加静态路由。

     静态路由配置示例：

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```

注释 *vxlan_tunnel_gw* 是数据子网的网关 IP 地址。

使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

使用自定义的 Azure 资源管理器 (ARM) 模板为 Azure GWLB 部署虚拟机规模集。请注意，以下步骤中提到的模板可从 GitHub 上获取。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure。

b) 使用所需的参数来修改 azure_ftdv_gwlb_cluster.json 和 azure_ftdv_gwlb_cluster_parameters.json 。

步骤 2 登录到 Azure 门户：https://portal.azure.com。

步骤 3 创建一个资源组。

a) 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。

b) 选择所需的**区域 (Region)**。

步骤 4 创建一个包含三个子网的虚拟网络：管理子网、数据子网和集群控制链路 (CCL) 子网。

a) 创建虚拟网络。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。点击 **下一个：IP 地址**。

在 **IP 地址** 选项卡中，点击 **添加子网** ，然后添加以下子网 - 管理、数据和集群控制链路。

b) 添加子网。

步骤 5 部署自定义模板。

a) 点击 **创建** > **模板部署**（**使用自定义模板部署**）。

b) 点击 **在编辑器中生成自己的模板**。

c) 点击 **加载文件**，然后上传 **azure_ftdv_gwlb_cluster.json**。

d) 点击**保存**。

步骤 6 配置实例详细信息。

a) 输入所需的值，然后点击**查看 + 创建 (Review + create)**。

b) 在验证通过后，点击**创建 (Create)**。

步骤 7 在实例开始运行后，通过登录到任何一个节点并输入 **show cluster info** 命令来验证集群部署。

图 *209: show cluster info*

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

步骤 8 在 Azure 门户中，点击函数应用以将集群注册到 防火墙管理中心。

注释
如果您不想使用函数应用，也可以使用 **添加** > **设备**（而不是**添加** > **集群**）直接将控制节点注册到 防火墙管理中心 。其余集群节点将自动注册。

步骤 9 通过点击 **部署中心** > **FTPS 凭证** > **用户范围** > **配置用户名和密码** 来创建 FTPS 凭证，然后点击 **保存**。

步骤 10 通过在本地终端中执行以下 **curl** 命令，将 Cluster_Function.zip 文件上传到 Function 应用。

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

注释
curl 命令可能需要几分钟（约 2 到 3 分钟）才能完成命令执行。

函数将被上传到函数应用。功能将启动，而您可以在存储帐户的出站队列中看到日志。系统将向管理中心发起设备注册。

图 *210:* 功能

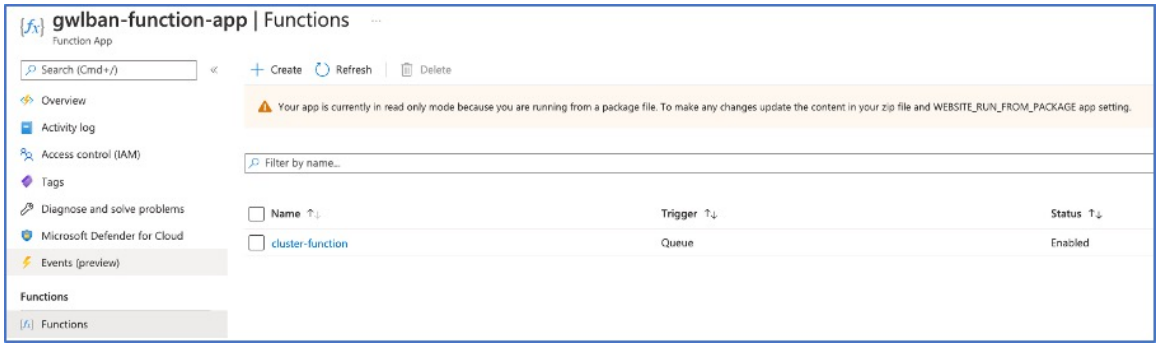


图 *211:* 队列

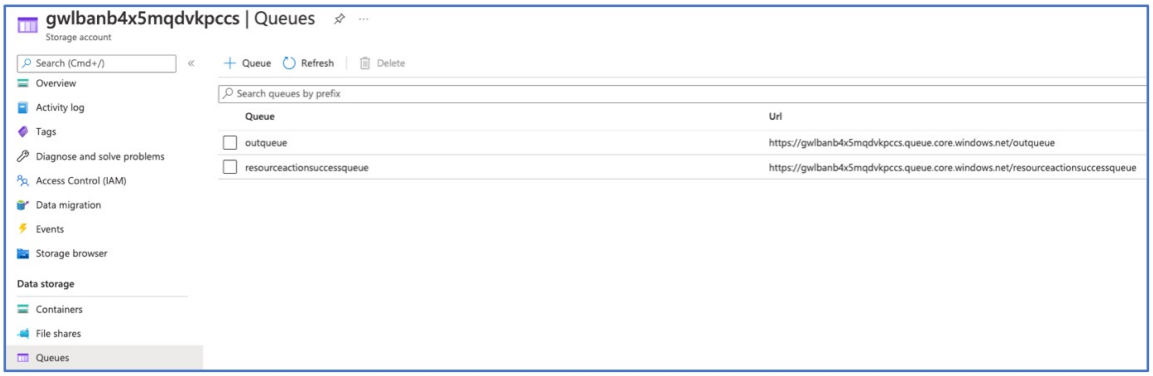
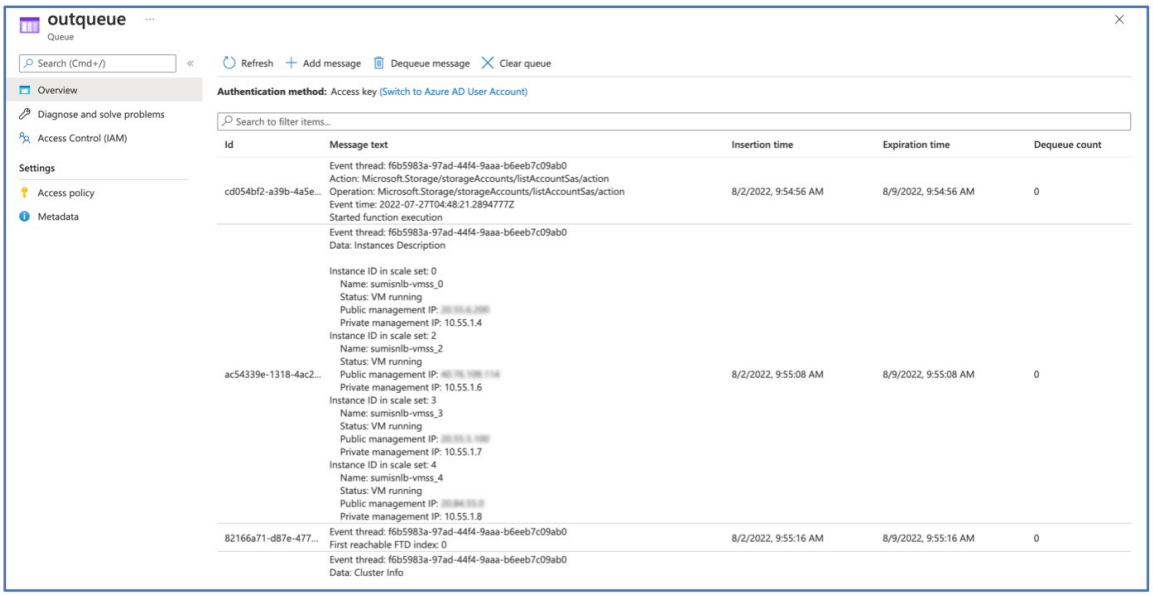
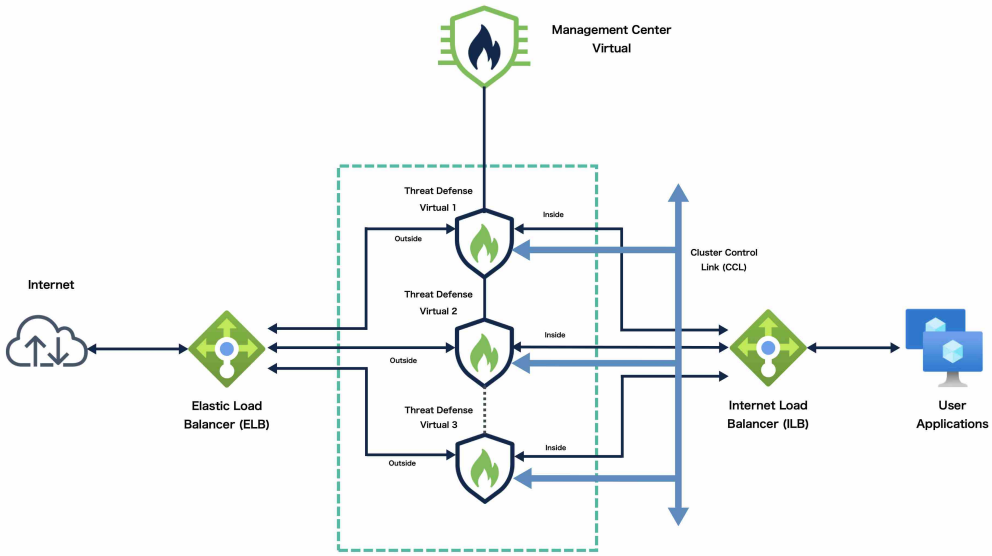


图 *212:* 出站队列



基于 NLB 的集群部署拓扑示例



此拓扑描述入站和出站流量。Threat Defense Virtual 集群夹在内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。

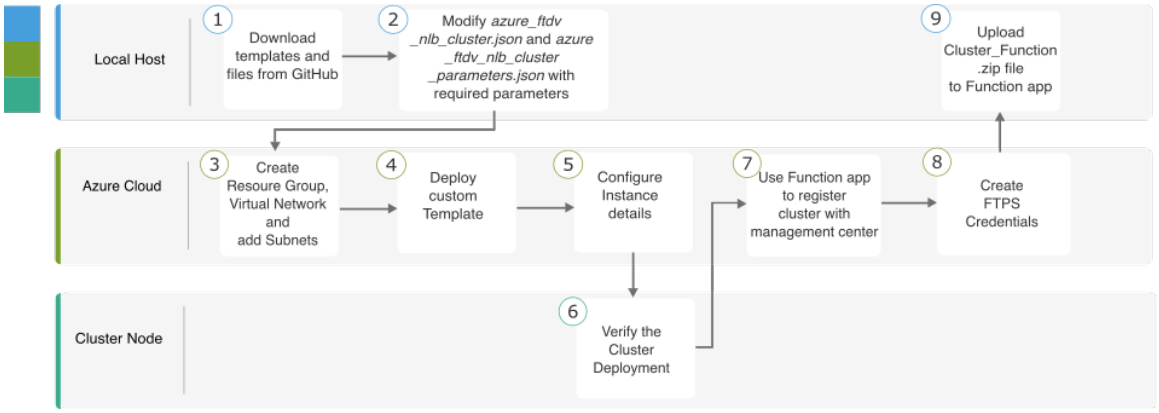
来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。集群中的 Threat Defense Virtual 实例检测到流量后，会将其转发到应用虚拟机。

来自应用虚拟机的出站流量将传输到内部负载均衡器。然后，流量会被转发到 Threat Defense Virtual 集群，然后再发送到互联网。

使用 NLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

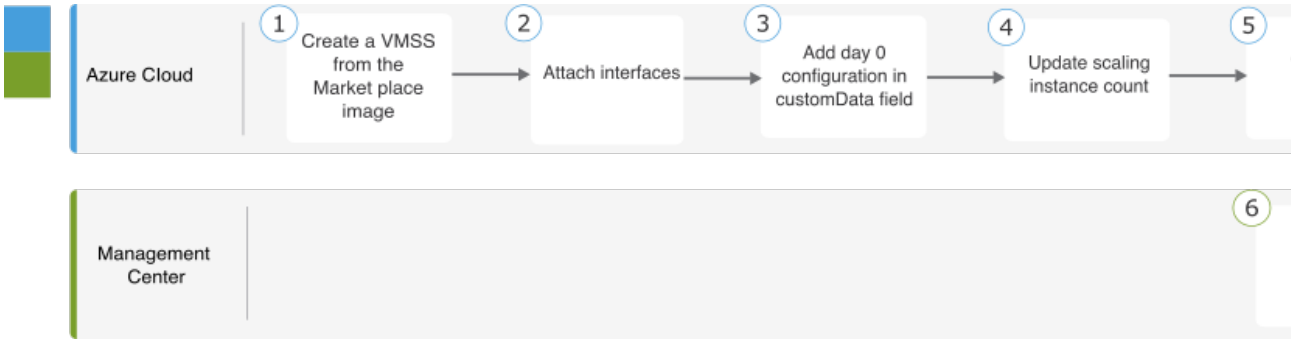
以下流程图说明了使用 NLB 在 Azure 中部署基于模板的 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	使用所需的参数来修改 *azure_ftdv_nlb_cluster.json* 和 *azure_ftdv_nlb_cluster_parameters.json* 。
3	Azure Cloud	创建资源组、虚拟网络和子网。
4	Azure Cloud	部署自定义模板。
5	Azure Cloud	配置实例详细信息。
6	集群节点	验证集群部署。
7	Azure Cloud	使用函数应用向管理中心注册集群。
8	Azure Cloud	创建 FTPS 凭证。
9	本地主机	将 *Cluster_Function.zip* 文件上传到 Function 应用。

手动部署

以下流程图说明了使用 NLB 在 Azure 中手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从市场映像创建 VMSS。
2	本地主机	连接接口。
3	本地主机	在 customData 字段中添加 Day 0 配置。
4	本地主机	更新扩展实例计数。

	工作空间	步骤
5	本地主机	配置 NLB。
6	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- azure_ftdv_nlb_cluster_parameters.json - 用于为具有 GWLB 的 Firewall Threat Defense Virtual 集群输入参数的模板
- azure_ftdv_nlb_cluster.json - 使用 GWLB 部署 Firewall Threat Defense Virtual 集群的模板。

前提条件

- 要允许集群自动注册到管理中心，请在管理中心创建具有网络管理员和维护用户权限的用户。具有这些权限的用户可以使用 REST API。请参阅 Cisco Secure Firewall Management Center 管理指南。
- 在管理中心添加与您将在模板部署期间指定的策略名称匹配的访问策略。
- 确保 Management Center Virtual 已获得适当许可。
- 将集群添加到 Management Center Virtual 后：
  1. 使用管理中心中的运行状况检查端口号配置平台设置。有关配置此功能的详细信息，请参阅平台设置。
  2. 为来自外部和内部接口的流量创建静态路由。有关创建静态路由的详细信息，请参阅 添加静态路由。

     外部接口的静态路由配置示例：

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```

注释 *ftdv-cluster-outside* 是外部子网的网关 IP 地址。

     内部接口的静态路由配置示例：

```
Network: any-ipv4
Interface: inside
```

```
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```

注释 *ftdv-cluster-inside-gw*是内部子网的网关 IP 地址。

3. 为数据流量配置 NAT 规则。有关配置 NAT 规则的详细信息，请参阅 网络地址转换。

使用 Azure 资源管理器模板通过 NLB 在 Azure 上部署集群

使用自定义的 Azure 资源管理器 (ARM) 模板为 Azure NLB 部署集群。请注意，以下步骤中提到的模板可从 GitHub 上获取。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure。

b) 使用所需的参数来修改 azure_ftdv_nlb_cluster.json 和 azure_ftdv_nlb_cluster_parameters.json。

步骤 2 登录到 Azure 门户：https://portal.azure.com。

步骤 3 创建一个资源组。

a) 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。

b) 选择所需的**区域 (Region)**。

步骤 4 创建具有四个子网的虚拟网络：管理、诊断、内部、外部和集群控制链路。

a) 创建虚拟网络。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. b) 选择所需的 **区域**。点击 **下一个：IP 地址**。

b) 添加子网。

在 **IP 地址** 选项卡中，点击 **添加子网** 并添加以下子网 - 管理、诊断、内部、外部和集群控制链路。

步骤 5 部署自定义模板。

a) 点击 **创建** > **模板部署**（**使用自定义模板部署**）。

b) 点击 **在编辑器中生成自己的模板**。

c) 点击 **加载文件**，然后上传 **azure_ftdv_nlb_cluster.json**。

d) 点击**保存**。

步骤 6 配置实例详细信息。

a) 输入所需的值，然后点击**查看 + 创建 (Review + create)**。

注释
对于集群控制链路的起始地址和结束地址，仅指定所需数量的地址（最多 16 个）。较大的范围可能会影响性能。

b) 在验证通过后，点击**创建 (Create)**。

步骤 7 在实例开始运行后，通过登录到任何一个节点并使用 **show cluster info** 命令来验证集群部署。

图 ***213: show cluster info***

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID          : 0
        Version     : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP      : 10.1.1.12
        CCL MAC     : 000d.3a55.5470
        Module      : NGFWv
        Resource    : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

步骤 8 在 Azure 门户中，点击函数应用以将集群注册到 防火墙管理中心。

注释
如果您不想使用函数应用，也可以使用 **添加 > 设备** （而不是 **添加 > 集群**）直接将控制节点注册到管理中心。其余集群节点将自动注册。

步骤 9 通过点击 **部署中心 > FTPS 凭证 > 用户范围 > 配置用户名和密码** 来创建 FTPS 凭证，然后点击 **保存**。

步骤 10 通过在本地终端中执行以下 **curl** 命令，将 Cluster_Function.zip 文件上传到 Function 应用。

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

注释
curl 命令可能需要几分钟（约 2 到 3 分钟）才能完成命令执行。

函数将被上传到函数应用。功能将启动，而您可以在存储帐户的出站队列中看到日志。系统将向管理中心发起设备注册。

在 Azure 中手动部署集群

要手动部署集群，请准备 day0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。

创建 Azure 的 Day0 配置

您可以使用固定配置或自定义配置。

使用 Azure 的固定配置创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

示例

下面给出了第 0 天的配置示例。

```
"Cluster": {
"CclSubnetRange": "10.45.3.4 10.45.3.30",     //mandatory user input
"ClusterGroupName": "ngfwv-cluster",          //mandatory user input
"HealthProbePort": "7777",                    //mandatory user input
"GatewayLoadBalancerIP": "10.45.2.4",         //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "2000",
"ExternalPort": "2001",
"InternalSegId": "800",
"ExternalSegId": "801"
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input**

对于 Azure 运行状况检查设置，请务必指定您在此处设置的 **HealthProbePort**。

对于 **CclSubnetRange** 变量，请指定从 xxx4 开始的 IP 地址范围。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始和结束 IP 地址的一些示例。

注释 所有集群基础设施子网都必须使用 /27 CIDR

表 *38:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

使用 Azure 的自定义配置创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

手动部署集群节点 - 基于 GWLB 的部署

部署集群节点，以便它们形成集群。

过程

步骤 1 登录到 Azure 门户：https://portal.azure.com

步骤 2 创建一个资源组。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。

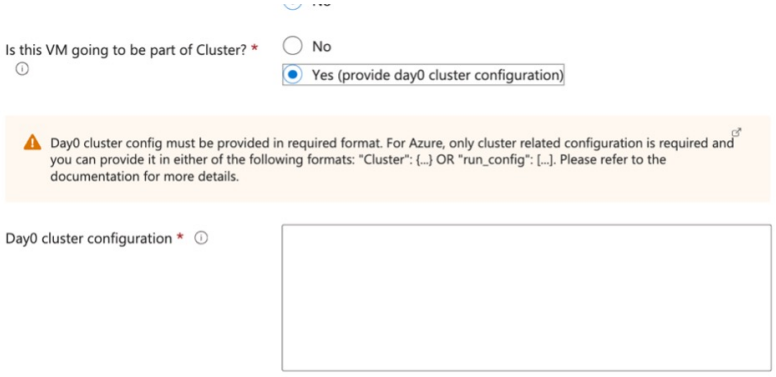
步骤 3 创建具有必要子网的虚拟网络：管理、数据和集群控制链路 (CCL)。

注释
根据需要使用最小子网配置 CCL。较宽的子网可能会影响性能。

请参阅有关创建虚拟网络和子网的 Azure 文档：https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

步骤 4 转到应用市场，搜索 **Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG**，然后点击**创建**。

步骤 5 填写必填详细信息，并为**此虚拟机是否将成为集群的一部分？**选择**是**。



将以下集群相关配置粘贴到文本框中。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name", //mandatory user input
"HealthProbePort": "port_number", //mandatory user input
"GatewayLoadBalancerIP": "ip_address",  //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

步骤 6 点击**下一步**，然后选择**虚拟网络和子网**。

步骤 7 点击**查看 + 创建**。等待 Threat Defense Virtual 部署完成。

步骤 8 连接到 Threat Defense Virtual 设备并使用 **show cluster info** 命令确认集群已成功建立。

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

步骤 9 配置 Azure 网关负载均衡器。有关详细信息，请参阅 Auto Scale 与 Azure 网关负载均衡器使用案例。

步骤 10 将控制节点添加到 防火墙管理中心。请参阅将集群添加到管理中心（手动部署），第 600 页。

手动部署集群节点 - 基于 NLB 的部署

部署集群节点，以便它们形成集群。

过程

步骤 1 登录到 Azure 门户：https://portal.azure.com

步骤 2 创建一个资源组。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。

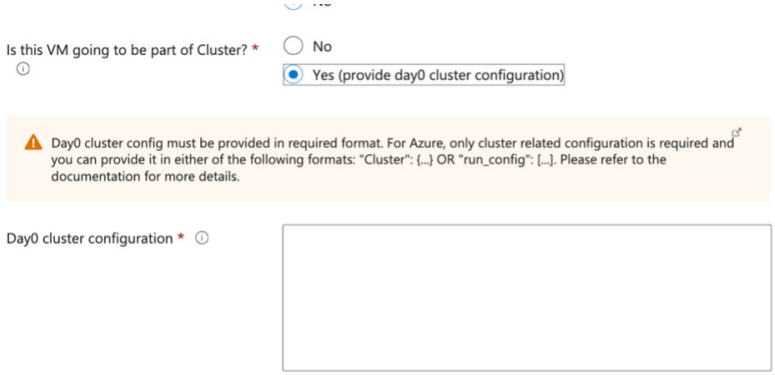
步骤 3 创建具有必要子网的虚拟网络：管理、内部、外部和集群控制链路 (CCL)。

注释
根据需要使用最小子网配置 CCL。较宽的子网可能会影响性能。

请参阅有关创建虚拟网络和子网的 Azure 文档：https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

步骤 4 转到应用市场，搜索 **Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG**，然后点击**创建**。

步骤 5 填写必填详细信息，并为**此虚拟机是否将成为集群的一部分？**选择**是**。



将以下集群相关配置粘贴到文本框中。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name" //mandatory user input
}
```

步骤 6 点击**下一步**，然后选择**虚拟网络和子网**。

步骤 7 点击**查看 + 创建**。等待 Threat Defense Virtual 部署完成。

步骤 8 连接到 Threat Defense Virtual 设备并使用 **show cluster info** 命令确认集群已成功建立。

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

步骤 9 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 600 页。

Azure 中的集群部署故障排除

- 问题：无流量

  故障排除：

  - 检查使用 GWLB 部署的 Threat Defense Virtual 实例的运行状况探测状态是否正常。
  - 如果 Threat Defense Virtual 实例的运行状况探测状态为不正常 -
    - 检查是否在 Management Center Virtual 中配置了静态路由。
    - 验证默认网关是否为数据子网的网关 IP。
    - 检查 Threat Defense Virtual 实例是否正在接收运行状况探测流量。
    - 检查在 Management Center Virtual 中配置的访问列表是否允许运行状况探测流量。

- 问题：集群未组建

  故障排除：

  - 检查 nve-only 集群接口的 IP 地址。确保您可以 ping 其他节点的仅 NVE 集群接口。
  - 检查仅 NVE 集群接口的 IP 地址是对象组的一部分。
  - 确保通过对象组来配置 NVE。
  - 集群组中的集群接口具有正确的 VNI 接口。此 VNI 接口具有相应对象组的 NVE。
  - 确保节点之间可相互 ping 通。由于每个节点都有自己的集群接口 IP，因此应该可以相互 ping 通。

- 验证模板部署期间提及的CCL子网的开始地址和结束地址是否正确。起始地址必须以子网中的第一个可用的 IP 地址开头。例如，如果子网为 192.168.1.0/27。那么起始地址应为 192.168.1.4（前三个 IP 地址由 Azure 保留）
- 检查 Management Center Virtual 是否具有有效的许可证。

- 问题：在同一资源组中再次部署资源时出现任何与角色相关的错误。

  故障排除：在终端上使用以下命令删除下面给出的角色。

  错误消息：

```
"error": {
"code": "RoleAssignmentUpdateNotPermitted",
"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be
updated.” }
```

  - **az role assignment delete --resource-group** <资源组名称> **--role "Storage Queue Data Contributor"**
  - **az role assignment delete --resource-group** <资源组名称> **--role "Contributor"**

Azure 中的 Firewall Threat Defense Virtual 集群 Autoscale 解决方案

Azure 区域中的典型集群部署包括规定数量的 Firewall Threat Defense Virtual 实例（节点）。当 Azure 区域流量变化时，如果没有动态扩展（自动扩展）节点，这种集群安排中的资源利用率可能未充分利用资源或导致延迟。思科在 7.7 及更高版本中为 Firewall Threat Defense Virtual 集群提供自动扩展解决方案，支持动态扩展 Azure 区域中的节点。它允许您根据网络流量从集群内向内扩展或横向扩展节点。它使用基于 Azure VMSS 指标（如 CPU 和内存指标）的资源利用率统计信息的逻辑，动态添加或删除集群中的节点。

Azure 中使用自动扩展解决方案的 Firewall Threat Defense Virtual 集群同时支持网络负载均衡器（NLB 或三明治拓扑）和网关负载均衡器 (GWLB)。请参阅拓扑示例，第 555 页

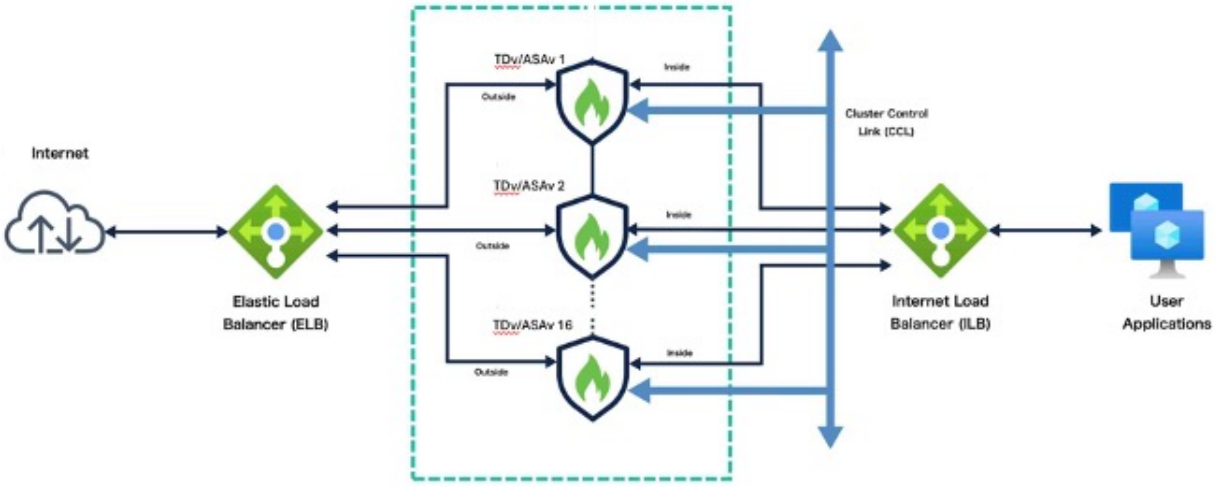
思科提供单独的 Azure 资源管理器 (ARM) 模板用于使用 NLB 和 GWLB 在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群，并提供基础设施和配置模板用于部署函数应用和逻辑应用等 Azure 服务。

拓扑示例

Firewall Threat Defense Virtual 使用三明治拓扑（网络负载均衡器）在 Azure 中通过自动扩展建立集群

Azure 中使用三明治拓扑结构 (NLB) 的自动扩展的 Firewall Threat Defense Virtual 集群用例是一种自动水平缩放解决方案，它将 Firewall Threat Defense Virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

在此拓扑中，Firewall Threat Defense Virtual 仅使用四个接口：管理、内部、外部和 CCL 子网。



Firewall Threat Defense Virtual 使用三明治拓扑 (NLB) 在 Azure 中通过自动扩展建立集群

下面简要介绍了 Firewall Threat Defense Virtual集群如何使用 NLB 功能在 Azure 中进行自动扩展：

- ELB 将流量从互联网分发到规模集中的 Firewall Threat Defense Virtual 实例；然后，防火墙将流量转发到应用。
- ILB 将出站互联网流量从应用分发到规模集中的 Firewall Threat Defense Virtual 实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 Firewall Threat Defense Virtual实例数将根据负载条件自动进行扩展和配置。

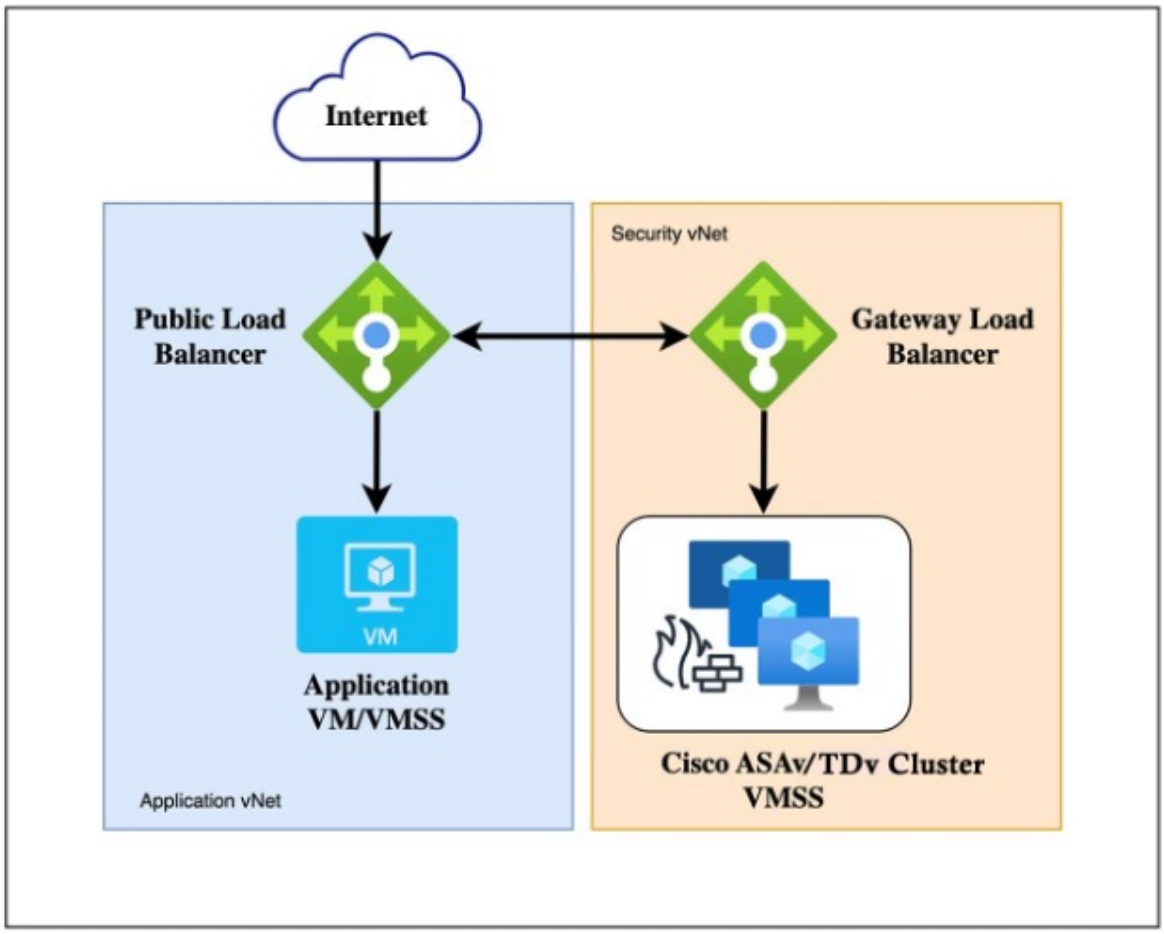
Firewall Threat Defense Virtual 使用网关负载均衡器在 Azure 中建立自动扩展集群

使用自动扩展解决方案的 Azure 网关负载均衡器 (GWLB) 与 Firewall Threat Defense Virtual 集群集成可简化集群设置中的实例部署、管理和扩展。Azure 网关负载均衡器 (GWLB) 可确保 Cisco Secure Firewall 检查进出 Azure VM（例如应用服务器）的互联网流量，而无需更改任何路由。这种集成还降低了操作复杂性，并为防火墙上的流量提供了单一的入口和出口点。应用和基础设施可以保持源 IP 地址的可视性，而这在某些环境中至关重要。

Firewall Threat Defense Virtual 在此使用案例中仅使用三个接口：管理、数据和 CCL 接口。

注释

- 如果要部署 Azure GWLB，则不需要网络地址转换 (NAT)。
- 仅支持 IPv4。



下面简要介绍了 Firewall Threat Defense Virtual集群如何使用 GWLB 功能在 Azure 中进行自动扩展：

- 来自互联网的入站流量会进入 GWLB 端点，然后由端点将流量传输到 GWLB。
- 然后，流量将路由到 Firewall Threat Defense Virtual 集群。
- 集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机。

前提条件

- 确保您在 Azure 订阅中具有所有者角色。
- 创建 Azure 资源组。确保已创建 Azure 虚拟网络以及必要的子网。
  - 基于 NLB 的集群接口：管理、诊断、内部、外部、CCL 和函数应用。
  - 基于 GWLB 的集群接口：管理、诊断、数据、CCL 和函数应用。
- 在管理中心上：

- 确保 Management Center Virtual 已正确授权。
- 创建访问控制策略。
- 为接口创建安全区域(SZ)对象。对于基于NLB的集群，为内部和外部接口创建安全区域。对于基于 GWLB 的集群，为数据接口创建安全区域。
- 为 Azure 函数创建单独的用户名和密码，以将 Threat Defense Virtual 实例添加到 Management Center Virtual 并配置这些实例。

- 在本地系统上安装 Azure CLI。
- 从 GitHub 将 Azure 集群自动扩展存储库下载到本地计算机，并运行命令 **python3 make.py build** 创建 Azure 函数 zip 文件。

Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑

扩展策略

在具有自动扩展的集群中，节点的扩展根据以下策略确定：

- 扩展策略 1 - 当一个集群节点超过资源使用限制时。
- 扩展策略 2 - 所有节点的总体平均资源利用率。

横向扩展

横向扩展是指当流量负载阈值超过任何一个集群节点上配置的CPU或内存限制时，向集群添加新节点的过程。

以下是在横向扩展期间向集群添加新节点的过程：

1. 已启动一个新的 Firewall Threat Defense Virtual 实例。
2. 相应配置将被应用于 Firewall Threat Defense Virtual。
3. 已应用适当的许可证。
4. 一个新的 Firewall Threat Defense Virtual 实例将被添加到集群中。

如果在横向扩展过程中，新的 Firewall Threat Defense Virtual 实例的配置失败（低概率），则会终止失败的实例，并启动和配置一个新实例。

内向扩展

内向扩展是指当配置的内向扩展阈值和群集实例总数超过最小集群规模时，将节点从群集中移除的过程。

以下是在内向扩展过程中终止集群中一个节点的过程：

1. 使用 VMSS 指标确定 CPU 或内存使用率最低的 Firewall Threat Defense Virtual 实例。
2. 如果有多个实例具有相同的最低利用率，则选择 VMSS 中 VM 索引较高的实例进行内向扩展。

3. 通过适当的配置和策略，该实例的任何新连接都会被禁用。
4. 实例会从智能许可中注销（适用于 BYOL）。
5. 实例将被终止。

Azure Functions（函数应用）

Function 应用可帮助启用 Firewall Threat Defense Virtual 群集并在管理中心注册。Function 应用还可以帮助您为支持自动扩展部署的 Firewall Threat Defense Virtual 集群选择托管计划。

提供以下两种类型的托管计划：

- 使用量
  - 这是具有自动扩展功能的 Firewall Threat Defense Virtual 集群的默认托管计划。
  - 该计划允许 Function 应用通过打开 SSH 端口连接到该区域的 Azure 数据中心 IP 地址，从而连接到 Firewall Threat Defense Virtual 实例。
- 高级
  - 您可以在部署期间为 Function 应用选择此托管计划。
  - 此计划支持将网络地址转换 (NAT) 网关添加到 Function 应用，以控制 Function 应用的出站 IP 地址。此计划仅允许从 NAT 网关的固定 IP 地址对 Firewall Threat Defense Virtual 实例进行 SSH 访问，从而增强安全性。

有关自动扩展解决方案组件概述的详细信息，请参阅《*Cisco Secure Firewall Threat Defense Virtual* 入门指南》中的自动扩展解决方案组件。

GitHub 上的部署和基础设施模板

思科提供 Azure 资源管理器 (ARM) 模板和脚本，用于使用多个 Azure 服务（包括函数应用、逻辑应用、自动扩展组等）部署 Firewall Threat Defense Virtual 集群的自动扩展组。

Firewall Threat Defense Virtual 集群的自动扩展解决方案是基于 ARM 模板的部署，可提供：

- 使用 Function 应用与管理中心进行完全自动化的 Firewall Threat Defense Virtual 实例注册和注销注册。
- 自动应用到横向扩展 Threat Defense Virtual 实例的 NAT 策略、访问控制策略和路由。
- 支持 GWLB 和 NLB 负载均衡器。
- 仅适用于管理中心；不支持设备管理器。

使用自动扩展解决方案模板的 Firewall Threat Defense Virtual 集群

Azure 资源管理器 (ARM) 模板

根据您在 Azure 中为集群使用的（NLB 或 GWLB）负载均衡器，为自动扩展解决方案提供了两套模板。

GitHub 上提供了以下模板：

- 使用 NLB 的 Firewall Threat Defense Virtual 集群的自动扩展解决方案模板：`azure_ftdv_nlb_cluster.json.json`，可从文件夹 `arm-templates` 获取。
- 使用 GWLB 的 Firewall Threat Defense Virtual 集群的自动扩展解决方案模板：`azure_ftdv_gwlb_cluster.json`，可从文件夹 `arm-templates` 获取。

设置 Azure 基础架构和配置

- 用于在 Firewall Threat Defense Virtual 实例上启用集群的函数应用：`cluster_functions.zip`。
- Firewall Threat Defense Virtual 用于部署、缩容和扩容工作流的逻辑应用代码：`logical_app.txt`。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，就可以在将 Azure 资源管理器 (ARM) 模板部署到 Azure 订阅时使用这些参数来创建 Firewall Threat Defense Virtual 设备。在使用 GWLB for Azure 的自动扩展集群中，还创建了网络基础设施，因此必须在模板中配置额外的输入参数。参数说明的含义不言自明。

表 *39:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*（3-10 个字符）	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。 示例：ftdv	New
virtualNetworkRg	字符串	虚拟网络资源组名称。 示例：cisco-virtualnet-rg	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）。 示例：cisco-virtualnet	现有
virtualNetworkCidr	CIDR 格式 x.x.x.x/y	虚拟网络的 CIDR（已创建）	现有
mgmtSubnet	字符串	管理子网名称（已创建） 示例：cisco-mgmt-subnet	现有

参数名	允许的值/类型	说明	资源创建类型
dataSubnet	字符串	数据子网名称（已创建） 示例：cisco-data-subnet	
cclSubnet	字符串	集群控制链路子网名称。 示例：cisco-ccl-subnet	
cclSubnetStartAddr	字符串	CCL 子网 IP 地址的起始范围。 示例：3.4.5.6	
cclSubnetEndAddr	字符串	CCL 子网 IP 地址的结束范围。 示例：5.6.7.8	
gwlbIP	字符串	GWLB 已在现有数据子网中创建。 示例：10.0.2.4	
dataNetworkGatewayIp	字符串	数据子网的网关 IP 地址。 示例：10.0.2.7	
outsideSecurityZoneName	字符串	在管理中心创建的安全区对象名称 示例：outside-sz	
TDvmManagementUserName	字符串	TDv 管理员用户名。 不允许提供“admin”作为用户名。	
diagSubnet	字符串	诊断子网名称（已创建）。 示例：cisco-diag-subnet	现有
insideSubnet	字符串	内部子网名称（已创建）。 示例：cisco-inside-subnet	现有
internalLbIp	字符串	内部子网的内部负载均衡器 IP 地址（已创建）。 例如：1.2.3.4	现有
insideNetworkGatewayIp	字符串	内部子网网关 IP 地址（已创建）。	现有
outsideSubnet	字符串	外部子网名称（已创建）。 示例：cisco-outside-subnet	现有

参数名	允许的值/类型	说明	资源创建类型
outsideNetworkGatewayIp	字符串	外部子网网关 IP（已创建）。	现有
deviceGroupName	字符串	防火墙管理中心中的设备组（已创建）	现有
insideZoneName	字符串	防火墙管理中心中的内部区域名称（已创建）	现有
outsideZoneName	字符串	防火墙管理中心中的外部区域名称（已创建）	现有
softwareVersion	字符串	Firewall Threat Defense Virtual 版本（在部署期间从下拉列表中选择）。	现有
vmSize	字符串	Firewall Threat Defense Virtual 实例的大小（在部署过程中从下拉列表中选择）。	不适用
ftdLicensingSku	字符串	Firewall Threat Defense Virtual 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
tdVmManagementUserName	字符串*	Firewall Threat Defense Virtual VM 管理管理员用户名。 这**不能**是“admin”。请参阅 Azure 以了解 VM 管理员用户名准则。	New
tdVmManagementUserPassword	字符串*	Firewall Threat Defense Virtual VM 管理管理员用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 **注释** 模板中不对此进行合规性检查。	New

参数名	允许的值/类型	说明	资源创建类型
ftdAdminUserPassword	字符串	Firewall Threat Defense Virtual 管理员用户密码。 **注释** 针对 **TDvmManagementUserPassword** 参数提到的条件也适用于此参数。	
fmcIpAddress	字符串 x.x.x.x	防火墙管理中心 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	防火墙管理中心用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 防火墙管理中心 用户名的防火墙管理中心密码（已创建）	现有
policyName	字符串	在 防火墙管理中心 中创建的安全策略（已创建）	现有
clusterGroupName	字符串	在将威胁防御设备注册到管理中心时使用的集群组名称。 示例：tdv-cluster	
healthCheckPortNumber	字符串	在网关负载均衡器中创建运行状况探测器时使用的运行状况检查端口号。 示例：8080	
functionHostingPlan	字符串	功能部署托管计划（消耗使用使用量托管计划，高级：使用高级托管计划）。 默认值：功耗	
functionAppSubnet	字符串	函数应用子网名称（已创建）。 示例：tdv-fapp-subnet	
functionAppSubnetCIDR	字符串	函数应用子网的 CIDR（已创建）。 示例：10.0.4.0/27	
scalingMetricsList	字符串	用于确定扩展决定的指标。 允许：CPU 和内存	

参数名	允许的值/类型	说明	资源创建类型
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 Firewall Threat Defense Virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 Firewall Threat Defense Virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 Firewall Threat Defense Virtual 设备的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	不适用
scalingMetricsList	字符串	用于制定扩展决策的指标。 允许：CPU、内存 默认值：CPU	不适用
cpuScaleInThreshold	字符串	CPU 指标的内向扩展阈值（以百分比为单位）。 默认值：10 当 Firewall Threat Defense Virtual 指标低于此值时，将触发扩展。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 558 页。	不适用

参数名	允许的值/类型	说明	资源创建类型
cpuScaleOutThreshold	字符串	CPU指标的横向扩展阈值（以百分比为单位）。 默认值：80 当 Firewall Threat Defense Virtual 指标高于此值时，将触发横向扩展。 “cpuScaleOutThreshold”应始终**大于**“cpuScaleInThreshold”。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 558 页。	不适用
memoryScaleInThreshold	字符串	内存指标的内向扩展阈值（以百分比为单位）。 默认值：0 当 Firewall Threat Defense Virtual 指标低于此值时，将触发扩展。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 558 页。	不适用
memoryScaleOutThreshold	字符串	内存指标的横向扩展阈值（以百分比为单位）。 默认值：0 当 Firewall Threat Defense Virtual 指标高于此值时，将触发横向扩展。 “memoryScaleOutThreshold”应始终**大于**“memoryScaleInThreshold”。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 558 页。	不适用
minFtdCount	整数	在任何给定时间，规模集中可用的最小 Firewall Threat Defense Virtual 实例数。 示例：2	不适用

参数名	允许的值/类型	说明	资源创建类型
maxFtdCount	整数	规模集中允许的最大 Firewall Threat Defense Virtual 实例数。 示例：10 **注释** 此数量受 防火墙管理中心 容量的限制。 Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值，并且基于此平均值做出扩展决定。 **注释** 由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用

参数名	允许的值/类型	说明	资源创建类型
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 Firewall Threat Defense Virtual 实例时。 BULK：Auto Scale 管理器将尝试一次并行部署“minFtdCount”数量的 Firewall Threat Defense Virtual 实例。 **注释** 启动采用并行方式，但由于 防火墙管理中心 的限制，需要按顺序注册到 防火墙管理中心。 STEP：Auto Scale 管理器将按照计划间隔逐个部署“minFtdCount”数量的 Firewall Threat Defense Virtual 设备。 **注释** STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 防火墙管理中心 进行配置，然后实现运行，但在调试时很有帮助。 BULK 选项启动所有“minFtdCount”数量的 Firewall Threat Defense Virtual 所花费的时间与一次 Firewall Threat Defense Virtual 启动相同（因为它是并行运行的），但 防火墙管理中心 注册是按顺序进行的。 部署“minFtdCount”数量的 Firewall Threat Defense Virtual 所花费的总时间 =（启动一个 Firewall Threat Defense Virtual 所用的时间 + 注册/配置一个 Firewall Threat Defense Virtual 所用的时间 * minFtdCount）。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

Firewall Threat Defense Virtual 具有自动扩展部署过程和资源的集群

Firewall Threat Defense Virtual 在 Azure 上部署具有自动扩展功能的集群涉及以下内容：

- 部署 ARM 模板。
- 构建并部署集群功能。
- 更新并启用逻辑应用。

Azure 资源管理器模板部署资源

对于三明治拓扑 **(NLB)** - `azure_ftdv_nlb_cluster_autoscale.json`，当使用 ARM 模板在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群时，会在资源组中创建以下资源

- 虚拟机规模集 (VMSS)
- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

当使用 GWLB - `azure_ftdv_gwlb_cluster_autoscale.json`在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群时，会在资源组中创建以下资源

- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网关负载均衡器 (GWLB)
- Azure 函数应用
- 逻辑应用
- 网络基础设施
- 部署所需的安全组和其他各种组件。

使用自动扩展解决方案部署 Firewall Threat Defense Virtual 集群

使用 ARM 模板在 Azure 上部署具有自动扩展解决方案的 Threat Defense Virtual 集群。根据拓扑结构、三明治 (NLB) 使用案例或 GWLB 使用案例，您需要下载并配置适当的 ARM 模板，以便在 Azure 上部署支持自动扩展的 Firewall Threat Defense Virtual 集群解决方案。

开始之前

从 GitHub 下载部署软件包

面向 Azure 的使用 NLB 解决方案的 Firewall Threat Defense Virtual 集群自动扩展是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

面向 Azure 的使用 GWLB 解决方案的 Firewall Threat Defense Virtual 集群是一种基于 ARM 模板的部署，可创建 GWLB、网络基础设施、Threat Defense Virtual 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

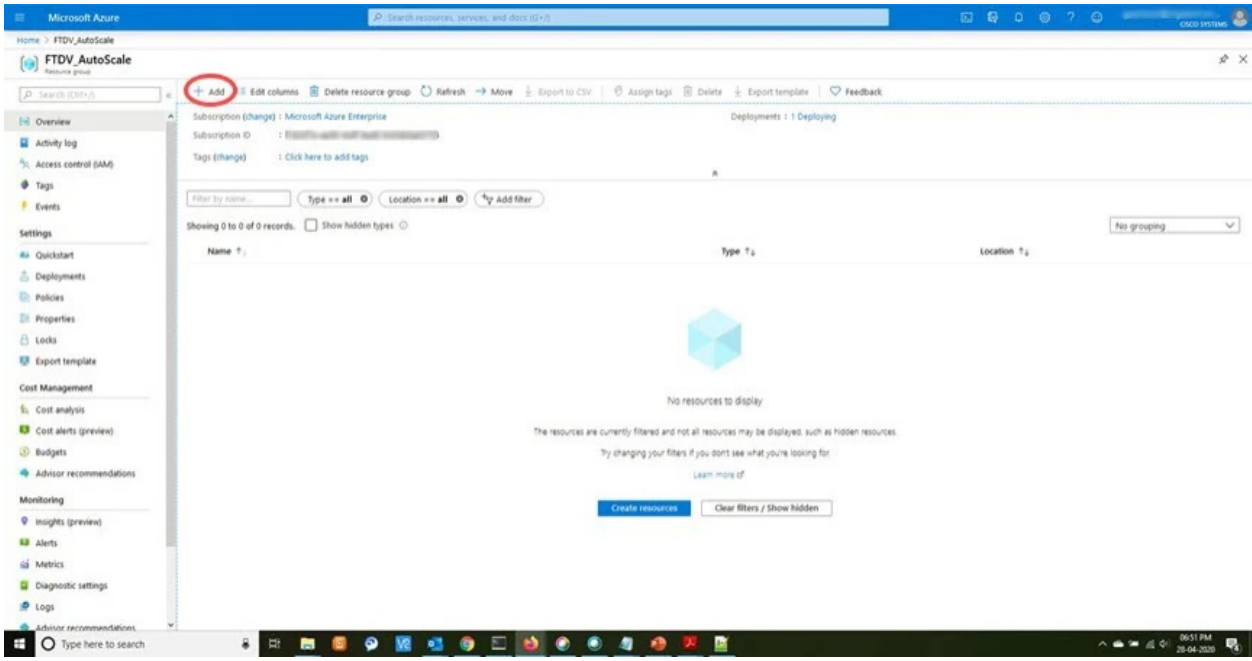
下载启动面向 Azure 的使用自动扩展解决方案的 Firewall Threat Defense Virtual 集群所需的文件。

您的版本的部署脚本和模板可从 GitHub 存储库获取。

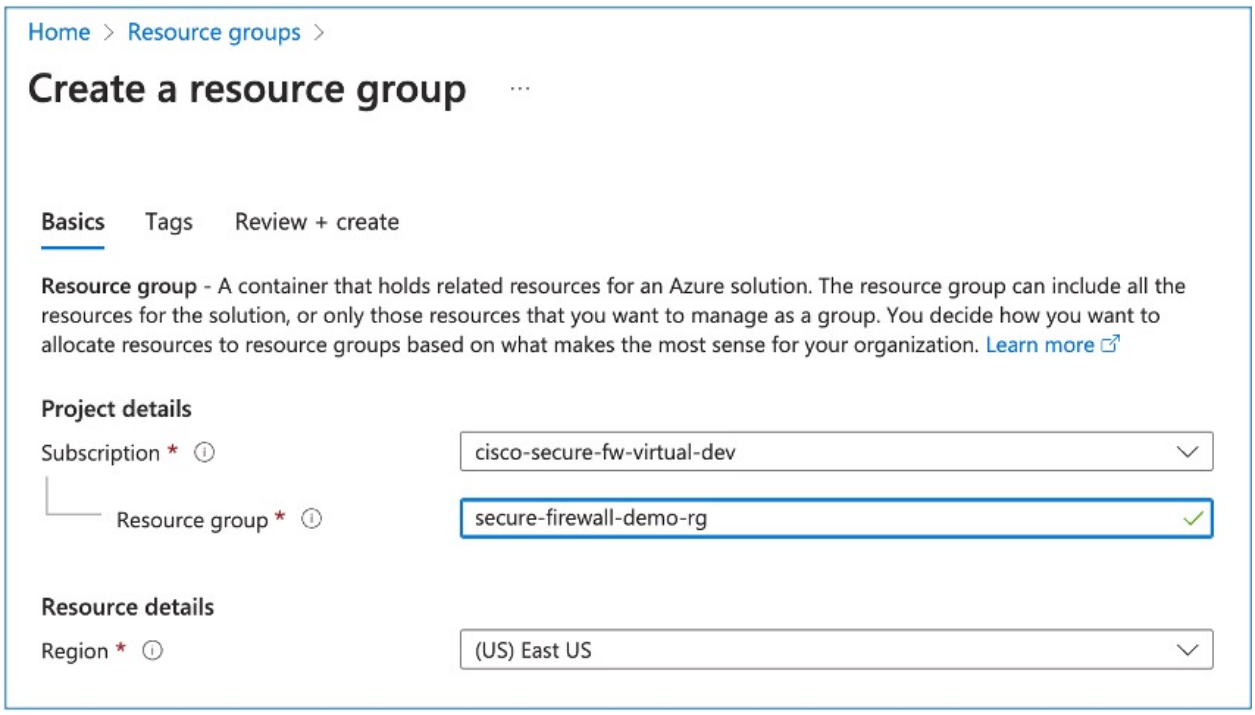
过程

步骤 1 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户 (https://portal.azure.com)。

步骤 2 点击服务菜单中的**资源组 (Resource groups)** 以访问**资源组 (Resource Groups)** 边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。创建一个新的资源组或选择一个现有的空资源组。例如， **threat defense virtual_AutoScale**。

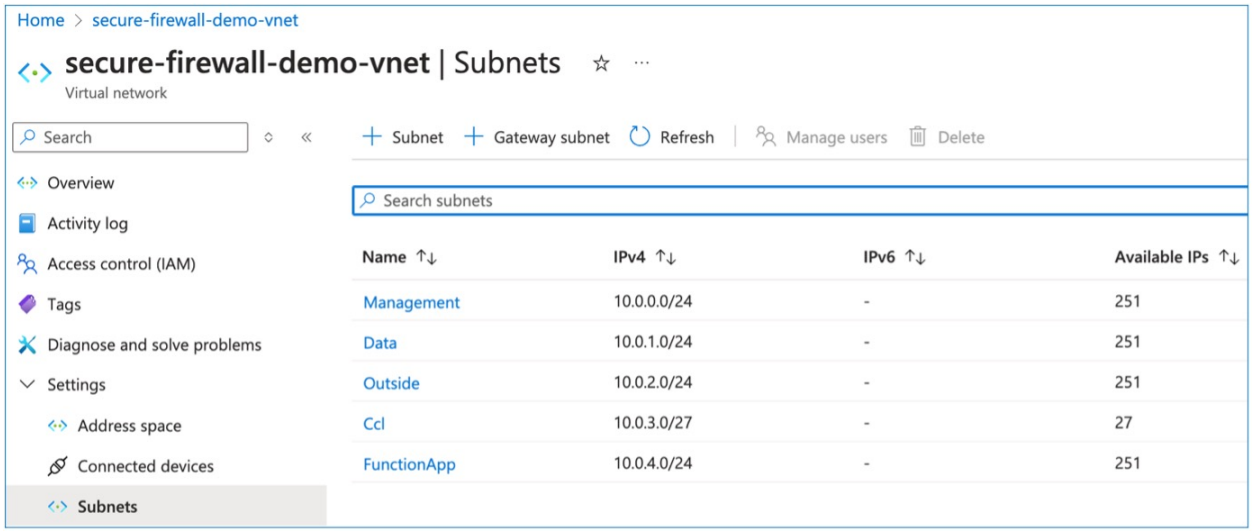


步骤 3 点击**创建资源 (+) (Create a resource [+])**，为模板部署创建新资源。此时将显示**创建资源组 (Create Resource Group)** 边栏选项卡。



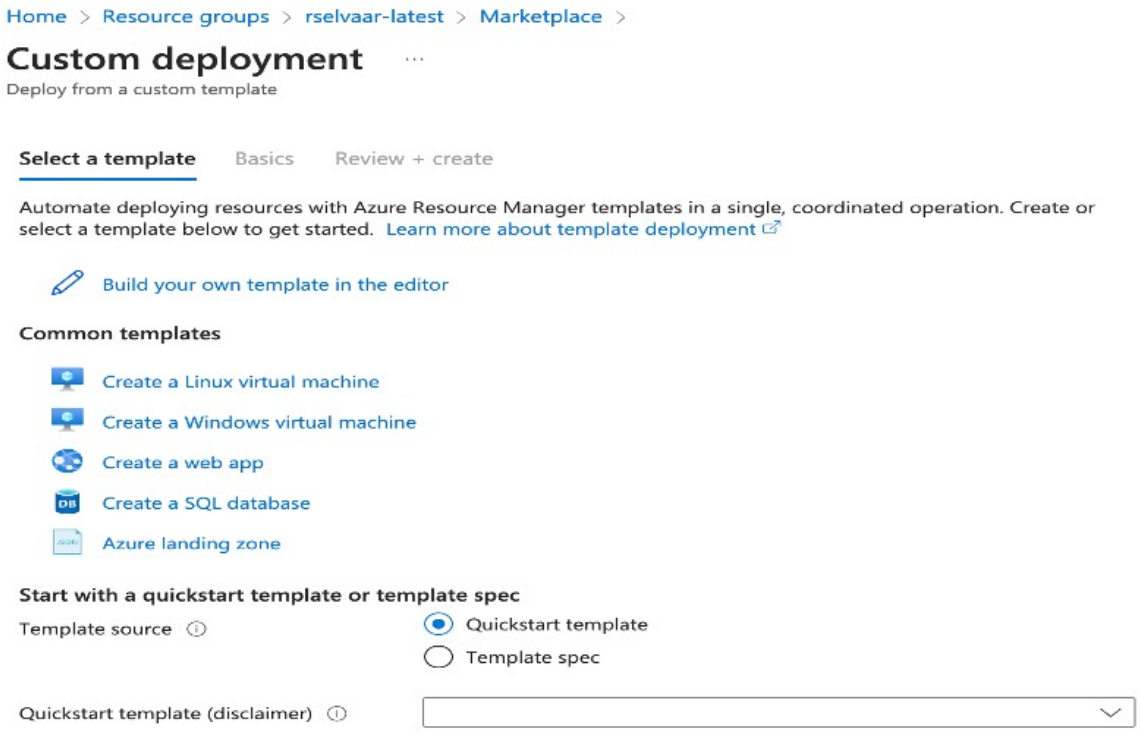
步骤 4 4. 点击服务菜单中的**虚拟网络 (Virtual Network)**，以访问“虚拟”(Virtual) 网络边栏选项卡。使用子网创建虚拟网络。

- 对于 GWLB 部署，创建包含管理、数据、CCL 子网和函数应用的虚拟网络。
- 对于 NLB 部署，创建包含管理、内部、外部、CCL 子网和函数应用的虚拟网络。

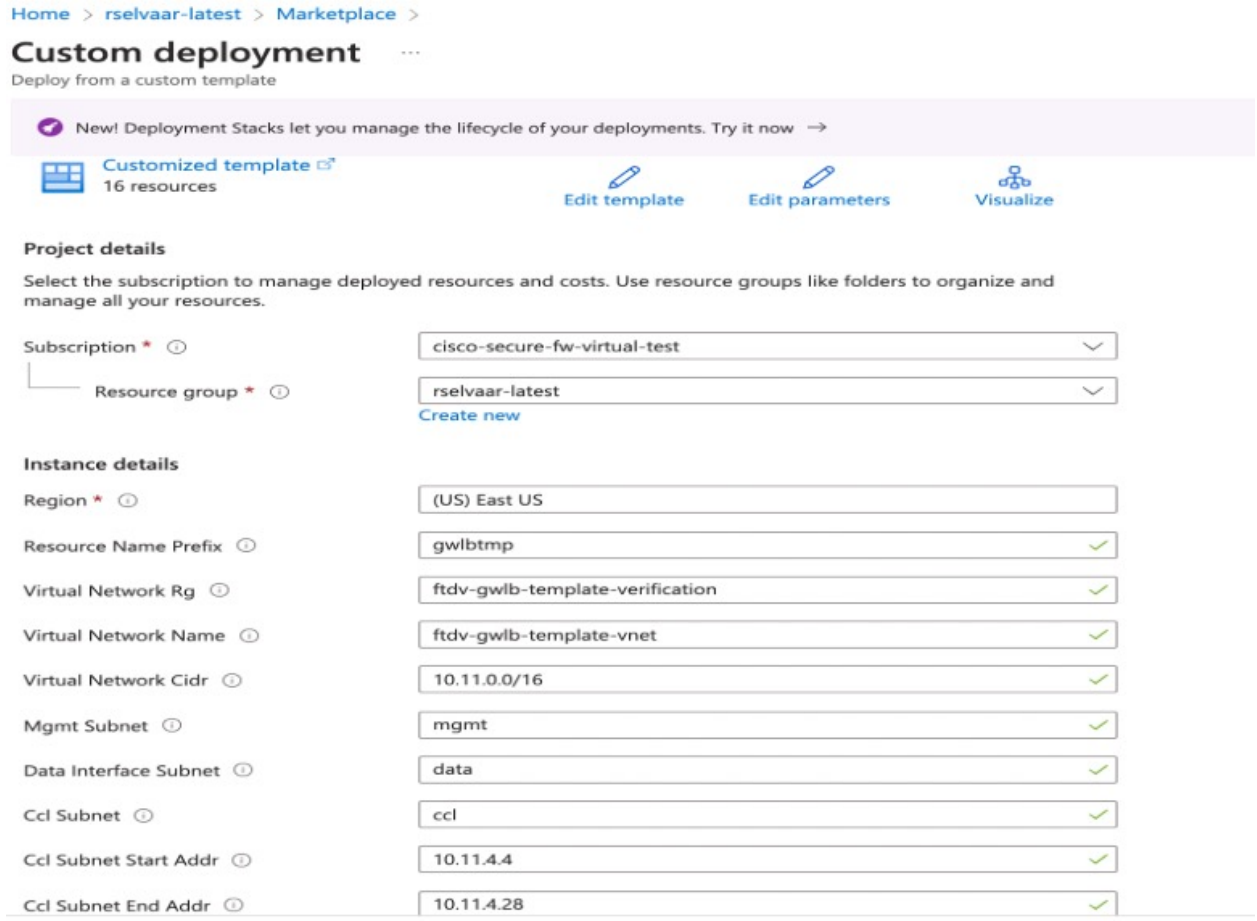


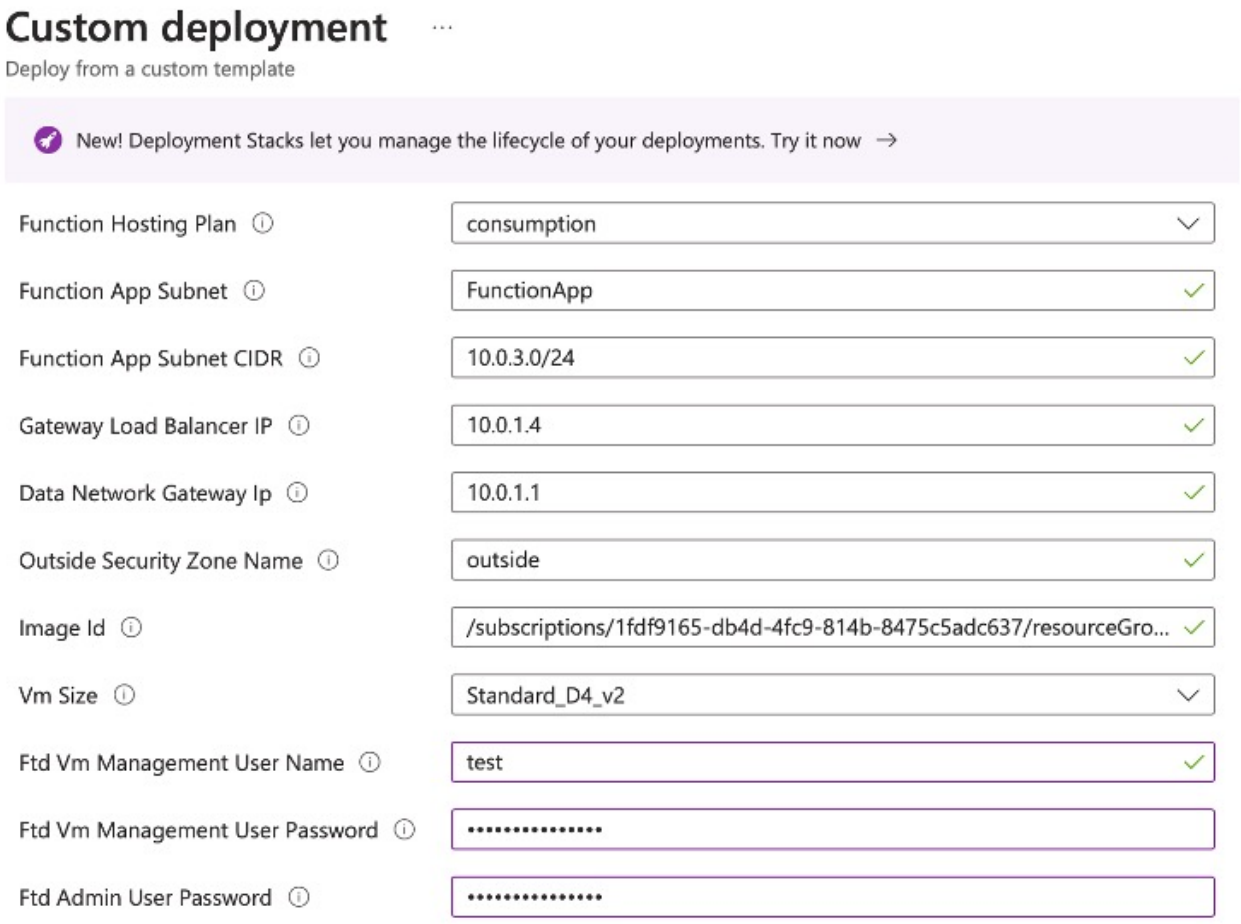
步骤 5 在**搜索市场 (Search the Marketplace)** 中，键入**模板部署 (Template deployment)**（使用自定义模板部署），然后按 **Enter**。

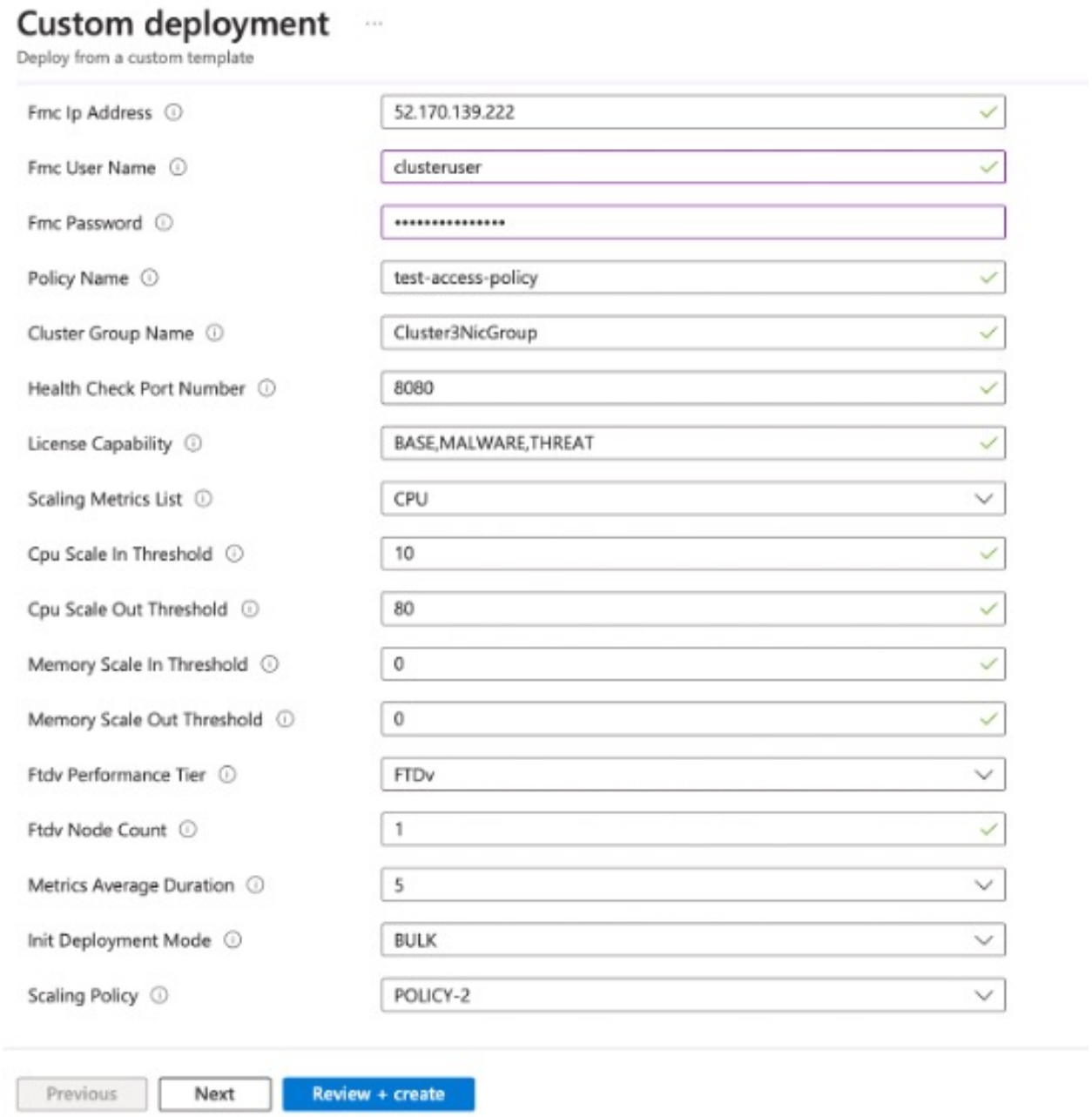
步骤 6 点击**创建 (Create)**。创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板 (Build your own template in editor)**。



步骤 7 在**编辑模板**窗口中，删除所有默认内容并从更新的 `azure_ftdv_gwlb_cluster_custom_image.json` 或 `azure_ftdv_nlb_cluster_custom_image.json`（具体取决于您在 Azure 上部署的自动扩展解决方案的类型）复制内容，然后点击**保存**。或者点击**加载文件 (Load file)**，从您的计算机浏览并上传此文件。


Home > rselvaar-latest > Marketplace >
Custom deployment
Deploy from a custom template
New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →
Customized template
16 resources
Edit template
Edit parameters
Visualize
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
cisco-secure-fw-virtual-test
Resource group *
rselvaar-latest
Create new
Instance details
Region *
(US) East US
Resource Name Prefix
gwlbtmp
Virtual Network Rg
ftdv-gwlb-template-verification
Virtual Network Name
ftdv-gwlb-template-vnet
Virtual Network Cidr
10.11.0.0/16
Mgmt Subnet
mgmt
Data Interface Subnet
data
Ccl Subnet
ccl
Ccl Subnet Start Addr
10.11.4.4
Ccl Subnet End Addr
10.11.4.28


Custom deployment
...
Deploy from a custom template
New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →
Function Hosting Plan
consumption
Function App Subnet
FunctionApp
Function App Subnet CIDR
10.0.3.0/24
Gateway Load Balancer IP
10.0.1.4
Data Network Gateway Ip
10.0.1.1
Outside Security Zone Name
outside
Image Id
/subscriptions/1fdf9165-db4d-4fc9-814b-8475c5adc637/resourceGro...
Vm Size
Standard_D4_v2
Ftd Vm Management User Name
test
Ftd Vm Management User Password
Ftd Admin User Password



步骤 8 在参数字段部分中填写所有参数。有关每个参数的详细信息，请参阅输入参数，然后点击**查看+创建 (Review+Create)**。

步骤 9 模板部署成功后，就会为 Azure 解决方案创建 Threat Defense Virtual 自动扩展所需的所有资源。请参阅下图中的资源。**类型 (Type)** 列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

下一步做什么

部署 Azure Functions 应用 ， 第 575 页。

部署 Azure Functions 应用

部署 ARM 模板时，Azure 会创建名称为 **<resourceNamePrefix>-function-app** 的功能应用。

过程

步骤 1 转到部署 ARM 模板时创建的 Function 应用，并执行以下操作：

从本地计算机运行以下命令，将集群自动扩展 Azure Functions 部署到函数应用。

```
az functionapp deployment source config-zip -g <Resource Group Name>
-n <Function App Name> --src  <cluster_functions.zip> --build-remote true
```

步骤 2 部署 Azure Functions 后，您可以在函数应用的概述部分中查看上传的函数。

更新 Azure 逻辑应用

逻辑应用充当Autoscale功能的协调器。ARM模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 协调器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项
在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。

以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
```

```
.
                        },
                        "Deploy_Changes_to_FTD": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                                }
.
.
                        "DeviceDeRegister": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                                }
                            },
                            "runAfter": {
                                "Delay_For_connection_Draining": [
```

d) （可选） 编辑触发间隔，或保留默认值 (5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 5
                },
```

e) （可选） 编辑要进行排空的时间，或保留默认值 (5)。这是内向扩展操作期间，在删除设备之前从 Firewall Threat Defense Virtual 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
         "actions": {
              "Branch_based_on_Scale-In_or_Scale-Out_condition": {
                  "actions": {
                      "Delay_For_connection_Draining": {
                          "inputs": {
                              "interval": {
                                  "count": 5,
                                  "unit": "Minute"
                              }
```

f) （可选） 编辑冷却时间，或保留默认值 (10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

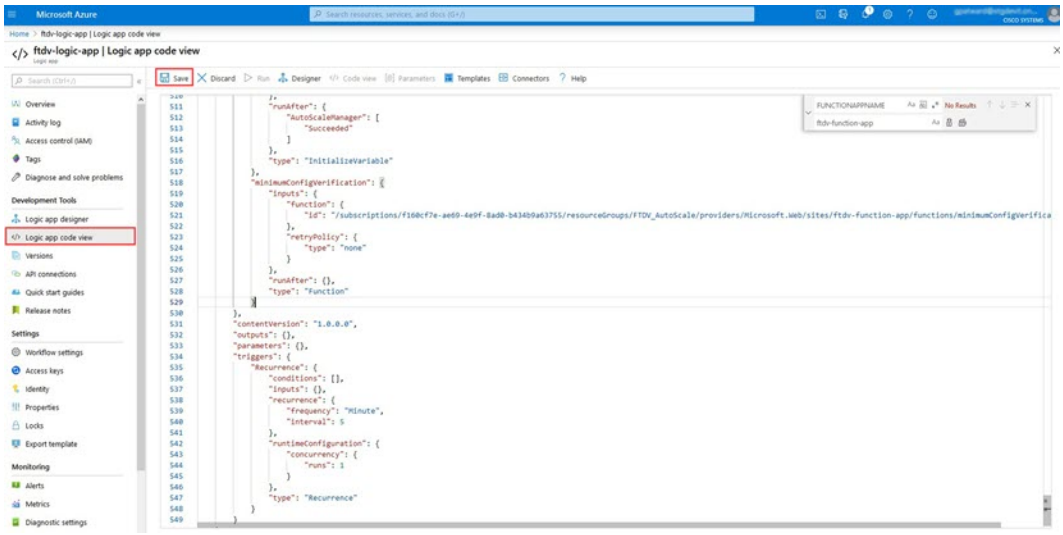
```
                "actions": {
                    "Branch_based_on_Scale-Out_or_Invalid_condition": {
                        "actions": {
                            "Cooldown_time": {
```

```
"inputs": {
    "interval": {
        "count": 10,
        "unit": "Second"
 }
```

注释
这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

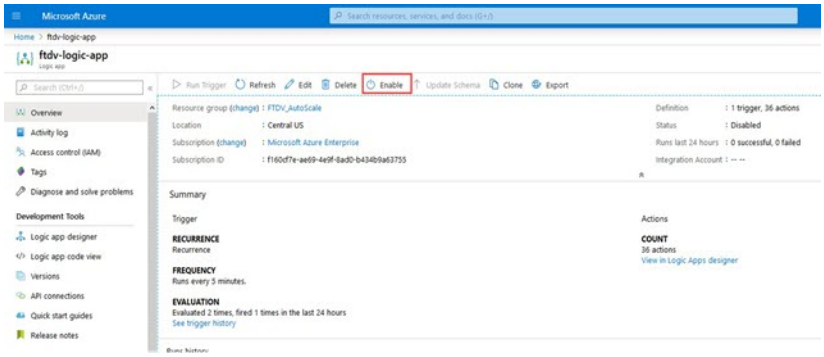
步骤 2 转至**逻辑应用代码视图 (Logic App code view)**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后点击**保存 (Save)**。

图 ***214:*** 逻辑应用代码视图



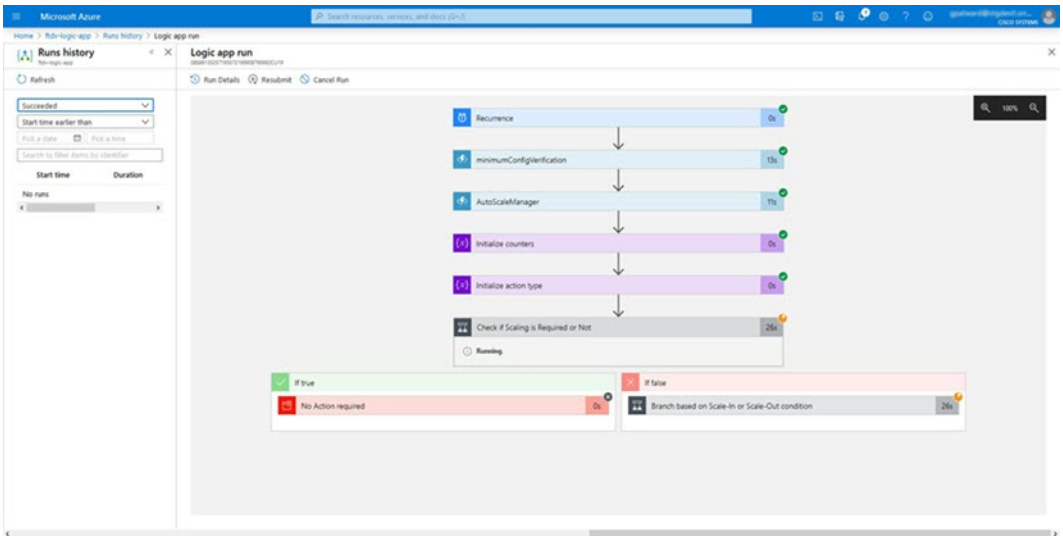
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请点击**启用 (Enable)**。

图 ***215:*** 启用逻辑应用



步骤 4 启用后，任务就会开始运行。点击“正在运行”(Running) 状态可查看活动。

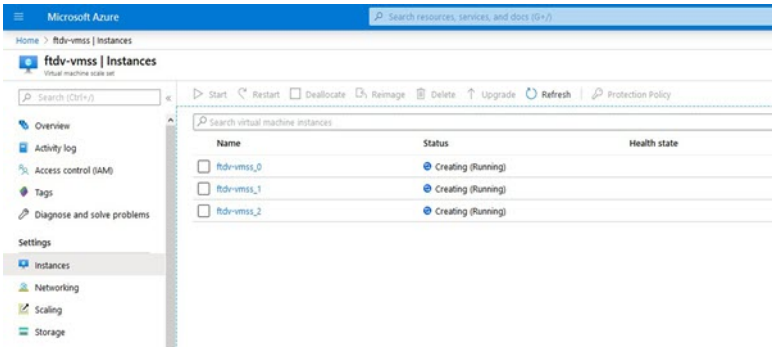
图 *216:* 逻辑应用运行状态



步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 Firewall Threat Defense Virtual 实例。

图 *217: Threat Defense Virtual* 实例运行



在此示例中，由于在 ARM 模板部署中将 'minFtdCount' 设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 Firewall Threat Defense Virtual 实例。

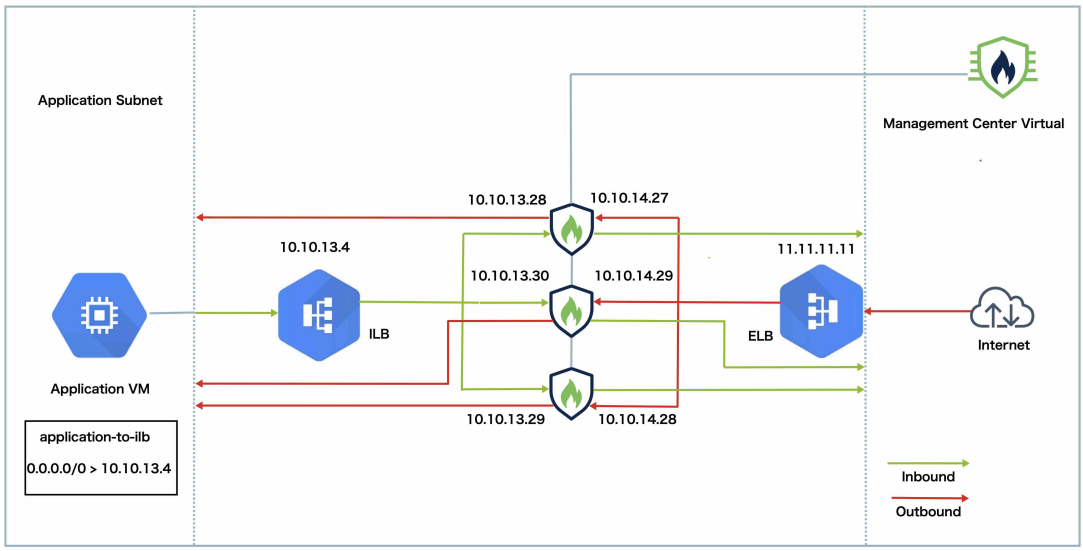
在 GCP 中部署集群

要在 GCP 中部署集群，您可以手动部署，或者使用实例模板来部署实例组。您可以将集群与本地 GCP 负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

注释 出站流量需要使用接口 NAT 并被限制为 64K 连接。

GCP 集群 Autoscale 解决方案的拓扑示例

图 *218:* 拓扑示例



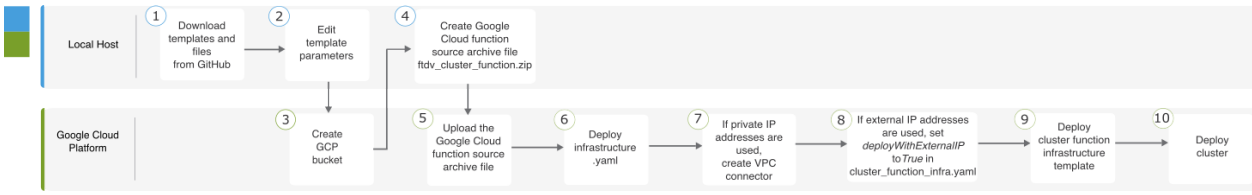
此拓扑描述入站和出站流量。

1. Threat Defense Virtual 集群位于内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。
2. 来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。
3. 集群中的 Threat Defense Virtual 实例会检查流量，在检查后会将流量转发到应用虚拟机。
4. 来自应用虚拟机的出站流量将传输到内部负载均衡器。负载均衡器会将此流量转发到 Threat Defense Virtual 集群，由该集群将其发送到互联网。

在 GCP 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

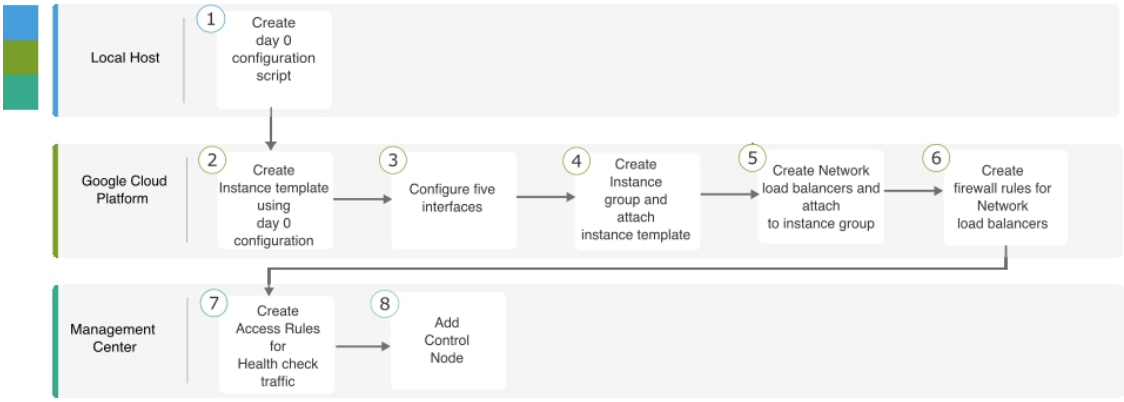
以下流程图说明了在 GCP 上基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	编辑模板参数。
3	Google Cloud Platform	创建 GCP 存储桶。
4	本地主机	创建 Google Cloud 函数源存档文件 *ftdv_cluster_function.zip*。
5	Google Cloud Platform	上传 Google 函数源存档文件。
6	Google Cloud Platform	部署 infrastructure.yaml。
7	Google Cloud Platform	如果使用私有 IP 地址，请创建 VPC 连接器。
8	Google Cloud Platform	如果使用外部 IP 地址，请在 *cluster_function_infra.yaml* 中将 *deployWithExternalIP* 设置为 *True*。
9	Google Cloud Platform	部署集群功能基础设施模板。
10	Google Cloud Platform	部署集群。

手动部署

以下流程图说明了在 GCP 上手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	创建 Day 0 配置脚本。
2	Google Cloud Platform	使用 Day 0 配置创建实例模板。

	工作空间	步骤
3	Google Cloud Platform	配置接口。
4	Google Cloud Platform	创建实例组并附加实例模板。
5	Google Cloud Platform	创建 NLB 并附加到实例组。
6	Google Cloud Platform	创建 NLB 的防火墙规则。
7	管理中心	创建运行状况检查流量的访问规则。
8	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- 东西流量的集群部署模板 - *deploy_ngfw_cluster_yaml*
- 南北流量的集群部署模板 - deploy_ngfw_cluster.yaml

使用实例模板在 GCP 中部署实例组

使用实例模板在 GCP 中部署实例组。

开始之前

- 使用 Google Cloud Shell 进行部署。或者，您可以在任何 macOS/Linux/Windows 计算机上使用 Google SDK。
- 要允许集群自动向管理中心注册，您需要在管理中心创建一个具有管理权限的用户，该用户可以使用 REST API。请参阅*Cisco Secure Firewall Management Center* 管理指南。
- 在管理中心中添加与您在 *cluster_function_infra.yaml*中指定的策略名称匹配的访问策略。

过程

步骤 1 将模板从 GitHub 下载到本地文件夹。

步骤 2 使用所需的 *resourceNamePrefix* 参数（例如 ngfwvcls）和其他所需的用户输入来编辑 **infrastructure.yaml**、**cluster_function_infra.yaml** 和 **deploy_ngfw_cluster.yaml**。

从 Cisco Secure Firewall 版本 7.4.1 开始，您可以在没有诊断接口的情况下部署集群。要部署仅具有外部、内部、管理和 CCL 接口的集群，请在 **Infrastructure.yaml** 和 **deploy_ngfw_cluster.yaml** 文件中将 *withDiagnostic* 变量设置为 **False** 。

请注意，GitHub 的 **east-west** 和 **north-south** 文件夹中都有一个 **deploy_ngfw_cluster.yaml** 文件。根据流量要求下载相应的模板。

步骤 3 使用 Google Cloud Shell 创建存储桶，以上传 Google 云函数源存档文件 *ftdv_cluster_function.zip*。

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

确保此处的 *resourceNamePrefix* 变量与您在 **cluster_function_infra.yaml**中指定的 *resourceNamePrefix* 变量匹配。

步骤 4 为集群基础设施创建一个存档文件。

示例：

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

步骤 5 上传您之前创建的 Google 源存档。

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

步骤 6 部署集群的基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

步骤 7 如果您使用的是专用 IP 地址，请执行以下步骤：

a) 使用 Threat Defense Virtual 管理 VPC 启动并设置 Management Center Virtual。

b) 创建 VPC 连接器，以将 Google Cloud 功能与 Threat Defense Virtual 管理 VPC 连接。

gcloud compute networks vpc-access connectors create *vpc-connector-name* **--region us-central1 --subnet** *resourceNamePrefix***-ftdv-mgmt-subnet28**

步骤 8 如果管理中心相对于 Threat Defense Virtual 是远程，并且 Threat Defense Virtual 需要外部 IP 地址，请确保在 **cluster_function_infra.yaml** 中将 **deployWithExternalIP** 设置为 **True** 。

步骤 9 部署集群功能基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

步骤 10 部署集群。

1. 对于北-南拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

2. 对于东-西拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

在 GCP 中手动部署集群

要手动部署集群，请准备 day0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。

为 GCP 创建 Day0 配置

您可以使用固定配置或自定义配置。

使用 GCP 的固定配置来创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
                "Diagnostic": "OFF",       //Optional user input from version 7.4.1 - use
to deploy cluster without Diagnostic interface
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
    }
}
```

例如：

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",     //mandatory user input
        "ClusterGroupName": "ftdv-cluster"               //mandatory user input
    }
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input** 。

请注意，对于 **CclSubnetRange** 变量，不能使用子网中的前两个 IP 地址和后两个 IP 地址。有关详细信息，请参阅 IPv4 子网中的保留 IP 地址 。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始和结束 IP 地址的一些示例。

注释 所有集群基础设施子网都必须使用 /27 CIDR。

表 *40:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253

使用 GCP 的自定义配置来创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
    }
```

以下是为集群控制链路创建包含管理接口、内部接口和外部接口的配置的示例。请注意，每个节点需要设置唯一的粗体值。

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
```

```
  "segment-id 1",
  "vtep-nve 1",
  "object network ccl#link",
  "range 10.1.90.2 10.1.90.17",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu outside 1400",
  "mtu inside 1400"
 ]
}
```



注释 对于集群控制链路网络对象，仅指定所需数量的地址（最多16个）。较大的范围可能会影响性能。

手动部署集群节点

部署集群节点，以便它们形成集群。对于GCP上的集群，您不能使用4 vCPU机器类型。4 vCPU机器类型仅支持4个接口，但需要5个接口。使用支持五个接口的机器类型，例如c2-standard-8。

过程

步骤1 使用day 0配置（在**元数据** > **启动脚本**部分中）创建具有5个接口的实例模板：外部、内部、管理、诊断和集群控制链路。

请参阅Cisco Secure Firewall Threat Defense Virtual 入门指南。

步骤2 创建实例组，然后附加实例模板。

步骤3 创建GCP网络负载均衡器（内部和外部），然后附加实例组。

步骤4 对于GCP网络负载均衡器，允许在管理中心上的安全策略中进行运行状况检查。请参阅允许对GCP网络负载均衡器进行运行状况检查，第585页。

步骤5 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第600页。

允许对 GCP 网络负载均衡器进行运行状况检查

Google Cloud可提供运行状况检查，以确定后端是否对流量做出响应。

请参阅https://cloud.google.com/load-balancing/docs/health-checks，以便为网络负载均衡器创建防火墙规则。然后，在防火墙管理中心中创建访问规则以允许运行状况检查流量。有关所需的网络范围，

请参阅https://cloud.google.com/load-balancing/docs/health-check-concepts。请参阅访问控制规则，第 1743 页。

您还需要配置动态手动 NAT 规则，以便将运行状况检查流量重定向到位于 169.254.169.254 的 Google 元数据服务器。请参阅配置动态手动 NAT，第 1319 页。

您可以设置跨所有接口进行 GCP 运行状况检查的路由，这些接口用于配置其运行状况探测。如果用于 GCP 运行状况检查的路由尚不可用，则可以通过在接口上创建具有更高指标的路由来实现此目的。

北-南 NAT 规则示例配置

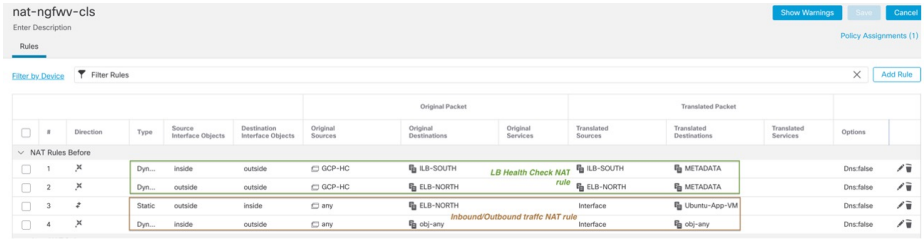
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



东-西 NAT 规则示例配置

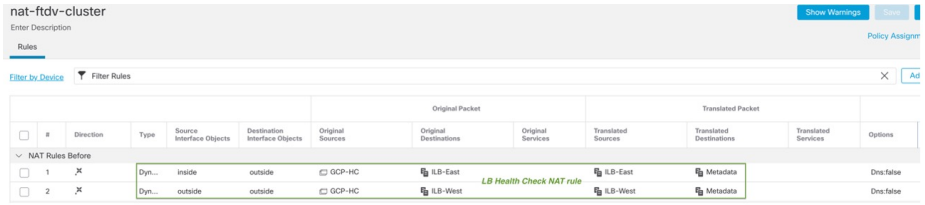
```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
```

```
network-object 209.85.204.0 255.255.252.0
network-object 209.85.152.0 255.255.252.0
```



南北和东西流量路由配置示例

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

如果没有默认路由，则可使用策略型路由来路由流量，以进行运行状况检查。

注释 将 NAT > 已转换目标端口设置为 80。

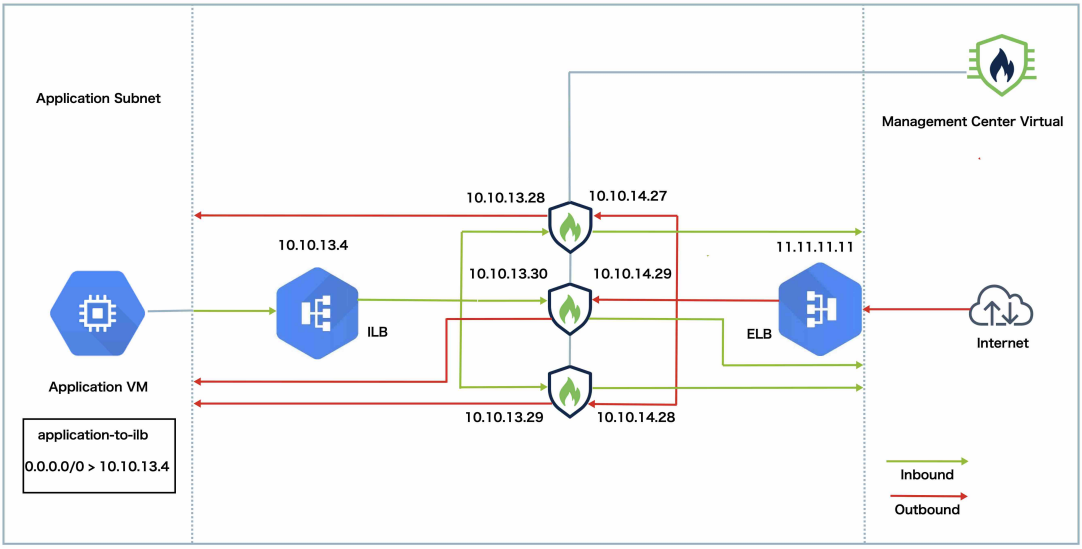
GCP 中的 Threat Defense Virtual 集群 Autoscale 解决方案

从版本 10.0.0 开始，通过动态自动扩展功能增强了 Google 云平台 (GCP) 中的 Threat Defense Virtual 集群解决方案。自动扩展解决方案基于 CPU 利用率指标，有助于实现最佳资源使用。它使用基于 Terraform 的模板进行部署。

您可以根据自己的要求选择扩展选项：动态集群或固定节点集群。您还可以定义CPU阈值，超过该阈值将启动扩展。

GCP 集群 Autoscale 解决方案的拓扑示例

图 *219:* 拓扑示例



此拓扑描述入站和出站流量。

1. Threat Defense Virtual 集群位于内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。
2. 来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。
3. 集群中的 Threat Defense Virtual 实例会检查流量，在检查后会将流量转发到应用虚拟机。
4. 来自应用虚拟机的出站流量将传输到内部负载均衡器。负载均衡器会将此流量转发到 Threat Defense Virtual 集群，由该集群将其发送到互联网。

要求和前提条件

本部分列出了 GCP 上的 Threat Defense Virtual 集群自动扩展解决方案的要求和支持的配置。

型号要求

- 支持的 Threat Defense Virtual 型号：FTDv20、FTDv30、FTDv50 和 FTDv100。
- 需要有效的 Google 云平台 (GCP) 账户。
- Google Cloud SDK 必须安装在本地，或者您应该有权访问 GCP Cloud Shell。
- 需要思科智能许可账户才能许可管理中心。

Firepower 管理中心系统要求

- 确保已配置访问控制策略。
- 确保已定义数据接口的安全区域。
- 需要具有管理角色的用户才能自动注册。
- 确保 NAT 规则配置为响应负载均衡器的运行状况检查。

许可

- 控制节点的许可证适用于集群中的所有数据节点，无论其在启动过程中的初始性能级别配置如何。
- 集群组建后，不允许更改任何单个 Threat Defense Virtual 的性能级别。
- 默认情况下，每台设备随附一个 100 kbps 评估许可证。
- 许可证注销
  - 重新启动前：设备保留现有吞吐量。
  - 重启后：吞吐量恢复为默认的 100 kbps。
- 仅支持 BYOL（自带许可证）许可证类型。
- 不支持 PAYG（即用即付）许可证类型。

支持的配置

- 集群大小：1-16 个节点。
- 流量拓扑：南北和东西向。
- 部署模式：使用 Terraform 模板部署。

模板

GitHub 上提供了以下模板：

- infrastructure/main.tf – 用于基础设施部署模板。
- cluster_deployment/main.tf – 用于集群部署模板。

在 GCP 上部署带有 Autoscale 的 Threat Defense Virtual 集群解决方案

部署过程分为两个步骤：

1. 基础设施部署（可选）- 部署所需的网络基础设施。
2. 集群部署 — 部署 Threat Defense Virtual 集群。

注释 如果选择使用自己的基础设施来部署 Threat Defense Virtual，则可以跳过基础设施部署步骤。但是，请务必确保提供使解决方案正常运行所需的所有资源。

基础设施部署参数

以下参数用于基础设施部署：

表 *41:* 用于基础设施部署的模板参数列表 *(infrastructure_params.tfvars)*

参数	说明	示例
project_id	GCP 项目 ID	test-project-12345
resource_name_prefix	字符串（仅限小写字母）。	demoftdv
region	要部署的 GCP 区域	us- Central1
mgmt_ip_cidr_range	子网 CIDR	10.112.0.0/27
vpc_connector_ip_cidr_range	仅管理 VPC 连接器 CIDR /28 子网	10.112.50.0/28
with_diagnostic	是否启用诊断接口。	true 或 false（false 是仅从版本 7.4.1 开始支持。）
diag_ip_cidr_range	诊断子网 CIDR	10.112.19.0/27
inside_ip_cidr_range	内部子网	10.112.1.0/27
outside_ip_cidr_range	外部子网 CIDR	10.112.2.0/27
ccl_ip_cidr_range	CCL 子网 CIDR（建议使用 /27 子网）	10.112.100.0/27

在 GCP 上使用 Terraform 部署基础设施

GCP 基础设施管理器可作为堆栈促进 Terraform 部署。从此界面中，可以管理资源并执行清理。

过程

步骤 1 导航到 GCP 控制台 并使用您的凭证登录。

步骤 2 打开 Cloud Shell 或本地终端。

如果您使用的是本地终端，请确保已在系统上配置 GCP CLI。

步骤 3 创建新目录。

示例：

使用命令 **mkdir infra** 在 Cloud Shell 或本地终端中创建名为 infra 的 目录。

步骤 4 导航到新创建的目录。

示例：

使用命令 **cd infra** 切换到新目录。

步骤 5 从 Cisco GitHub 存储库复制或下载 infrastructure_params. tfvars 文件，并将其保存到新的 infra 文件夹。

步骤 6 打开 infrastructure_params. tfvars 文件，并根据需要更新所有占位符值。请参阅 基础设施部署参数，第 590 页。

步骤 7 更新占位符值后，使用以下命令启动部署。

```
gcloud infra-manager deployments \
apply
"projects/<project_id>/locations/<region>/deployments
/<deployment_name>" \
--location="<region>" \
--git-source-repo="<repo name>" \
--git-source-directory="infrastructure” \
--git-source-ref="<branch name>" \
--serviceaccount="
projects/<project_id>/serviceAccounts/<servi
ce_account_name>" \
--artifacts-gcs-bucket="gs://<bucket_name>/artifacts"
\
--inputs-file="/path/to/your/infra_params.tfvars"
```

表 *42:* 参数说明

参数	说明
deployment_name	将显示在 GCP 基础设施管理器中的 Terraform 部署堆栈的名称。
location	将应用部署的位置或区域。
git-source-repo	包含源代码的 Git 存储库的名称（Cisco GitHub 链接）。
git-source-directory	Git 存储库中基础设施代码所在的目录。
git-source-ref	Git 存储库中用于部署的分支名称。
service-account	服务账户的名称。
artifacts-gcs-bucket	用于存储与部署相关的构件的 Google Cloud Storage 存储桶（可选）。
inputs-file	基础设施配置的输入参数的文件路径。

注释
如果不使用该模板来部署基础设施，则必须提供以下资源，以便正确部署解决方案并确保解决方案正常运行。

- 管理 VPC 的名称。
  - 管理子网
  - VPC 连接器的管理子网
  - 管理防火墙规则的名称。
- 内部 VPC
  - 内部子网
  - 防火墙规则名称
- 外部 VPC
  - 外部子网
  - 外部防火墙规则的名称
  - NAT GW
- CCL VPC
  - CCL 子网
  - 防火墙规则名称
- 诊断 VPC（可选）
  - 诊断子网
  - 诊断防火墙规则名称
- 具有管理子网的 VPC 连接器

集群部署参数：

以下输入参数用于部署集群。

表 *43:* 适用于集群部署的模板参数列表

参数	说明	示例
常规配置		
type_of_deployment	部署类型 (north_south 或 east_west)	north_south
项目信息		

参数	说明	示例
project_id	GCP 项目 ID	test-project-12345
region	部署区域	us-east1
zone1	部署区域	a
zone2	部署区域	b
zone3	部署区域	c
resource_name_prefix	用于命名资源的前缀	democluster
serviceAccountMailId	服务账户电子邮件	service-account-mail@example-project.iam.gserviceaccount.com
VPC 和子网配置		
mgmt_vpc_name	管理 VPC 名称	<resource-name>-ftdv-mgmt-vpc
mgmt_subnet_name	管理子网名称。	<resource-name>-ftdv-mgmt-子网
inside_vpc_name	内部 VPC 名称	<resource-name>-ftdv-inside-vpc
inside_subnet_name	内部子网	<resource-name>-ftdv-inside-subnet
outside_vpc_name	外部 VPC 名称	<resource-name>-ftdv-outside-vpc
OutsideSubnetNames	外部子网名称	<resource-name>-ftdv-outside-子网
diag_vpc_name	VPC 名称 “诊断”	<resource-name>-ftdv-diag-vpc
diag_subnet_name	子网名称“诊断”	<resource-name>-ftdv-diag-subnet
ccl_vpc_name	CCL VPC 名称	<resource-name>-ftdv-ccl-vpc
ccl_subnet_name	输入 CCL 子网名称	<resource-name>-ftdv-ccl-subnet
防火墙规则		
diag_firewall_rule_name	用于诊断的防火墙规则	<resource-name>-ftdv-diag-firewall-rule
ccl_firewall_rule_name	用于 CCL 的防火墙规则	<resource-name>-ftdv-ccl-firewall-rule
mgmt_firewall_rule_name	用于管理的防火墙规则	<resource-name>-ftdv-mgmt-firewall-rule
inside_firewall_rule_name	内部网络的防火墙规则	<resource-name>-ftdv-inside-firewall-rule
outside_firewall_rule_name	外部网络的防火墙规则	<resource-name>-ftdv-outside-firewall-rule
inside_hc_firewall_rule_name	内部网络的防火墙规则	<resource-name>-ftdv-inside-hc-firewall-rule
outside_hc_firewall_rule_name	外部网络的防火墙规则	<resource-name>-ftdv-outside-hc-firewall-rule
实例详细信息		
machine_type	GCP 计算机类型支持	n1-standard-8

参数	说明	示例
source_image_url	Threat Defense Virtual 的源映像位置	项目/cisco-public/global/images/cisco-ftdv-10-0-0
public_key	用于 SSH 访问的公钥	ssh-rsa AAAAB3NzaC1yc2EAAADAQAAAAAAQC4v
自动扩展详细信息		
auto_scaling	启用自动扩展	true/false
cpu_utilization_target	自动扩展的目标 CPU 使用率 [0.0-1.0]	0.60
min_ftd_count	Threat Defense Virtual 的最小实例数	0
max_ftd_count	Threat Defense Virtual 的最大实例数	2
Threat Defense Virtual 特定配置		
ftd_password_secret_name	密钥管理器中用于设备将使用此密码的新管理员密码的 Threat Defense Virtual 密钥的名称，设备将在首次登录后使用此密码。	ftd-password-secret
hostname	Threat Defense Virtual 的主机名	cisco-ngfwv
ccl_subnet_range	CCL 的子网范围，空格分隔	10.112.100.2 10.112.100.30
cluster_grp_name	Threat Defense Virtual 的集群组名称	ftdv-cluster
with_diagnostic	是否启用诊断	true/false
Assign_public_ip_to_mgmt	是否将公共 IP 分配给管理接口	true/false
ftd_reg_ via_public_ip	是否向公共 IP 注册 Threat Defense Virtual	true/false
管理中心信息和 Threat Defense Virtual 配置		
reg_id	管理中心注册 ID	cisco
nat_id	管理中心的 NAT ID	cisco

参数	说明	示例
policy_id	在管理中心创建的初始策略 ID	ftdv-ini-pol
fmc_ip	源 Firewall Management Center 的 IP 地址	10.112.0.2 / 34.113.15.29
fmc_password_secret_name	密钥管理器中新管理员密码的 FMC 密钥名称，设备将在首次登录后使用此密码。	fmc-password-secret
fmc_username	管理中心登录用户名	restapi
license_caps	许可证功能	BASE, MALWARE, URLFilter, THREAT
performance_tier	Threat Defense Virtual 的性能级别	FTDv20、FTDv30
vpc_connector_name	VPC 连接器的名称	<resource-name>-connector
检查负载均衡器配置		
ilb_frontend_protocol	前端协议 (TCP/UDP)	TCP
ilb_backend_protocol	后端协议:	TCP
ilb_health_check_port	ILB运行状况检查平衡器端口，管理中心需要 NAT	8989
ilb_timeout_sec	负载均衡器超时（秒）	5
ilb_draining_timeout_sec	排空连接超时（秒）	60
ilb_check_interval_sec	ILB运行状况检查的间隔（秒）	10
ilb_unhealthy_threshold	标记为不正常之前失败的运行状况检查数	1
仅在north_south 部署情况下外部负载均衡器特定配置		
elb_frontend_protocol	外部负载均衡器的前端协议名称 (TCP/UDP)	TCP
elb_backend_protocol	外部负载均衡器的后端协议名称 (TCP/UDP/未指定)	TCP
elb_front_end_ports	ELB前端（侦听程序）端口列表	all 或 [22, 80, 443]

参数	说明	示例
elb_health_check_port	ELB运行状况检查端口，管理中心需要 NAT	87878
elb_timeout_sec	负载均衡器超时（秒）	5
elb_unhealthy_threshold	标记为不正常之前失败的运行状况检查数	2
elb_check_interval_sec	ELB运行状况检查的间隔（秒）。	10
elb_draining_timeout_sec	排空连接超时（秒）	60

使用 Terraform on GCP 部署集群

GCP 基础设施管理器可作为堆栈促进 Terraform 部署。从此界面中，可以管理资源并执行清理。

过程

步骤 1 导航到 GCP 控制台 并使用您的凭证登录。

步骤 2 打开 Cloud Shell 或本地终端。

如果您使用的是本地终端，请确保已在系统上配置 GCP CLI。

步骤 3 创建新目录。

示例：

使用命令 **mkdir cluster** 在 Cloud Shell 或本地终端中创建名为 cluster 的目录。

步骤 4 导航到新创建的目录。

示例：

使用命令 **cd cluster** 切换到新目录。

步骤 5 从思科 GitHub 存储库复制或下载 cluster_params.tfvars 文件，并将其保存到新的 集群 文件夹。

步骤 6 打开 cluster_params.tfvars 文件并根据需要更新所有占位符值。请参阅 集群部署参数：，第 592 页。

步骤 7 更新占位符值后，使用以下命令启动部署。

```
gcloud infra-manager deployments \
apply "projects/<project_id>/locations/<region>/deployments/<deployment_name>" \
--location="<region>" \
--git-source-repo="<repo name>" \
--git-source-directory="cluster_deployment" \
--git-source-ref="<branch name>" \
--service-account="projects/<project_id>/serviceAccounts/<service_account_name>" \
--artifacts-gcs-bucket="gs://<bucket_name>/artifacts" \
--inputs-file="/path/to/cluster_params.tfvars"
```

表 *44:* 参数说明

参数	说明
deployment_name	将显示在 GCP 基础设施管理器中的 Terraform 部署堆栈的名称。
location	将应用部署的位置或区域。
git-source-repo	包含源代码的 Git 存储库的名称（Cisco GitHub 链接）。
git-source-directory	Git 存储库中基础设施代码所在的目录。
git-source-ref	Git 存储库中用于部署的分支名称。
service-account	服务账户的名称。
artifacts-gcs-bucket	用于存储与部署相关的构件的 Google Cloud Storage 存储桶，例如 Terraform 状态文件。
inputs-file	集群部署输入参数的文件路径。

集群部署后的部署配置

要在 VPC 内创建路由以通过 Google Cloud Shell 上的内部负载均衡器转发所需流量，请执行以下步骤：

```
gcloud compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```



注释 您也可以从 GCP UI 中创建路由。要从 GCP UI 创建路由，请执行以下步骤：

1. 在GCP UI中，导航至路由 (Routes)、路由管理 (Route Management)、创建路由 (Create route)。
2. 填写 Create a route 对话框。
   1. **名称 (Name)**：指定路由名称。
   2. **网络**：选择<inside-vpc-name>请参阅
   3. 选择 **静态路由**。
   4. **目标 IPv4 范围 (Destination IPv4 range)**：输入 **0.0.0.0/0**。
   5. **优先级**：设置为 **1000**。
   6. **下一跳**：选择 **指定内部直通 网络负载均衡器的转发规则**。
   7. **转发规则名称**：选择<forwarding-rule-for-ilb>请参阅
3. 点击**创建 (Create)** 以创建角色。

在 GCP 中手动部署集群

为 GCP 创建 Day0 配置

要手动部署集群，请准备 Day-0 配置并部署每个节点。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Diagnostic": "OFF",       //Optional user input from version 7.4.1
    "Cluster": {
      "CclSubnetRange": "ip_address_start ip_address_end",
      "ClusterGroupName": "cluster_name"
    }
}
```

例如：

```
{
"AdminPassword": “C15co@!23",
"Hostname": "cisco-ftd",
"FirewallMode": "routed",
"Diagnostic": "OFF",
"ManageLocally": "No",
"Cluster": {
  "CclSubnetRange”: “10.10.65.2 10.10.65.29”,
  "ClusterGroupName": “gcp-cls-ftd"
}
}
```

允许对 GCP 网络负载均衡器进行运行状况检查

Google Cloud 可提供运行状况检查，以确定后端是否对流量做出响应。

请参阅https://cloud.google.com/load-balancing/docs/health-checks，以便为网络负载均衡器创建防火墙规则。然后，在防火墙管理中心中创建访问规则以允许运行状况检查流量。有关所需的网络范围，请参阅https://cloud.google.com/load-balancing/docs/health-check-concepts。请参阅访问控制规则，第 1743 页。

您还需要配置动态手动 NAT 规则，以便将运行状况检查流量重定向到位于 169.254.169.254 的 Google 元数据服务器。请参阅配置动态手动 NAT，第 1319 页。

您可以设置跨所有接口进行 GCP 运行状况检查的路由，这些接口用于配置其运行状况探测。如果用于 GCP 运行状况检查的路由尚不可用，则可以通过在接口上创建具有更高指标的路由来实现此目的。

北-南 NAT 规则示例配置

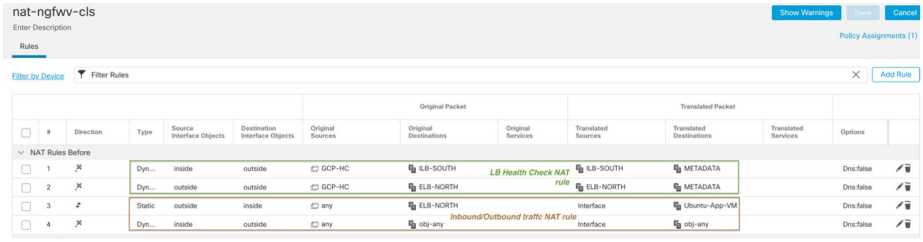
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



东-西 NAT 规则示例配置

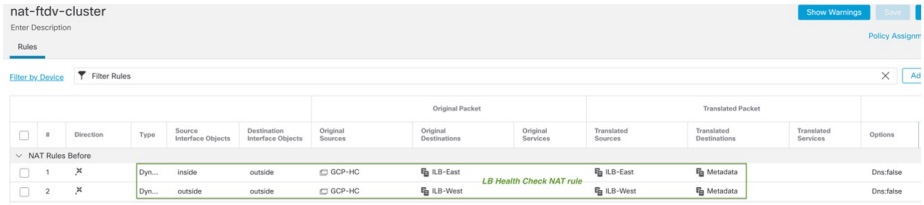
```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
```

```
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



南北和东西流量路由配置示例

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

如果没有默认路由，则可使用策略型路由来路由流量，以进行运行状况检查。

注释 将 NAT > 已转换目标端口设置为 80。

通过 Autoscale 对 GCP 集群进行故障排除

问题：集群未组建

解决办法

- 检查 nve-only 集群接口的 IP 地址。确保您可以 ping 其他节点的仅 NVE 集群接口。
- 检查仅 NVE 集群接口的 IP 地址是对象组的一部分。
- 确保为 NVE（网络虚拟化边缘）接口配置了相应的对象组。
- 集群组中的集群接口具有正确的 VNI 接口。此 VNI 接口具有相应对象组的 NVE。
- 每个节点都有自己的集群接口 IP 地址。确保节点可以相互执行 ping 操作，以验证连接性。

将集群添加到管理中心（手动部署）

如果您手动部署了集群，请使用此程序将集群添加到防火墙管理中心。如果您使用模板，则集群会自动注册到 防火墙管理中心。

将集群设备之一作为新设备添加到 防火墙管理中心；防火墙管理中心 会自动检测所有其他集群成员。

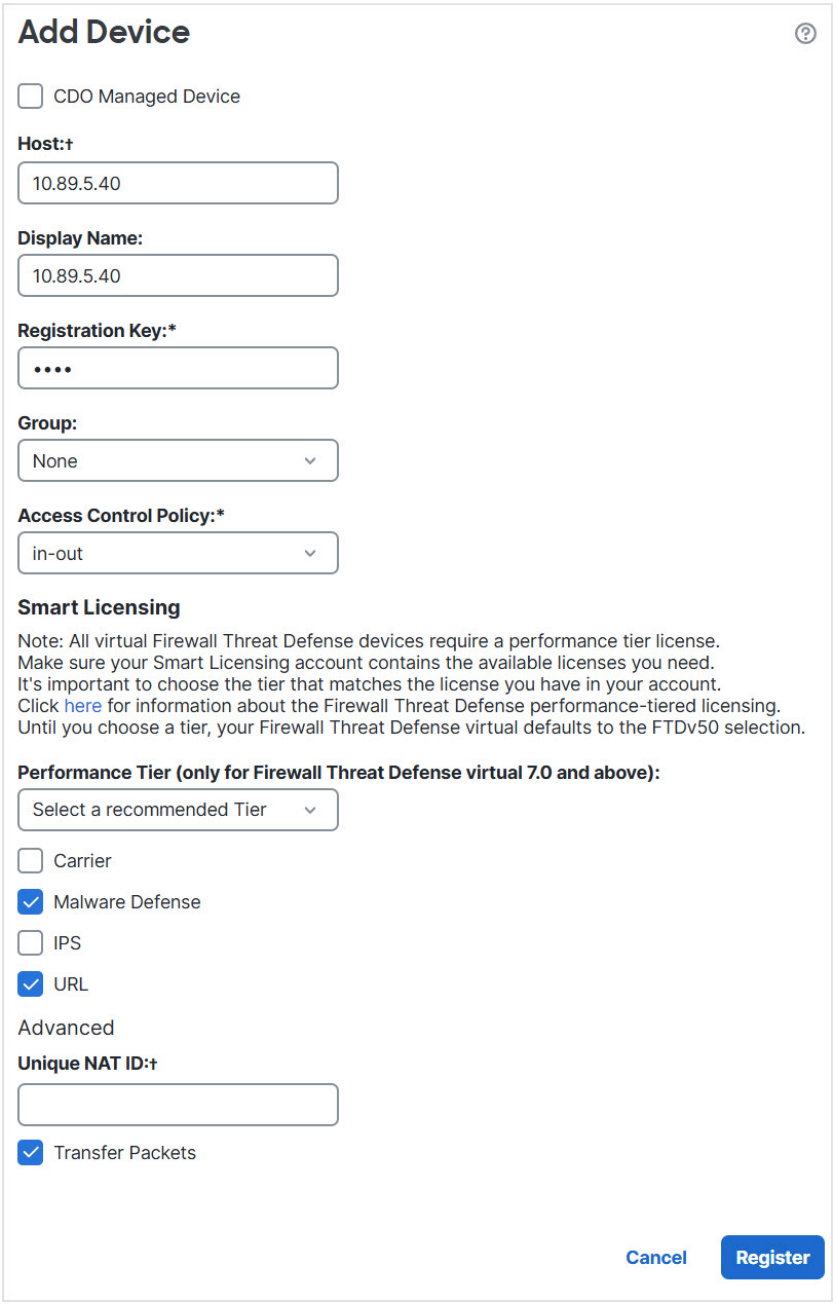
开始之前

- 所有集群设备必须位于成功建立的集群中，才能将集群添加到 防火墙管理中心。还应检查哪个是控制单元。使用 Firewall Threat Defense **show cluster info** 命令。

过程

步骤 1 在 防火墙管理中心 中，选择 **设备** > **设备管理**，然后选择**添加** > **添加设备**以使用管理 IP 来添加控制设备。

图 *220:* 添加设备



a) 在 **主机** 字段中，输入控制单元的 IP 地址或主机名。

虽然您可以添加任何集群单元，但我们建议添加控制单元备以获得最佳性能。

如果在设备设置期间使用了 NAT ID，则可能不需要输入此字段。有关详细信息，请参阅NAT 环境，第 7 页。

b) 在 **显示名称** 字段中，输入要在 防火墙管理中心中显示的控制单元名称。

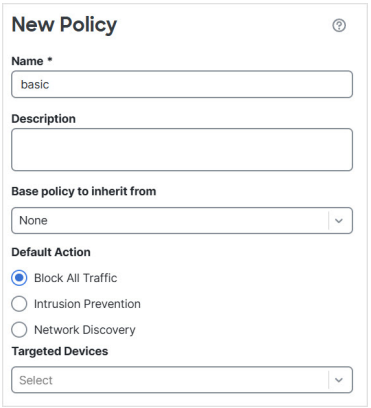
此显示名称不适用于集群；它仅适用于要添加的控制单元。您可以稍后更改其他集群成员的名称和集群显示名称。

c) 在**注册密钥 (Registration Key)** 字段中，输入在设备设置时所使用的同一注册密钥。注册密钥是一个一次性的共享密钥。

d) （可选） 将设备添加到设备 **组**。

e) 选择初始**访问控制策略**以在注册时部署到设备，或创建一个新策略。

如果创建新策略，则仅创建基本策略。您可以稍后根据需要自定义策略。



f) 选择要应用到设备的许可证。

g) 如果在设备安装过程中使用了 NAT ID，请展开**高级**部分，并在**唯一 NAT ID** 字段中输入相同的 NAT ID。

h) 选中**传输数据包**复选框以允许设备将数据包传输到 防火墙管理中心。

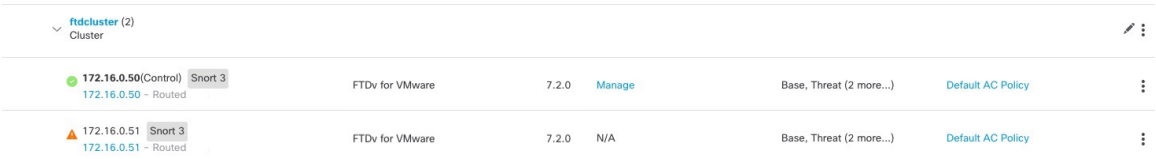
默认情况下，此选项已启用。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 防火墙管理中心进行检测。如果禁用此选项，则仅发送事件信息到 防火墙管理中心，不发送数据包数据。

i) 点击**注册 (Register)**。

防火墙管理中心 会识别并注册控制单元，接着注册所有数据单元。如果控制单元未注册成功，则不会添加集群。如果集群未运行或存在其他连接问题，则注册会失败。在这种情况下，我们建议尝试重新添加集群设备。

集群名称显示在 **设备** > **设备管理** 页面上；展开集群可查看集群单元。

图 *221:* 集群管理



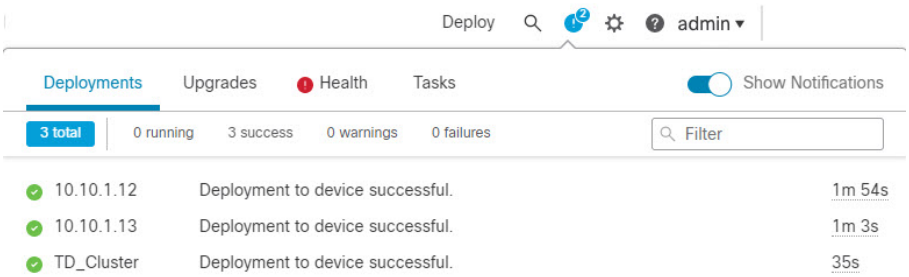
当前正在注册的设备会显示加载图标。

图 *222:* 节点注册



注释
在集群节点发现过程中，GCP 会优先选择具有公共 IP 地址的节点。要确保 Firewall Threat Defense Virtual 集群使用专用 IP 地址注册到 Management Center Virtual，您必须先在 Firewall Threat Defense Virtual 集群节点上禁用公有 IP 地址。这将允许 GCP 节点发现使用向 Management Center Virtual 注册节点的专用 IP 地址继续。

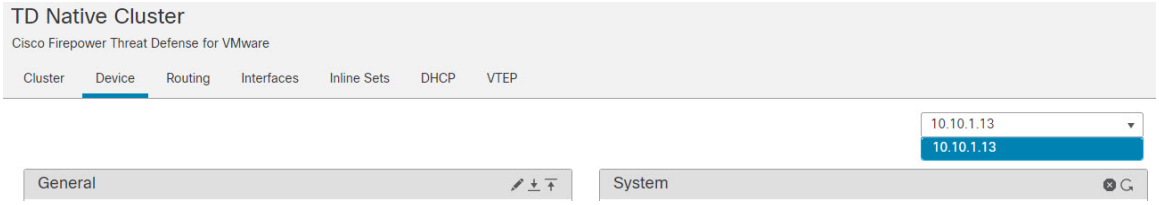
您可以通过点击 **通知** 图标并选择 **任务** 来监控集群设备的注册情况。防火墙管理中心 会在每个设备注册时更新“集群注册”任务。如有任何设备无法注册，请参阅调整集群节点，第 613 页。



步骤 2 通过点击集群的 **编辑** (✎)，配置设备特定设置。

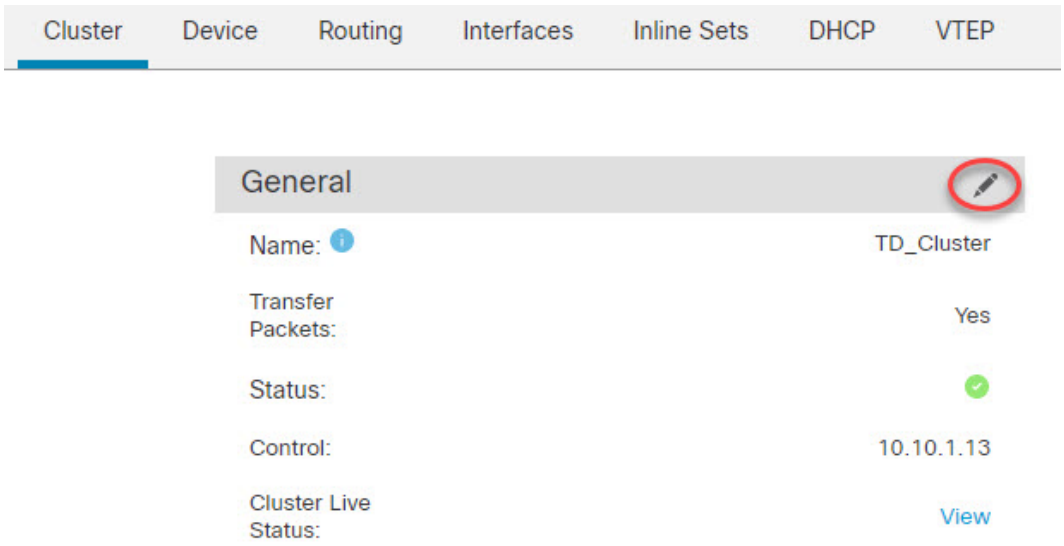
大多数配置可以应用于整个集群，而不适用于集群中的节点。例如，可以更改每个节点的显示名称，但只能配置整个集群的接口。

步骤 3 在 **设备** > **设备管理** 上选择**添加**、**集群**屏幕，您会看到**常规**、**许可证**、**系统**和**运行状态**设置。

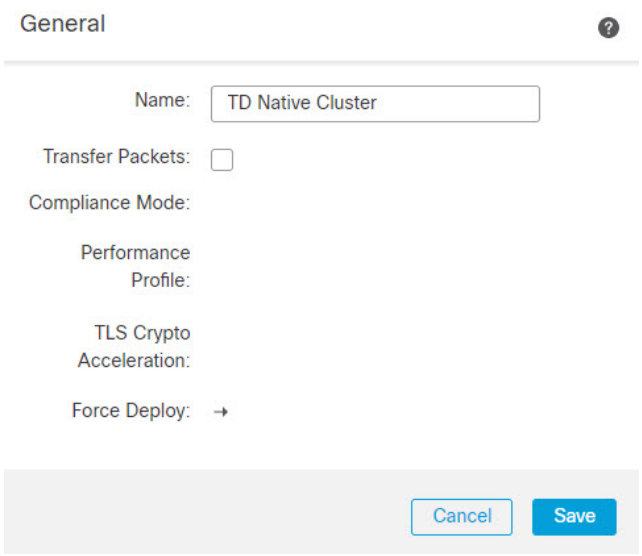


请参阅以下集群特定项：

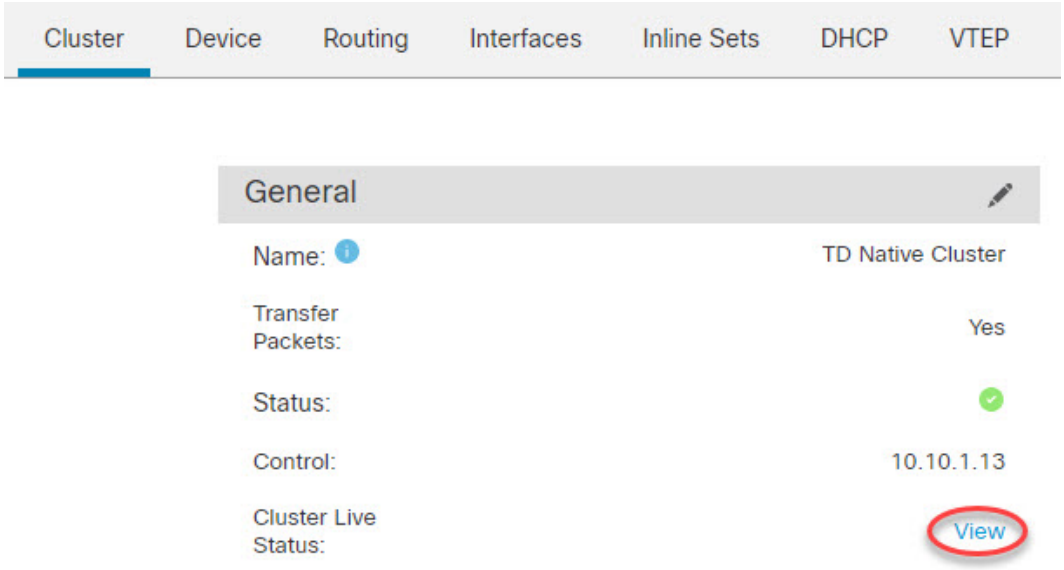
- **常规 (General)** > **名称 (Name)** - 通过点击 **编辑** (✎)更改集群显示名称。



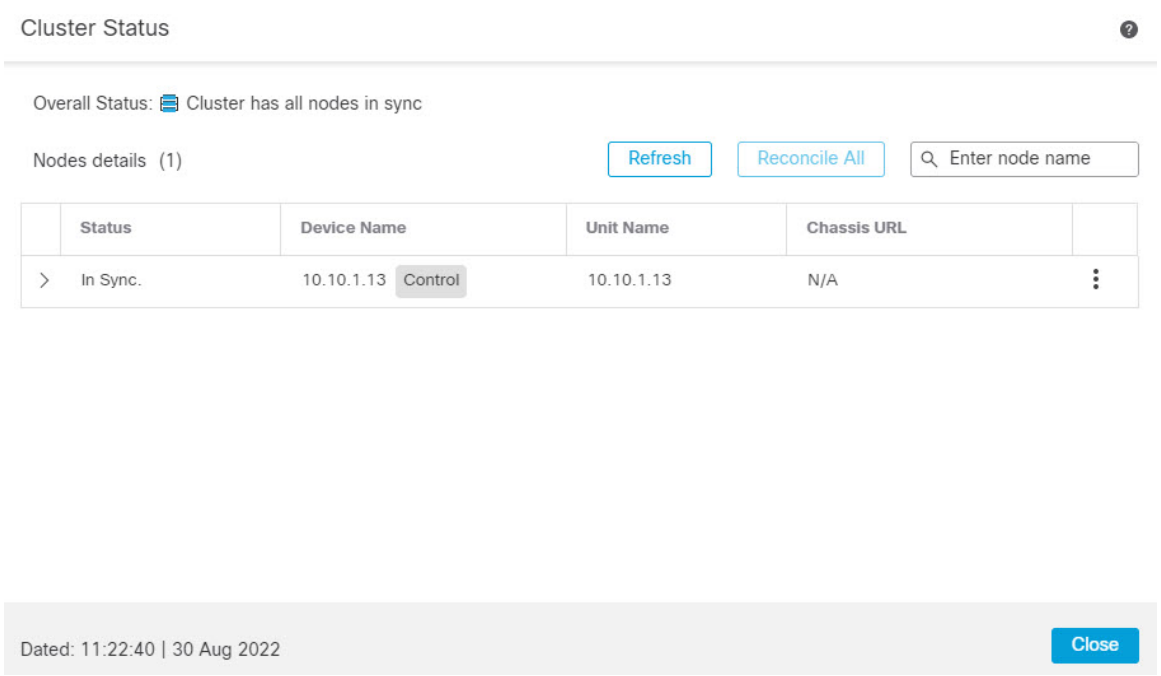
然后设置 **名称** 字段。



- **常规 (General)** > **查看集群状态 (View cluster status)** - 点击 **查看 (View)** 链接来打开 **集群状态 (Cluster Status)** 对话框。

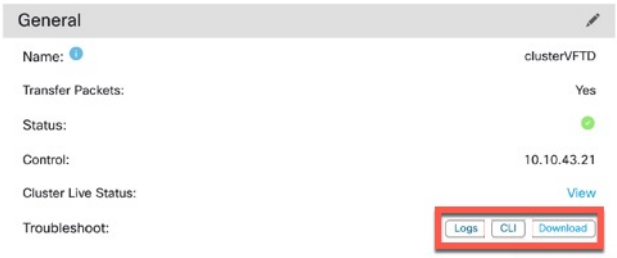


还可在**集群状态 (Cluster Status)** 对话框中点击**协调 (Reconcile)** 以重新注册数据单元。您还可以从节点 ping 通集群控制链路。请参阅在集群控制链路上执行 Ping，第 621 页。



- **常规 > 故障排除**- 可以生成和下载故障排除日志，还可以查看集群 CLI。请参阅对集群进行故障排除，第 621 页。

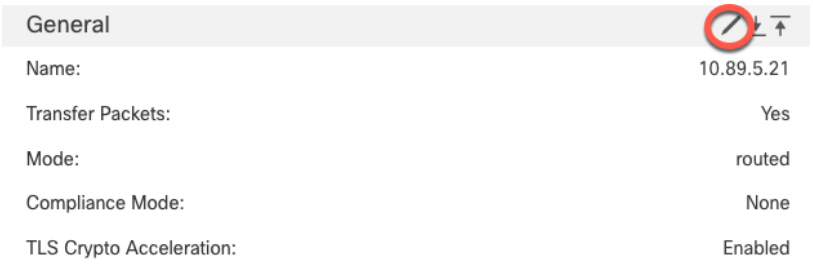
图 *223:* 故障排除



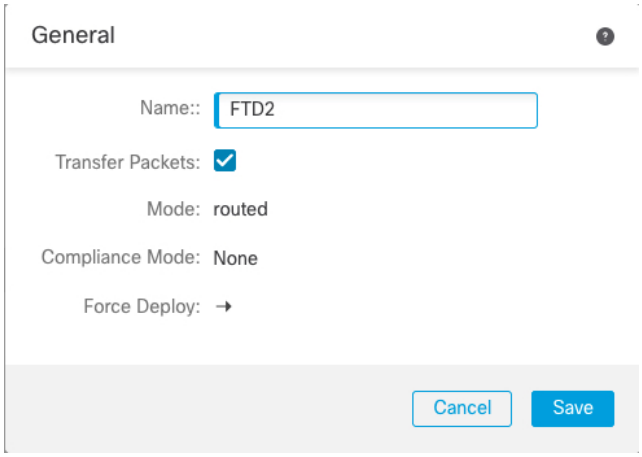
- **许可证** - 点击 **编辑** (✎) 可设置许可证授权。

步骤 4 在 **设备** > **设备管理** 上，然后点击**添加** > **设备**，您可以从右上角的下拉菜单中选择集群中的每个成员并配置以下设置。

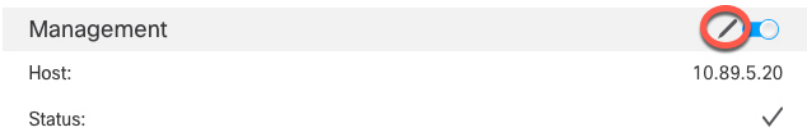
- **常规 (General)** > **名称 (Name)** - 通过点击 **编辑** (✎)更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理** > **主机**-如果在设备配置中更改了管理 IP 地址，则必须在 防火墙管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备；编辑 **管理** 区域中的 **主机** 地址。



配置集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *224:* 集群运行状况监控设置

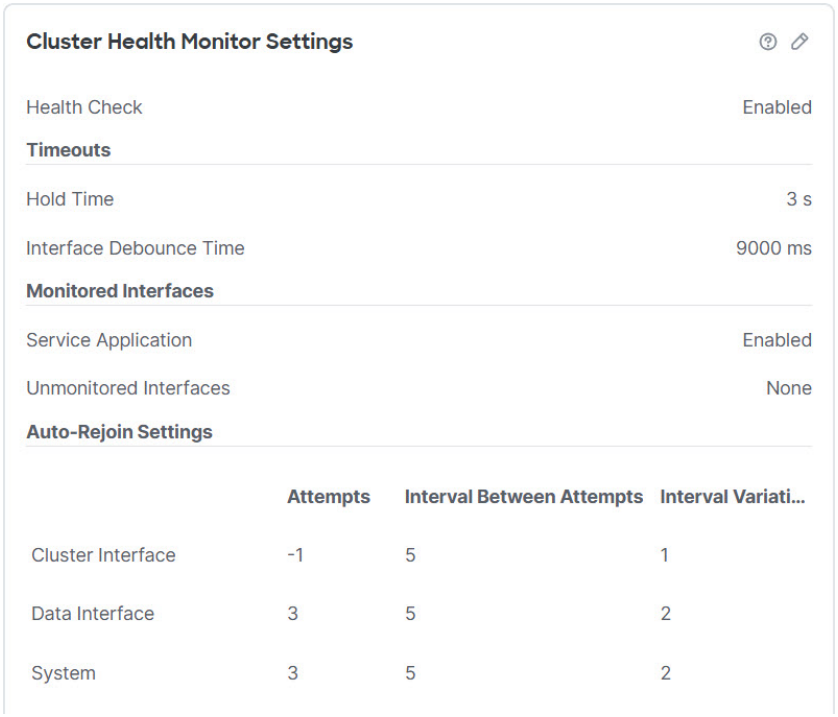


表 *45:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。

字段	说明
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。

注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

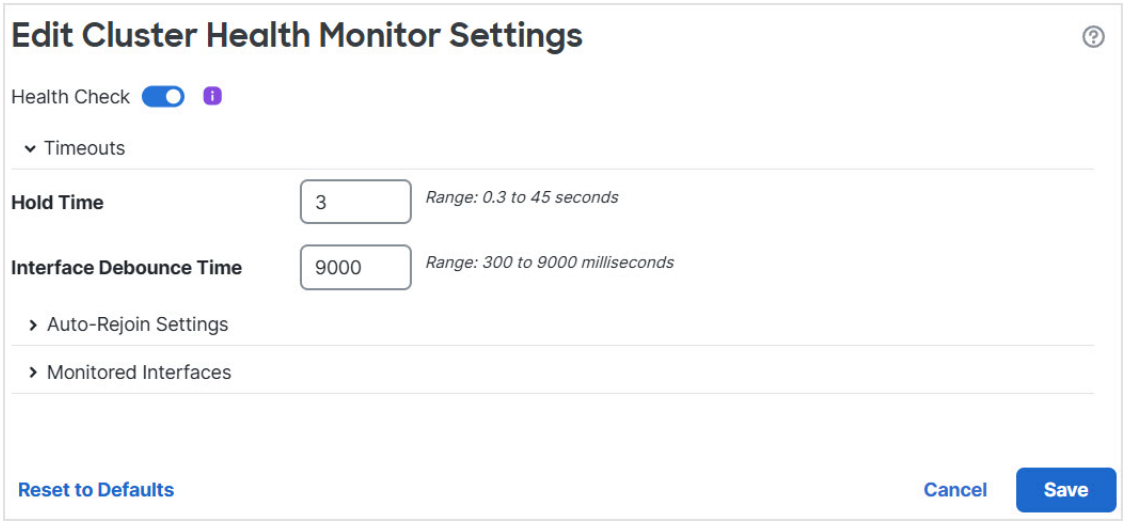
步骤 2 在要修改的集群旁边，点击 **编辑** ()。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *225:* 禁用系统运行状况检查



当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

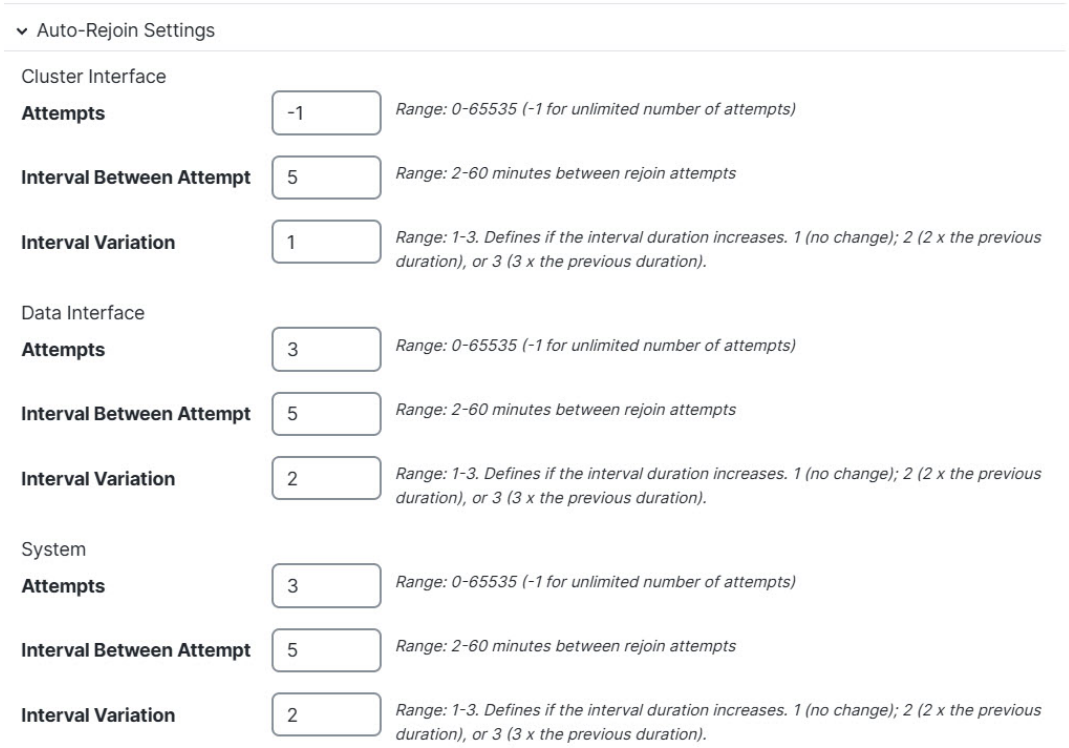
步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。

- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *226:* 配置自动重新加入设置



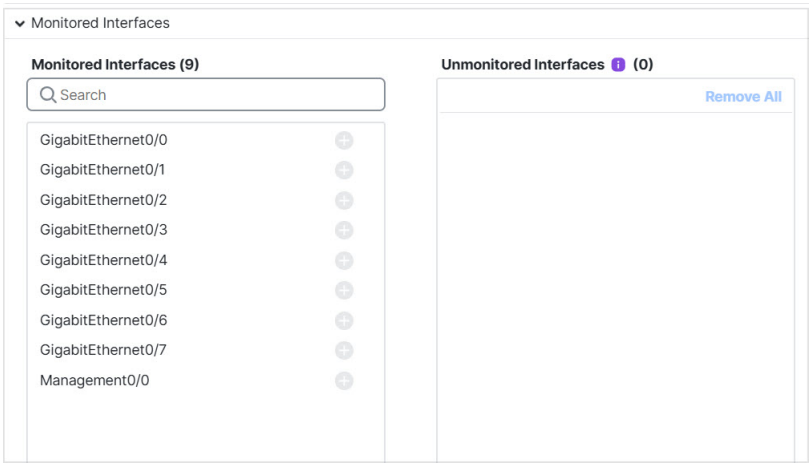
为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后

进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *227:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改，第 180 页。

管理集群节点

禁用集群

您可能需要停用节点，以准备删除节点，或临时进行维护。此程序旨在暂时停用节点；节点仍将显示在 防火墙管理中心 设备列表中。当节点变为非活动状态时，所有数据接口都将关闭。

注释 在禁用集群之前，请勿关闭节点。

过程

步骤 1 对于要禁用的设备，选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**禁用节点集群**。

步骤 2 确认要在节点上禁用集群。

该节点在 **设备** > **设备管理** 列表中其名称旁边会显示（**已禁用**）。

步骤 3 重新启用集群，请参阅 重新加入集群，第 613 页。

重新加入集群

如果从集群中删除了某个节点（例如对于出现故障的接口），或者如果您手动禁用集群，必须手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除节点的原因的更多信息，请参阅重新加入集群，第 630 页。

过程

步骤 1 对于要重新激活的设备，请选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**启用节点集群**。

步骤 2 确认要在节点上启用集群。

调整集群节点

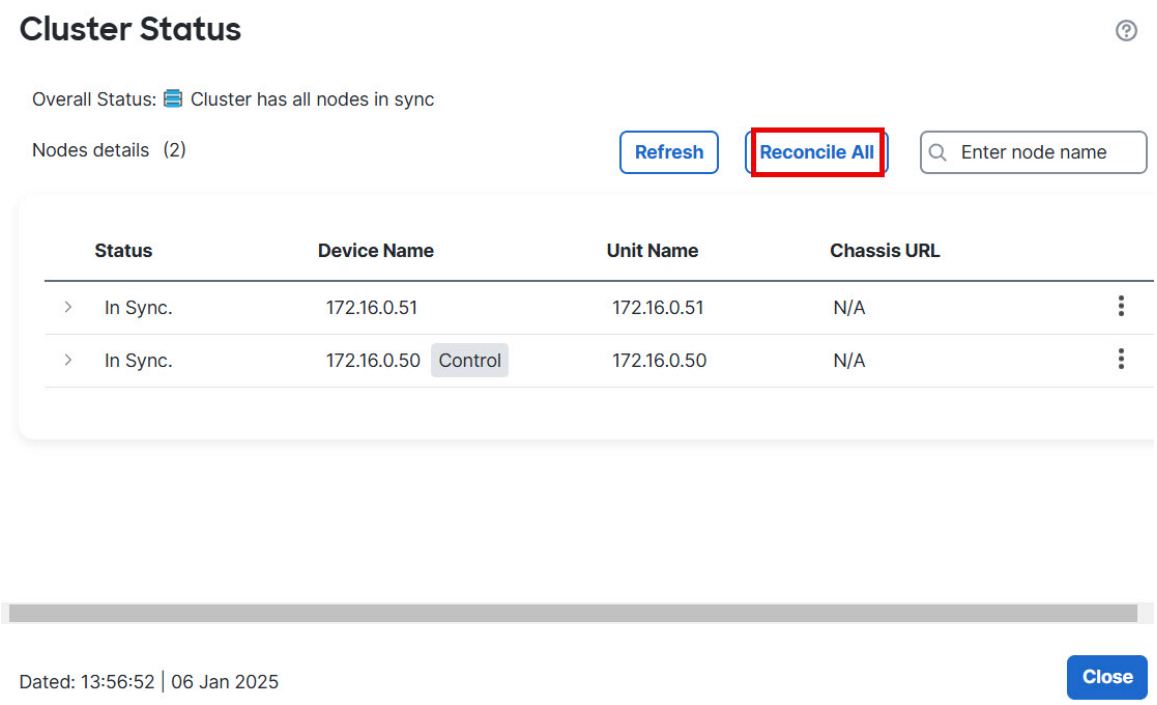
如果集群节点注册失败，则可将集群成员身份从设备协调至防火墙管理中心。例如，数据节点在防火墙管理中心 被占用或存在网络问题时注册失败的情况下。

过程

步骤 1 选择集群的 **设备** > **设备管理** **更多** (⋮)，然后选择**集群实时状态**，以打开**集群状态**对话框。

步骤 2 点击**协调全部 (Reconcile All)**。

图 *228:* 协调全部



有关集群状态的详细信息，请参阅监控集群，第 615 页。

取消注册集群或节点并注册到新防火墙管理中心

您可以从 防火墙管理中心 中取消注册集群，从而使集群保持不变。如果要将集群添加到新的 防火墙管理中心，则可能需要取消注册该集群。

您还可以从 防火墙管理中心 取消注册节点，而不会中断集群中的节点。虽然该节点不会显示在 防火墙管理中心 中，但它仍然是集群的一部分，并且它会继续传递流量，甚至可能成为控制节点。您无法取消注册当前的控制节点。如果无法再从防火墙管理中心访问该节点，您可能会希望将其取消注册，但在排除管理连接故障时，您仍希望将其作为集群的一部分。

取消注册集群：

- 会切断 防火墙管理中心和该集群之间的所有通信。
- 从 **设备管理** 页面删除集群。
- 如果集群的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将集群返回本地时间管理。
- 保持配置不变，以便集群继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将集群再次注册到相同或不同的防火墙管理中心会导致配置被删除，因此集群将在该点停止处理流量；集群配置保持不变，因此您可以将集群作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

开始之前

此过程需要 CLI 对一个节点拥有访问权限。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群或节点的 **更多** (⋮)，然后选择**取消注册**。

步骤 2 系统会提示您取消注册集群或节点；点击**是**。

步骤 3 您可以通过将其中一个集群成员添加为新设备来将集群注册到新的（或相同的）防火墙管理中心集群。

您只用将其中一个集群节点添加为设备，然后便可发现其余集群节点。

a) 连接到一个集群节点的 CLI，并使用 **configure manager add** 命令识别新 防火墙管理中心。

b) 选择 **设备** > **设备管理**，然后点击**添加设备**。

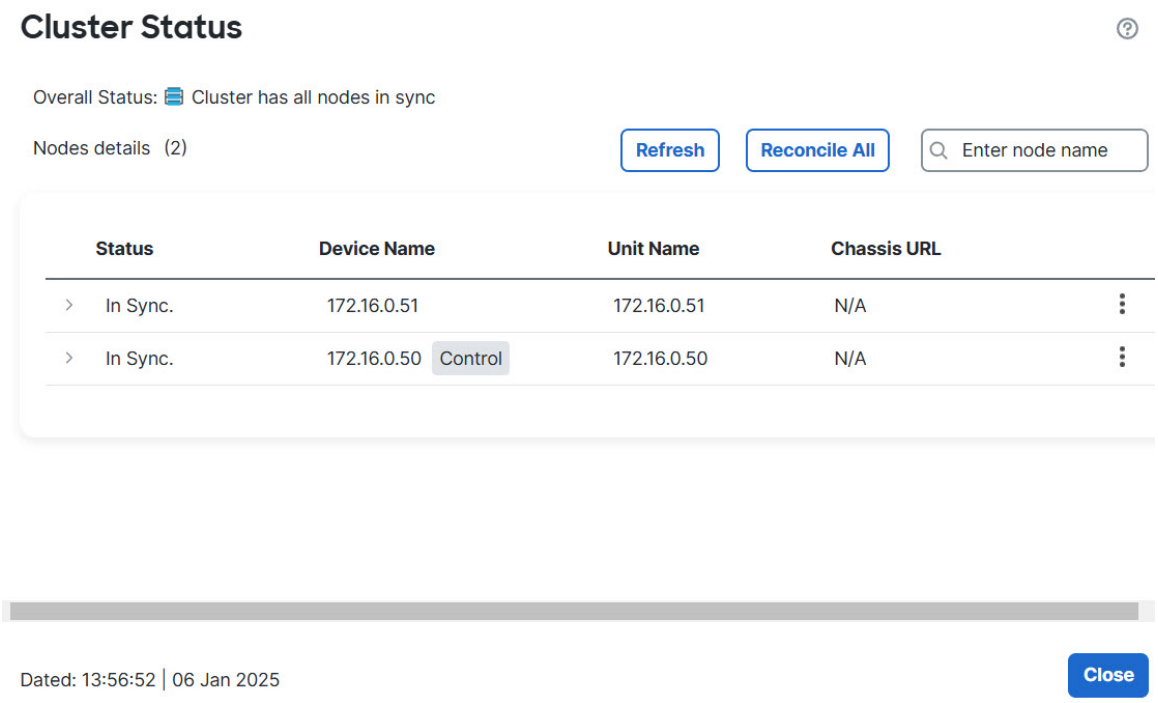
步骤 4 要重新添加已删除的节点，请参阅调整集群节点，第 613 页。

监控集群

您可以在 防火墙管理中心 中和 Firewall Threat Defense CLI 上监控集群。

- **集群状态**对话框，可从 **设备** > **设备管理**、**更多** (⋮) 图标或 **设备** > **设备管理** 访问，或点击**添加**，选择**集群**页面**常规**区域**集群实时状态**链接。

图 *229:* 集群状态



控制节点有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 (In Sync.) - 节点已向 防火墙管理中心 注册。
- 待处理注册 (Pending Registration) - 节点是集群的一部分，但尚未向 防火墙管理中心 注册。如果节点注册失败，则可点击**协调所有 (Reconcile All)** 以重试注册。
- 集群已禁用 (Clustering is disabled) - 节点已向 防火墙管理中心 注册，但它是集群的非活动成员。如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除节点。
- “正在加入集群...”(Joining cluster...) - 节点正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 防火墙管理中心 注册。

对于每个节点，您可以查看**摘要 (Summary)** 或**历史记录 (History)**。

图 *230:* 节点摘要

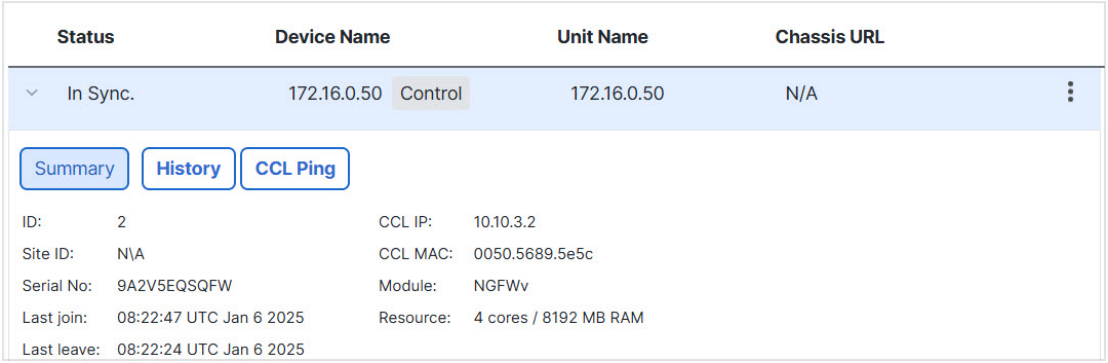
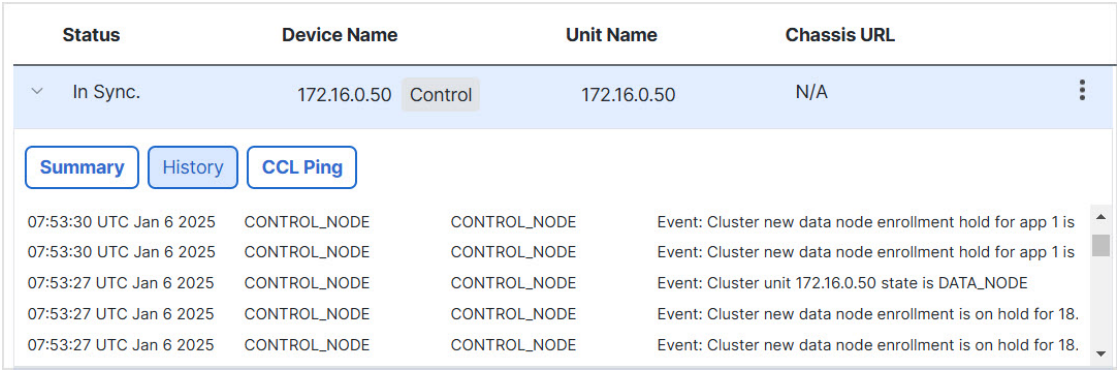


图 *231:* 节点历史记录



- **系统** (⚙) > **任务** 页面。

  任务 (Tasks) 页面会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

- **设备** > **设备管理** 然后点击**添加** > **设备** *cluster_name*。

  展开设备列表页面上的集群时，您可以看到所有成员节点，包括 IP 地址旁显示其角色的控制节点。对于仍在注册的节点，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

集群运行状况监控器控制面板

集群运行状况监控器

当 Firewall Threat Defense 是集群的控制节点时， 防火墙管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加（在公共云集群中，不属于防火墙管理中心的其他节点）或 正常（节点的理想状态）。
  - 集群统计信息部分显示集群的当前指标，包括CPU使用率、内存使用率、输入速率、输出速率、活动连接和 NAT 转换。

注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

  - 指标图表（即CPU使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。

- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。
  - “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。

- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU使用率、内存使用率、输入速率、输出速率、活动连接和NAT转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从防火墙管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（∨） 以展开和折叠托管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 **添加新的控制面板**（＋），通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

集群指标

集群运行状况监控器跟踪与集群及其节点相关的统计信息，以及负载分布、性能和CCL流量统计信息的汇总。

表 *46:* 集群指标

指标	说明	格式
CPU	集群节点上的CPU指标平均值（分别针对数据平面和 snort）。	percentage
Memory	集群节点上的平均内存指标（分别用于数据平面和 snort）。	percentage
数据吞吐量	集群的传入和传出数据流量统计信息。	bytes
CCL 吞吐量	集群的传入和传出 CCL 流量统计信息。	bytes
连接	集群中的活动连接计数。	数字
NAT 转换	集群的 NAT 转换计数。	数字
分布	集群中每秒的连接分布计数。	数字
数据包数	集群中每秒的数据包分发计数。	数字

对集群进行故障排除

您可以使用 **CCL Ping** 工具确保集群控制链路正常运行。 您还可以使用以下适用于设备和集群的工具：

- 故障排除文件-如果节点未能加入集群，系统将自动生成故障排除文件。您还可以从 **设备** > **设备管理** > **集群** > **常规** 区域生成和下载故障排除文件。请参阅生成故障排除文件。

  您还可以通过点击 **更多** (⋮) 并选择 **文件故障排除** ，从 **设备管理**页面生成文件。

- CLI 输出-从 **设备** > **设备管理** > **集群** > **常规**区域，您可以查看一组预定义的 CLI 输出，帮助您排除集群的故障。系统会自动为集群运行以下命令：

  - **show running-config cluster**
  - **show cluster info**
  - **show cluster info health**
  - **show cluster info transport cp**
  - **show version**
  - **show asp drop**
  - **show counters**
  - **show arp**
  - **show int ip brief**
  - **show blocks**
  - **show cpu detailed**
  - **show interface** *ccl_interface*
  - **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

  您还可以在命令字段中输入任何 **show** 命令。有关详细信息，请参阅查看 CLI 输出。

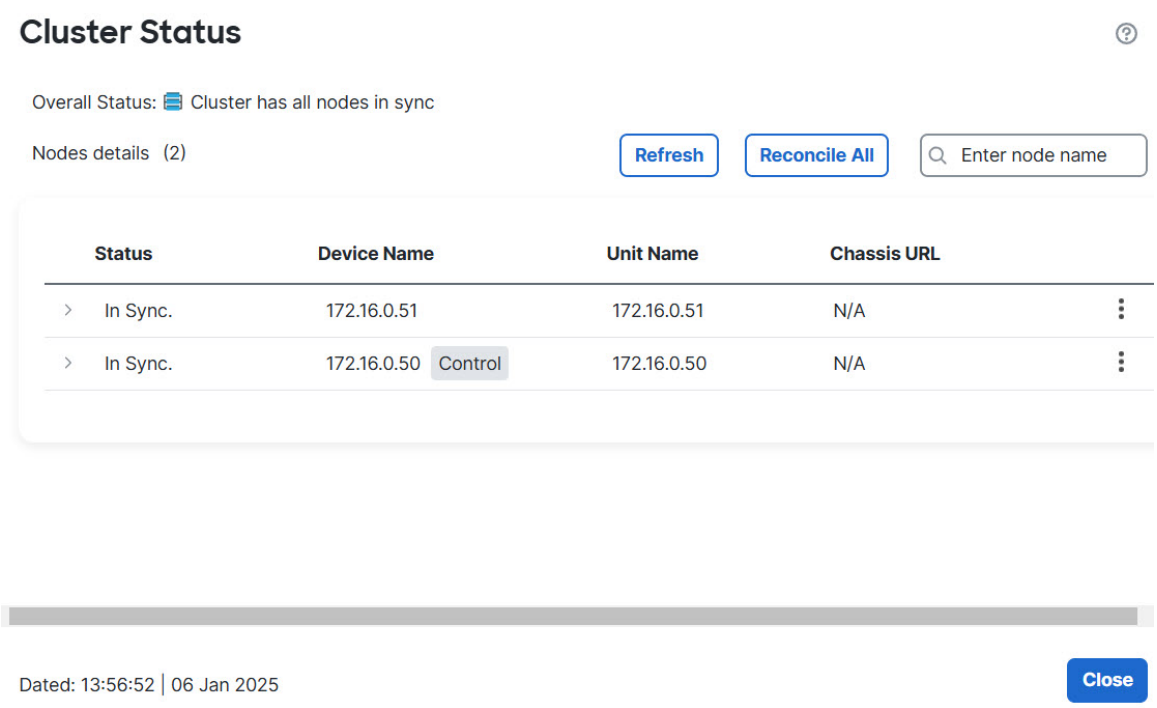
在集群控制链路上执行 Ping

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。如果您遇到集群控制链路连接问题，此工具允许您手动 ping 所有已加入集群的节点。

过程

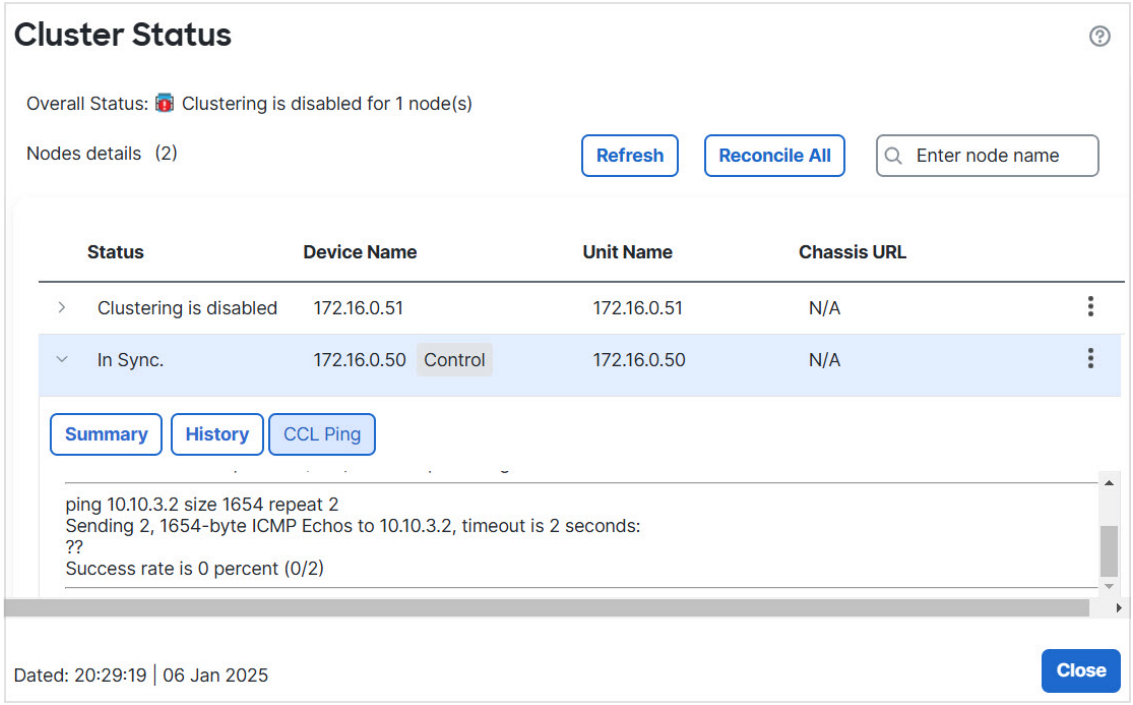
步骤 1 选择 **设备** > **设备管理**，点击集群旁边的 **更多** (⋮) 图标，然后选择**集群实时状态**。

图 *232:* 集群状态



步骤 2 展开其中一个节点，然后点击 **CCL Ping**。

图 *233: CCL Ping*



节点使用与最大 MTU 匹配的数据包大小在集群控制链路上向每个其他节点发送 ping 命令。

升级集群

要升级 Firewall Threat Defense Virtual 集群，请执行以下步骤。

开始之前

- 在公共云中升级集群之前，请将目标版本映像复制到云映像存储库，并更新集群部署模板中的映像 ID（实际上，我们建议使用修改后的副本替换现有模板）。这可确保在升级后，新实例（例如，在集群扩展期间启动的实例）将使用正确的版本。如果市场没有您需要的映像，例如在集群修补后，请从运行正确版本的独立Firewall Threat Defense Virtual实例的快照创建一个自定义映像，无需实例特定的 (Day 0) 配置。
- 对于 AWS 的Firewall Threat Defense Virtual，请在自动扩展的集群升级之前暂停 HealthCheck 和 ReplaceUnhealthy 进程。这可确保在升级后重新启动期间 Auto Scaling 组不会终止实例。您可以稍后恢复挂起的进程。有关说明，请参阅《Amazon EC2 Auto Scaling 用户指南： 暂停和恢复 Amazon EC2 Auto Scaling 进程》 。

过程

步骤 1 将目标映像版本上传到云映像存储。

步骤 2 使用更新后的目标映像版本来更新集群的云实例模板。

a) 使用目标映像版本来创建实例模板的副本。

b) 将新创建的模板附加到集群实例组。

注释
如果用户希望保留旧的接口命名约定，请在 Day 0 配置中使用"IfNamingConvention"： "Old"键值对。

步骤 3 将目标映像版本升级包上传到 防火墙管理中心。

步骤 4 对要升级的集群执行就绪性检查。

步骤 5 成功进行就绪性检查后，开始安装升级包。

步骤 6 防火墙管理中心 会一次升级一个集群节点。

步骤 7 成功升级集群后，防火墙管理中心 会显示通知。

升级后，实例的序列号和 UUID 不会变化。

集群参考

本部分包括有关集群工作原理的详细信息。

威胁防御功能和集群

部分 Firewall Threat Defense 功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

不支持的功能和集群

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略。

- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 在公共云中不支持站点间 VPN（基于策略和路由）。
- DHCP 客户端、服务器和代理。支持 DHCP 中继。

- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- 防火墙管理中心 UCAPL/CC 模式

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。



注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。



注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅 FlexConfig 策略，第 1041 页。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- 静态路由监控

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

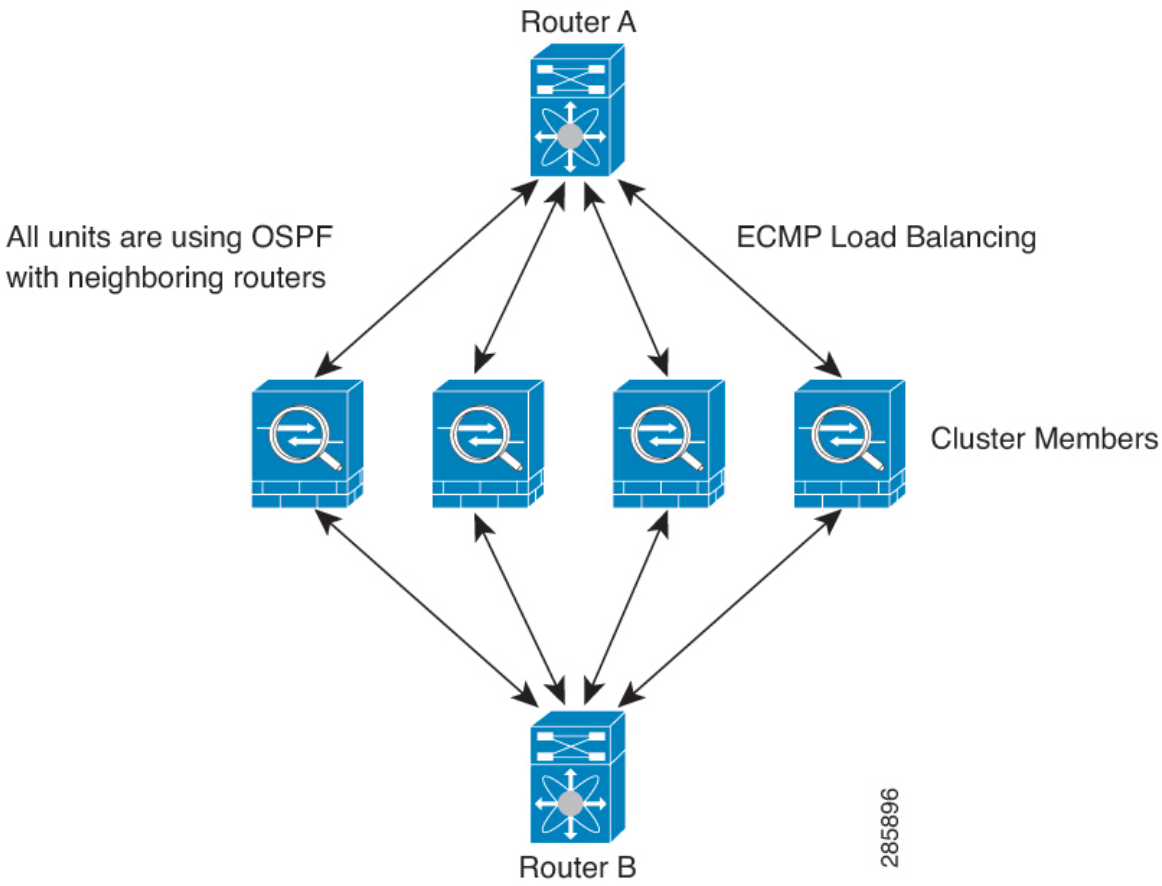
连接设置和集群

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *234:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

NAT 和集群

对于 NAT 用途，请参阅以下限制。

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 Firewall 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 Firewall 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。

- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。

- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混

合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。

- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。



注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。



注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

监控所有物理接口；只能监控已命名的接口。 可以选择性地禁用对每个接口的监控。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。节点将在 500 毫秒后删除。

发生故障后的状态

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

Firewall Threat Defense将自动尝试重新加入集群，具体取决于故障事件。



注释 当 Firewall Threat Defense 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - Firewall Threat Defense 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 Firewall Threat Defense应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。Firewall Threat Defense应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。
- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *47:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	支持	—
动态路由	支持	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。
- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

ICMP/ICMPv6 散列详细信息：

- 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
- 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
- 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

端口地址转换连接

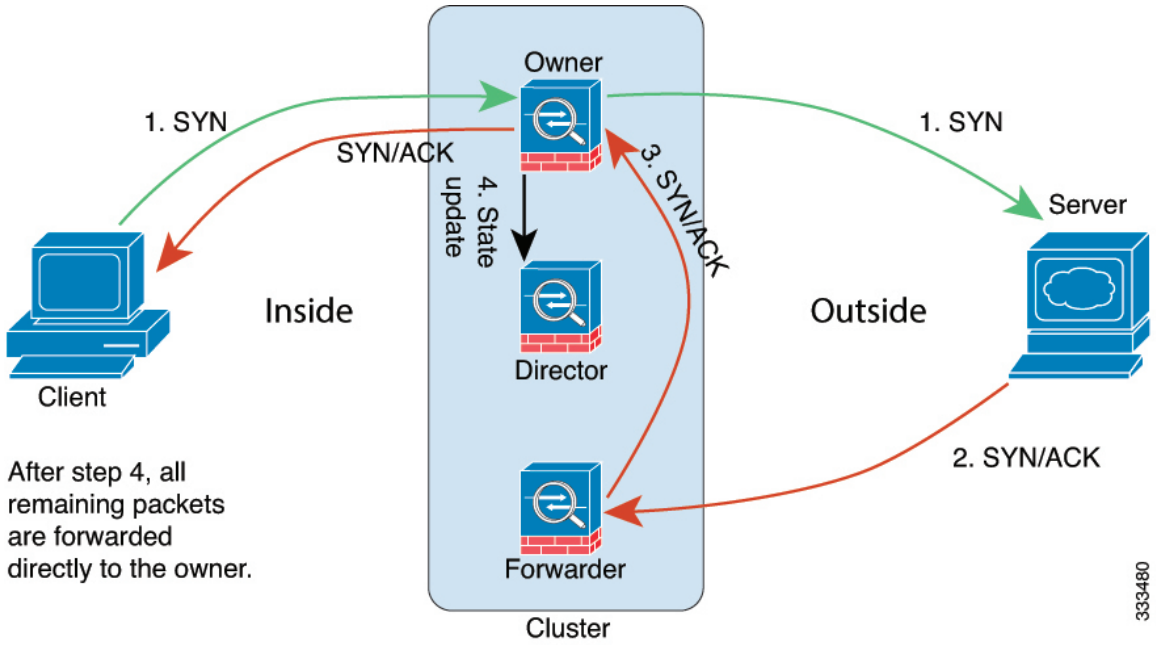
新连接所有权

此版本不支持流量重定向。通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。同一连接的所有后续数据包都应到达同一节点。如果任何连接数据包到达其他节点，它们将被丢弃。如果反向流量到达其他节点，也将被丢弃。对于集中功能，如果连接不到达控制节点，则它们会被丢弃。

默认情况下，AWS GWLB 使用 5 元组来保持流粘性。建议在 AWS GWLB 上启用 2 元组或 3 元组粘性，以确保将相同的流发送到同一节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

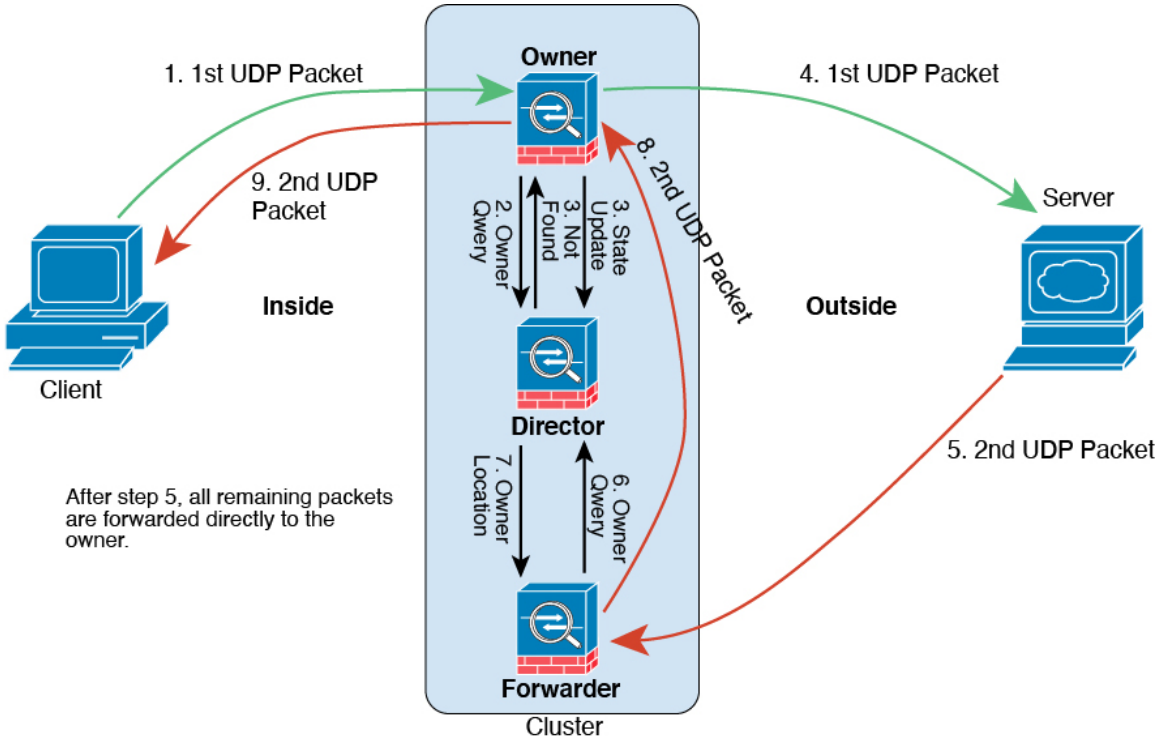


1. SYN 数据包从客户端发出，被传送到一台 Firewall 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 Firewall 威胁防御（基于负载均衡方法）。此 Firewall 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *235: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个Firewall 威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

关于公共云中的 Threat Defense Virtual 集群的历史记录

表 48:

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群节点加入时的 MTU ping 测试通过尝试较小的 MTU 来提供更多信息	10.0.0	10.0.0	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，它将尝试除以 MTU，并继续除以 2，直到 MTU ping 成功。成功的 ping 值会显示在 **show cluster info trace** 中，因此您可以将 MTU 调整为可用值，然后重试。 即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。 我们建议将交换机 MTU 的大小增加到建议的值，但如果您无法更改交换机配置，则可以使用集群控制链路的工作值来形成集群。 添加/修改的命令：**show cluster info trace**、**show cluster history**。
关于节点加入时时间节点的 MTU ping 测试	7.6.0	7.6.0	节点加入集群时，会向控制节点发送数据包大小为集群控制链路 MTU 两倍的 Ping 请求，以检查 MTU 兼容性。此前，仅控制节点发送 Ping。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。 添加/修改的命令：**show cluster history**。
集群控制链路 ping 工具。	7.2.67.4.1	任意	您可以通过执行 ping 来检查是否所有集群节点都能通过集群控制链路相互连接。节点无法加入集群的一个主要原因是集群控制链路配置不正确，例如，集群控制链路 MTU 设置可能高于连接交换机的 MTU。 新增/修改的屏幕：**设备** > **设备管理** > **更多** > **集群实时状态**。
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
集群运行状况监控器控制面板。	7.3.0	任意	您现在可以在集群运行状况监控控制面板上查看集群运行状况。 新增/修改的屏幕：**系统** > **运行状况** > **监控器**
Azure 中的 Firewall Threat Defense Virtual 集群。	7.3.0	7.3.0	现在，您可以在 Azure 中为 Azure 网关负载均衡器或外部负载均衡器配置最多 16 个节点 Firewall Threat Defense Virtual 的集群。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：Azure 中的 Firewall Threat Defense Virtual
公共云（Amazon Web 服务和 Google Cloud Platform）上 Firewall Threat Defense Virtual 的集群。	7.2.0	7.2.0	Firewall Threat Defense Virtual 支持公共云（AWS 和 GCP）上最多 16 个节点的单个接口集群。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加设备 (Add Device)** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：AWS 和 GCP 上的 Firewall Threat Defense Virtual



第 13 章

集群： Firepower 4100/9300

通过集群，您可以将多个 Firewall Threat Defense 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 691 页。

- 关于 Firepower 4100/9300 机箱上的集群，第 637 页
- 集群许可证，第 641 页
- 集群要求和前提条件，第 642 页
- 集群准则和限制，第 645 页
- 配置集群，第 649 页
- FXOS：删除集群设备，第 675 页
- FMC：管理群集成员，第 677 页
- 防火墙管理中心：监控集群，第 682 页
- 防火墙管理中心：对集群进行故障排除，第 687 页
- 集群示例，第 689 页
- 集群参考，第 691 页
- 集群的历史记录，第 703 页

关于 Firepower 4100/9300 机箱上的集群

在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 对于本地实例集群： 为设备间通信创建 集群控制链路 （默认情况下，使用端口通道 48）。

  对于多实例集群：您应该在一个或多个集群类型 Etherchannel 上预配置子接口；每个实例都需要自己的集群控制链路。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，此链路利用 Firepower 9300 背板进行集群通信。

  对于多机箱集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。

- 在应用中创建集群引导程序配置。

  在部署集群时，机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。

- 将数据接口作为跨网络 接口分配给集群。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，跨网络接口不限于 EtherChannel，就像用于多个机箱的集群一样。 Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。 对于多机箱集群，必须对所有数据接口使用跨网络 EtherChannel。

注释 除管理接口以外，不支持独立接口。

- 向集群中的所有设备分配管理接口。

有关集群的详细信息，请参阅以下各节：

引导程序配置

在部署集群时，Firepower 4100/9300 机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。

集群成员

集群成员协调工作来实现安全策略和流量的共享。

一个集群成员是**控制**设备。系统自动确定控制设备。所有其他成员都是**数据**设备。

您必须仅在控制设备上执行所有配置；然后，配置将复制到数据设备。

有些功能在集群中无法扩展，控制设备将处理这些功能的所有流量。。

集群控制链路

对于本地实例集群：使用端口通道 48 接口自动创建集群控制链路。

对于多实例群集：您应该在一个或多个集群类型 Etherchannel 上预配置子接口；每个实例都需要自己的集群控制链路。

对于与一个 Firepower 9300 机箱内的安全模块隔离的集群，此接口没有成员接口。此群集类型 EtherChannel 利用 Firepower 9300 背板进行集群通信。 对于多机箱群集，必须将一个或多个接口添加到 EtherChannel。

对于 2 个机箱群集，请勿直接将群集控制链路从一个机箱连接到另一个机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

群集控制链路流量包括控制流量和数据流量。

确定集群控制链路规格

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

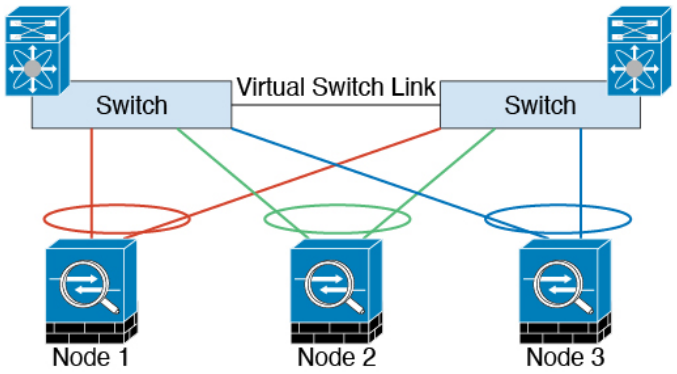
- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS)、虚拟端口通道 (vPC)、StackWise 或 StackWise Virtual 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是冗余系统的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到冗余系统中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。 对于多实例集群（通常使用同一 EtherChannel 的不同 VLAN 子接口），由于 VLAN 分离，同一 IP 地址可用于不同的集群。集群控制链路网络不能包括设备之间的任何路由器；仅可执行第 2 层交换。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

必须为集群分配管理类型的接口。此接口是与跨网络接口相对立的一种特殊接口。通过管理接口，可以直接连接到每个设备。此管理接口不同于设备上的其他接口。它用于设置设备并将其注册到 Secure Firewall Management Center。它会使用自己的本地身份验证、IP 地址和静态路由。每个集群成员都使用您作为部分引导程序配置的管理网络中的独立 IP 地址。

集群接口

对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，可以为集群分配物理接口或 EtherChannel 接口（也称为端口通道）。分配给集群的接口是对集群各个成员间的流量进行负载均衡的跨网络接口。

对于多机箱集群，只能为集群分配数据 EtherChannel 接口。这些跨网络 EtherChannel 在每个机箱上都包括相同的成员接口；在上游交换机上，所有这些接口都包括在一个 EtherChannel 内，因此交换机不知道它连接到多台设备。

您可以使用常规防火墙接口或仅 IPS 接口（内联集或被动接口）。

除管理接口以外，不支持独立接口。

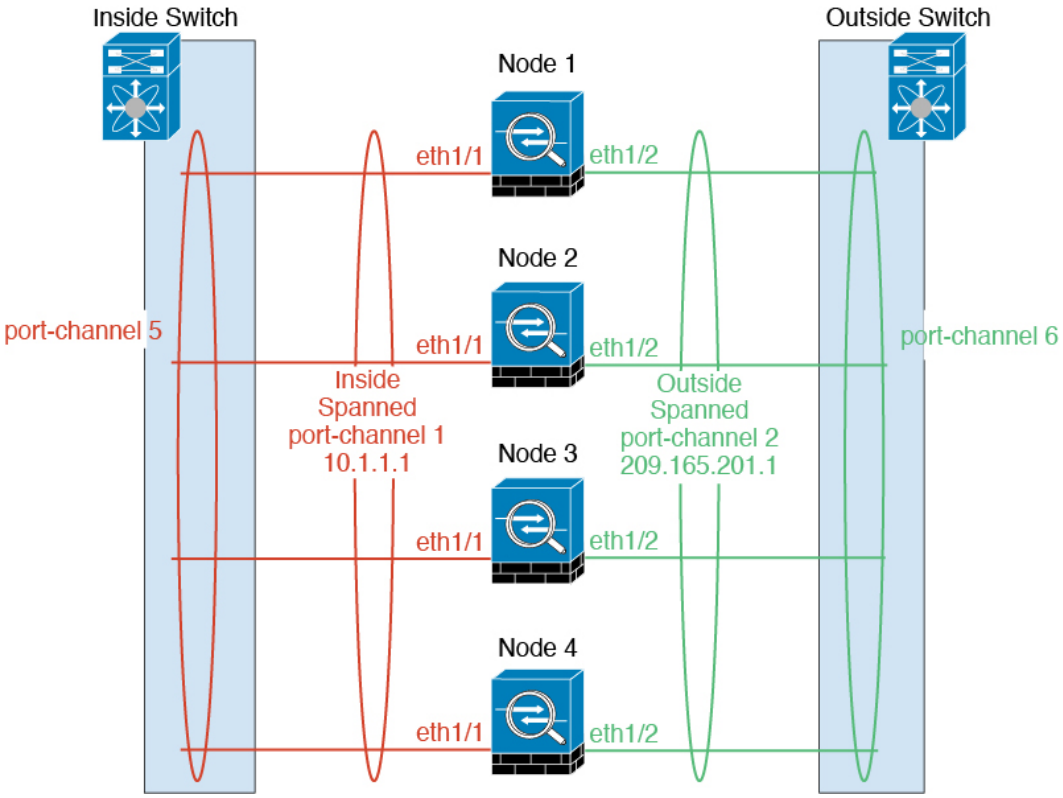
跨网络 EtherChannel

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。

对于常规防火墙接口：在路由模式和透明防火墙模式下均可配置跨区以太网通道。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。

负载均衡属于 EtherChannel 固有的基本操作。

对于多实例集群，每个集群都需要专用数据 Etherchannel，不能使用共享接口或 VLAN 子接口。



连接到冗余交换机系统

我们建议将 EtherChannel 连接到冗余交换机系统（例如 VSS、vPC、StackWise 或 StackWise Virtual 系统），以便为接口提供冗余。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

集群许可证

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将集群节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。您可以在 **设备** > **设备管理** 中修改集群的许可证，然后选择**添加**、**集群**，然后选择**许可证**区域。

注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

集群要求和前提条件

集群型号支持

Firewall Threat Defense 在以下型号上支持集群：

- Firepower 9300-您可以在集群中包含最多 16 个节点。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。支持多个机箱的集群，以及与一个机箱内的安全模块隔离的集群。
- Firepower 4100-使用多机箱集群时，最多支持 16 个节点。

用户角色

- 管理员
- 访问管理员
- 网络管理员

集群硬件和软件要求

集群中的所有机箱：

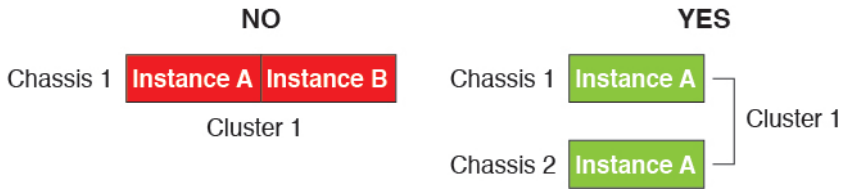
- 本地实例集群 -对于 Firepower 4100：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 容器实例集群 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



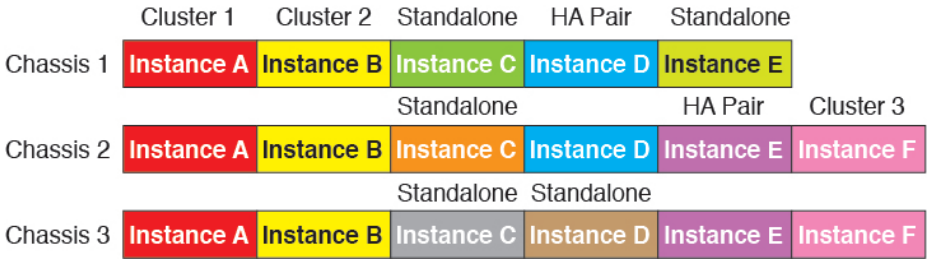
- 除进行映像升级外，必须运行完全相同的 FXOS 和应用软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。 对于 防火墙威胁防御， 防火墙管理中心 必须使用同一台 NTP 服务器。请勿手动设置时间。

多实例集群要求

- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。



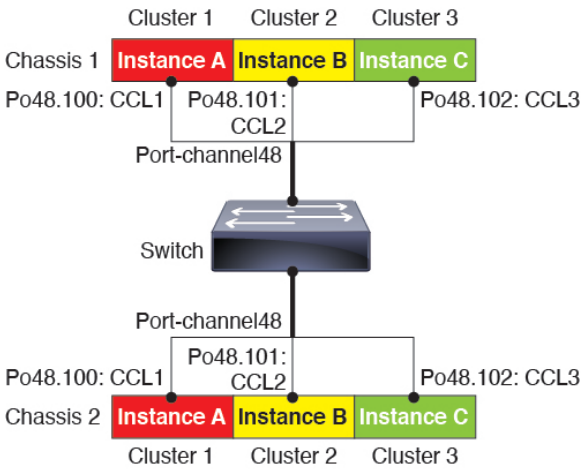
- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。



- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。

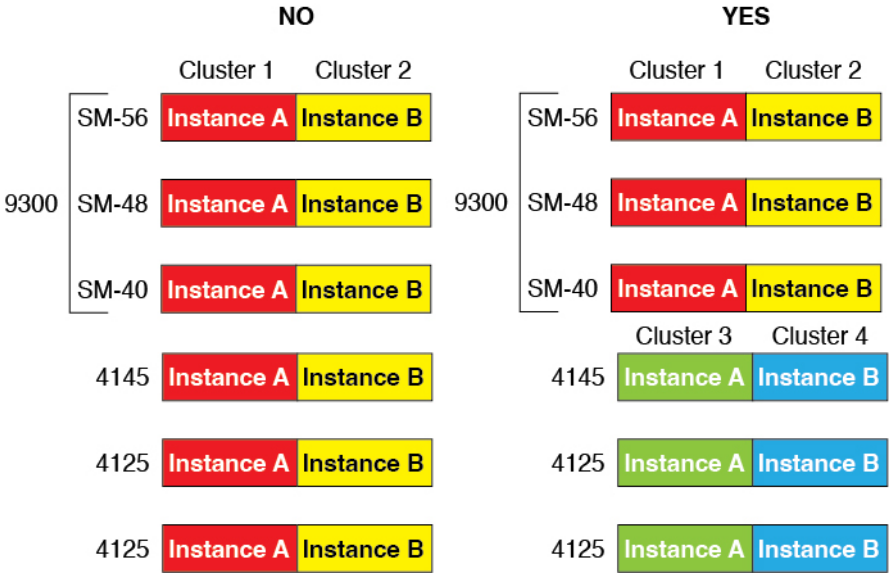


- 匹配资源配置文件 - 建议集群中的每个节点都使用相同的资源配置文件属性；但是，在将集群节点更改为使用其他资源配置文件或使用不同型号时，允许使用不匹配的资源。
- 专用集群控制链路 - 对于具有多个机箱的集群，每个集群都需要专用的集群控制链路。例如，每个集群可以在同一集群类型 EtherChannel 上使用单独的子接口，也可以使用单独的 Etherchannel。



- 无共享接口 - 集群不支持共享类型接口。但是，多个集群可以使用相同的管理接口和事件接口。
- 无子接口 - 多实例集群无法使用 FXOS 定义的 VLAN 子接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。
- 混合机箱型号 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器

实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



- 最多 6 个节点 - 在一个集群中最多可以使用六个容器实例。

交换机要求

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机的特性，请参阅思科 FXOS 兼容性。

集群准则和限制

集群的交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。

- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **src-dst-mixed-ip-port**（请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

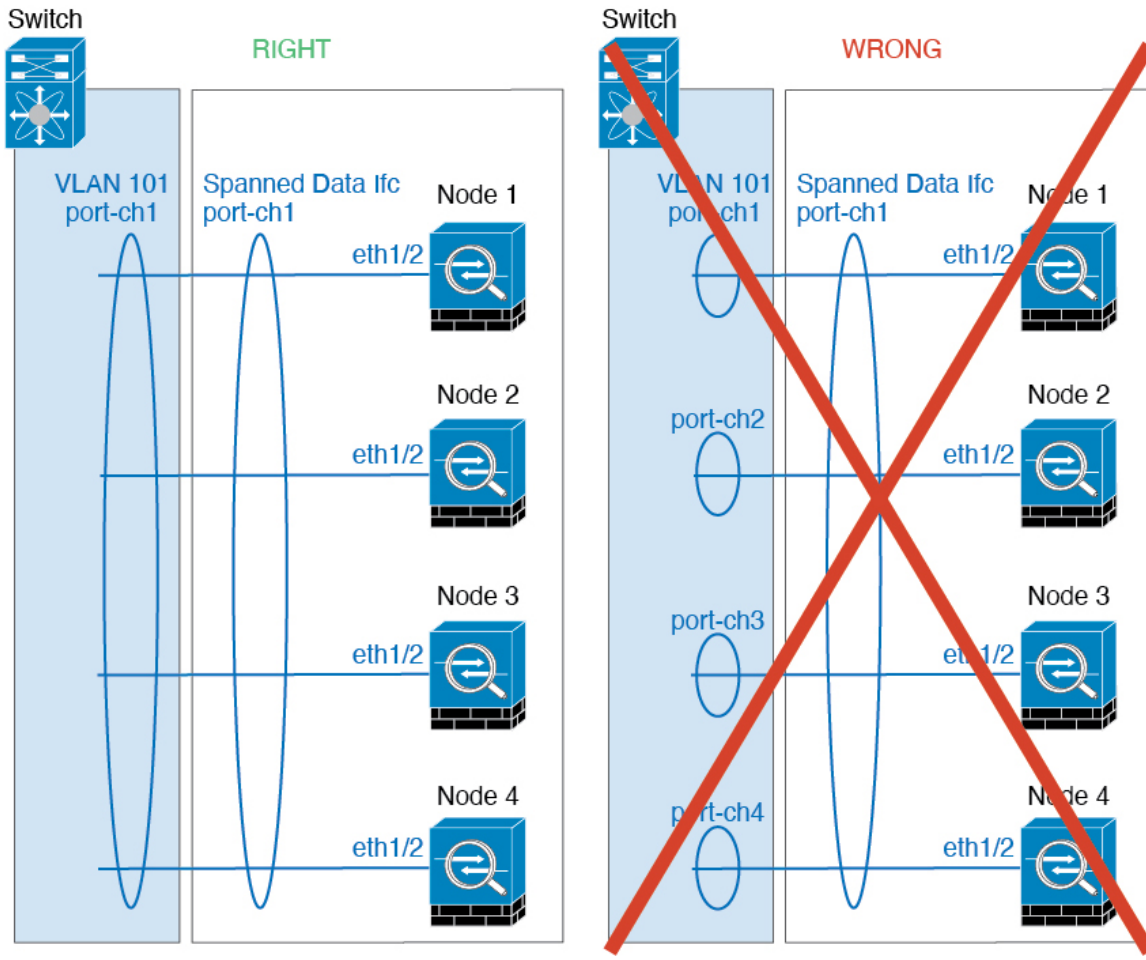
  router(config)# **port-channel** *id* **hash-distribution fixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

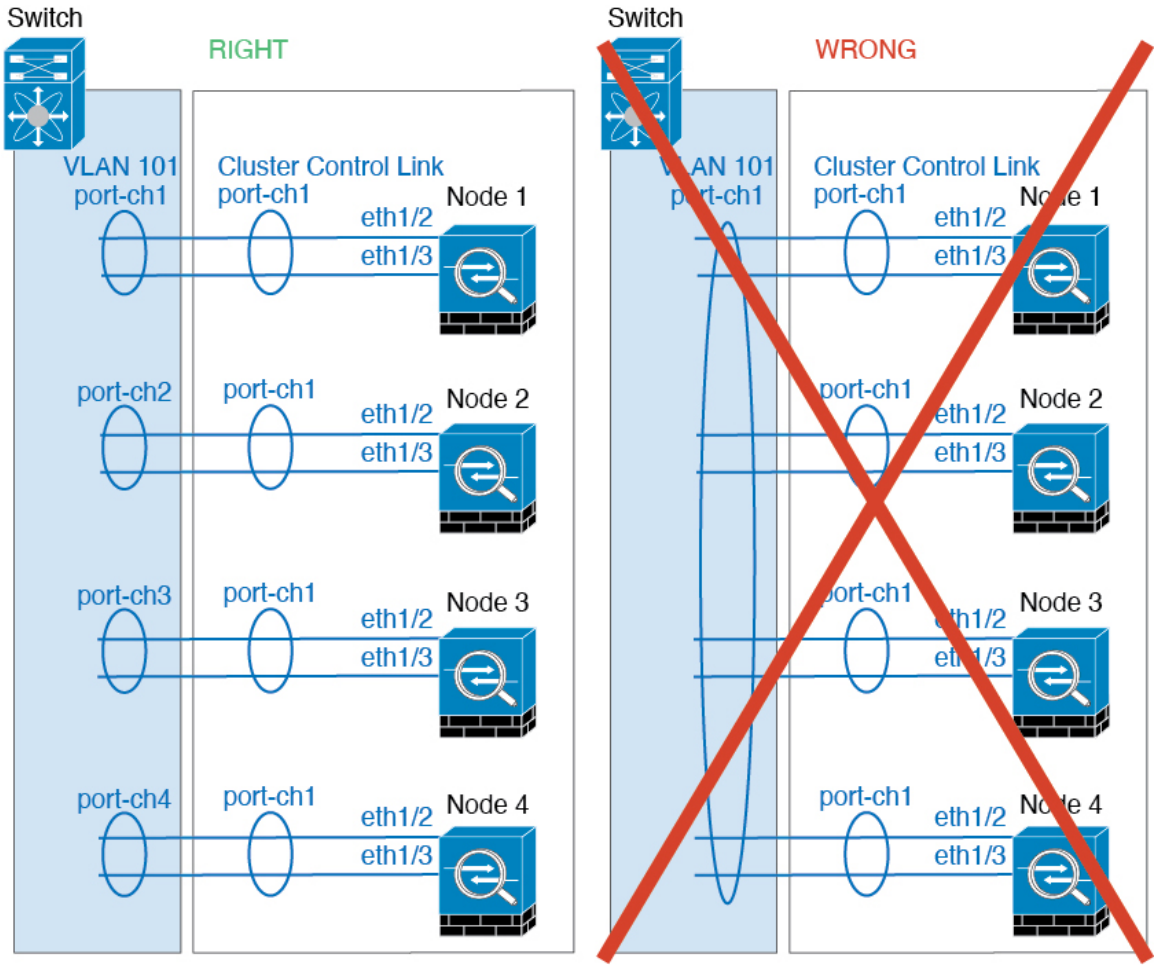
- Firepower 4100/9300 集群支持 LACP 正常融合。因此， 您可以在连接的 Cisco Nexus 交换机上启用 LACP 正常融合。
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

集群的 EtherChannel

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。
  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firepower 4100/9300 机箱 或交换机上的接口、添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。在某些情况下，丢弃的数据包可能会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包会使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨区以太网通道接口的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器未限制 ICMP 错误消息时，会有大量 ICMP 消息被发回集群。这些消息可能会导致集群的某些设备出现高 CPU 问题，从而可能影响性能。因此，我们建议您限制 ICMP 错误信息。
- 我们建议将 EtherChannel 连接到 VSS、vPC、StackWise 或 StackWise Virtual，以实现冗余。
- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。

- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要建立新连接以连通新设备。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。

默认值

- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 出现故障的集群控制链路的集群自动重新加入功能设置为无限次尝试，每隔 5 分钟进行一次。
- 出现故障的数据接口的集群自动重新加入功能设置为尝试 3 次，每 5 分钟一次，递增间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

配置集群

您可以从 Firepower 4100/9300管理引擎轻松部署集群。自动为每台设备生成所有初始配置。然后，可将设备添加到防火墙管理中心，再将它们组合成一个集群。

FXOS： 添加 防火墙威胁防御 群集

在本地模式下： 可以将集群添加到与机箱内的安全模块隔离的单个 Firepower 9300 机箱，也可以使用多个机箱。

在多实例模式下：您可以将一个或多个集群添加到与机箱内的安全模块隔离的单个 Firepower 9300 机箱（必须在每个模块上包含一个实例），或者在多个机箱上添加一个或多个集群。

对于多机箱群集，您必须单独配置每个机箱。在一个机箱上添加群集；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署

创建 防火墙威胁防御 集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。

对于多机箱集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

在 Firepower 9300 机箱中，必须对全部 3 个模块插槽或容器实例（每个插槽中有一个容器实例）启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传至 Firepower 4100/9300 机箱。
- 对于容器实例，如果您不想使用默认配置文件，则请根据为容器实例添加资源配置文件，第315页添加资源配置文件。

- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择**安全模块 (Security Modules)** 或**安全引擎 (Security Engine)**，然后点击重新初始化图标（）。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。
- 收集以下信息：
  - 管理接口 ID、IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的防火墙管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址
  - 防火墙威胁防御 主机名和域名

过程

步骤 1 配置接口。

a) 部署集群之前，至少添加一个“数据”类型接口或 EtherChannel（也称为端口通道）。请参阅添加 EtherChannel（端口通道），第 311 页或配置物理接口，第 310 页。

对于多机箱集群，所有数据接口必须为至少带有一个成员接口的跨区以太网通道。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 645 页。

对于多实例集群，禁止在集群中使用 FXOS 定义的 VLAN 子接口或数据共享接口。仅支持应用定义的子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 276 页。

b) 添加“管理”类型接口或 EtherChannel。请参阅添加 EtherChannel（端口通道），第 311 页或配置物理接口，第 310 页。

管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口不同（在FXOS中，您可能会看到机箱管理接口显示为 MGMT、management0 或其他类似名称）。

对于多机箱集群，在各机箱上添加相同的管理接口。

对于多实例集群，可以在同一机箱上的多个集群之间或与独立实例共享同一管理接口。

c) 对于多机箱集群，将成员接口添加到集群控制链路 EtherChannel（默认情况下为端口通道48）。请参阅 添加 EtherChannel（端口通道），第 311 页。

请勿为与一个 Firepower 9300 机箱内的安全模块隔离的集群添加成员接口。例如，如果添加成员，则机箱假设此集群将使用多机箱，且将仅允许您使用跨区以太网通道。

在**接口**选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态**将显示为**失败**。对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，此 EtherChannel 无需任何成员接口，您可忽略此运行状态。

在各机箱上添加相同的成员接口。 集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 645 页。

对于多实例集群，可以创建其他集群类型 Etherchannel。与管理接口不同，集群控制链路不可在多台设备之间共享，因此每个集群都需要一个集群接口。但是，建议使用 VLAN 子接口而不是多个 EtherChannel；请参阅下一步，将 VLAN 子接口添加到集群接口。

d) 对于多实例集群，将 VLAN 子接口添加到集群 EtherChannel，以便每个集群都有一个子接口。请参阅 为容器实例添加 VLAN 子接口，第 313 页。

如果向某个集群接口添加子接口，则不能将该接口用于本地集群。

e) （可选） 添加事件接口。请参阅添加 EtherChannel（端口通道），第 311 页或配置物理接口，第 310 页。

此接口是 Firewall Threat Defense 设备的辅助管理接口。要使用此接口，您必须在 Firewall Threat Defense CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅 Firewall Threat Defense 命令参考中的 **configure network** 命令。

对于多机箱集群，在各机箱上添加相同的事件接口。

步骤 2 选择**逻辑设备 (Logical Devices)**。

步骤 3 依次点击**添加 (Add)** > **集群 (Cluster)**，并设置以下参数：

图 ***236:*** 本地集群

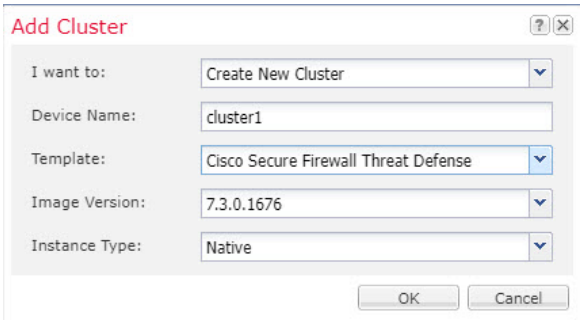
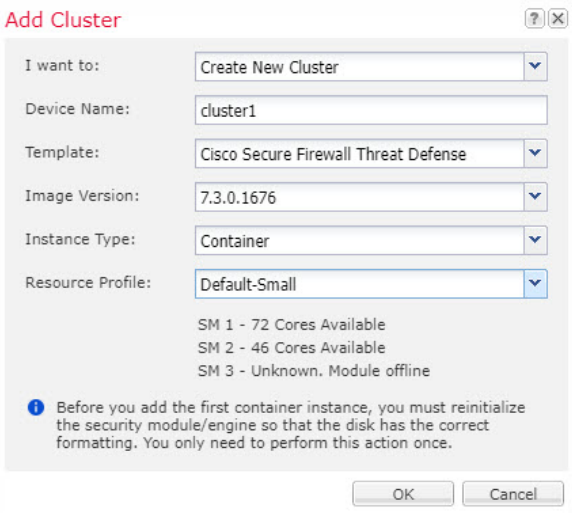


图 *237:* 多实例集群



a) 选择**我想：(I want to:)** > **新建集群 (Create New Cluster)**

b) 提供**设备名称**。

此名称由机箱管理引擎在内部用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

c) 对于**模板**，请选择 **Cisco Firepower Threat Defense**。

d) 选择**映像版本 (Image Version)**。

e) 对于**实例类型 (Instance Type)**， 类型选择**本地 (Native)** 或**容器 (Container)**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此您仅可安装一个本地实例。容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。

f) （仅限容器实例）对于**资源类型 (Resource Type)**，请从下拉列表中选择一个资源配置文件。

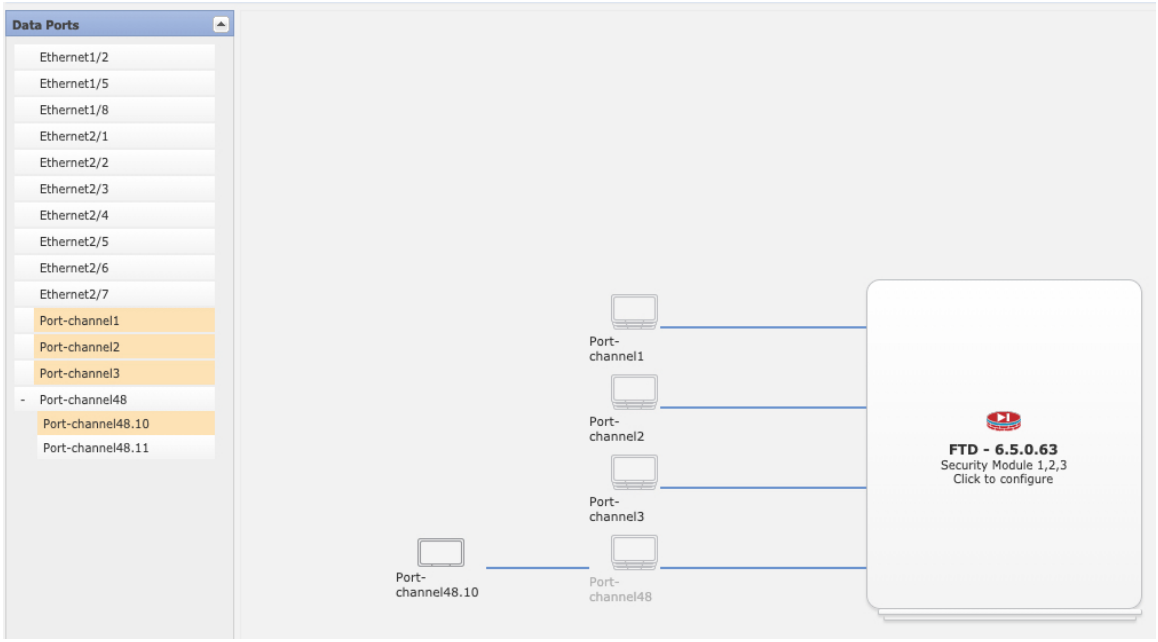
对于 Firepower 9300，此配置文件将应用于每个安全模块上的每个实例。例如，如果您使用的是不同的安全模块类型，并且想要在更低端型号上使用更多 CPU 时，可以稍后在此过程中为每个安全模块设置不同的配置文件。建议您在创建集群之前选择正确的配置文件。如果您需要创建新配置文件，请取消集群创建操作，然后使用 为容器实例添加资源配置文件，第 315 页添加一个配置文件。

注释
如果将不同的配置文件分配给已建立的集群中的实例，则允许不匹配的配置文件，则首先在数据节点上应用新的配置文件；重新启动并恢复后，您可以将新的配置文件应用于控制节点。

g) 点击**确定**。

屏幕会显示调配 - 设备名称窗口。

步骤 4 选择要分配给此集群的接口。



对于本地模式集群：默认情况下会分配所有有效接口。 如果定义了多个集群类型接口，请取消选中除一个接口外的所有接口。

对于多实例集群：选择要分配到集群的每个数据接口，并选择集群类型端口-通道或端口-通道子接口。

步骤 5 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 6 在**集群信息 (Cluster Information)** 页面上，完成以下操作。

图 *238:* 本地集群

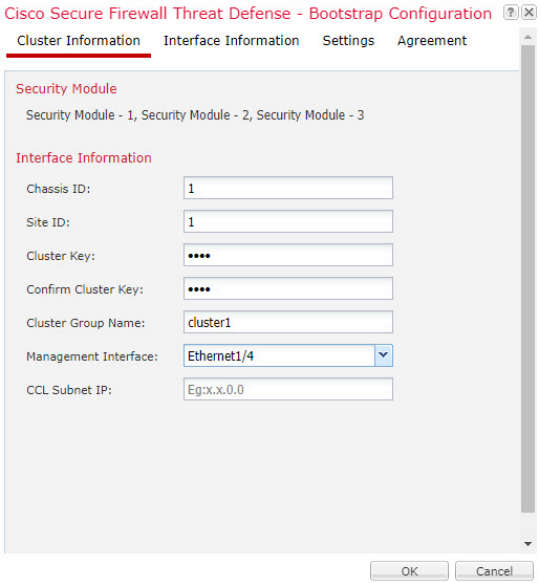
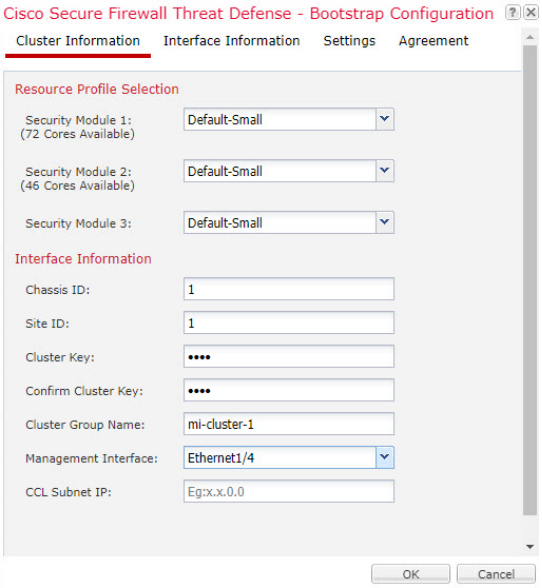


图 *239:* 多实例集群



a) （仅适用于 Firepower 9300 的容器实例）在**安全模块 (SM) 和资源配置文件选择 (Security Module (SM) and Resource Profile Selection)** 区域中，例如，如果您使用的是不同的安全模块类型，并且想要在更低端型号上使用更多 CPU 时，可以为每个模块设置不同的资源配置文件。

b) 对于多机箱集群，在 **机箱 ID** 中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

仅当向集群控制链路端口通道 48 添加成员接口时，才会显示此字段。

c) 对于站点间集群，在**站点 ID (Site ID)** 字段中输入此机箱的站点 ID（1 和 8 之间的整数）。FlexConfig 功能。仅可通过使用 防火墙管理中心 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。

d) 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

e) 设置**集群组名称**，即逻辑设备配置中的集群组名称。

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

重要事项
从版本 2.4.1 开始，集群组名称中的空格将被视为特殊字符，并且在部署逻辑设备时可能会导致错误。为避免此问题，必须重命名集群组名称并不能带有空格。

f) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

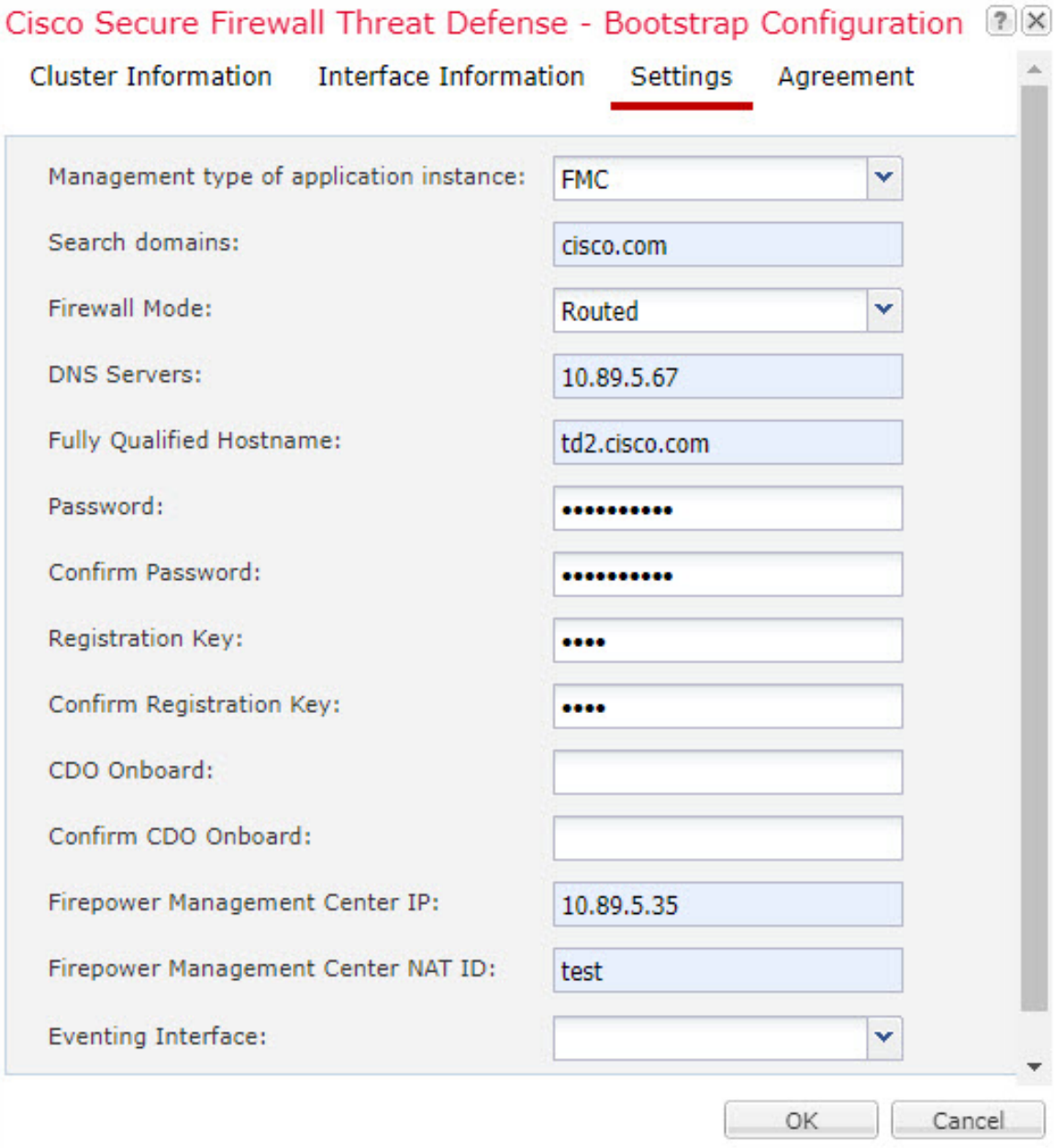
如果您分配一个支持硬件旁路功能的接口作为管理接口，则会收到一条警告消息，确认您是故意这样分配。

g) （可选） 将 **CCL 子网 IP** 设为 ***a.b*.0.0**。

默认情况下， 集群控制链路使用 127.2.0.0/16 网络。但是，某些网络部署不允许 127.2.0.0/16 流量通过。在这种情况下，请对集群指定唯一网络上的任意 /16 网络地址，环回 (127.0.0.0/8)、组播 (224.0.0.0/4) 和内部 (169.254.0.0/16) 地址除外。如果将该值设置为 0.0.0.0，则系统会使用默认网络。

机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：*a.b.chassis_id.slot_id*。

步骤 7 在**设置 (Settings)** 页面上，执行以下操作。



a) 在 **注册密钥** 字段中，输入注册期间 防火墙管理中心 与集群成员之间要共享的密钥。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加防火墙威胁防御时，需要在防火墙管理中心上输入相同的密钥。

b) 输入供防火墙威胁防御管理员用户用于 CLI 访问的**密码**。

c) 在 **Firepower 管理中心 IP** 字段中，输入执行管理 防火墙管理中心的 IP 地址。如果您不知道防火墙管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中输入口令。

d) （可选） 对于容器实例，选择**是否允许 FTD SSH 会话专家模式：是** 或**否**。专家模式提供 防火墙威胁防御 shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择**是**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否**以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 防火墙威胁防御 CLI 中使用 **expert** 命令。

e) （可选） 在**搜索域 (Search Domains)** 字段中，输入管理网络的搜索域逗号分隔列表。

f) （可选） 从**防火墙模式**下拉列表中选择**透明**或**路由**。

在路由模式中，防火墙威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

g) （可选） 在 **DNS 服务器 (DNS Servers)** 字段中，输入用逗号分隔的 DNS 服务器列表。

例如，如果指定 防火墙管理中心 主机名，则 防火墙威胁防御 使用 DNS。

h) （可选） 在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中，输入在添加集群作为新设备时还将在 防火墙管理中心 上输入的口令。

通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同一个注册密钥）：防火墙管理中心指定设备 IP 地址，设备指定 防火墙管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。您可以将长度介于 1 到 37 个字符之间的任意文本字符串指定为 NAT ID。防火墙管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

i) （可选） 在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入 防火墙威胁防御设备的完全限定名称。

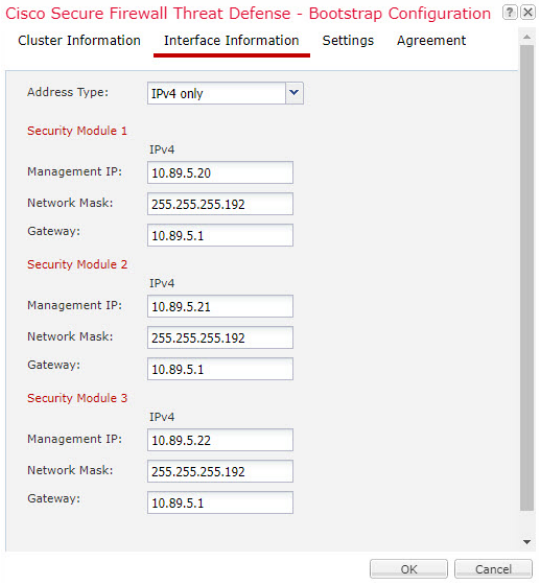
有效字符是从 a 到 z 的字母、从 0 到 9 的数字、点 (.) 和连字符(-)；最大字符数为 253。

j) （可选） 从 **事件接口** 下拉列表中，选择发送事件时应当使用的接口。如果未指定，系统将使用管理接口。

要指定发送事件所用的独立接口，必须将接口配置为 *firepower-eventing* 接口。如果您分配一个支持硬件旁路功能的接口作为事件接口，则会收到一条警告消息，以确认您是故意这样分配的。

步骤 8 在**接口信息 (Interface Information)** 页面上，为集群中的每个安全模块配置一个管理 IP 地址。从**地址类型 (Address Type)** 下拉列表中选择地址类型，然后为每个安全模块填写以下字段。

注释
您必须为机箱中全部 3 个模块插槽设置 IP 地址，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。



a) 在**管理 IP (Management IP)** 字段中，配置 IP 地址。

在同一网络上为每个模块指定唯一 IP 地址。

b) 输入**网络掩码**或**前缀长度**。

c) 输入**网络网关**地址。

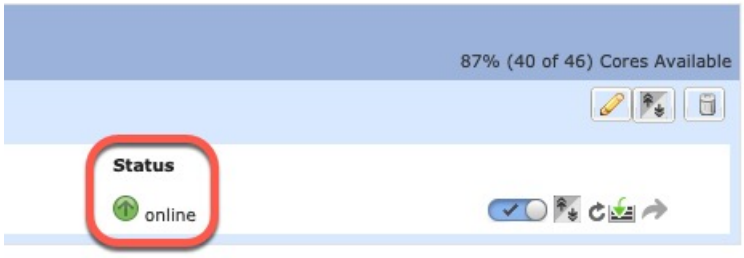
步骤 9 在**协议**选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 10 点击**确定 (OK)** 关闭配置对话框。

步骤 11 点击**保存 (Save)**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其**状态**显示为**在线**时，您可以添加剩余的集群机箱；对于一个 Firepower 9300 机箱内集群，则可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。





步骤 12 对于多机箱集群，将下一个机箱添加到集群中：

a) 在第一个 防火墙机箱管理器机箱上，点击右上角的 **显示配置图标** ，复制显示的集群配置

b) 连接到下一个机箱上的 防火墙机箱管理器，然后按照此程序添加逻辑设备。

c) 选择**我想要：(I want to:) > 加入现有集群 (Join an Existing Cluster)**。

d) 点击**确定**。

e) 在**复制集群详细信息**对话框中，粘贴第一个机箱的集群配置，然后点击**确定**。

f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

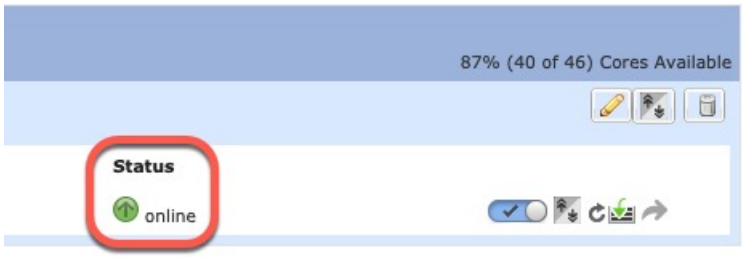
- **机箱 ID** - 输入唯一的机箱 ID。
- **站点 ID** - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。仅可通过使用 防火墙管理中心 FlexConfig 功能，来配置用于增强冗余性和稳定性的其他站点间集群自定义项目，例如导向器本地化、站点冗余和集群流移动性。
- **集群密钥** -（未预填充）输入相同的集群密钥。
- **管理 IP** - 将每个模块的管理地址更改为与其他集群成员位于同一网络中的唯一 IP 地址。

点击**确定**。

g) 点击**保存 (Save)**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在每个集群成员的**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当每个集群成员的逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。





步骤 13 使用管理 IP 地址将控制设备添加到 防火墙管理中心。

所有集群设备必须位于 FXOS 上成功建立的集群中，才能将它们添加到 防火墙管理中心。

然后，防火墙管理中心 会自动检测数据设备。

添加更多集群节点

在现有集群中添加或替换 防火墙威胁防御 集群节点。 在 FXOS 中添加新的集群节点时， 防火墙管理中心 会自动添加该节点。

注释 此程序中的 FXOS 步骤仅适用于添加新机箱；如果将新模块添加或替换到已启用群集的 Firepower 9300，则该模块将自动添加。

开始之前

- 如果是替换，则必须从 防火墙管理中心中删除旧的集群节点。当您将其替换为一台新节点时，它将被视为 防火墙管理中心上的一个新设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

过程

步骤 1 如果之前使用 防火墙管理中心升级了 防火墙威胁防御 映像，请在集群中 的每个机箱上执行以下步骤。

当您从 防火墙管理中心升级时，FXOS 配置中的启动版本未更新，并且机箱上未安装独立软件包。这两个项目都需要手动设置，以便新节点可以使用正确的映像版本加入集群。

注释
如果仅应用了补丁版本，则可以跳过此步骤。Cisco 不为补丁提供独立软件包。

a) 使用 **系统** > **更新** 页面在机箱上安装运行 防火墙威胁防御 映像。
b) 点击 **逻辑设备** ，然后点击 设置版本图标（）。对于具有多个模块的 Firepower 9300，请设置每个模块的版本。

启动版本 显示您部署时使用的原始软件包。**当前版本** 显示升级到的版本。

c) 在 **新版本** 下拉菜单中，选择您上传的版本。此版本应与显示的 **当前版本** 匹配，并将启动版本设置为与新版本匹配。
d) 在新机箱上，确保安装了新映像包。

步骤 2 在现有集群机箱 防火墙机箱管理器上，点击 **逻辑设备**。

步骤 3 点击右上角的**显示配置图标**；复制显示的集群配置。

步骤 4 连接到新机箱上的 防火墙机箱管理器 ，然后点击 **添加** > **群集**。

步骤 5 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

步骤 6 点击**确定**。

步骤 7 在**复制集群详细信息**对话框中，粘贴第一个机箱的集群配置，然后点击**确定**。

步骤 8 点击屏幕中心的设备图标。集群信息已部分预填充，但您必须填写以下设置：

图 *240:* 集群信息

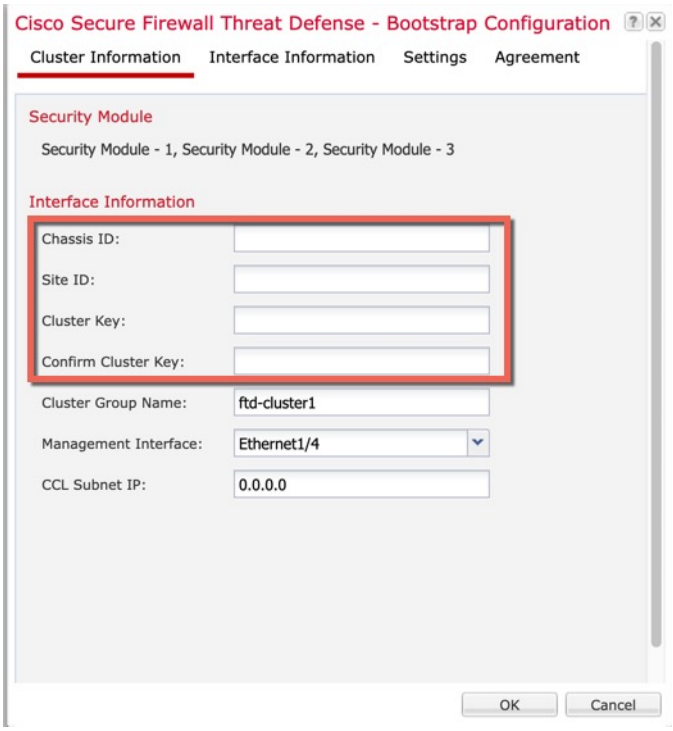


图 *241:* 接口信息

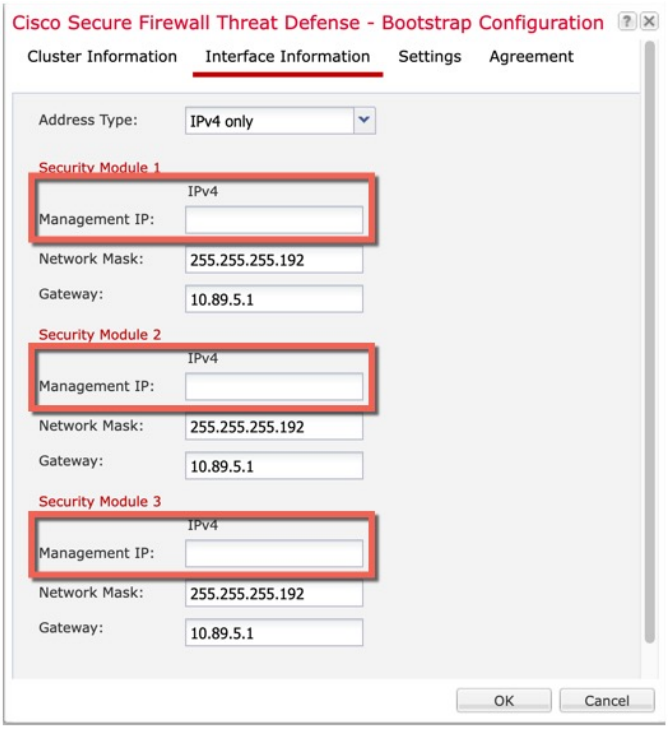
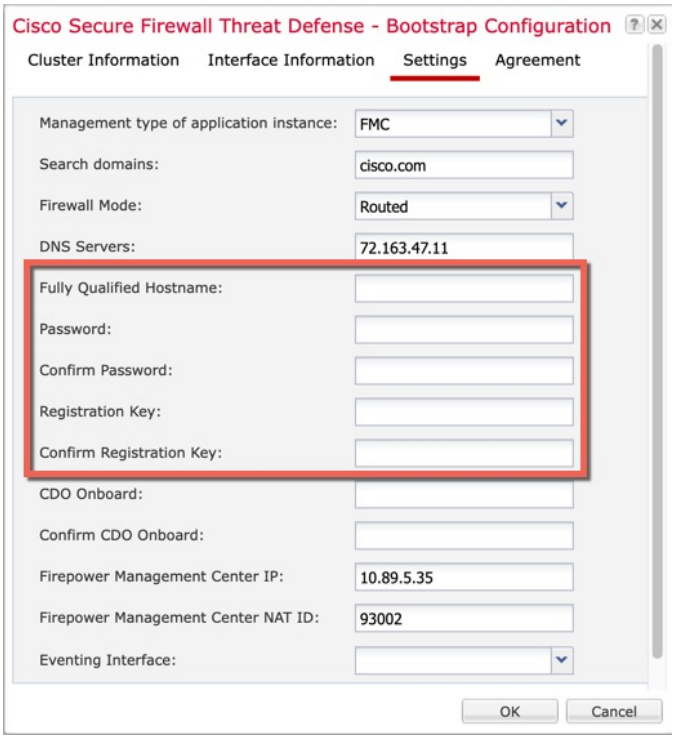


图 *242:* 设置

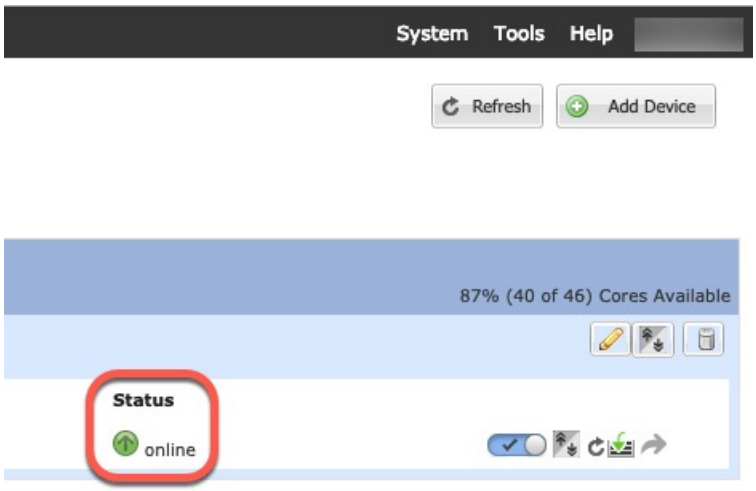


- **机箱 ID**-输入 唯一 机箱 ID。
- **站点 ID** - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。此功能仅可使用 防火墙管理中心 FlexConfig 功能进行配置。
- **集群密钥**-输入 相同 集群密钥。
- **管理 IP**-将每个模块的管理地址更改为与其他集群成员位于同一网络中的 唯一 IP 地址。
- **完全限定主机名**-使用 相同 主机名。
- **密码**-输入 相同 密码。
- **注册密钥**-输入 相同 注册密钥。

点击**确定**。

步骤 9 点击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在每个集群成员的**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当每个集群成员的逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置集群。您可能会在此过程中看到“安全模块未响应”状态；此状态为正常状态，并且是临时的。



防火墙管理中心：添加集群

将集群设备之一作为新设备添加到 Secure Firewall Management Center；防火墙管理中心 会自动检测所有其他集群成员。

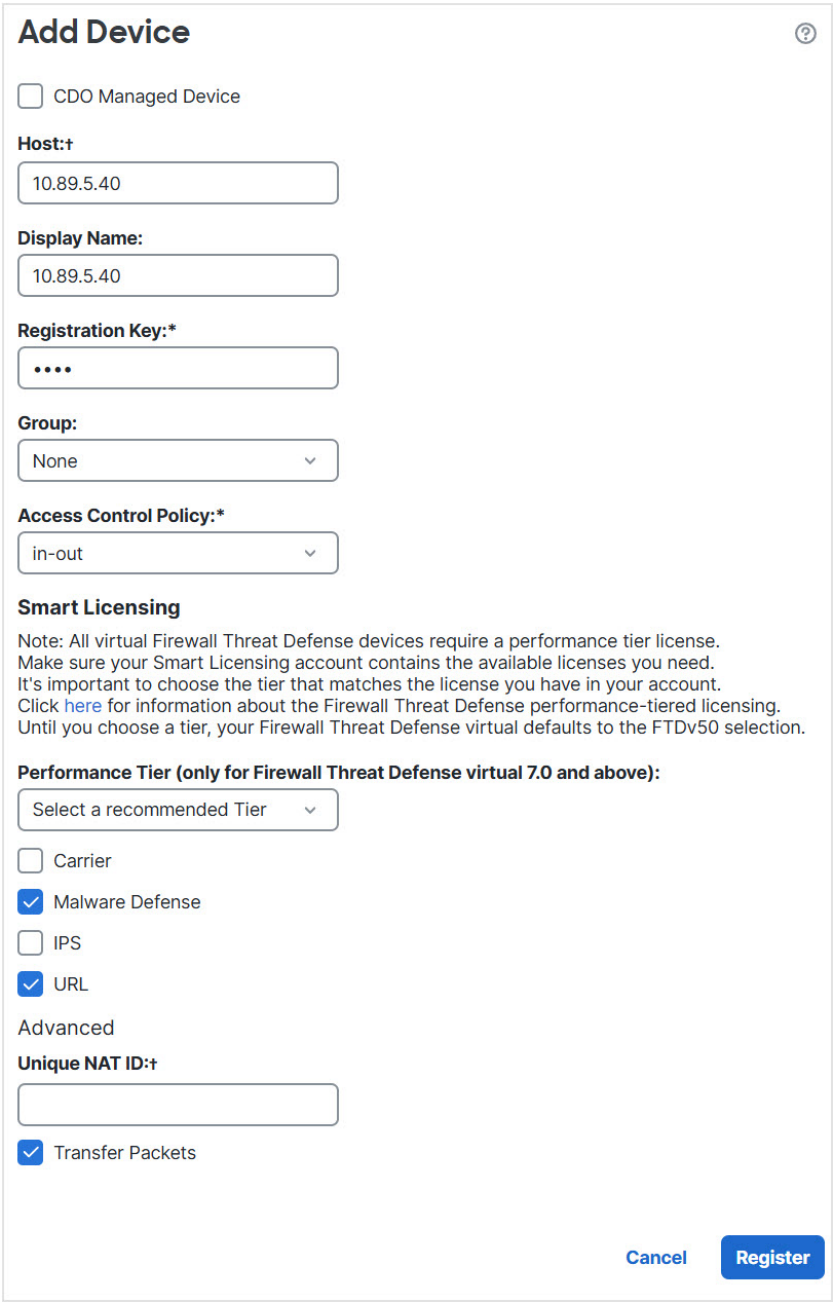
开始之前

- 所有集群设备必须位于 FXOS 上成功建立的集群中，才能将集群添加到 防火墙管理中心。还应检查哪个是控制单元。请参阅防火墙机箱管理器 **逻辑设备 (Logical Devices)** 屏幕或使用 Firewall Threat Defense **show cluster info** 命令。

过程

步骤 1 在防火墙管理中心中，选择**设备** > **设备管理**，然后选择**添加** > **添加设备**，使用部署集群时分配的控制单元管理 IP 地址添加该控制单元。

图 *243:* 添加设备



a) 在 **主机** 字段中，输入控制单元的 IP 地址或主机名。

虽然您可以添加任何集群单元，但我们建议添加控制单元备以获得最佳性能。

如果在设备设置期间使用了 NAT ID，则可能不需要输入此字段。有关详细信息，请参阅NAT 环境，第 7 页。

b) 在 **显示名称** 字段中，输入要在 防火墙管理中心中显示的控制单元名称。

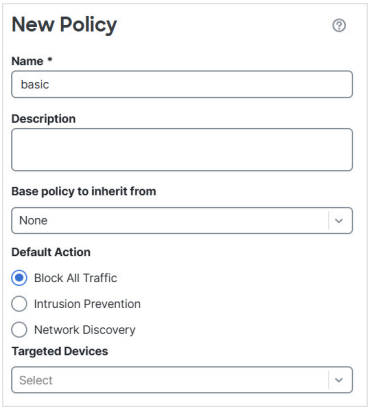
此显示名称不适用于集群；它仅适用于要添加的控制单元。您可以稍后更改其他集群成员的名称和集群显示名称。

c) 在 **注册密钥** 字段中，输入在 FXOS 中部署集群时所使用的同一注册密钥。注册密钥是一个一次性的共享密钥。

d) （可选） 将设备添加到设备 **组**。

e) 选择初始**访问控制策略**以在注册时部署到设备，或创建一个新策略。

如果创建新策略，则仅创建基本策略。您可以稍后根据需要自定义策略。



f) 选择要应用到设备的许可证。

g) 如果在设备安装过程中使用了 NAT ID，请展开**高级**部分，并在**唯一 NAT ID** 字段中输入相同的 NAT ID。

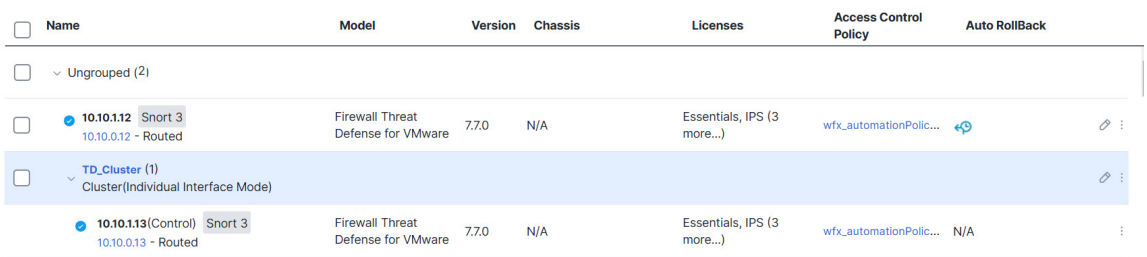
h) 选中**传输数据包**复选框以允许设备将数据包传输到 防火墙管理中心。

默认情况下，此选项已启用。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 防火墙管理中心进行检测。如果禁用此选项，则仅发送事件信息到 防火墙管理中心，不发送数据包数据。

i) 点击**注册 (Register)**。

防火墙管理中心 会识别并注册控制单元，接着注册所有数据单元。如果控制单元未注册成功，则不会添加集群。如果集群未在机箱上运行或存在其他连接问题，则注册会失败。在这种情况下，我们建议尝试重新添加集群设备。

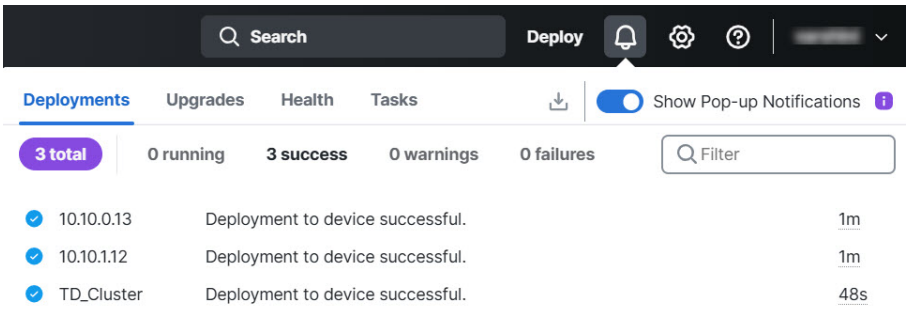
集群名称显示在 **设备** > **设备管理** 页面上；展开集群可查看集群单元。



当前正在注册的设备会显示加载图标。



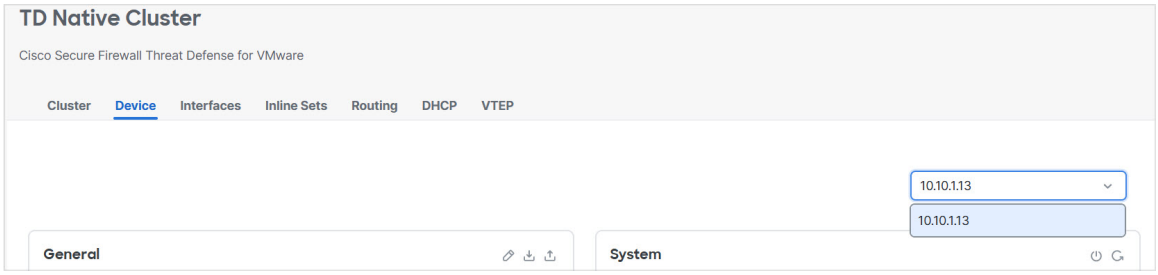
您可以通过点击**通知**图标并选择**任务**来监控集群设备的注册情况。防火墙管理中心会在每个设备注册时更新“集群注册”任务。如有任何设备无法注册，请参阅调整集群成员，第 682 页。



步骤 2 通过点击集群的 **编辑** (✎)，配置设备特定设置。

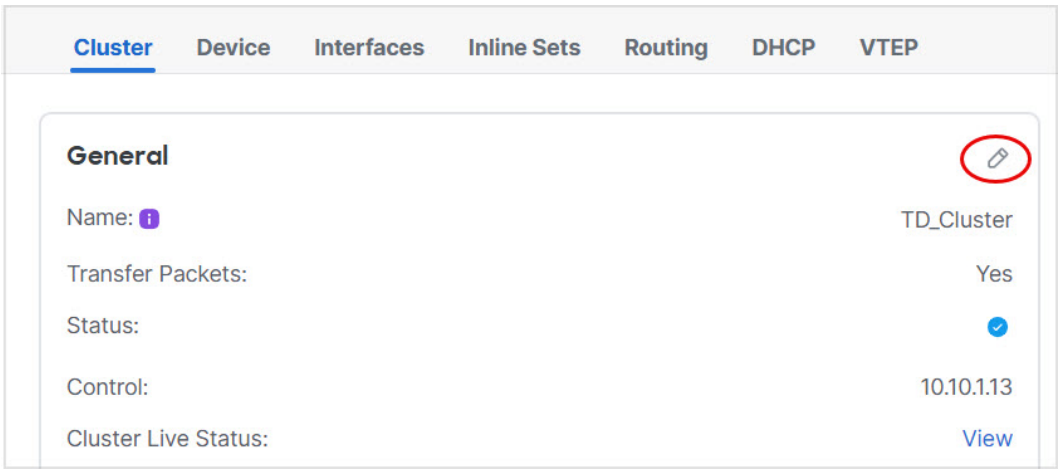
大多数配置可以应用于整个集群，而不适用于集群中的成员设备。例如，可以更改每台设备的显示名称，但只能配置整个集群的接口。

步骤 3 在 **设备** > **设备管理** 上选择**添加**、**集群**屏幕，可以查看**常规**、**许可证**、**系统**和**运行状况**设置。

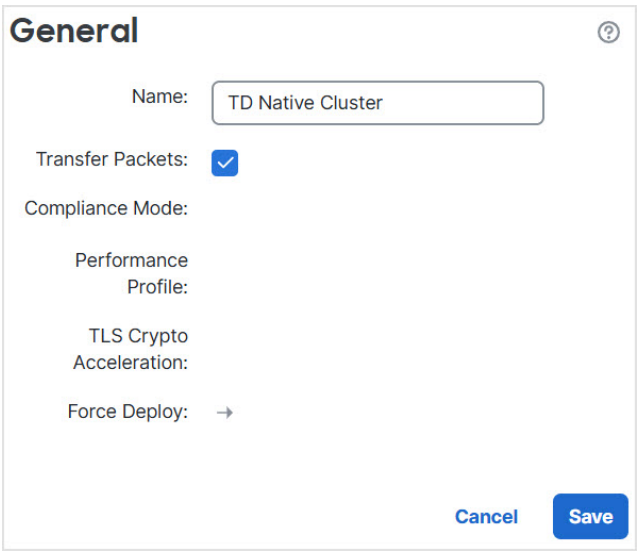


请参阅以下集群特定项：

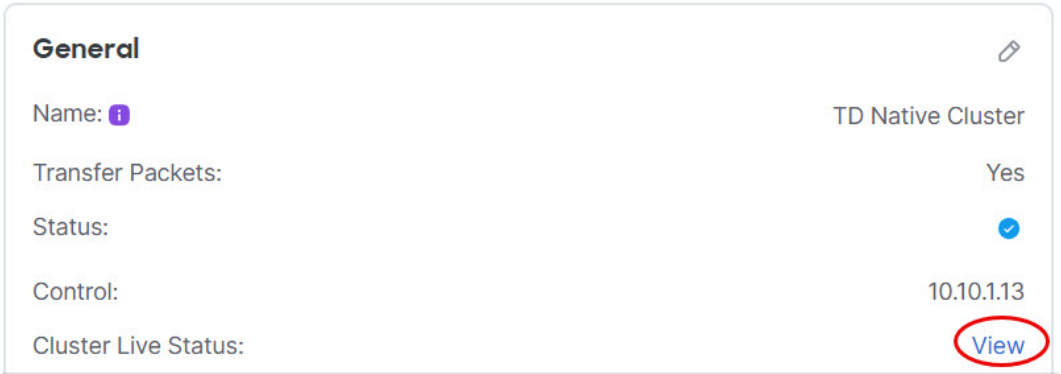
- **常规 (General)** > **名称 (Name)** - 通过点击 **编辑** (✎)更改集群显示名称。



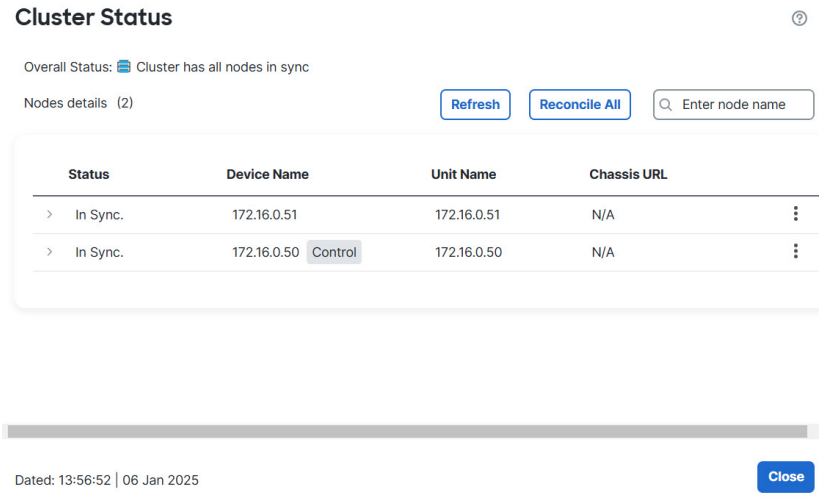
然后设置 **名称** 字段。



- **常规 (General)** > **查看集群状态 (View cluster status)** - 点击 **查看集群状态 (View cluster status)** 链接来打开**集群状态 (Cluster Status)** 对话框。

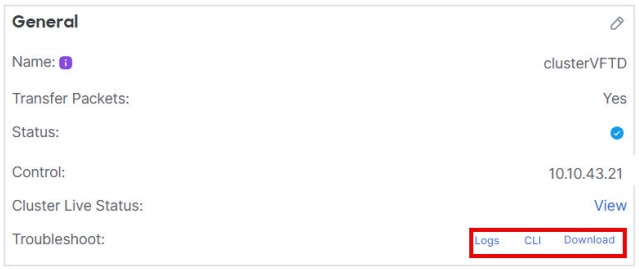


还可在**集群状态 (Cluster Status)** 对话框中点击**协调 (Reconcile)** 以重新注册数据单元。



- **常规 > 故障排除**- 可以生成和下载故障排除日志，还可以查看集群 CLI。请参阅防火墙管理中心：对集群进行故障排除，第 687 页。

  图 ***244:*** 故障排除



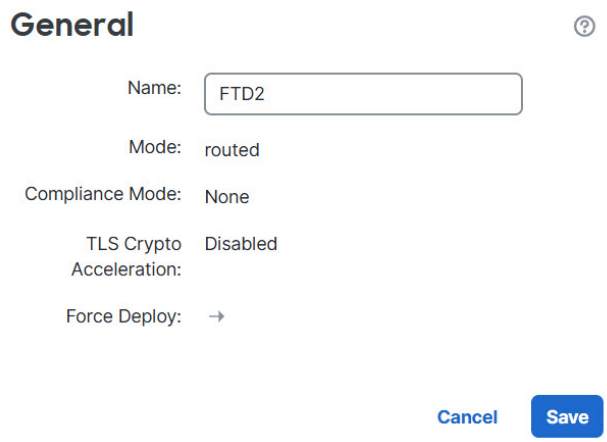
- **许可证** - 点击 **编辑** (✎) 可设置许可证授权。

步骤 4 在 **设备** > **设备管理** 上选择**添加**、**设备**，您可从右上方的下拉菜单中选择集群中的每个成员并配置以下设置。

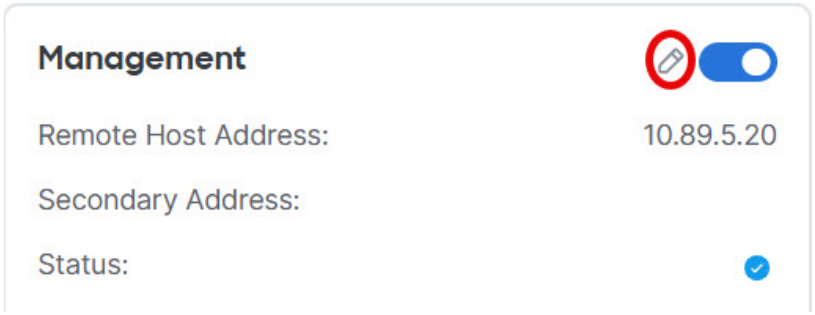
- **常规 (General) > 名称 (Name)** - 通过点击 **编辑** (✎)更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理 > 主机**-如果在设备配置中更改了管理 IP 地址，则必须在 防火墙管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备；编辑 **管理** 区域中的 **主机** 地址。



防火墙管理中心：配置集群、数据 接口

此程序配置您在 FXOS 中部署集群时为其分配的每个数据接口的基本参数。对于多机箱集群，数据接口始终是跨区以太网通道接口。对于与一个 Firepower 9300 机箱内的安全模块隔离的集群控制链路接口，必须将 MTU 从默认值增加。

注释 将跨网络 EtherChannel 用于多机箱集群时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的设备。

过程

步骤 1 选择 **设备** > **设备管理**，然后点击集群的 **编辑** (✎)。

步骤 2 点击**接口 (Interfaces)**。

步骤 3 配置群集控制链路。

对于多机箱集群，将集群控制链路 MTU 设置为比数据接口的最高 MTU 至少高 100 字节。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。我们建议将 MTU 设置为最大 9184；最小值为 1400 个字节。例如，由于最大 MTU 为 9184，因此最高的数据接口 MTU 可以是 9084，而群集控制链路则可以设置为 9184。

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。

对于本地集群：默认情况下，集群控制链路接口为端口通道48。如果您不知道哪个接口是集群控制链路，请为分配给集群的集群类型接口检查机箱的 FXOS 配置。

a) 点击 **编辑** (✎) 以打开集群控制链路接口。
b) 在 **常规** 页面的 **MTU** 字段中，输入1400 和 9184 之间但排除 2561 和 8362 之间的值。由于块池处理，此 MTU 大小不是系统运行的最佳值。我们建议使用最大值 9184。
c) 点击**确定**。

步骤 4 配置数据接口。

a) （可选） 对于常规防火墙接口，请在数据接口上配置 VLAN 子接口。本程序的其余部分适用于子接口。请参阅添加子接口，第 772 页。
b) 点击数据接口的 **编辑** (✎) 。
c) 配置名称和其他参数。 对于常规防火墙接口，请参阅配置路由模式接口，第 792 页；对于透明模式，请参阅配置网桥组接口，第 797 页。对于仅 IPS 接口，请参阅内联集和被动接口，第 833 页。。

   注释
   如果集群控制链路接口 MTU 不比数据接口 MTU 高出至少 100 个字节，您将看到必须降低数据接口 MTU 的错误。请参阅 步骤 3，第 670 页 以增加集群控制链路 MTU，之后您可以继续配置数据接口。

d) 对于多机箱集群，请为 EtherChannel 设置唯一的手动全局 MAC 地址。点击 **高级**， 在 **主用 Mac 地址** 字段，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

   例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

   请勿设置 **备用 Mac 地址**；它会被忽略。

   您必须为跨 EtherChannel 配置网络中当前未使用的唯一 MAC 地址，以避免潜在的网络连接问题。如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的 MAC 地址用于该接口，而这可能导致临时网络故障。

e) 点击**确定**。对其他数据接口重复上述步骤。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

防火墙管理中心：配置集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 ***245:*** 集群运行状况监控设置

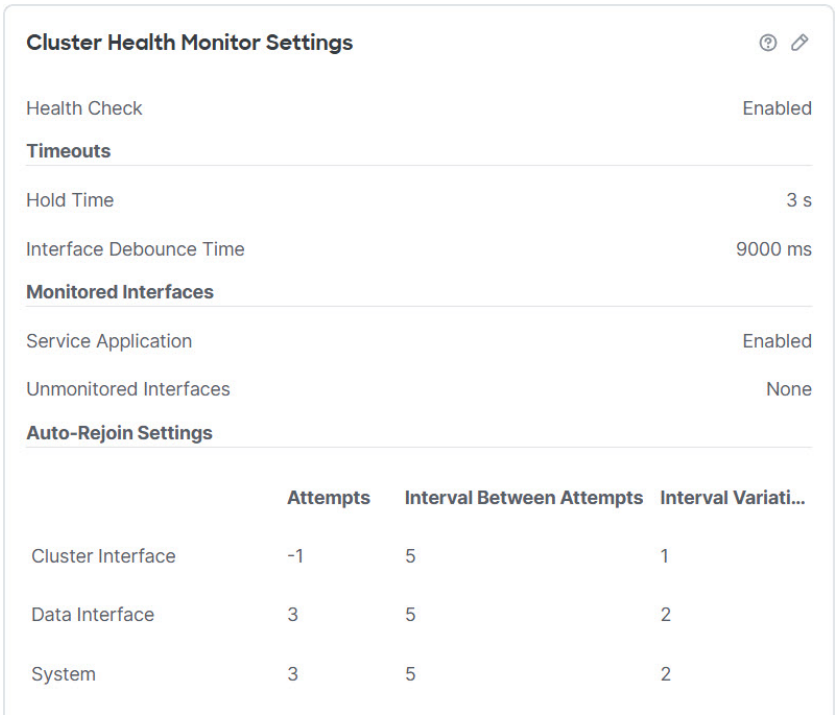


表 ***49:*** 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。

字段	说明
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。

注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

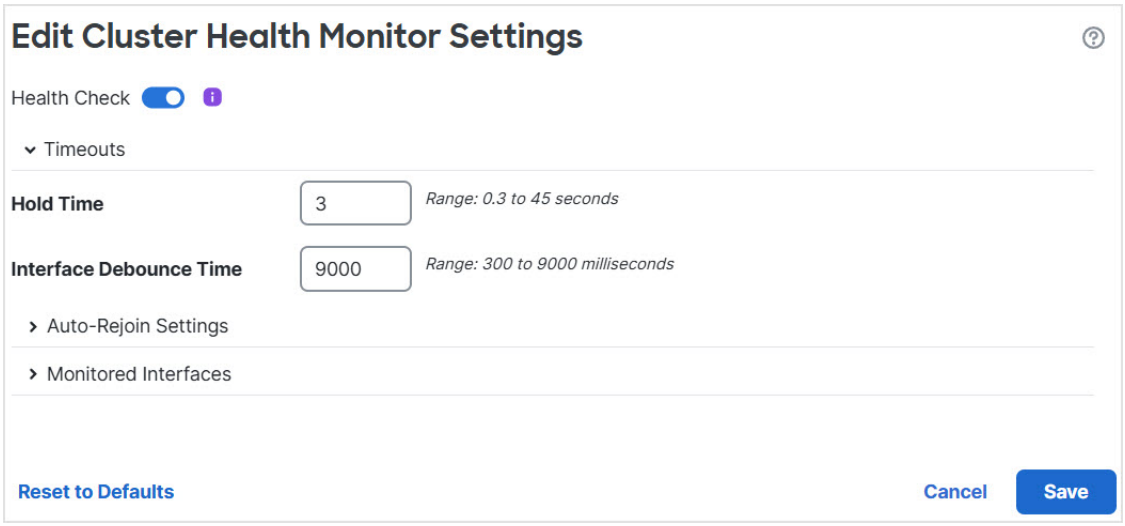
步骤 2 在要修改的集群旁边，点击 **编辑** (✎)。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** (✎)。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *246:* 禁用系统运行状况检查



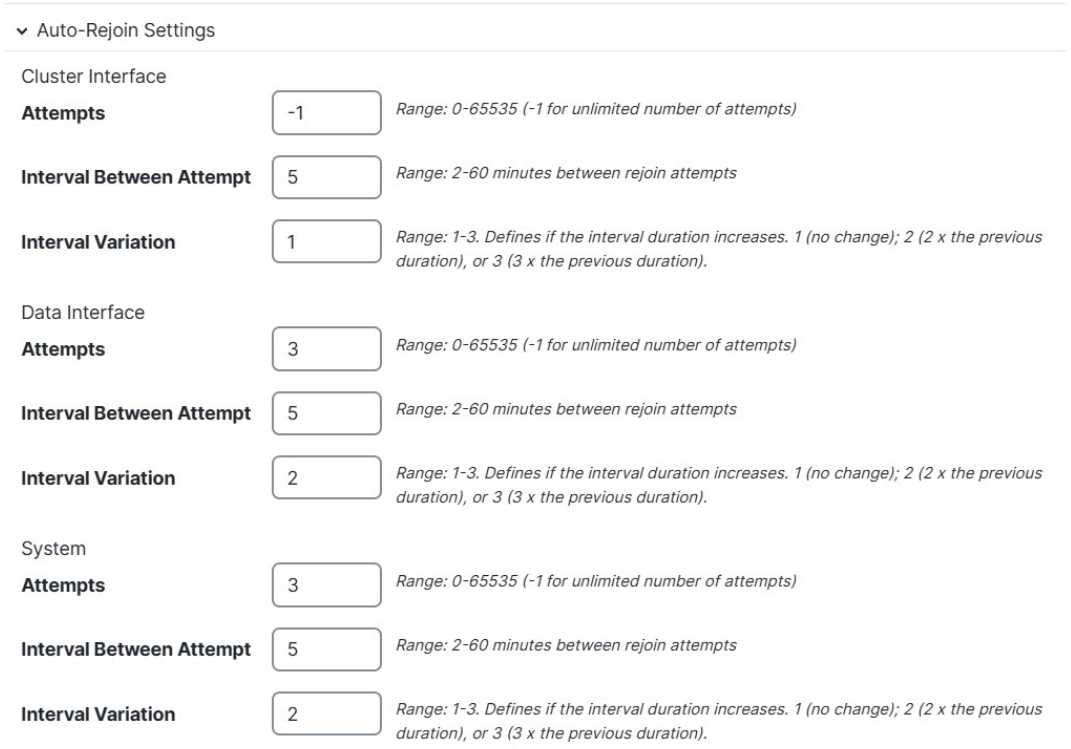
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *247:* 配置自动重新加入设置

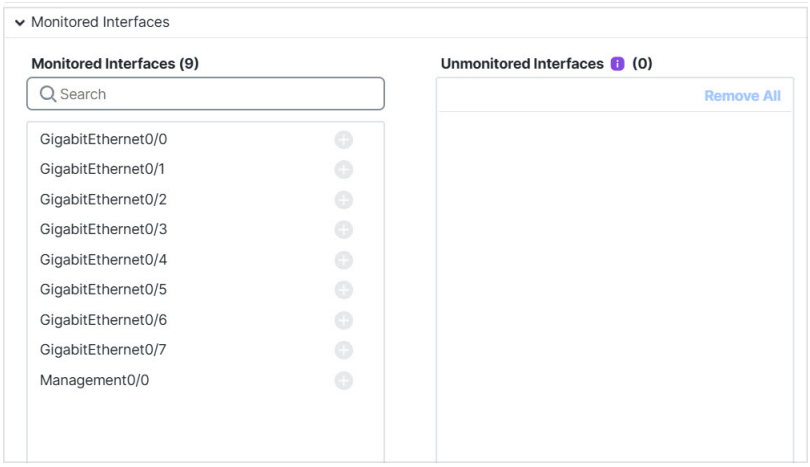


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *248:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改，第 180 页。

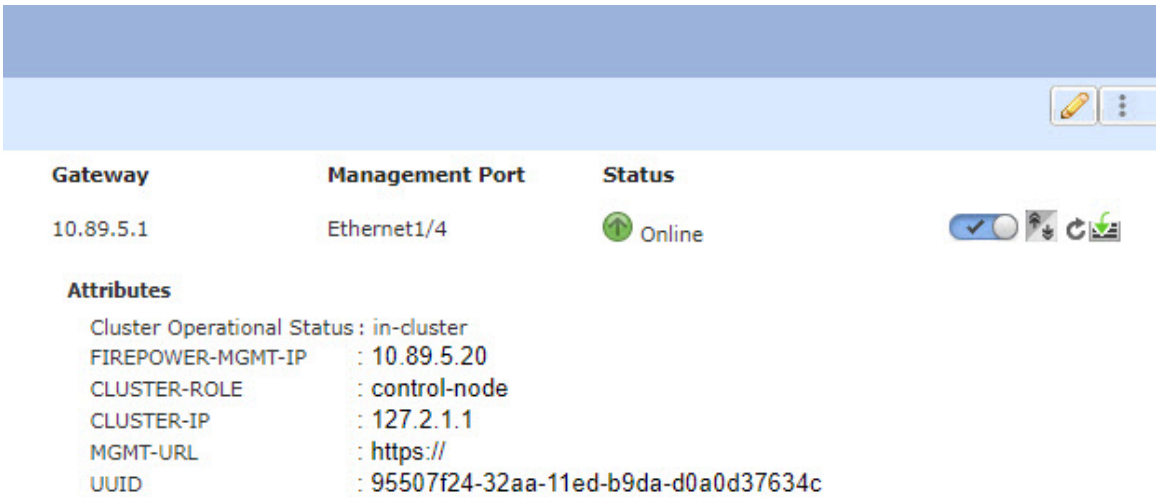
FXOS：删除集群设备

以下部分介绍如何临时或永久删除集群中的节点。

临时删除

例如，出现硬件或网络故障时，集群节点会自动从集群中删除。此删除是临时的，故障消除后，它们可以重新加入集群。您也可以手动禁用集群。

要检查设备当前是否在集群中，登录 防火墙机箱管理器 **逻辑设备**页面查看集群状态：



对于使用 防火墙管理中心 的Firewall Threat Defense，应该将设备留在防火墙管理中心 设备列表中，以便在重新启用集群后，它可以恢复全部功能。

- 在应用中禁用集群 - 您可以使用应用 CLI 禁用集群。输入 **cluster remove unit** 名称 命令删除除您登录的设备以外的所有节点。引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

  当设备处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从引导程序配置接收的IP地址。但如果您重新加载，而节点仍在集群中处于非主用状态，管理接口将被禁用。

  要重新启用集群，请在 Firewall Threat Defense 上输入 **cluster enable**。

- 禁用应用实例 -在 防火墙机箱管理器 的 **逻辑设备** 页面，点击 **滑块已启用**（ ）。您可以稍后使用 **滑块已禁用**（ ） 重新启用它。

- 关闭 安全模块/引擎 - 在 防火墙机箱管理器 的**安全模块/引擎**页面，点击**关闭电源图标**。

- 关闭机箱 -在 防火墙机箱管理器 的 **“概述”** 页面，点击 **关机图标**。

永久删除

您可以使用以下方法永久删除集群节点。

对于使用 防火墙管理中心 的 Firewall Threat Defense，确保在机箱上禁用集群后，从 防火墙管理中心 设备列表删除节点。

- 删除逻辑设备 -在 防火墙机箱管理器 的 **“逻辑设备”** 页面，点击 **删除**（ ）。然后，您可以部署独立的逻辑设备、新的集群，还可以在同一集群中添加新的逻辑设备。

- 从服务中删除机箱或安全模块 - 如果从服务中删除设备，则可以将替换硬件添加为集群的新节点。

FMC：管理群集成员

部署集群后，您可以更改配置和管理集群成员。

添加新的集群成员

在 FXOS 中添加新的集群成员时，Secure Firewall Management Center会自动添加该成员。

开始之前

- 请确保其他机箱的替换设备上的接口配置相同。

过程

步骤 1 在 FXOS 中将新设备添加到集群。请参阅《FXOS 配置指南》。

等待新设备添加到集群。请参阅 防火墙机箱管理器 **逻辑设备**屏幕或使用 Firewall Threat Defense **show cluster info** 命令查看集群状态。

步骤 2 新集群成员将自动添加。要监控替换设备的注册情况，请查看以下信息：

- **集群状态**对话框（可通过 **设备** > **设备管理**、**更多** (⋮) 图标或从 **设备** > **设备管理** 选择**添加**、**集群**选项卡**常规**区域**集群实时状态**链接查看）— 在机箱上正在加入集群的设备会显示“正在加入集群...” 设备加入集群后，防火墙管理中心 会尝试注册该设备，状态会更改为“可供注册”。完成注册后，状态会更改为“正在同步”。如果注册失败，设备将停留在“可供注册”状态。此时，通过点击**协调**可强制重新注册。
- 系统状态 **任务** - 防火墙管理中心 显示所有注册事件和失败情况。
- **设备** > **设备管理**，然后选择**添加** **设备** — 展开设备列表页面上的集群时，可以看到左侧显示加载图标的设备正在进行注册。

替换集群成员

您可以替换现有集群中的集群成员。防火墙管理中心会自动检测替换设备。但是，您必须在 防火墙管理中心中手动删除旧集群成员。此程序也适用于已重新初始化的设备；此时，虽然硬件未发生变动，但会显示为新成员。

开始之前

- 请确保其他机箱的替换设备上的接口配置相同。

过程

步骤 1 如果可能的话，对于新机箱，请在 FXOS 中从旧机箱备份配置并予以恢复。

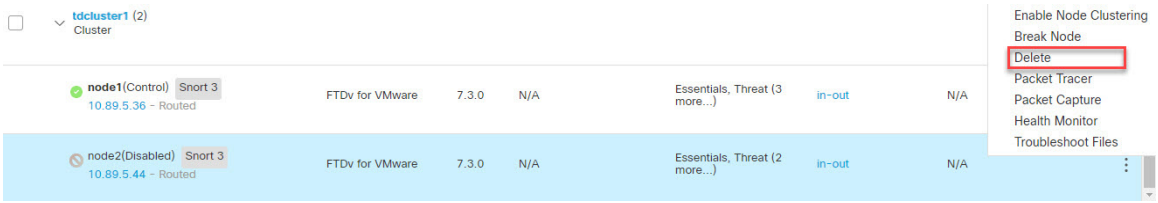
如要更换 Firepower 9300 中的模块，则无需执行这些步骤。

如果没有旧机箱的 FXOS 备份配置，请首先执行添加新的集群成员，第 677 页中的步骤。

有关以下所有步骤的信息，请参阅《FXOS 配置指南》。

a) 使用配置导出功能导出包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件。
b) 将配置文件导入替换机箱。
c) 接受许可协议。
d) 如有必要，可升级逻辑设备应用实例版本以配合集群其余成员。

步骤 2 在旧设备的 防火墙管理中心 中，选择 **设备** > **设备管理**、**更多** (⋮) > **删除**。



步骤 3 确认要删除该设备。

集群和防火墙管理中心设备列表中将删除该设备。

步骤 4 新的或已重新初始化的集群成员将自动添加。要监控替换设备的注册情况，请查看以下信息：

- **集群状态**对话框（**设备** > **设备管理**、**更多** (⋮) 图标或 **设备** > **设备管理**，然后选择**添加**、**集群**页面、**常规**区域、**集群实时状态**链接）— 机箱上正在加入集群的设备显示“正在加入集群...” 设备加入集群后，防火墙管理中心 会尝试注册该设备，状态会更改为“可供注册”。完成注册后，状态会更改为“正在同步”。如果注册失败，设备将停留在“可供注册”状态。此例中，通过点击 **协调** **所有**可强制重新注册。
- 点击通知，然后点击**任务** — 防火墙管理中心 显示所有注册事件和失败情况。
- **设备** > **设备管理**，然后点击**添加** > **设备**— 展开设备列表页面上的集群时，可以看到左侧显示加载图标的设备正在进行注册。

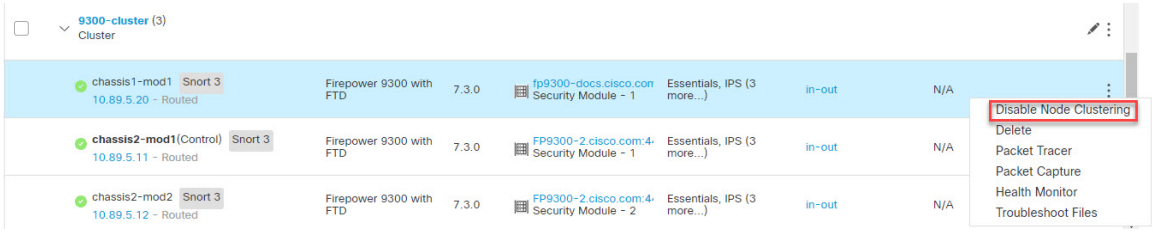
停用成员

您可能需要停用成员，以准备删除设备，或临时进行维护。此程序旨在暂时停用成员；设备仍将显示在 防火墙管理中心 设备列表中。

注释 当单元处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用设备从引导程序配置接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台来进行任何进一步配置。

过程

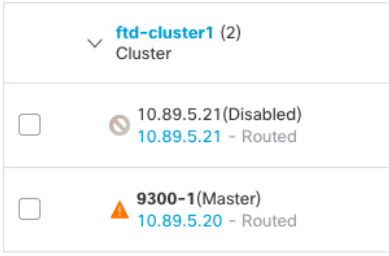
步骤 1 对于要停用的设备，请选择 **设备** > **设备管理**、**更多** (⋮)，然后选择**禁用群集技术**。



您也可以从**集群状态**对话框（**设备** > **设备管理**、**更多** (⋮) 和**集群实时状态**）中停用设备。

步骤 2 确认要在设备上禁用集群。

该设备在 **设备** > **设备管理** 列表中其名称旁边会显示（**已禁用**）。



步骤 3 重新启用集群，请参阅 重新加入集群，第 679 页。

重新加入集群

如果从集群中删除了某个设备（例如对于出现故障的接口），或者如果您手动禁用集群，必须通过访问设备 CLI 。确保故障已解决，再尝试重新加入集群。有关可从集群中删除设备的原因的更多信息，请参阅 重新加入集群，第 698 页。

过程

步骤 1 对于要重新激活的单元，选择 **设备** > **设备管理**、**更多** (⋮) > **启用群集技术**。



您也可以从**集群状态**对话框（**设备** > **设备管理**、**更多** (⋮) > **集群实时状态**）中重新激活设备。

步骤 2 确认要在设备上启用集群。

注销 数据节点

如果需要永久删除集群节点（例如，如果您删除 Firepower 9300上的模块，或删除机箱），应从 防火墙管理中心将其取消注册。

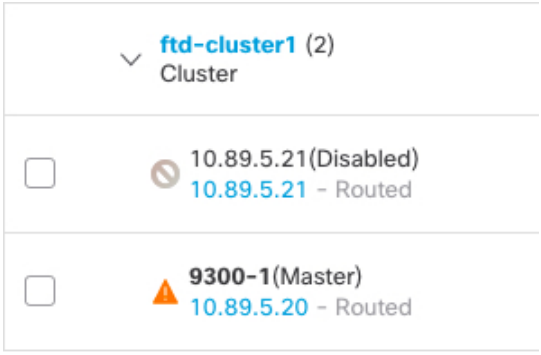
如果该节点仍然是集群的正常运行部分，或者如果您只想临时禁用该成员，请不要删除该节点。要从 FXOS 中的集群中永久删除，请参阅 FXOS：删除集群设备，第 675 页。如果将其从 防火墙管理中心中取消注册，并且它仍然是集群的一部分，它将继续传递流量，甚至可能成为控制节点-防火墙管理中心 不再能够管理的控制节点。

开始之前

要手动停用节点，请参阅 停用成员，第 678 页。在取消注册节点之前，节点必须处于手动或由于运行状况故障而处于非活动状态。

过程

步骤 1 确保准备好从 防火墙管理中心取消注册节点。在 **设备** > **设备管理** 上，确保节点显示（**已禁用**）。



您还可从 **更多** (⋮)的 **集群状态** 对话框中查看每个节点的状态。如果状态过时，请点击 **集群状态** 对话框上的 **协调全部** 进行强制更新。

步骤 2 在要删除的数据节点的 防火墙管理中心 中，选择 **设备** > **设备管理**，然后点击**添加** > **设备更多** (⋮) > **取消注册**。

步骤 3 确认要 取消注册 节点。

从集群和 防火墙管理中心 设备列表中将删除该节点。

变更控制单元

⚠

注意 要更改控制单元，最好的方法是在控制单元上禁用群集，等到新的控制选举后再重新启用群集。如果必须指定要成为控制单元的具体单元，请使用本节中的程序。请注意，对集中功能而言，如果强制更改控制设备，则所有连接都将断开，而您必须在新的控制设备上重新建立连接。

要更改控制单元，请执行以下步骤：

过程

步骤 1 通过选择 **设备** > **设备管理**、**更多** (⋮) > **集群实时状态**打开**集群状态**对话框。

您还可以从 **设备** > **设备管理** 访问**集群状态**对话框，然后选择**添加**、**集群**页面、**常规**区域和**集群实时状态**链接。

步骤 2 对于要成为控制设备的设备，请选择 **更多** (⋮) > **将角色更改为控制**。

步骤 3 系统将提示您确认角色更改。选中复选框，然后点击**确定**。

调整集群成员

如果集群成员注册失败，则可将集群成员身份从机箱协调至 Secure Firewall Management Center。例如，数据单元在 防火墙管理中心 被占用或存在网络问题时注册失败的情况下。

过程

步骤 1 选择集群的 **设备** > **设备管理** **更多** (⋮)，然后选择**集群实时状态**，以打开**集群状态**对话框。

您也可以从**设备** > **设备管理**页面的**常规**区域**集群实时状态**链接打开**集群状态**对话框。

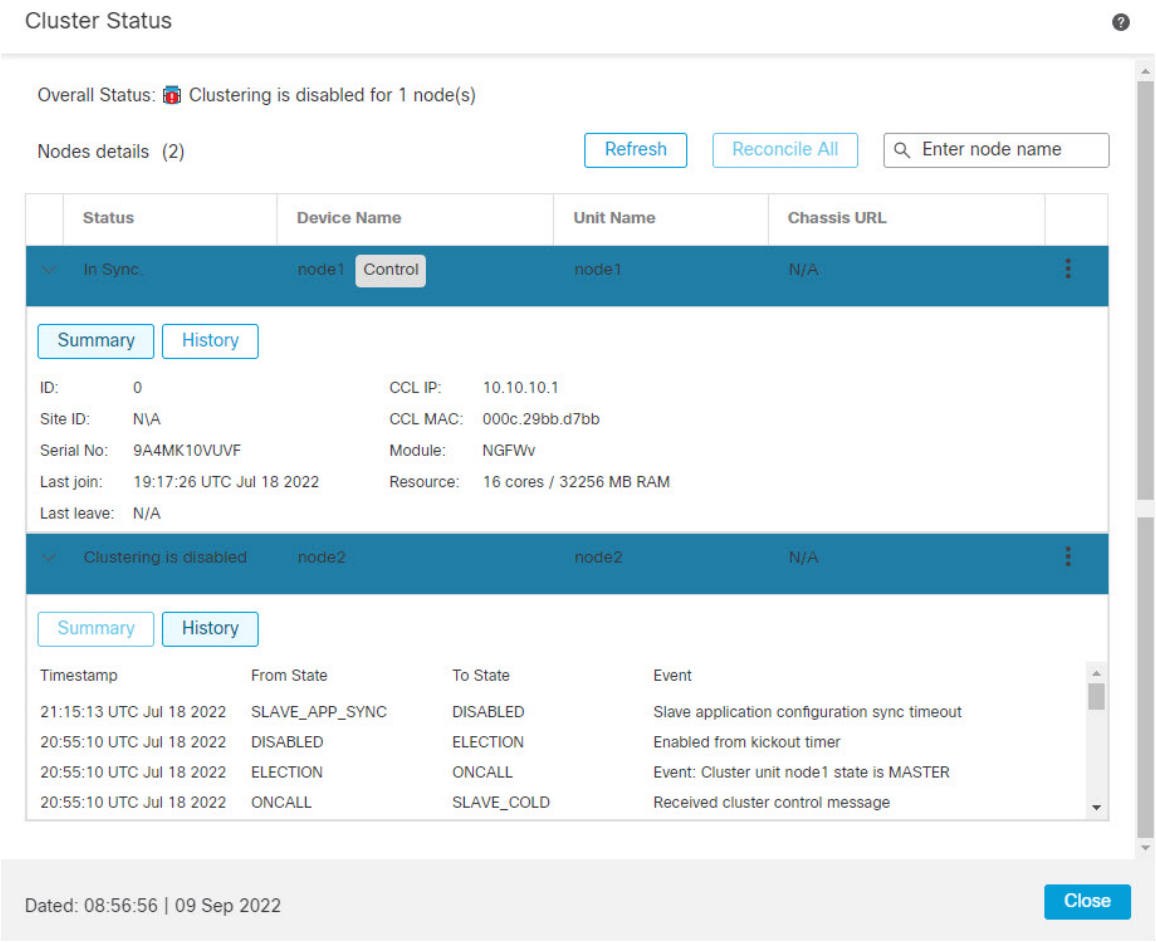
步骤 2 点击 **协调** **所有**。

有关集群状态的详细信息，请参阅防火墙管理中心：监控集群 ，第 682 页。

防火墙管理中心：监控集群

您可以监控 Secure Firewall Management Center 中和 Firewall Threat Defense CLI 上的集群。

- **集群状态**对话框，可通过 **设备** > **设备管理**、**更多** (⋮) 图标或从 **设备** > **设备管理** 然后选择**添加**、**集群**页面、**常规**区域、和**集群实时状态**链接进行访问。



控制单元有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 - 设备已向 防火墙管理中心 注册。
- 待定注册-设备属于集群，但尚未向 防火墙管理中心注册。如果设备注册失败，则可点击 **协调 所有**以重试注册。
- 集群已禁用可供删除-设备已向注册，但是集群的非活动成员。防火墙管理中心如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除设备。
- 正在加入集群... - 设备正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 防火墙管理中心 注册。

对于每台设备，您可以查看 **摘要** 或 **历史记录**。

对于 **更多** (⋮) 菜单中的每台设备，您可以执行以下状态更改：

- **禁用集群**
- **启用集群**

- 将角色更改为控制角色

- 点击通知，然后点击**任务**。

  任务 页面会在每个设备注册时更新“集群注册”任务。

- **设备** > **设备管理** 然后选择**添加设备** *cluster_name*。

  展开设备列表页面上的集群时，可看到所有成员设备，包括 IP 地址旁显示的设备。对于仍在注册的设备，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

集群运行状况监控器控制面板

集群运行状况监控器

当 Firewall Threat Defense 是集群的控制节点时， 防火墙管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加（在公共云集群中，不属于 防火墙管理中心的其他节点）或 正常（节点的理想状态）。
  - 集群统计信息部分显示集群的当前指标，包括 CPU 使用率、内存使用率、输入速率、输出速率、活动连接和 NAT 转换。

注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

  - 指标图表（即 CPU 使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。

- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。

- “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。

- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU使用率、内存使用率、输入速率、输出速率、活动连接和NAT转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从防火墙管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（∨） 以展开和折叠托管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 **添加新的控制面板**（+），通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

集群指标

集群运行状况监控器跟踪与集群及其节点相关的统计信息，以及负载分布、性能和CCL流量统计信息的汇总。

表 *50:* 集群指标

指标	说明	格式
CPU	集群节点上的CPU指标平均值（分别针对数据平面和 snort）。	percentage
Memory	集群节点上的平均内存指标（分别用于数据平面和 snort）。	percentage
数据吞吐量	集群的传入和传出数据流量统计信息。	bytes
CCL 吞吐量	集群的传入和传出 CCL 流量统计信息。	bytes
连接	集群中的活动连接计数。	数字
NAT 转换	集群的 NAT 转换计数。	数字
分布	集群中每秒的连接分布计数。	数字
数据包数	集群中每秒的数据包分发计数。	数字

防火墙管理中心：对集群进行故障排除

您可以使用 **CCL Ping** 工具确保集群控制链路正常运行。 您还可以使用以下适用于设备和集群的工具：

- 故障排除文件-如果节点未能加入集群，系统将自动生成故障排除文件。您还可以从**设备**>**设备管理** > **集群** > **常规** 区域生成和下载故障排除文件。请参阅生成故障排除文件。

  您还可以通过点击 **更多** (⋮) 并选择 **文件故障排除** ，从 **设备管理**页面生成文件。

- CLI 输出-从 **设备** > **设备管理** > **集群** > **常规**区域，您可以查看一组预定义的 CLI 输出，帮助您排除集群的故障。系统会自动为集群运行以下命令：
  - **show running-config cluster**
  - **show cluster info**
  - **show cluster info health**
  - **show cluster info transport cp**
  - **show version**
  - **show asp drop**
  - **show counters**
  - **show arp**
  - **show int ip brief**

- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

您还可以在命令字段中输入任何 **show** 命令。有关详细信息，请参阅查看 CLI 输出。

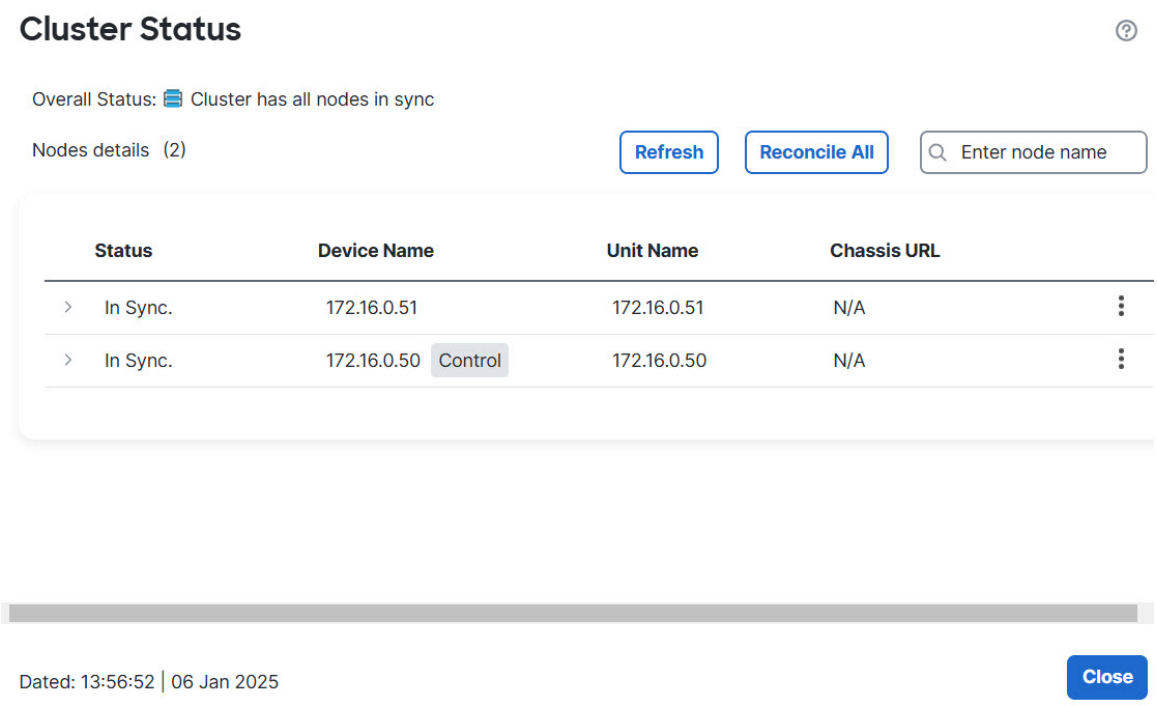
在集群控制链路上执行 Ping

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。如果您遇到集群控制链路连接问题，此工具允许您手动 ping 所有已加入集群的节点。

过程

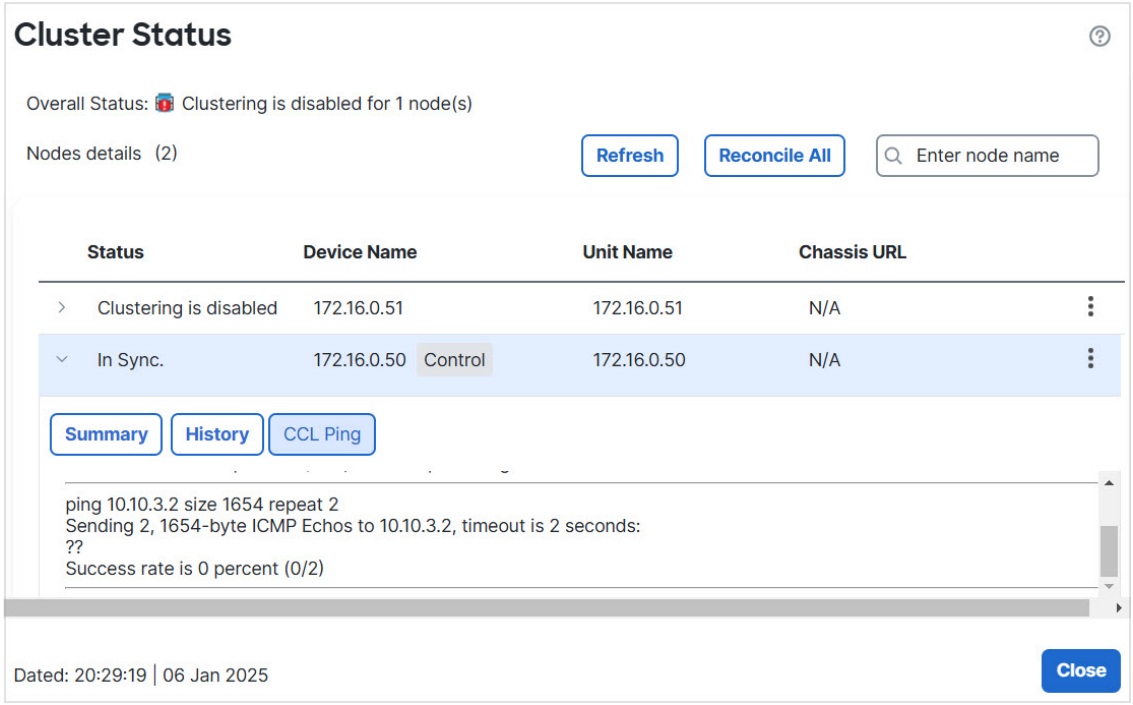
步骤 1 选择 **设备** > **设备管理**，点击集群旁边的 **更多** (⋮) 图标，然后选择**集群实时状态**。

图 *249:* 集群状态



步骤 2 展开其中一个节点，然后点击 **CCL Ping**。

图 *250: CCL Ping*

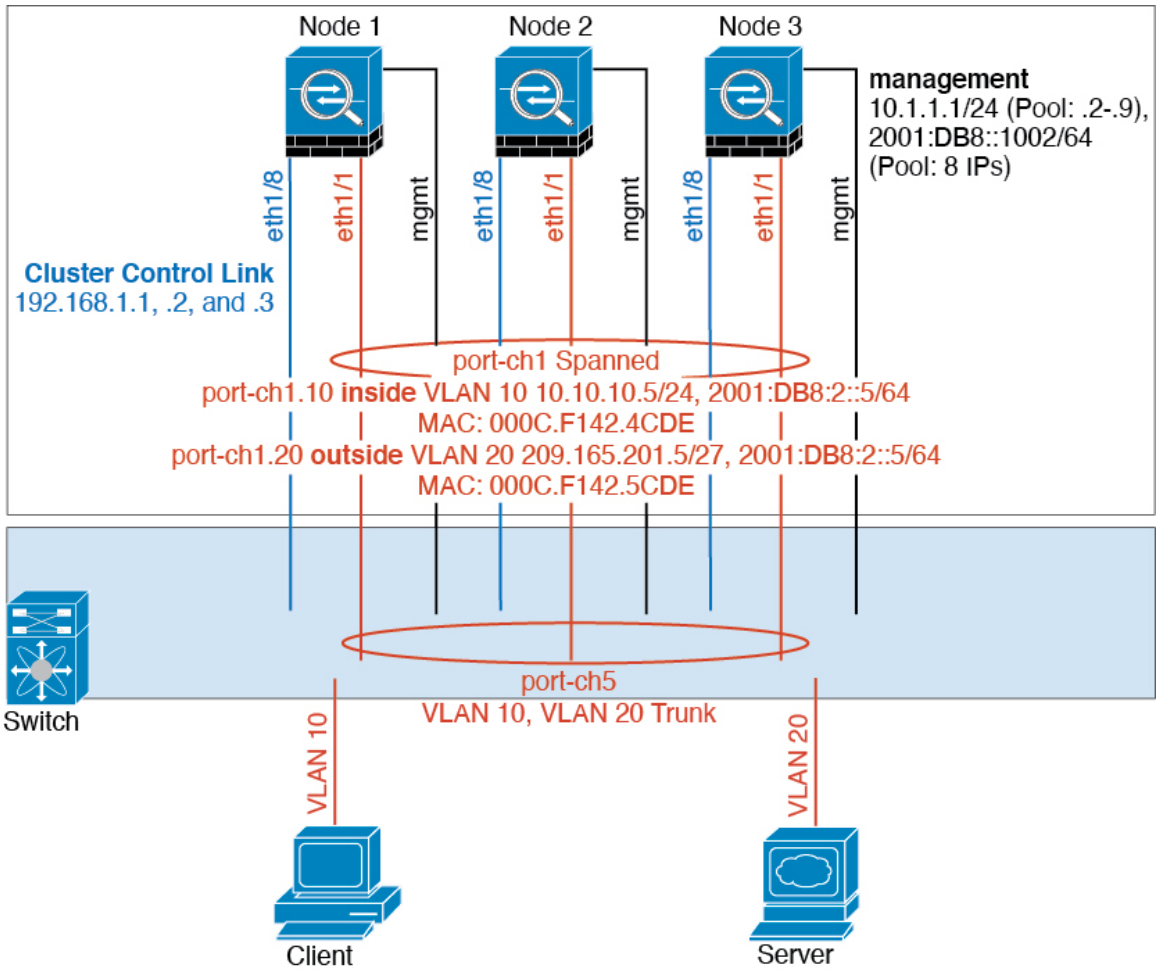


节点使用与最大 MTU 匹配的数据包大小在集群控制链路上向每个其他节点发送 ping 命令。

集群示例

这些示例包含典型部署。

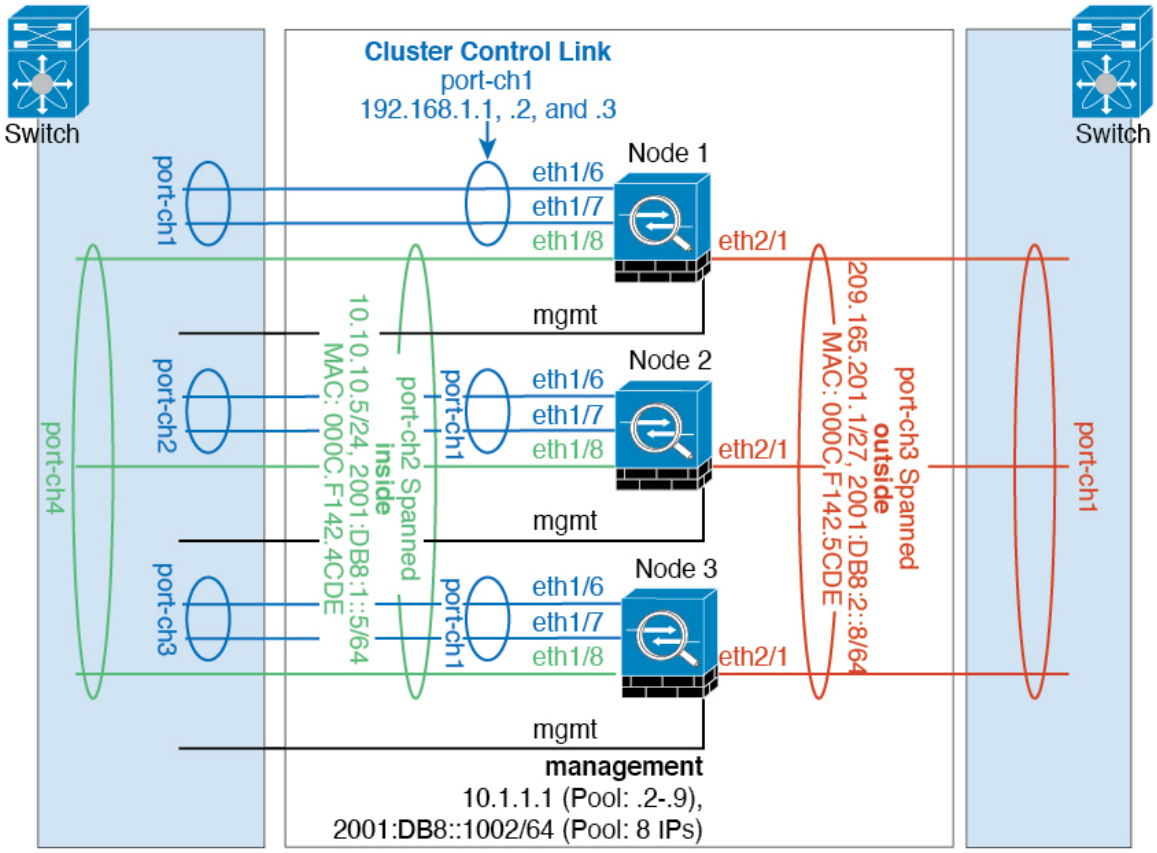
单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如，VLAN 10 用于内部网络，而 VLAN 20 用于外部网络。每台 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机侧分组为一个 EtherChannel。如果一台 变得不可用，交换机将在其余设备之间再均衡流量。

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

集群参考

本部分包括有关集群工作原理的详细信息。

Firewall Threat Defense功能和集群

部分 Firewall Threat Defense 功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略，第 1041 页。

- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 在公共云中不支持站点间 VPN（基于策略和路由）。
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- 防火墙管理中心 UCAPL/CC 模式
- DHCP 客户端、服务器和代理。支持 DHCP 中继。

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略，第 1041 页。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP

- RSH
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 站点间 VPN
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由

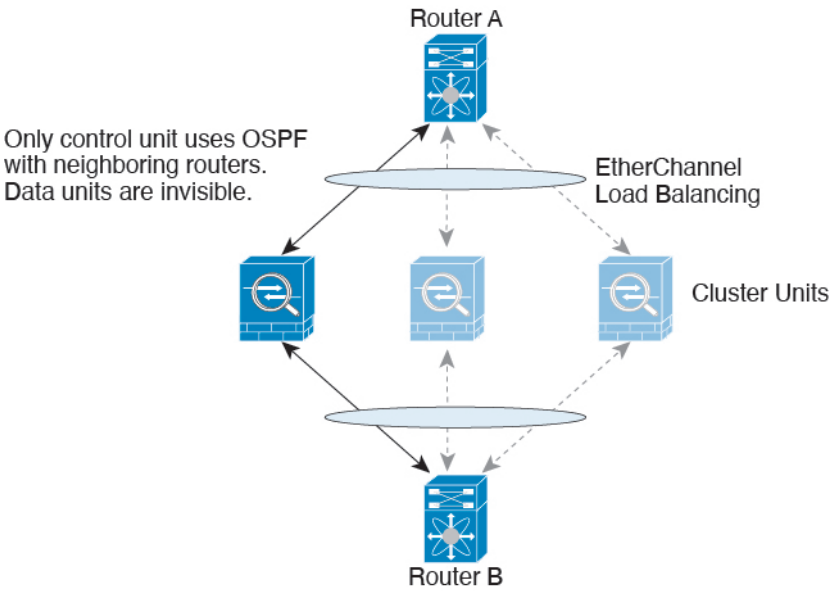
连接设置

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

路由进程仅在控制单元上运行，而路由通过控制单元获知并复制到从属设备。如果路由数据包到达数据设备，它将重定向到控制设备。

图 ***251:*** 动态路由



在数据设备向控制设备学习路线后，每个设备将单独做出转发决策。

OSPF LSA 数据库不会从控制设备同步到数据设备。如果切换了控制设备，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

组播路由和集群

在建立快速路径转发之前，控制单元会处理所有的组播路由数据包和数据数据包。在连接建立之后，每台数据设备都可以转发组播数据包。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 Firewall 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 Firewall 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。
- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT

连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。

- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会

看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

TLS / SSL 连接和群集

TLS/SSL 连接的解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要建立新连接以连通新设备。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

站点间 VPN 是集中功能；只有控制单元支持 VPN 连接。

注释 群集不支持远程接入 VPN。

VPN 功能仅限控制设备使用，且不能利用群集的高可用性功能。如果控制单元发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。

与 VPN 相关的密钥和证书将被复制到所有设备。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

以 TCP 吞吐量为例，含 3 个 SM-40 模块的 Firepower 9300 在单独运行时大约可处理 135 Gbps 的实际防火墙流量。2 个机箱的最大合并吞吐量约为 270 Gbps（2 个机箱 x 135 Gbps）的 80%：216 Gbps。

控制设备选择

集群成员通过集群控制链路通信，如下选举控制设备：

1. 当您部署集群时，每台设备会每隔 3 秒广播一次选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级在您部署集群时设置且不可配置。
3. 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为控制设备。

注释 如果多台设备并列获得最高优先级，则使用集群设备名称和序列号确定控制设备。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制设备；现有控制设备始终保持为控制设备，除非它停止响应，此时会选择新的控制设备。
5. 在“裂脑”场景中，当临时存在多个控制单元时，具有最高优先级的单元将会保留角色，其他单元则恢复为数据单元角色。



注释 您可以手动强制一台设备成为控制设备。对集中功能而言，如果强制更改控制设备，则所有连接都将断开，而您必须在新的控制设备上重新建立连接。

集群中的高可用性

集群通过监控机箱、设备和接口的运行状态并在设备之间复制连接状态来提供高可用性。

机箱应用监控

机箱应用运行状况监控始终处于启用状态。Firepower 4100/9300 机箱 管理引擎会定期检查 Firewall 威胁防御应用（每秒）。如果 Firewall 威胁防御设备已启动且无法与 Firepower 4100/9300 机箱管理引擎通信达到 3 秒，则 Firewall 威胁防御设备会生成系统日志消息并离开集群。

如果 Firepower 4100/9300 机箱管理引擎在 45 秒后仍无法与应用通信，则会重新加载 Firewall 威胁防御设备。如果 Firewall 威胁防御设备无法与管理引擎通信，则会将自身从集群中删除。

设备运行状况监控

每台设备通过集群控制链路定期发送广播keepalive keepalive心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何 keepaliveheartbeat 数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。有关详细信息，请参阅控制设备选择，第 696 页。

接口监控

每个节点都会监控使用中的所有硬件接口的链路状态，并向控制节点报告状态更改。对于多机箱集群，跨网络 EtherChannel 使用集群链路聚合控制协议 (cLACP)。每个机箱都会监控链路状态和 cLACP 协议消息，以确定端口在 EtherChannel 中是否仍处于活动状态，并在接口关闭时通知 Firewall 威胁防御应用。当启用运行状况监控时，默认情况下监控有物理接口（包括 EtherChannel 接口的主 EtherChannel）。仅可监控处于开启状态的命名接口。例如，只有 EtherChannel 的所有成员端口都出现故障时，才会从集群中删除指定的 EtherChannel。 可以选择性地禁用对每个接口的监控。

如果受监控接口在特定节点上发生故障，但在其他节点上处于活动状态，则该节点将从集群中删除。Firewall 威胁防御设备在多长时间后从集群中删除节点取决于该节点是既定成员还是正在加入集群的设备。Firewall 威胁防御设备 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 Firewall 威胁防御设备从集群中删除。对于既定成员，节点将在 500 毫秒后删除。

对于多机箱集群，如果从集群添加或删除一个 EtherChannel，则接口运行状况监控将暂停 95 秒，以确保您有时间在每个机箱上进行更改。

修饰符应用监控

在接口上安装某种修饰符应用时，例如 Radware DefensePro 应用，Firewall 威胁防御设备和该修饰符应用必须处于运行状态，以保留在集群中。只有两个应用都处于运行状态，设备才会加入集群。加入集群后，设备每 3 秒钟监控一次修饰符应用的运行状况。如果修饰符应用关闭，设备将从集群中移除。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

Firewall 威胁防御将自动尝试重新加入集群，具体取决于故障事件。



注释 当 Firewall 威胁防御 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - Firewall Threat Defense 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 Firewall Threat Defense应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。Firewall Threat Defense应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。
- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。

如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

- 机箱-应用通信故障 - 当 Firewall Threat Defense应用检测到机箱-应用运行状况恢复时，会自动尝试重新加入集群。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *51:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	支持	—
动态路由	支持	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。



注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

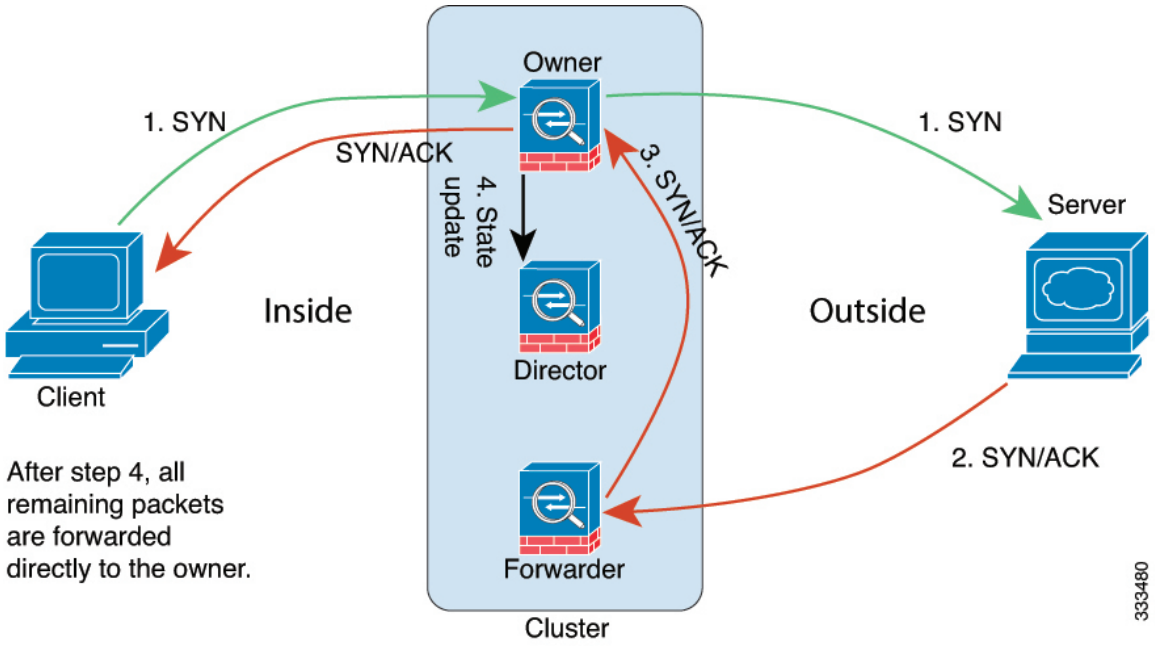
端口地址转换连接

新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

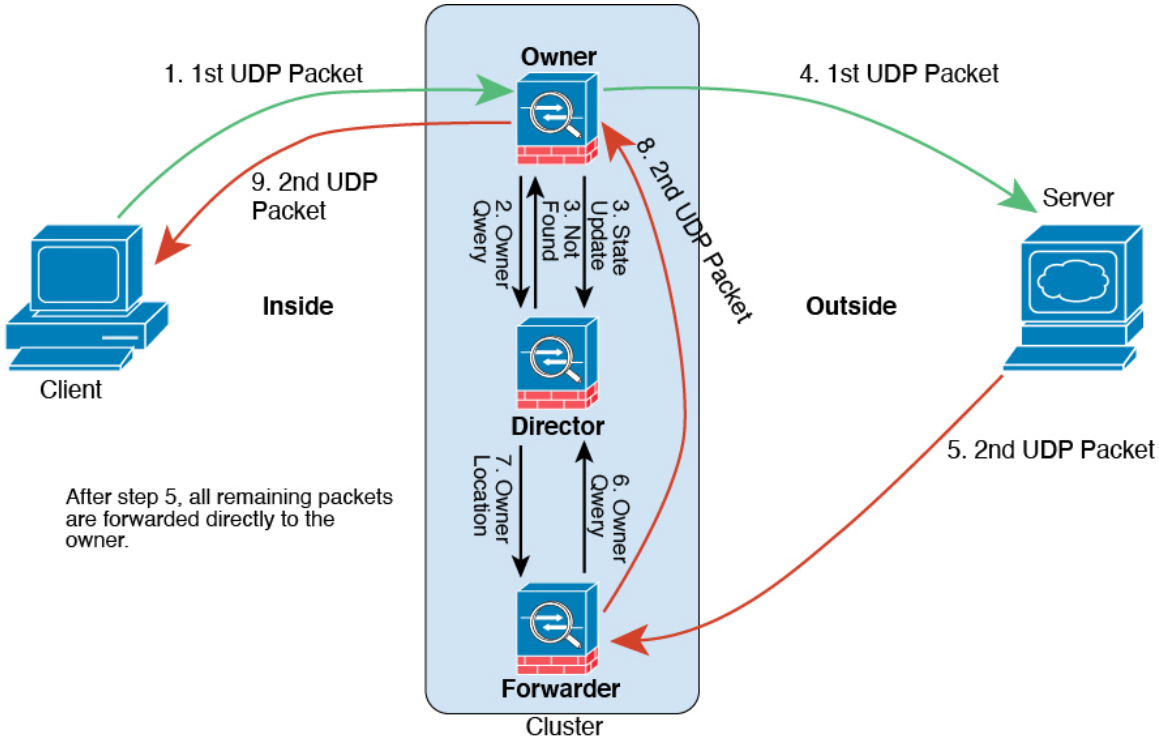


1. SYN 数据包从客户端发出，被传送到一台 Firewall 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 Firewall 威胁防御（基于负载均衡方法）。此 Firewall 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *252: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个Firewall 威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

集群的历史记录

表 *52:*

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群节点加入时的 MTU ping 测试通过尝试较小的 MTU 来提供更多信息	10.0.0	10.0.0	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，它将尝试除以 MTU，并继续除以 2，直到 MTU ping 成功。成功的 ping 值会显示在 **show cluster info trace** 中，因此您可以将 MTU 调整为可用值，然后重试。 即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。 我们建议将交换机 MTU 的大小增加到建议的值，但如果您无法更改交换机配置，则可以使用集群控制链路的工作值来形成集群。 添加/修改的命令：**show cluster info trace**、**show cluster history**。
关于节点加入时时间节点的 MTU ping 测试	7.6.0	7.6.0	节点加入集群时，会向控制节点发送数据包大小为集群控制链路 MTU 两倍的 Ping 请求，以检查 MTU 兼容性。此前，仅控制节点发送 Ping。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。 添加/修改的命令：**show cluster history**。
集群控制链路 ping 工具。	7.2.67.4.1	任意	您可以通过执行 ping 来检查是否所有集群节点都能通过集群控制链路相互连接。节点无法加入集群的一个主要原因是集群控制链路配置不正确，例如，集群控制链路 MTU 设置可能高于连接交换机的 MTU。 新增/修改的屏幕：**设备** > **设备管理** > **更多** > **集群实时状态**。
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
集群运行状况监控器控制面板。	7.3.0	任意	您现在可以在集群运行状况监控控制面板上查看集群运行状况。 新增/修改的屏幕：**系统** > **运行状况** > **监控器**
支持 16 节点集群。	7.2.0	7.2.0	您现在可以为 Firepower 4100/9300 配置 16 个节点集群。以前，最多只能部署 6 台设备。 新增/修改的屏幕：无。 支持的平台：Firepower 4100/9300
用于防火墙更改的集群部署更快完成。	7.1.0	7.1.0	防火墙更改的集群部署现在完成更快。 新增/修改的屏幕：无。
改进了集群的 PAT 端口块分配。	7.0.0	7.0.0	改进的PAT端口块分配可确保控制设备保留端口以供加入节点，并主动回收未使用的端口。为了最好地优化分配，您可以使用 **cluster-member-limit** 命令和FlexConfig 设置您计划在集群中拥有的最大节点数。然后，控制单元可以分配端口块到计划的节点数量，并且不必为您不打算使用的额外节点预留端口。默认值为 16 节点。您还可以监控系统日志 747046，以确保有足够的端口可用于新节点。 新增/经修改的命令： **cluster-member-limit** (FlexConfig)、 **show nat pool cluster summary**、 **show nat pool ip detail**
Snort 的集群部署更改完成得更快，并且在发生事件时失败更快。	6.7.0	6.7.0	Snort 更改的集群部署现在可以更快完成。此外，当集群发生导致 防火墙管理中心 部署失败的事件时，故障现在会更快发生。 新增/修改的屏幕：无。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
改进了集群管理。	6.7.0	6.7.0	防火墙管理中心改进了以前只能使用CLI完成的集群管理功能，包括： • 启用和禁用集群设备 • 从设备管理页面显示集群状态，包括每台设备的历史记录和摘要 • 变更角色为控制单元 新建/修改的菜单项： • **设备** > **设备管理** > **更多** 菜单 • **设备** > **设备管理** > **集群** > **常规** 区域 > **集群实时状态** 链接 **集群状态** 支持的平台：Firepower 4100/9300
多实例集群。	6.6.0	6.6.0	您现在可以使用容器实例来创建集群。在 Firepower 9300 上，必须在集群中的每个模块上包含一个容器实例。不能为每个安全引擎/模块向集群添加多个容器实例。我们建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同Firepower 9300安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。 新增/修改的 FXOS 命令：**set port-type cluster** 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **添加集群** • **接口** > **所有接口** > **新增**下拉菜单**子接口类型字段** 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense
并行配置同步到数据设备。	6.6.0	6.6.0	控制设备现在默认将配置更改并行同步到数据设备。以前，同步是按顺序发生的。 新增/修改的屏幕：无。
集群加入失败或逐出的消息已添加到 **show cluster history**。	6.6.0	6.6.0	关于集群设备无法加入集群或离开集群的新消息添加到了 **show cluster history** 命令。 新增/修改的命令：**show cluster history** 新增/修改的屏幕：无。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群中的“死连接检测”(DCD) 支持的发起方和响应方信息。	6.5.0	6.5.0	如果启用死连接检测(DCD)，则可以使用该**show conn detail**命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 **show conn** 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出） 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense
添加集群更容易。	6.3.0	6.3.0	现在可将集群中的任何设备添加到防火墙管理中心，并会自动检测其他集群设备。以前，必须将每个集群设备作为独立设备予以添加，然后将其组合到集群中。现在也可以自动添加集群设备了。请注意，必须手动删除设备。 新增/修改的屏幕： **设备** > **设备管理** > **添加**下拉菜单**设备** > **添加设备**对话框 **设备** > **设备管理** > **集群**选项卡**常规**区域**集群注册状态** **当前集群摘要**链接**集群状态**对话框 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense
支持将集群作为集中功能的站点间 VPN	6.2.3.3	6.2.3.3	现在可以配置使用集群的站点间 VPN。站点间 VPN 是集中功能；只有控制单元支持 VPN 连接。 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense
内部故障后自动重新加入集群。	6.2.3	6.2.3	过去，许多内部错误条件导致集群设备从集群中移除，并且在解决问题后需要手动重新加入集群。现在，设备将尝试以下列时间间隔自动重新加入集群：5 分钟、10 分钟以及 20 分钟。内部故障包括：应用同步超时、不一致的应用状态等。 新增/修改的命令：**show cluster info auto-join** 未修改任何屏幕。 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
6 个模块的多机箱集群；Firepower 4100 支持。	6.2.0	6.2.0	使用 FXOS 2.1.1，您现在可以在 Firepower 9300 和 4100 上启用多机箱集群。对于 Firepower 9300，最多可以包含 6 个模块。例如，您可以在 6 个机箱中使用 1 个模块，或者在 3 个机箱中使用 2 个模块，也可以使用最多提供 6 个模块的任意组合。对于 Firepower 4100，最多可以包含 6 个机箱。 注释 也支持站点间集群。然而，仅可通过使用 FlexConfig 功能来配置用以增强冗余性和稳定性自定义功能，例如指定站点的 MAC 和 IP 地址、导向器本地化、站点冗余和集群流移动性。 未修改任何屏幕。 支持的平台：Firepower 4100/9300 上的 Firewall Threat Defense
使用一个 Firepower 9300 机箱在多个模块上集群。	6.0.1	6.0.1	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **添加集群 (Add Cluster)** **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：Firepower 9300 上的 Firewall Threat Defense



第 III 部分

接口和设备设置

- 接口概述， 第 711 页
- 常规防火墙接口， 第 753 页
- 内联集和被动接口， 第 833 页
- 设备设置， 第 847 页
- DHCP 和 DDNS， 第 955 页
- 平台设置， 第 973 页
- FlexConfig 策略， 第 1041 页



第 14 章

接口概述

Firewall Threat Defense 设备包括可在不同模式下配置的数据接口，以及管理 接口。

- 管理接口， 第 711 页
- 接口模式和类型， 第 712 页
- 安全区域和接口组， 第 713 页
- Auto-MDI/MDIX 功能， 第 714 页
- 冗余接口（已弃用），第 714 页
- 接口默认设置， 第 714 页
- 创建安全区域和接口组对象， 第 715 页
- 启用物理接口并配置以太网参数， 第 716 页
- 配置 EtherChannel 接口， 第 719 页
- 与 防火墙管理中心同步接口更改 ， 第 727 页
- 管理 Cisco Secure Firewall 3100/4200/6100的网络模块， 第 728 页
- 合并管理和诊断接口， 第 743 页
- 接口的历史记录， 第 750 页

管理接口

在 7.3 及更早版本中，物理管理接口由诊断逻辑接口和管理逻辑接口共用。在 7.4 及更高版本中，为简化用户体验，诊断接口与管理接口进行了合并。

管理接口

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到防火墙管理中心。它使用自己的 IP 地址和静态路由。您可以在 CLI 中使用 **configure network** 命令配置其设置。您也可以在 **设备** > **设备管理** 页面上查看其状态。如果在将 IP 地址添加到 防火墙管理中心 后在 CLI 中更改该地址，则可以在 **设备** > **设备管理** 区域的 Secure Firewall Management Center 中匹配该 IP 地址。

您也可以使用数据接口而不是管理接口来管理 Firewall Threat Defense 。

诊断接口

对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。

如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。

如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。要手动合并管理接口和诊断接口，请参阅合并管理和诊断接口，第 743 页。阻止自动合并的配置包括：

- 名为“management”的数据接口 - 此名称保留用于合并的管理接口。
- 诊断接口中的 IP 地址
- 诊断接口中启用了 DNS
- 系统日志、SNMP、RADIUS 或 AD（对于远程访问 VPN）源接口为诊断接口
- RADIUS 或 AD（对于远程访问 VPN）未指定源接口，并且至少有一个接口配置为管理专用接口（包括诊断接口）-这些服务的默认路由查找已从管理专用路由表更改为数据路由表，没有回退到管理。因此，除管理外，不能对使用管理专用接口。
- 诊断接口中的静态路由
- 诊断接口中的动态路由
- 诊断接口中的HTTP 服务器
- 诊断接口中的 ICMP
- 诊断接口的 DDNS
- 使用诊断接口的 FlexConfig

有关旧诊断接口工作方式的详细信息，请参阅本指南的 7.3 版本。

接口模式和类型

您可以在两种模式下部署 Firewall Threat Defense 接口：常规防火墙模式和仅 IPS 模式。您可以在同一设备上同时配置防火墙和仅 IPS 接口。

常规防火墙模式

防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅透明或路由防火墙模式，第 123 页。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。

- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。 在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

仅 IPS 模式

您可以被动或内联 IPS 部署方式配置设备。在被动部署中，您可以在网络流量的带外部署系统。在内联部署中，可通过将两个接口绑定到一起在网段上透明地配置系统。

安全区域和接口组

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以把一个或多个设备上的“内部”接口分配到“内部”区域；而把“外部”接口分配到“外部”区域。然后，您可以配置访问控制策略，以便为使用相同区域的每台设备启用从内部区域到外部区域的流量。

要查看属于每个对象的接口，请选择**对象**然后点击**接口**。此页面列出托管设备上配置的区域安全区域和接口组。您可以展开每个接口对象以查看每个接口对象中的接口类型。

注释 适用于**任何**区域的策略（全局策略）也适用于区域中的接口以及未分配给区域的任何接口。

注释 管理接口不属于区域或接口组。

安全区域 vs. 接口组

有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

  您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用接口组，也可以使用直接指定接口名称的功能，例如系统日志服务器或 DNS 服务器。

某些策略仅支持安全区域，而其他策略则支持区域和组。除非您需要接口组提供的功能，否则应默认使用安全区域，因为所有功能都支持安全区域。

不能将现有安全区域更改为接口组（反之亦然）；而必须创建新接口对象。

注释 尽管隧道区域不是接口对象，但您可以在某些配置中使用它们代替安全区域；请参阅使用隧道区域在隧道级别应用访问控制，第 2238 页。

接口对象类型

请参阅以下接口对象类型：

- 被动 - 适用于仅 IPS 被动或 ERSPAN 接口。
- 内联 - 适用于仅 IPS 内联集接口。
- 已交换 - 适用于常规防火墙网桥组接口。
- 已路由 - 适用于常规防火墙路由接口。
- ASA -（仅安全区域）适用于旧版 ASA FirePOWER 设备接口。
- 管理 -（仅接口组）用于管理专用接口。
- 环回 -（仅限接口组）用于环回接口。

接口对象中的所有接口都必须为同一类型。创建接口对象后，不能更改其包含的接口类型。

接口名称

请注意，接口（或区域名称）本身不提供有关安全策略的任何默认行为。我们建议使用自描述的名称，以避免在未来的配置中出错。好的名称能表明逻辑网段或流量规范，例如：

- 内部接口的名称 - InsideV110、InsideV160、InsideV195
- DMZ 接口的名称 - DMZV11、DMZV12、DMZV-TEST
- 外部接口的名称 - Outside-ASN78、Outside-ASN91

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

冗余接口（已弃用）

冗余接口仅支持 ASA 5500-X 平台。不建议为其他平台配置冗余接口。

接口默认设置

本部分列出接口的默认设置。

接口的默认状态

接口的默认状态取决于类型。

- 物理接口 - 已禁用。对初始设置启用的管理接口是个例外。物理接口包括交换机端口。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- EtherChannel port-channel 接口 （ISA 3000）- 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel 端口-通道接口（Firepower 和 Cisco Secure Firewall 型号）- 已禁用。



注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和 防火墙管理中心 上的接口。为使接口正常运行，必须同时在两个操作系统中启用该接口。由于接口状态可独立控制，因此机箱与 防火墙管理中心 之间可能出现不匹配的情况。

默认速度和双工

默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。

默认情况下，光纤 (SFP) 接口的速度和双工会被设为最大速度，同时启用自动协商。如果通过 50G 电缆连接到该端口的对等交换机不支持自动协商，请确保也在该交换机和威胁防御接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持通过 50G 电缆进行自动协商。因此，要连接该端口，您必须在平台和交换机上禁用默认的自动协商。

对于 Cisco Secure Firewall 3100/4200/6100，速度设置为检测已安装的 SFP 速度。

以太网 1/10 上已安装的 SFP 速度。

创建安全区域和接口组对象

添加您可以为其分配设备接口的安全区域和接口组。



提示 可以创建空的接口对象并随后向其添加接口。要添加接口，该接口必须具有名称。您还可以配置接口时创建安全区域（但不是接口组）。

开始之前

了解每种类型的接口对象的使用要求和限制。请参阅安全区域和接口组 ， 第 713 页。

过程

步骤 1 选择**对象** > **接口**。

步骤 2 点击**添加 (Add) > 安全区域 (Security Zone)** 或**添加 (Add) > 接口组 (Interface Group)**。

步骤 3 输入 **Name**。

请勿使用与网络或端口对象相同的名称。这些对象名称便于部署到设备，重复的名称会导致部署失败。

步骤 4 选择**接口类型 (Interface Type)**。

步骤 5 （可选）从**设备 (Device) > 接口 (Interfaces)** 下拉列表中，选择包含要添加的接口的设备。

您不需要在此屏幕上分配接口；您可以在配置接口时将接口分配给区域或组。

步骤 6 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口。默认情况下，物理接口处于禁用状态（管理接口除外）。
- 设置特定的速度和复用。默认情况下，速度和复用设置为“自动”。

此过程仅涵盖一小部分接口设置。此时不能设置其他参数。例如，不能命名要用作 EtherChannel 接口一部分的接口。具体的接口选项因型号和接口类型而异。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。有关详细信息，请参阅配置物理接口，第 310 页。

注释 有关交换机端口的信息，请参阅配置交换机端口，第 754 页。

您也可以点击设备上的**虚拟频道**以查看基于路由的 VPN 的动态和静态 VTI 的详细信息。有关详细信息，请参阅 查看虚拟隧道信息，第 1488 页。

开始之前

如果在将设备添加到防火墙管理中心后更改了设备上的物理接口，需要点击**接口 (Interfaces)** 左上角的**从设备同步接口 (Sync Interfaces from device)** 刷新接口列表。 对于支持热插拔的 Cisco Secure Firewall 3100/4200，在更改设备上的接口之前，请参阅管理 Cisco Secure Firewall 3100/4200/6100的网络模块，第 728 页。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 （可选） 通过点击 **硬件配置 (Hardware Configuration)** > **速度 (Speed)**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。但是，Cisco Secure Firewall 220 的 SFP 接口 (Ethernet 1/5) 支持**全双工**和**半双工**。
- **速度**-选择速度（因型号而异）。对于 SFP，选择 **检测 SFP** 以检测已安装 SFP 模块的速度，并使用相应的速度。双工模式始终为全双工，自动协商始终启用，且 FEC 设置为自动。对于双速收发器，将使用较低速度。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。某些交换机和收发器不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。例如，Cisco Secure Firewall 6100 上的 SFP-H25GB-CU1M 不支持自动协商或 FEC，因此您必须手动设置速度、禁用**自动协商**并禁用**前向纠错模式**。

  注释
  您无法修改高可用性或集群控制链路接口的速度。

- **自动协商** - 设置接口以协商速度、链路状态和流量控制。

  1100除外，自动协商与速度分开设置。某些交换机不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。

- **前向纠错模式** - 对于 25 Gbps 及更高速率的接口，请启用前向纠错 (FEC)。

  对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。如果从 EtherChannel 中删除接口，则重新启动后可能需要为该接口重新配置 FEC。

  有些交换机不支持 FEC 自动模式，尤其是较大的接口。请根据交换机支持情况确保手动配置该设置。不建议禁用 FEC；如果禁用，EtherChannel 可能无法正常启用。

  使用 **自动** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *53:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

注释
从版本 7.4.2 开始，防火墙威胁防御支持 SFP 10G_25G_CSR_S 模块。为避免重启后出现链路断开问题，必须在这些接口上启用前向纠错 (FEC)。

步骤 6 （可选） 通过点击**硬件配置** > **网络连接** 启用链路层发现协议 (LLDP)。

- **启用 LLDP 接收**-启用防火墙以从其对等体接收 LLDP 数据包。
- **启用 LLDP 传输**-启用防火墙以将 LLDP 数据包发送到其对等体。

步骤 7 （可选） (Cisco Secure Firewall 3100) ）通过点击**硬件配置 (Hardware Configuration)** > **网络连接 (Network Connectivity)**，然后选中**流量控制发送 (Flow Control Send)** 来为流量控制启用暂停 (XOFF) 帧。

流量控制通过允许拥塞节点在另一端暂停链路操作，从而让连接的以太网端口能够在拥塞期间控制流量速率。如果威胁防御端口遇到拥塞（内部交换机上的排队资源耗尽）并且无法接收更多流量，则它会通过发送暂停帧来通知另一个端口停止发送，直到状况恢复正常为止。在收到暂停帧后，发送设备会停止发送任何数据包，从而防止在拥塞期间丢失任何数据包。

注释
Firewall Threat Defense 支持传输暂停帧，以便远程对等体可以对流量进行速率控制。

但是，不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池，而每个缓冲区都有 250 个字节，并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记（2 MB [8000 个缓冲区]）时，会在每个启用了流量控制的接口上发送暂停帧；当特定接口的缓冲区超过端口高水位标记（0.3125 MB [1250 个缓冲区]）时，会从该接口发送暂停帧。在发送暂停后，如果缓冲区使用率降低至低水位标记之下（全局 1.25 MB [5000 个缓冲区]；每个端口 0.25 MB [1000 buffers]），则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 8 在**模式**下拉列表中，选择以下选项之一：

- **无** - 为常规防火墙接口和内联集选择此设置。该模式将基于后续配置自动更改为路由、交换或内联。

- **被动** - 为被动仅限 IPS 接口选择此设置。
- **Erspan** - 为 ERSPAN 被动仅限 IPS 接口选择此设置。

步骤 9 在 **优先级** 字段中，输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口分配流量。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 12 继续配置接口。

- 常规防火墙接口，第 753 页
- 内联集和被动接口，第 833 页

配置 EtherChannel 接口

本节介绍如何配置 EtherChannel 接口。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅添加 EtherChannel（端口通道），第 311 页。

关于 EtherChannels

本节介绍 EtherChannel 。

关于 EtherChannel

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

通道组接口

各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

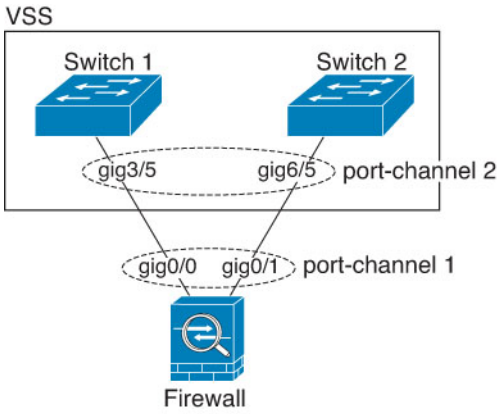
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到其他设备上的 EtherChannel

Firewall Threat DefenseEtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，则可以将同一 EtherChannel 内的 Firewall Threat Defense接口连接到 VSS/vPC 中的单独交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。

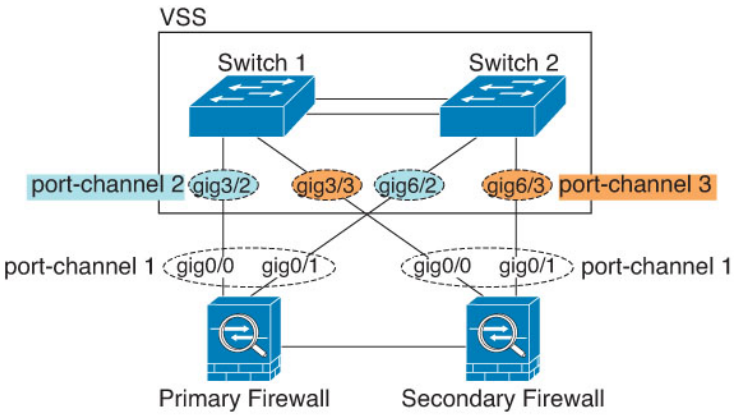
图 *253:* 连接至 *VSS/vPC*



注释 如果 Firewall Threat Defense 设备处于透明防火墙模式下，并且将 Firewall Threat Defense 设备置于两组 VSS/vPC 交换机之间，请确保在使用 EtherChannel 连接到 Firewall Threat Defense 设备的所有交换机端口上禁用单向链路检测 (UDLD)。如果启用 UDLD，则交换机端口可能会接收来自另一个 VSS/vPC 对中的两台交换机的 UDLD 数据包。接收交换机会将接收接口置于关闭状态，原因是“UDLD 邻居不匹配”。

如果您在主用/备用故障转移部署中使用 Firewall Threat Defense 设备，则需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个 Firewall Threat Defense 设备创建一个。在每个 Firewall Threat Defense 设备上，单个 EtherChannel 连接至两台交换机。即使您可以将所有的交换机接口分组到连接两个 Firewall Threat Defense 设备的一个 EtherChannel 中（在这种情况下，将不会建立 EtherChannel，因为 Firewall Threat Defense 系统 ID 是单独的），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用 Firewall Threat Defense 设备。

图 *254:* 主用/备用故障转移和 ***VSS/vPC***



链路聚合控制协议

链路聚合控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 被动 - 接收 LACP 更新。备用 EtherChannel 只能与主用 EtherChannel 建立连接。在硬件型号上不受支持。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

负载均衡

Firewall Threat Defense 设备通过对数据包的源 IP 地址和目标 IP 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障转移对其他网络设备是透明的。

EtherChannel MAC 地址

属于通道组一部分的所有接口都共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。

Firepower 和 Cisco Secure Firewall 硬件

端口通道接口使用内部接口 Internal-Data 0/1 的 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。机箱上的所有 EtherChannel 接口都使用相同的 MAC 地址，因此请注意，例如，如果使用 SNMP 轮询，则多个接口将具有相同的 MAC 地址。



注释 成员接口仅在重新启动后使用内部数据 0/1 MAC 地址。在重新启动之前，成员接口使用自己的 MAC 地址。如果在重新启动后添加新的成员接口，则必须再次重新启动以更新其 MAC 地址。

EtherChannel 的准则

桥接组

在路由模式下，不支持将 防火墙管理中心-定义的 EtherChannel 接口作为桥接组成员。Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

- 如果要将 EtherChannel 接口用作 链路，则必须在 对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为复制需要 链路本身。
- 如果要将 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。Firepower 4100/9300 机箱 的所有接口（包括 EtherChannel）均需在两台设备上进行预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 接口 (。如果主用成员接口故障转移到备用接口，则此活动不会在监控设备级时导致 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，EtherChannel 接口或 EtherChannel 接口才会出现故障（对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 如果将 EtherChannel 接口用于或状态链路，然后防止无序数据包，则仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作链路时对其进行修改。要修改配置，您需要暂时禁用，以防止在此期间发生。

型号支持

- 无法在 防火墙管理中心 中添加用于 Firepower 4100/9300 或 Firewall Threat Defense Virtual的 EtherChannel。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。
- 无法在 Etherchannel 中使用 Firepower 1010 或 Cisco Secure Firewall 1210/1220 交换机端口或 VLAN 接口。

《通用 EtherChannel 准则》

- 最多可以配置 48 个 Etherchannel，具体取决于型号可用的接口数量。

- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 添加第一个成员接口时，它会设置所有成员接口所需的硬件属性。
  - 成员接口的介质类型可以是 RJ-45 或 SFP；不同类型（铜缆和光纤）的 SFP 可混合使用。RJ-45 和 SFP 接口不能混用。
  - 所有接口必须设置为相同的速度和双工模式。
  - 第一个接口会设置速度容量，后续无法更改。
    - 对于 SFP 检测接口 - 您可包含具有不同速度容量的接口，只要它们有共同速度即可。当您将速度设置为“SFP 检测”（默认）时，速度会动态设置为最高共同速度。如果后续更改成员接口以提高共同速度，则 EtherChannel 速度也会自动提高。

      您可以设置特定速度，但只能设置第一个成员接口上可用的速度。例如，如果第一个接口是 1/10GB，则 EtherChannel 的可用速度为 1GB、10GB 和 SFP 检测。如果后续删除 1/10GB 接口并替换为 1/10/25GB 接口，则无法手动将速度设置为 25GB。在这种情况下，您可以通过 SFP 检测来使用 25GB 速度。
    - 对于非 SFP 检测接口 - 所有其他接口必须具有相同的速度容量。例如，如果您的第一个接口速度容量为 10MB/100MB/1GB，则必须添加其他 10MB/100MB/1GB 接口。您可以将 EtherChannel（及其成员接口）设置为上述任一速度。后续不能将 1/10GB 接口添加到 EtherChannel，即使删除容量较低的接口也不行。也不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。
- Firewall Threat DefenseEtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- Firewall Threat Defense 设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则 Firewall Threat Defense 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- LACP 值取决于型号。设置速率（正常或快速）时，设备会向连接的交换机请求该速率。作为回报，设备将按照连接的交换机请求的速率进行发送。我们建议您在两端设置相同的速率。
  - Firepower 4100/9300 — LACP 速率在 FXOS 中默认设置为“快速”，但您可以将其配置为正常（也称为慢速）。
  - Cisco Secure Firewall 3100/4200 6100- 默认情况下，LACP 速率设置为正常（慢速），但您可以在设备上将其配置为快速。
  - 所有型号-LACP 速率设置为正常（慢），并且不可配置，这意味着设备将始终从连接的交换机请求慢速速率。我们建议将交换机上的速率设置为慢速，以便两端以相同的速率发送 LACP 消息。
- 在低于 15.1(1)S2 的 Cisco IOS 软件版本中， Firewall Threat Defense 不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接 Firewall Threat Defense EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将

stack-mac persistent timer 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

- 所有 Firewall Threat Defense 配置均引用 EtherChannel 接口，而不是成员物理接口。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何向 EtherChannel 分配接口，以及如何自定义 EtherChannel。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅添加 EtherChannel（端口通道），第 311 页。

开始之前

- 添加第一个成员接口时，它会设置所有成员接口所需的硬件属性。有关成员接口要求的详细信息，请参阅EtherChannel 的准则，第 722 页。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先删除该名称。

注释 如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

过程

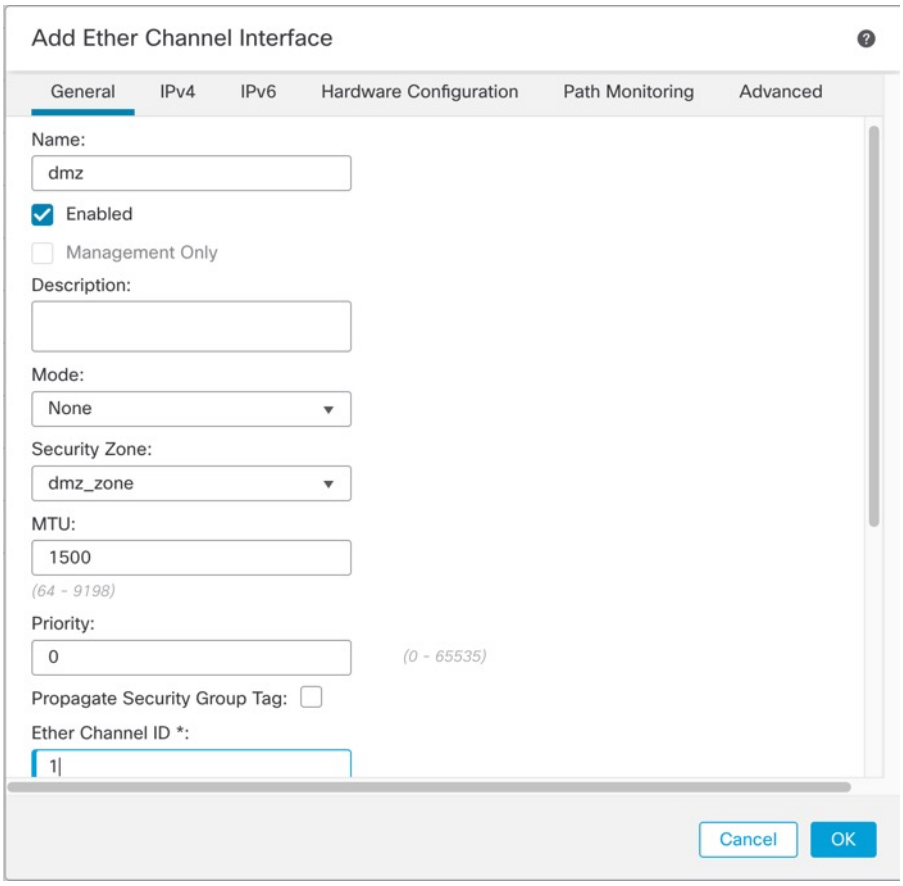
步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 根据启用物理接口并配置以太网参数，第 716 页启用成员接口。

步骤 3 点击**添加接口 (Add Interfaces)** > **以太通道接口 (Ether Channel Interface)**。

步骤 4 在**常规 (General)** 选项卡上，将**以太通道 ID (Ether Channel ID)** 设置为介于 1 和 48 之间的数字（1-8 针对于 Firepower 1010和 Cisco Secure Firewall 1210，1-10 针对 Cisco Secure Firewall 1220）。

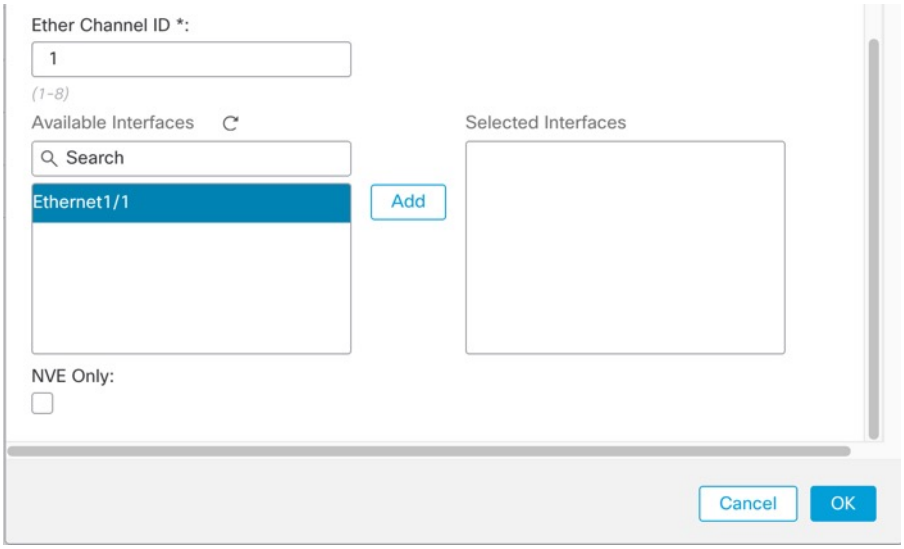
图 *255:* 添加以太网通道接口



步骤 5 在**可用接口 (Available Interfaces)**区域中，点击某个接口对，然后点击**添加 (Add)**，以将其移动至**选定的接口 (Selected Interfaces)** 区域。对要使其成为成员的所有接口重复此步骤。

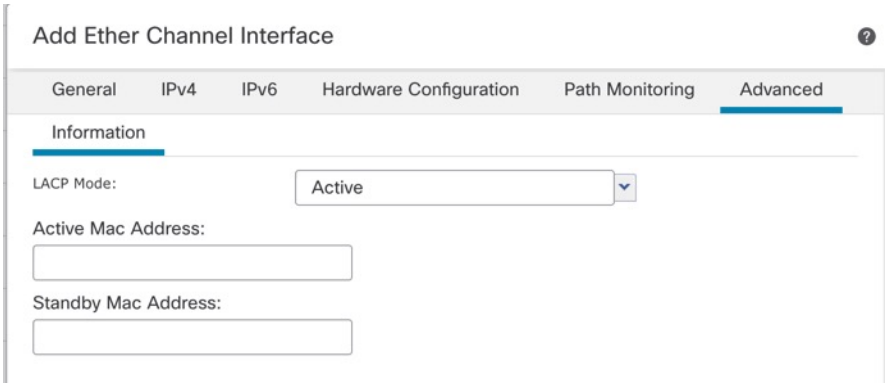
确保所有接口的类型和速度相同。

图 *256:* 可用接口



步骤 6 （可选） 点击**高级 (Advanced)** 选项卡可自定义 EtherChannel。在**信息**子选项卡上设置下列参数：

图 *257:* 高级



- （仅限ISA 3000） **负载均衡**-选择在组通道接口之间对数据包进行负载均衡所用的条件。默认情况下，Firewall Threat Defense 根据数据包的源 IP 地址和目标 IP 地址来均衡接口上的数据包负载。如果要更改分类数据包所依据的属性，请选择另一组条件。例如，如果流量严重偏向于相同的源 IP 地址和目标 IP 地址，则分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。有关负载均衡的详细信息，请参阅负载均衡，第 721 页。
- **LACP 模式** - 选择“主动”、“被动”或“启用”。我们建议使用 Active 模式（默认）。被动模式仅适用于 ISA 3000。
- （仅限 Cisco Secure Firewall 3100/4200 ） LACP 速率— 选择“默认”、“正常”或“快速”。默认值为“正常”(Normal)（也称为“慢速”）。设置通道组中物理接口的 LACP 数据单元接收速率。我们建议您在两端设置相同的速率。
- （仅限 ISA 3000） **主用物理接口: 范围**-从左侧的下拉列表中，选择 EtherChannel 要作为主用接口所需的最小主用接口数量（1 到 16）。默认值为 1。从右侧的下拉列表中，选择 EtherChannel

中允许的最大主用接口数量（1 到 16）。默认值为 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。

- **主用 Mac 地址** - 如果需要，请设置手动 MAC 地址。mac_address 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。

步骤 7 点击**硬件配置 (Hardware Configuration)** 选项卡，并为所有成员接口设置复用和速度。

步骤 8 点击**确定**。

步骤 9 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 10 （可选） 对于常规防火墙接口，请添加 VLAN 子接口。请参阅添加子接口，第 772 页。

步骤 11 对于常规防火墙接口，配置路由或透明模式接口参数：配置路由模式接口，第 792 页或配置网桥组接口，第 797 页。对于仅 IPS 接口，请参阅内联集和被动接口，第 833 页。

与 防火墙管理中心同步接口更改

在设备上进行的添加或删除物理接口可能导致 防火墙管理中心 和设备不同步。防火墙管理中心 可以通过以下方法之一检测到接口更改：

- 设备发送的事件
- 部署时同步 防火墙管理中心

  当 防火墙管理中心 尝试部署时检测到接口更改，部署将失败。必须先接受接口更改。

- 手动同步

添加新接口或删除未使用接口对 Firewall Threat Defense 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 Firewall Threat Defense 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 防火墙管理中心上进行同步。

当 防火墙管理中心 检测到更改时，“**接口**” 页面会在每个接口左侧显示状态（已删除、已更改或已添加）。

本程序介绍在需要时如何手动同步接口。如果接口更改为临时性的，则不应在防火墙管理中心中保存更改；而应等待设备稳定后重新同步。

开始之前

- 用户角色：
  - 管理员
  - 访问管理员

- 网络管理员

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 如果需要，请点击**接口 (Interfaces)** 右上角的**同步接口 (Sync Interfaces)**。

步骤 3 检测到更改后，请参阅以下步骤。

a) 您可以在 **接口** 上看到红色横幅，表明接口配置已发生更改。点击**点击了解详细信息**链接以查看接口更改。

b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

c) 点击**保存**。

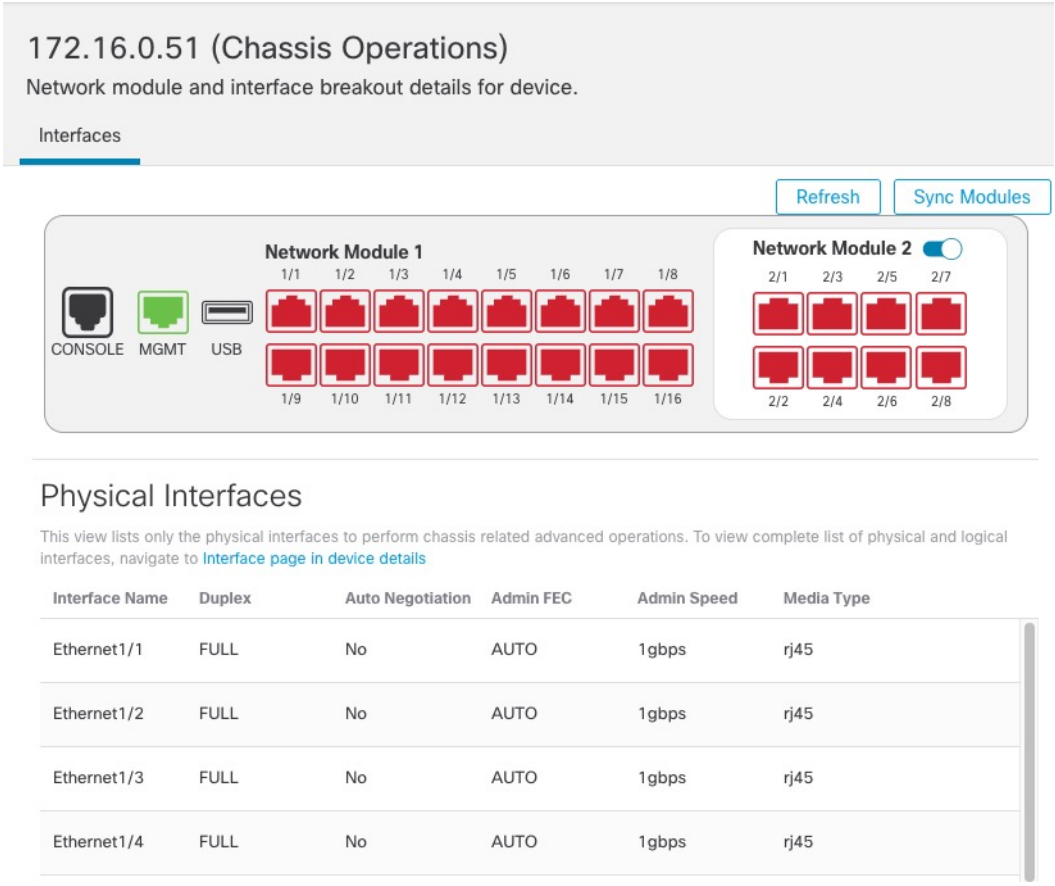
此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。

管理 Cisco Secure Firewall 3100/4200/6100的网络模块

如果在首次打开设备之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

要查看设备的物理接口详细信息并管理网络模块，请打开**机箱操作 (Chassis Operations)** 页面。从 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备。系统将打开设备 **机箱操作** 页面。

图 *258:* 机箱操作



点击 **刷新** 以刷新接口状态。如果您在需要检测的设备上进行了硬件更改，请点击 **同步模块**。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置更小的分支端口。此程序介绍如何断开和重新加入端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。例如，可以从 40GB 接口 划分为四个 10GB 端口，或从 200GB 接口划分为四个 25GB 端口。端口的确切大小和数量取决于型号。

更改会立即生效；您不需要部署到设备。在中断或重新加入后，您无法回滚到之前的接口状态。

开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 在中断或重新加入之前，接口不能用于以下对象：
  - 故障切换链路

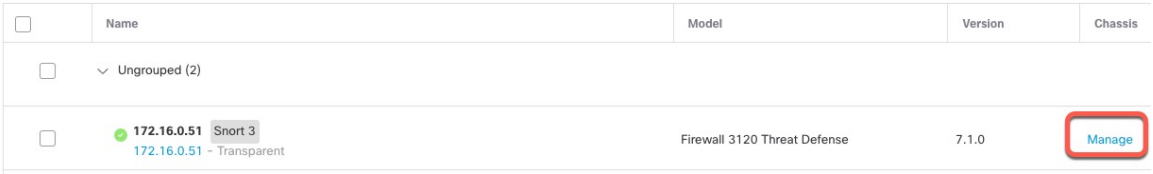
- 集群控制链路
- 拥有一个子接口
- EtherChannel 成员
- BVI 成员
- 管理器访问接口

- 中断或重新加入直接用于安全策略中的接口可能会影响配置；但是，操作不会被阻止。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 *259:* 管理机箱



系统将打开设备的 **机箱操作** 页面 （在多实例模式下，此页面称为 **机箱管理器**）。此页面会显示设备的物理接口详细信息。

步骤 2 从 40GB 或更高的接口分支出端口。

a) 点击接口右侧的 **中断**（）。

在确认对话框中点击**是**。如果接口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试分支。

例如，要拆分出 Ethernet2/1 40GB 接口，生成的子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

在接口图形上，断开的端口具有以下外观：

图 *260:* 分支端口



b) 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 *261:* 转到接口页面



c) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 *262:* 查看接口更改

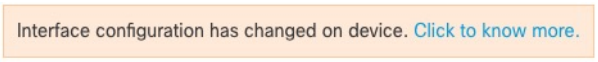
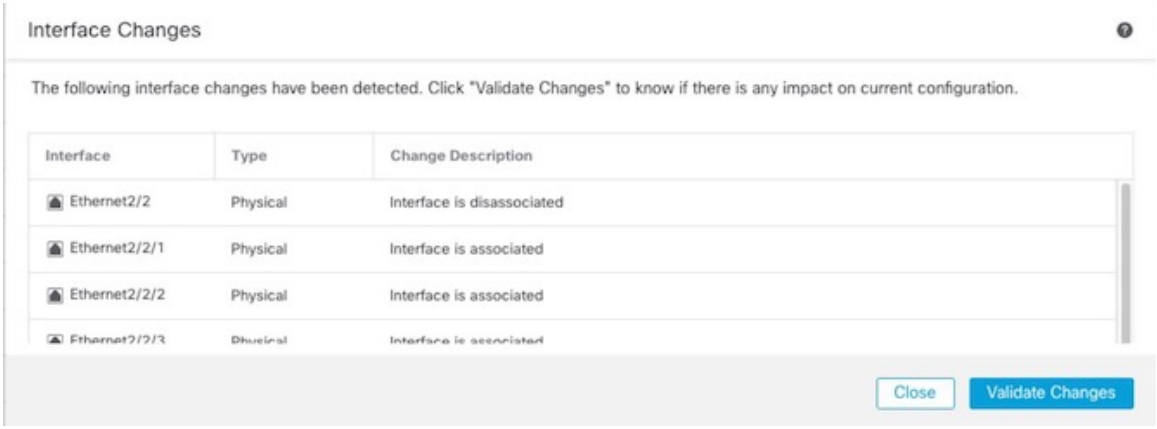


图 *263:* 接口更改



d) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

但是，删除安全策略中使用的接口会对配置造成影响。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

e) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

f) 点击**保存**，以便将接口更改保存到防火墙。

g) 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

您无需部署即可保存分支端口更改。

步骤 3 重新加入分支端口。

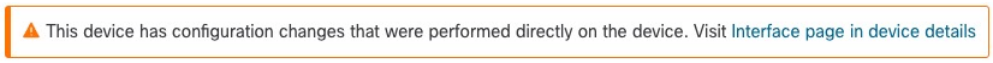
您必须重新加入该接口的所有子端口。

a) 点击接口右侧的 **加入**（）。

在确认对话框中点击**是**。如果有任何子端口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试重新加入。

b) 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 *264:* 转到接口页面



c) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 *265:* 查看接口更改

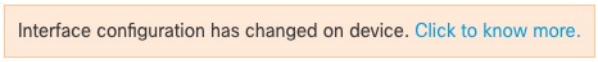
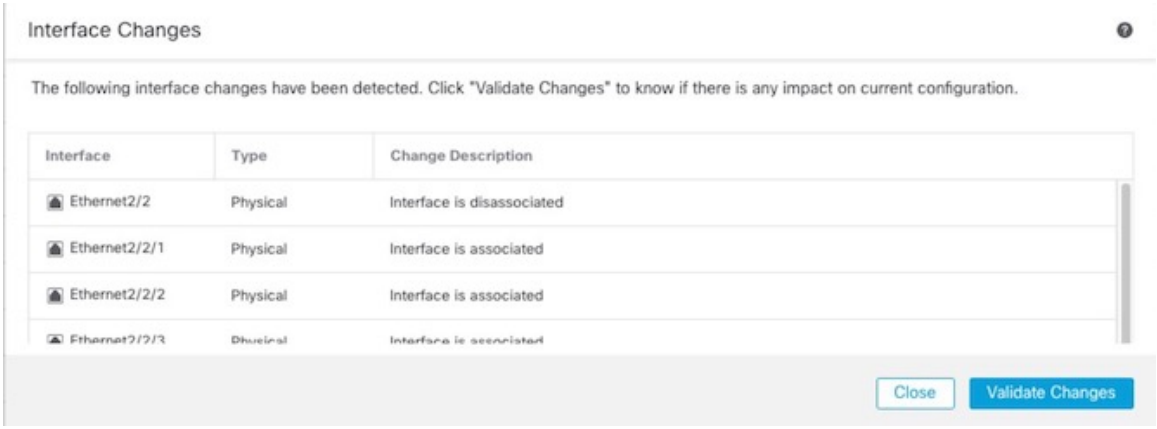


图 *266:* 接口更改



d) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

替换安全策略中使用的子接口可能会对配置造成影响。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

e) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

f) 点击**保存**，以便将接口更改保存到防火墙。

g) 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

您无需部署即可保存分支端口更改。

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新启动。

过程

步骤 1 根据硬件安装指南安装网络模块。

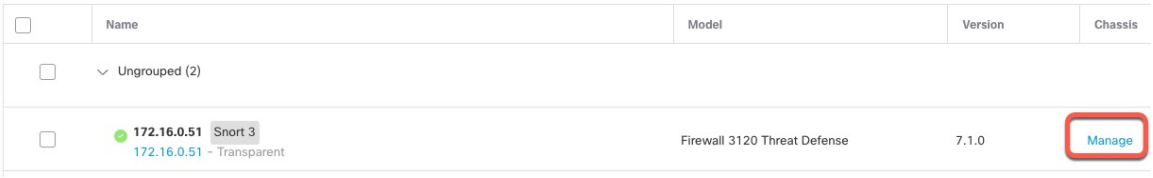
对于集群或高可用性，请在所有节点上安装网络模块。

步骤 2 重新启动防火墙；请参阅关闭或重新启动设备，第 64 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点，第 415 页）或主用设备（请参阅在 Firewall Threat Defense 高可用性对中切换主用对等体，第 361 页），并重新启动之前的控制节点/主用设备。

步骤 3 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 *267:* 管理机箱

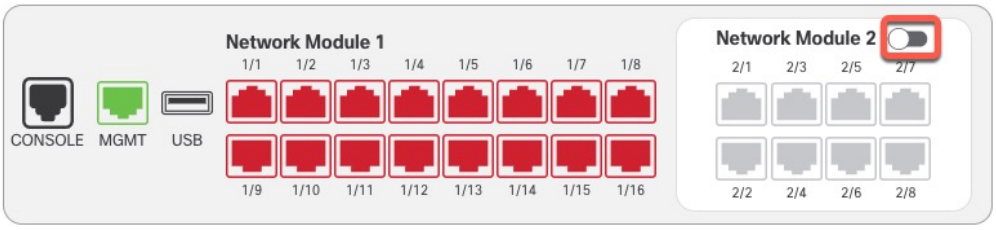


系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 4 点击**同步模块 (Sync Modules)**，使用新的网络模块详细信息更新页面。

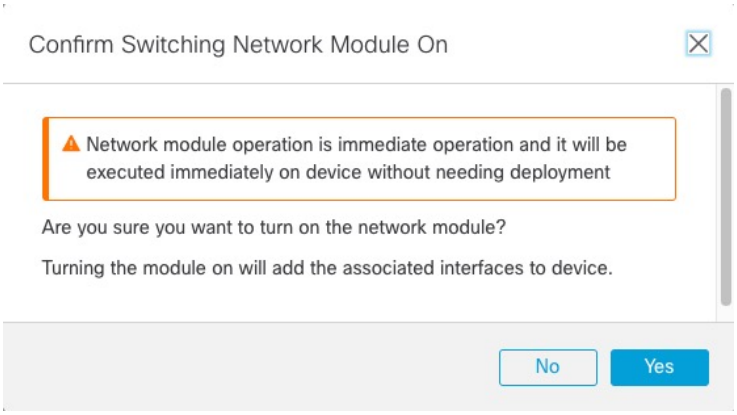
步骤 5 在接口图形上，点击滑块 (⬭) 以启用网络模块。

图 *268:* 启用网络模块



步骤 6 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 *269:* 确认启用



步骤 7 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 *270:* 转到接口页面



步骤 8 （可选）在**接口 (Interfaces)** 页面顶部，您会看到接口配置已更改的消息。您可以点击**点击了解更多 (Click to know more)** 打开**接口更改 (Interface Changes)** 对话框以查看更改。

图 *271:* 查看接口更改

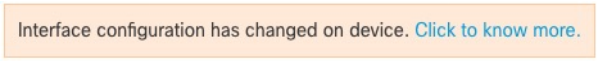
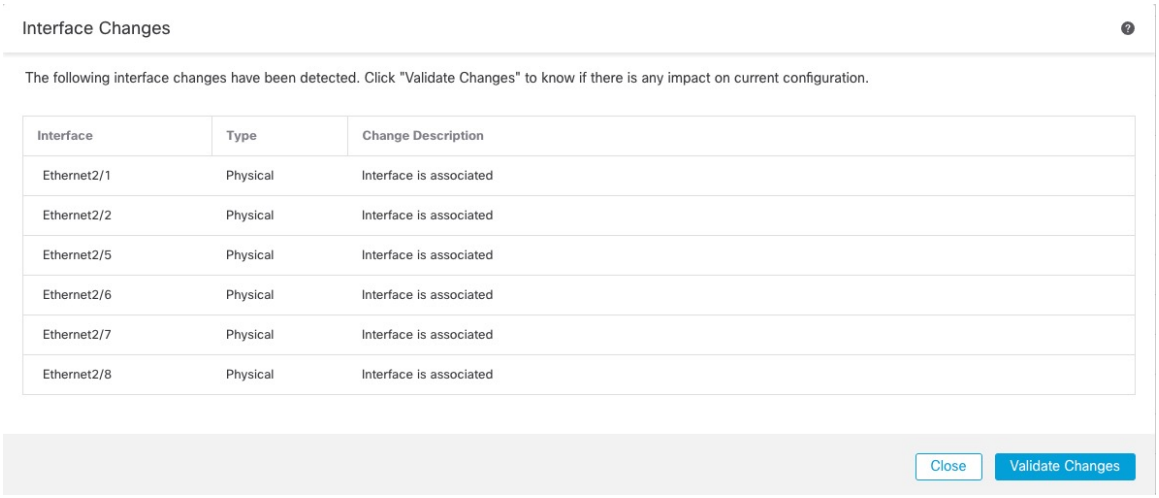


图 *272:* 接口更改



点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。（由于您要添加新模块，因此不应有任何配置影响，所以您无需点击**验证更改 (Validate Changes)**。）

步骤 9 点击**保存**，以便将接口更改保存到防火墙。

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新启动。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。如果集群控制链路/故障转移链路在模块上，则不能禁用该模块。

开始之前

过程

步骤 1 对于集群或高可用性，请执行以下步骤。

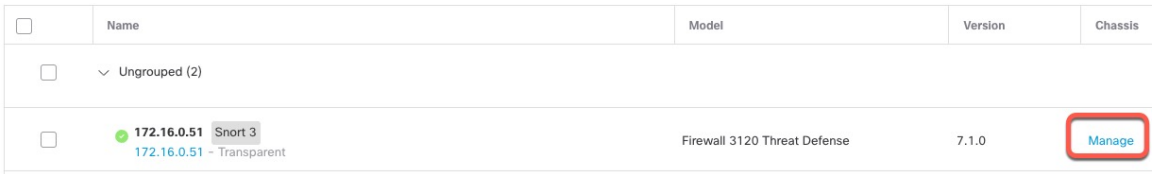
- **集群 (Clustering)** - 确保要执行热插拔的设备是数据节点（请参阅更改控制节点，第 415 页）；然后中断节点，使其不再位于集群中。请参阅中断节点，第 412 页。

  在执行热插拔后，您需要将节点添加回集群。或者，您可以在控制节点上执行所有操作，然后网络模块更改将同步到所有数据节点。但在热插拔期间，您将无法在所有节点上使用这些接口。

- **高可用性 (High Availability)** - 要在禁用网络模块时避免故障切换，请执行以下操作：
  - 如果故障切换链路位于网络模块上，则必须中断高可用性。请参阅中断高可用性对，第 365 页。不允许禁用具有主动故障转移链路的网络模块。
  - 对网络模块上的接口禁用接口监控。请参阅配置备用 IP 地址和接口监控，第 359 页。

步骤 2 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

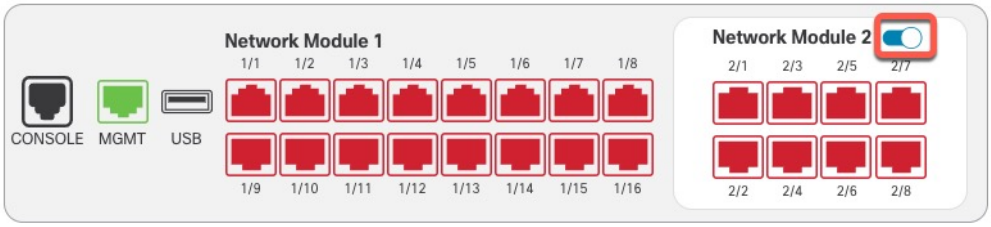
图 *273:* 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 3 在接口图形上，点击滑块 ( ) 以禁用网络模块。

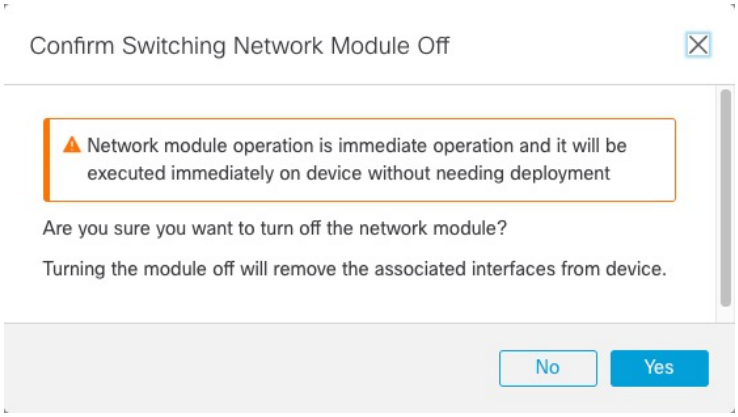
图 *274:* 禁用网络模块



不要在**接口 (Interfaces)** 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

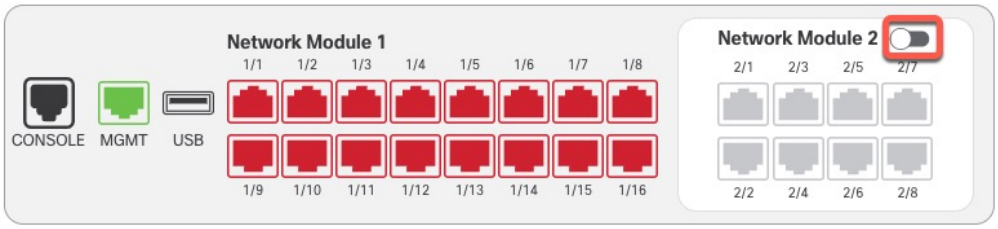
图 *275:* 确认禁用



步骤 5 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。

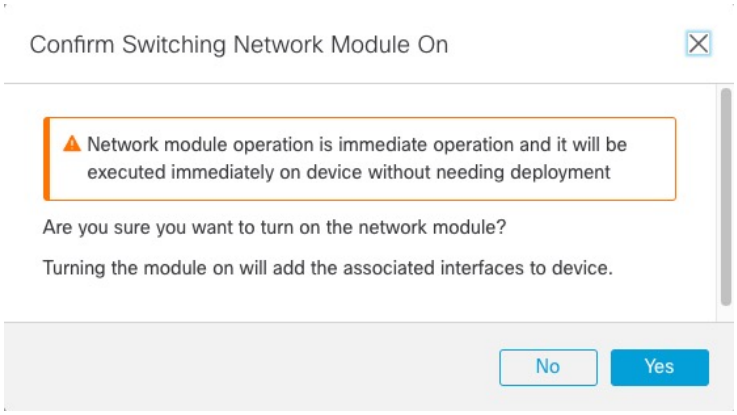
步骤 6 在 防火墙管理中心 中，通过点击滑块 () 来启用新模块。

图 *276:* 启用网络模块



步骤 7 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 *277:* 确认启用



步骤 8 对于集群或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 将节点添加回集群。请参阅添加新的集群节点，第 410 页。
- **高可用性 (High Availability)** -
  - 如果您中断了高可用性，则要重新构建高可用性。请参阅添加高可用性对，第 356 页。
  - 为网络模块上的接口重新启用接口监控。请参阅配置备用 IP 地址和接口监控，第 359 页。

将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新启动。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。

开始之前

对于高可用性，如果故障切换链路在模块上，则不能禁用该网络模块。您必须中断高可用性（请参阅中断高可用性对，第 365 页），这意味着您会在重新启动主用设备时遇到停机。设备完成重新启动后，您可以重新设置高可用性。

过程

步骤 1 对于集群或高可用性，请执行以下步骤。

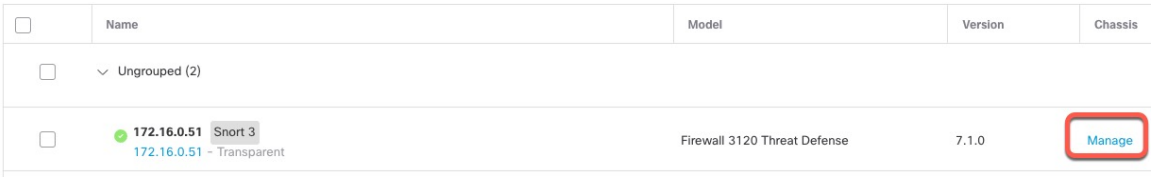
- **群集** - 为避免停机，您可以一次中断每个节点，使其在执行网络模块更换时不再位于集群中。请参阅中断节点，第 412 页。

  执行替换后，您需要将节点添加回集群。

- **高可用性** - 要在更换网络模块时避免故障转移，请对网络模块上的接口禁用接口监控。请参阅配置备用 IP 地址和接口监控，第 359 页。

步骤 2 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

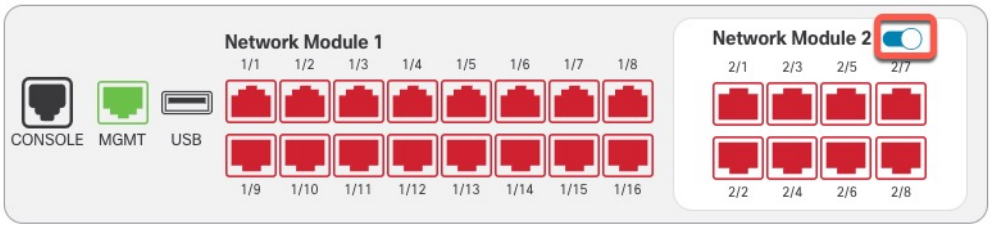
图 *278:* 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 3 在接口图形上，点击滑块 () 以禁用网络模块。

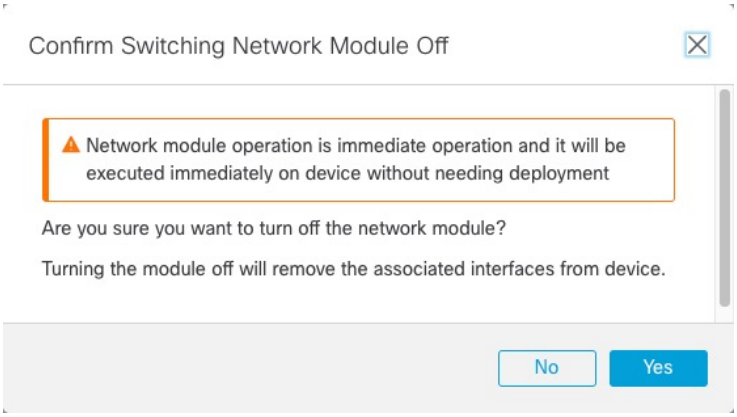
图 *279:* 禁用网络模块



不要在**接口 (Interfaces)** 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 *280:* 确认禁用



步骤 5 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。

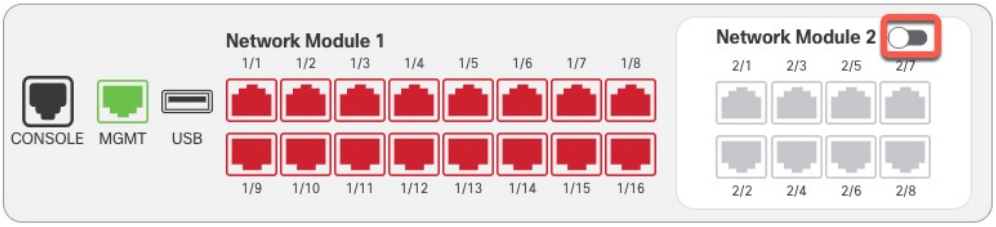
步骤 6 重新启动防火墙；请参阅关闭或重新启动设备，第 64 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点，第 415 页）或主用设备（请参阅在 Firewall Threat Defense 高可用性对中切换主用对等体，第 361 页），并重新启动之前的控制节点/主用设备。

步骤 7 在 防火墙管理中心 中，点击**同步模块 (Sync Modules)** 以便使用新的网络模块详细信息来更新页面。

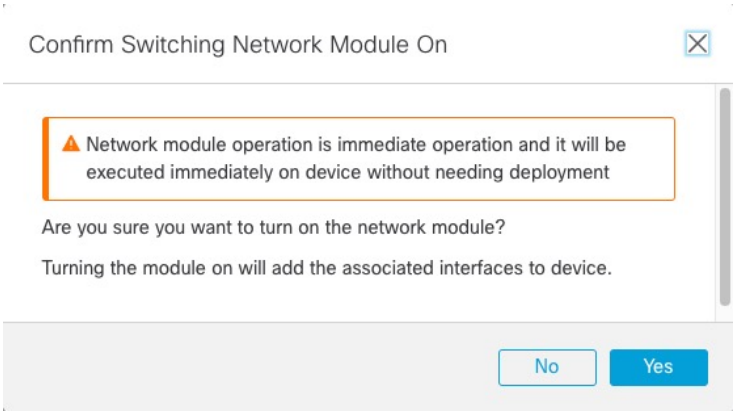
步骤 8 通过点击滑块启用新模块 ()。

图 ***281:*** 启用网络模块



步骤 9 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 ***282:*** 确认启用



步骤 10 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 ***283:*** 转到接口页面



步骤 11 如果网络模块的接口较少：

a) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 ***284:*** 查看接口更改

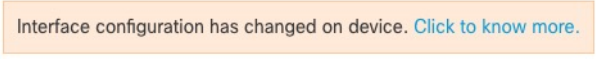
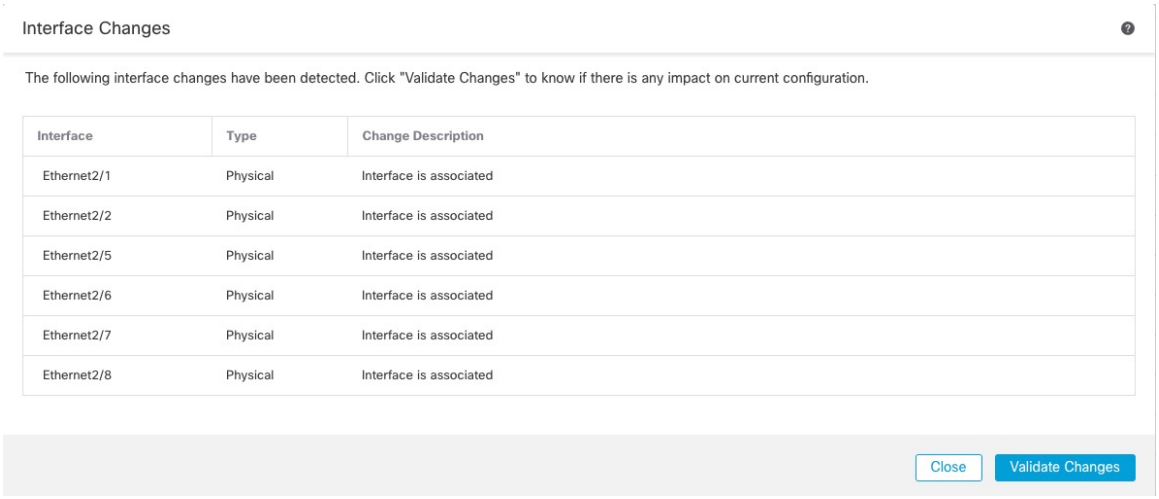


图 *285:* 接口更改



b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

c) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

步骤 12 要更改接口速度，请参阅 启用物理接口并配置以太网参数，第 716 页。

默认速度设置为“检测 SFP”，用于检测已安装的 SFP 的正确速度。仅当您手动将速度设置为特定值并且现在需要新的速度时，才需要修复速度。

步骤 13 点击**保存**，以便将接口更改保存到防火墙。

步骤 14 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

无需部署即可保存网络模块更改。

步骤 15 对于集群或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 将节点添加回集群。请参阅添加新的集群节点，第 410 页。
- **高可用性 (High Availability)** - 对网络模块上的接口重新启用接口监控。请参阅配置备用 IP 地址和接口监控，第 359 页。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新启动。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。

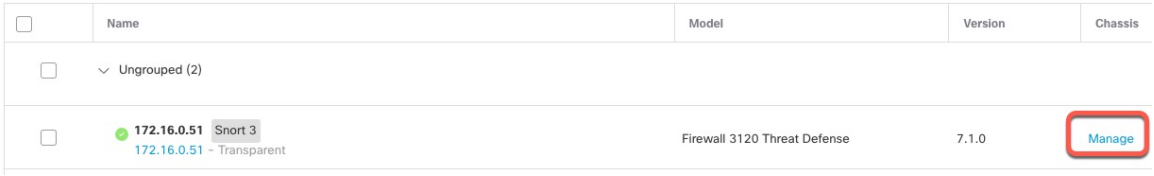
开始之前

对于集群或高可用性，请确保集群/故障转移链路不在网络模块上。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

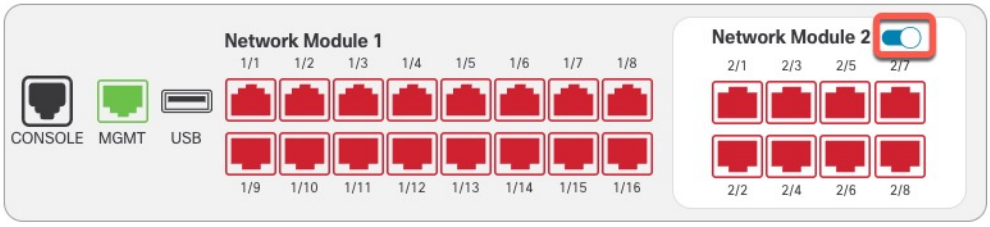
图 *286:* 管理机箱



系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

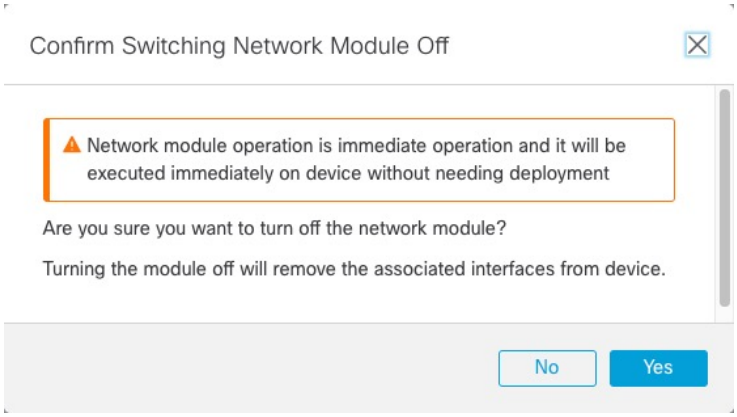
步骤 2 在接口图形上，点击滑块 () 以禁用网络模块。

图 *287:* 禁用网络模块



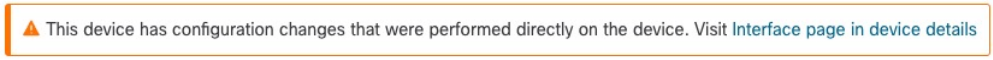
步骤 3 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 *288:* 确认禁用



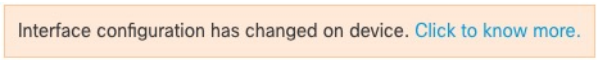
步骤 4 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 *289:* 转到接口页面



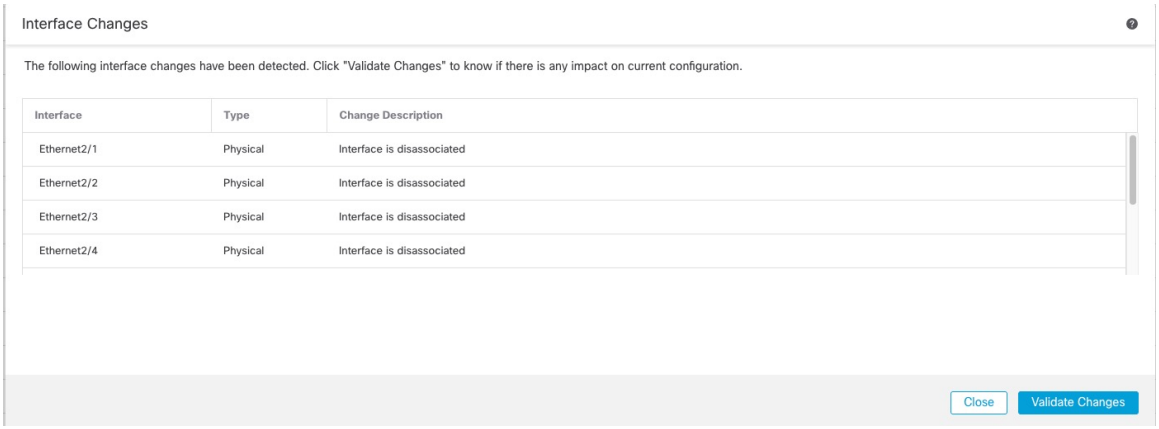
步骤 5 在**接口 (Interfaces)** 页面顶部，您会看到接口配置已更改的消息。

图 *290:* 查看接口更改



a) 点击**点击了解更多 (Click to know more)** 打开**接口更改 (Interface Changes)** 对话框以查看更改。

图 *291:* 接口更改



b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

c) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

步骤 6 点击**保存**，以便将接口更改保存到防火墙。

步骤 7 如果您必须更改任何配置，请转至**部署 (Deploy)** > **部署 (Deployment)** 并部署策略。

步骤 8 重新启动防火墙；请参阅关闭或重新启动设备，第 64 页。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅更改控制节点，第 415 页）或主用设备（请参阅在 Firewall Threat Defense 高可用性对中切换主用对等体，第 361 页），并重新启动之前的控制节点/主用设备。

合并管理和诊断接口

Firewall Threat Defense 7.4 及更高版本支持合并的管理和诊断接口。如果有任何使用诊断接口的配置，则不会自动合并接口，您需要执行以下程序。此程序要求您确认配置更改，在某些情况下，需要手动修复配置。

备份/恢复和 防火墙管理中心 配置回滚功能可保存和恢复合并状态（非合并或合并）。例如，如果合并接口，然后恢复之前的非合并配置，则恢复的配置将处于非合并状态。

下表显示了旧诊断接口上的可用配置，以及完成合并的方式。

表 *54:* 防火墙管理中心 合并管理接口支持

旧版诊断接口配置	合并行为	在管理接口上受支持？
接口		“管理”接口现在在**接口**页面上以只读模式显示。
• IP 地址	需要手动删除。	改为使用当前的管理 IP 地址。 对于高可用性和集群，管理接口不支持备用 IP 地址或 IP 地址池；每台设备有自己的IP地址，故障转移期间将保持这些地址。因此，不能使用单个管理 IP 地址与当前主用/控制设备通信。 使用 **configure network ipv4** 或 **configure network ipv6** 命令在 CLI 中设置。
• 名称“诊断”	自动更改为“管理”。 **注释** 任何其他接口都不能命名为“管理”。您必须更改名称才能继续合并。	更改为“管理”。

旧版诊断接口配置	合并行为	在管理接口上受支持？
静态路由	需要手动删除。	**不支持**。 管理接口具有与数据接口不同的 Linux 路由表。Firewall Threat Defense 实际上有两个“数据”路由表：一个用于数据接口，另一个用于管理专用接口（过去包括“诊断”接口，但也包括设置为管理专用的任何接口）。根据流量类型， Firewall Threat Defense 会检查一个路由表，然后回退到另一个路由表。此路由查找不再包括诊断接口，也不包括管理接口的 Linux 路由表。有关详细信息，请参阅管理流量的路由表，第 1098 页。 您可以使用 **configure network static-routes** 命令在 CLI 中为 Linux 路由表添加静态路由 **注释** 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认路由。
动态路由	需要手动删除。	**不支持**。
HTTP 服务器	无更改。	**不支持**。 此设置在合并后的设备上不再有效，但不会从平台设置中删除。平台设置可用于多台设备，其中有一些可能尚未合并。
ICMP	无更改。	**不支持**。 此设置在合并后的设备上不再有效，但不会从平台设置中删除。平台设置可用于多台设备，其中有一些可能尚未合并。
系统日志服务器	自动改为管理接口。	是。 系统日志服务器配置已具有从管理接口发送系统日志的选项（从 6.3 开始）。如果您特意为系统日志选择了诊断接口，系统会将其改为使用管理接口。 **注释** 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 **注释** 合并的管理接口不支持安全系统日志。
SMTP	无更改。	**不支持**。 Firewall Threat Defense 仅检查 SMTP 服务器的数据路由表，因此不能使用管理接口或任何其他仅管理接口。有关详细信息，请参阅管理流量的路由表，第 1098 页。

旧版诊断接口配置	合并行为	在管理接口上受支持？
SNMP	自动改为管理接口。	是。 SNMP 主机配置已具有允许在管理接口上使用 SNMP 主机的选项（从 6.3 开始）。如果您特意为 SNMP 选择了诊断接口，系统会将其改为使用管理接口。 **注释** 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。
RADIUS 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。 **注释** 如果您指定了路由查找来查找源接口，则 Firewall Threat Defense 将无法再从管理专用接口发送流量；您必须明确选择“管理”接口作为源接口。不能使用其他管理专用接口。
AD 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。 **注释** 如果您指定了路由查找来查找源接口，则 Firewall Threat Defense 将无法再从管理专用接口发送流量；您必须明确选择“管理”接口作为源接口。不能使用其他管理专用接口。
DDNS	需要手动删除。	**不支持**。
DHCP 服务器	需要手动删除。	**不支持**。
DNS 服务器	自动改为管理接口。	是。 如果选中**同时通过诊断接口启用 DNS 查找**复选框，系统会将其改为使用管理接口。不选择任何接口或选中**同时通过诊断/管理接口启用 DNS 查找**复选框时，路由查找会发生变化：Firewall Threat Defense 仅使用数据路由表，不会回退到使用管理专用路由表。因此，除管理接口外，不能对 DNS 使用管理专用接口。 **注释** 管理接口还具有仅用于其管理流量的单独DNS查找设置。使用**configure network dns** 命令在 CLI 中设置。
FlexConfig	需要手动删除。	**不支持**。

开始之前

- 要查看设备的当前模式，请在 Firewall Threat Defense CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

- 对于高可用性对和集群，请在主用/控制设备中执行此任务。合并的配置将自动复制到备用/数据设备。

过程

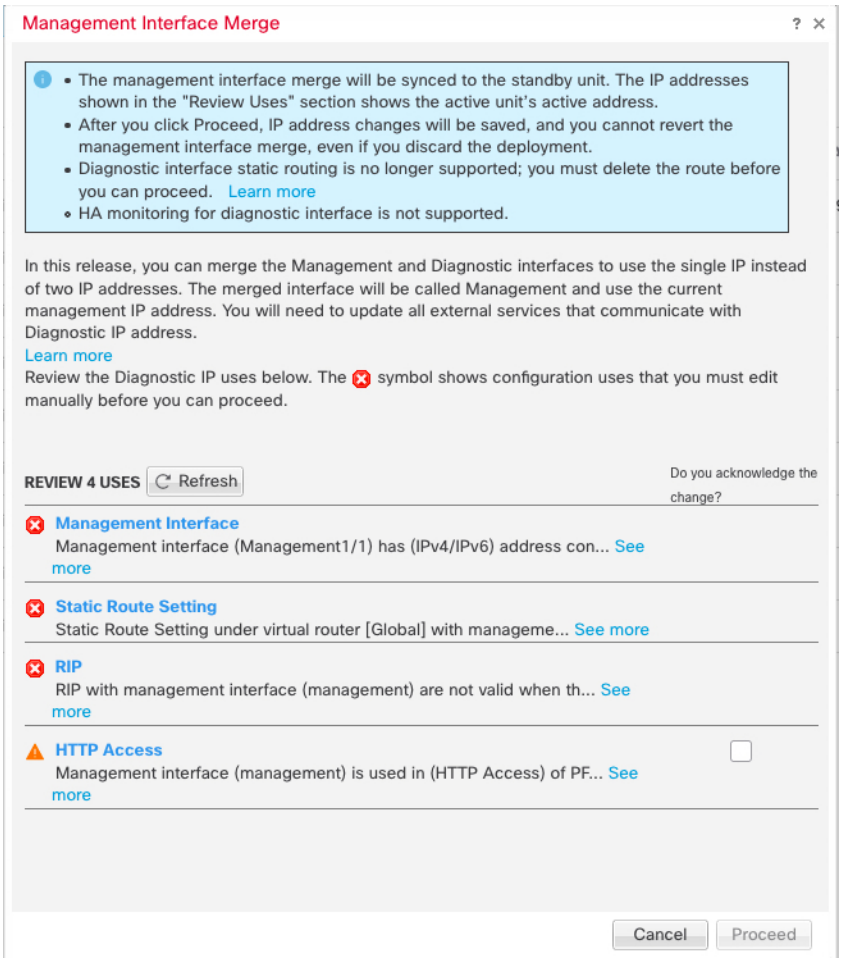
步骤 1 选择 **设备** > **设备管理**，然后点击 **编辑** ()Firewall Threat Defense。系统默认选择**接口 (Interfaces)** 页面。。

步骤 2 编辑诊断接口，并删除 IP 地址。

在删除诊断 IP 地址之前，您无法完成合并。

步骤 3 点击**所需管理接口操作**区域中的**管理接口合并**。

管理接口合并 (Management Interface Merge) 对话框显示配置中所有使用诊断接口的情况。任何需要您手动删除或更改配置的情况将显示警告图标。在您的设备上不再有效的平台设置标有警告图标，需要您确认。



步骤 4 如果需要手动删除或更改任何列出的配置，请执行以下操作。

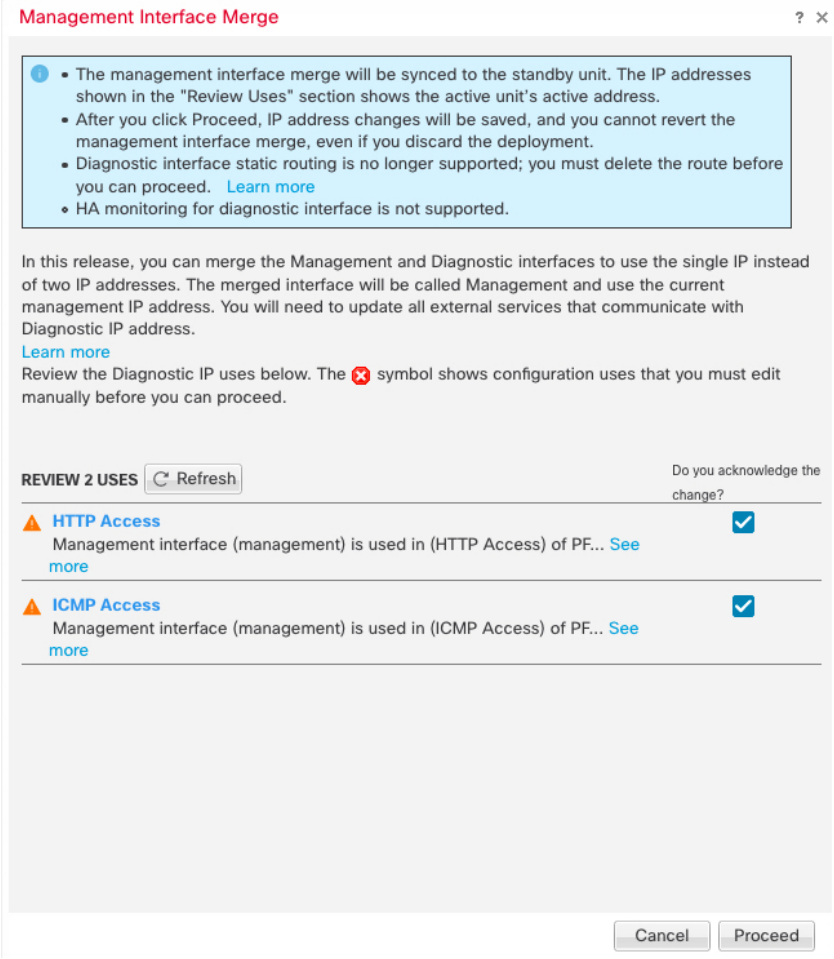
a) 点击**取消**以关闭**管理接口合并**对话框。

b) 导航至功能区域。然后，您可以删除项目，或者改为选择数据接口。

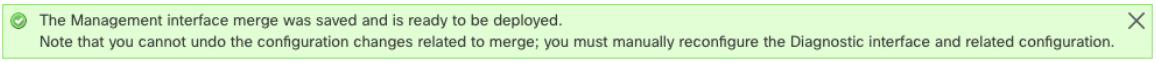
c) 重新打开**管理接口合并**对话框。

此时不应再显示任何警告。

步骤 5 对于每个配置警告，请点击**您是否确认更改？**列中的框，然后点击**继续**。



合并配置后，您会看到成功横幅：



步骤 6 部署新的合并配置。

注意
部署合并的配置后，可以从防火墙管理中心中取消合并接口；但是，诊断接口必须手动重新配置。请参阅取消合并管理接口，第 749 页。此外，如果恢复未合并配置，或回退到未合并配置，设备将恢复为该未合并配置。

合并后，管理接口显示在**接口**页面上，但它是只读状态。

步骤 7 合并后，如果有任何与诊断接口通信的外部服务，您需要将其配置更改为使用管理接口 IP 地址。

例如：

- SNMP 客户端

- RADIUS 服务器 - RADIUS 服务器通常会验证传入流量的 IP 地址，因此您需要将该 IP 地址更改为管理地址。此外，对于高可用性对，您需要允许可同时使用主管理 IP 地址和辅助管理 IP 地址；诊断接口用于支持与主用设备一起使用的单个“浮动”IP地址，但管理接口不支持该功能。

取消合并管理接口

Firewall Threat Defense 7.4 及更高版本支持合并的管理和诊断接口。如果您需要取消合并您的接口，请执行此程序。建议您在将网络迁移到合并模式部署时暂时使用未合并模式。可能并非所有未来版本都支持单独的管理接口和诊断接口。

取消合并接口不会恢复原始诊断配置（如果您是先升级然后再合并接口）。您需要手动重新配置诊断接口。此外，管理接口现在命名为“management”；不能将其重命名为“diagnostic”。

或者，如果您使用备份功能保存旧的未合并配置，则可以恢复该配置，或者您可以使用或者 防火墙管理中心 配置回滚功能，设备将处于未合并状态，诊断配置保持不变。

开始之前

- 要查看设备的当前模式，请在 Firewall Threat Defense CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

- 对于高可用性对和集群，请在主用/控制设备中执行此任务。合并的配置将自动复制到备用/数据设备。

过程

步骤 1 选择 **设备** > **设备管理**，然后点击 **编辑** ()Firewall Threat Defense。系统默认选择**接口 (Interfaces)** 页面。。

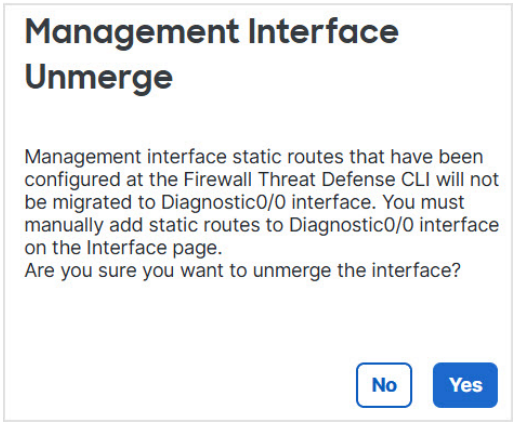
步骤 2 对于管理接口，请点击 **取消合并管理接口** ()。

图 *292:* 管理接口选择



步骤 3 点击**是 (Yes)** 确认要取消合并接口。

图 *293:* 取消合并确认



步骤 4 部署新的未合并配置。

注释
如果恢复合并配置，或回退到合并配置，设备将恢复为该合并配置。

合并后，管理接口将显示在 **接口** 页面上，并且不再在该页面上配置。

接口的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
同步设备现在称为**同步接口**	7.7.0	7.7.0	**同步设备**更改为**同步接口**，以指明此功能仅适用于接口更改。此功能不再检测对管理器访问界面所做的更改；请参阅**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问详细信息：配置 (Manager Access Details: Configuration)**。 在恢复配置模式下在诊断 CLI 上执行的其他带外配置更改需要在**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **运行状况 (Health)** > **带外状态 (Out of Band Status)**中查找。 新增/修改的屏幕： **设备** > **设备管理** > **接口**
环回和管理类型接口组对象	7.4.0	7.4.0	现在，您可以创建仅包含管理专用接口或仅包含环回接口的接口组对象。然后，您可以将这些组用于管理功能，例如 DNS 服务器、HTTP 访问或 SSH。支持环回接口的任何功能都支持环回组。请注意，DNS 不支持管理接口。 新增/修改的屏幕： **对象** > **对象管理** > **接口** > **添加** > **接口组**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
合并的管理接口和诊断接口	7.4.0	7.4.0	对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。 如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 新增/修改的屏幕： **设备** > **设备管理** > **接口** 新增/修改的命令：**show management-interface convergence**
Cisco Secure Firewall 3100固定端口上的默认前向纠错 (FEC) 从第 74 条 FC-FEC 更改为第 108 条 RS-FEC，适用于 25 GB+ SR、CSR 和 LR 收发器	7.2.4	7.2.4	当您在 Cisco Secure Firewall 3100 固定端口上将 FEC 设置为自动时，对于 25 GB+ SR、CSR 和 LR 收发器，默认类型现在设置为 Clause 108 RS-FEC，而不是 Clause 74 FC-FEC。
对 Firepower 2100，Cisco Secure Firewall 3100 的 LLDP 支持	7.2.0	7.2.0	您可以为 Firepower 2100 和 Cisco Secure Firewall 3100 接口启用链路层发现协议 (LLDP)。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **硬件配置 (Hardware Configuration)** > **网络连接 (Network Connectivity)** 新增/修改的命令：**show lldp status, show lldp neighbors, show lldp statistics**
为 Cisco Secure Firewall 3100暂停流量控制的帧	7.2.0	7.2.0	如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **硬件配置 (Hardware Configuration)** > **网络连接 (Network Connectivity)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持热插拔 Cisco Secure Firewall 3100 的网络模块	7.1.0	7.1.0	您可以在防火墙通电时在 Cisco Secure Firewall 3100 上添加或删除网络模块。要将某个模块替换为相同类型的另一个模块，则无需重新启动。初始启动后，添加模块、永久删除模块或用新类型替换模块都需要重新启动。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **机箱操作 (Chassis Operations)**
支持 Cisco Secure Firewall 3100 的前向纠错	7.1.0	7.1.0	Cisco Secure Firewall 3100 25 Gbps 接口支持前向纠错 (FEC)。FEC 默认为启用并会设为“自动”(Auto)。 新增/修改的屏幕： **设备** > **设备管理** > **接口** > **编辑物理接口** > **硬件配置**
支持基于 SFP 为 Cisco Secure Firewall 3100 设置速度	7.1.0	7.1.0	Cisco Secure Firewall 3100 支持基于安装的 SFP 的接口速度检测。检测 SFP 默认为启用。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。 新增/修改的屏幕： **设备** > **设备管理** > **接口** > **编辑物理接口** > **硬件配置**
对 Firepower 1100 的 LLDP 支持	7.1.0	7.1.0	您可以为 Firepower 1100 接口启用链路层发现协议 (LLDP)。 新增/修改的屏幕：**设备** > **设备管理** > **接口** > **硬件配置** > **LLDP** 新增/修改的命令：**show lldp status, show lldp neighbors, show lldp statistics**
接口自动协商现在独立于速度和双工设置，改进了接口同步	7.1.0	7.1.0	接口自动协商现在独立于速度和双工设置此外，当您在防火墙管理中心中同步接口时，可以更有效地检测硬件更改。 新增/修改的屏幕：**设备** > **设备管理** > **接口** > **硬件配置** > **速度** 支持的平台：Firepower 1000、2100、Cisco Secure Firewall 3100
Firepower 1100 / 2100 系列光纤接口现在支持禁用自动协商。	6.7.0	6.7.0	现在，您可以配置 Firepower 1100/2100 系列光纤接口以禁用流量控制和链路状态协商。 以前，在这些设备上设置光纤接口速度（1000 或 10000 Mbps）时，会自动启用流量控制和链路状态协商。您无法禁用它。 现在，您可以取消选择**自动协商 (Auto-negotiation)** 并将速度设置为 1000，以禁用流量控制和链路状态协商。您无法在 10000 Mbps 时禁用协商。 新增/修改的屏幕： **设备** > **设备管理** > **接口** > **硬件配置** > **速度**



第 15 章

常规防火墙接口

本章包括常规防火墙 Firewall Threat Defense 接口配置，包括 EtherChannel、VLAN 子接口、IP 寻址等。

注释 有关 Firepower 4100/9300上的初始接口配置，请参阅配置接口，第 310 页。

- 常规防火墙接口的要求和前提条件，第 753 页
- 配置交换机端口，第 754 页
- 配置环回接口，第 765 页
- 配置 VLAN 子接口和 802.1Q 中继，第 770 页
- 配置 VXLAN 接口，第 774 页
- 配置路由和透明模式接口，第 789 页
- 配置高级接口设置，第 814 页
- 常规防火墙接口的历史记录，第 824 页

常规防火墙接口的要求和前提条件

型号支持

Firewall Threat Defense

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置交换机端口

可以将每个 1010/1210/1220 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。这部分包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将它们分配给 VLAN。本节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

关于交换机端口

本部分介绍具有第 2 层交换机的型号的交换机端口。

了解交换机端口和接口

端口和接口

对于每个物理接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- 物理防火墙接口 - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。 在透明模式下，这些接口是桥接组成员，用于在第 2 层同一网络上的接口之间转发流量，使用已配置的安全策略应用防火墙服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。您也可将这些接口配置为仅 IPS 模式（被动接口）。
- 物理交换机端口 - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 Firewall Threat Defense安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。默认情况下，以太网 1/2 及更高 配置为 VLAN 1 上的接入交换机端口。不能将 管理接口配置为交换机端口。
- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口仅 IPS 接口（内联集和被动接口）或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 Firewall Threat Defense 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略 Firewall Threat Defense的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

PoE 适用于以下端口：

- Cisco Secure Firewall 1210CP - 以太网 1/5、1/6、1/7 和 1/8，使用 IEEE 802.3af (PoE)、802.3at (PoE+)和 802.3bt（PoE++ 和 Hi-PoE），每个端口最高 90 瓦，合计最高 120 瓦。

注释 1010E、220、1210CE 和 1220CX 不支持 PoE。

PoE+ 或更高版本使用链路层发现协议 (LLDP) 来协商功率级别。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

Auto-MDI/MDIX 功能

如果是所有交换机口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

交换机端口的前提条件

型号支持

- Cisco Secure Firewall 200
- Firepower 1010
- Cisco Secure Firewall 1210/1220

交换机端口准则和限制

集群

- 无集群支持。
- 使用时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口 (SVI)

- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。VLAN 1 保留用于交换机端口的逻辑 VLAN 接口。
- MAC 地址：

- 路由防火墙模式 - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一MAC地址，可手动分配MAC地址。请参阅配置MAC地址，第 820 页。
- 透明防火墙模式 - 每个 VLAN 接口都有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 820 页。

桥接组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 等价多路径路由 (ECMP)
- 内联集或被动接口
- EtherChannels-交换机端口不能成为 EtherChannel 的一部分。EtherChannel 中的端口也不支持 PoE。
- 故障转移和状态链路
- 安全组标记 (SGT)

其他准则和限制

- 您最多可以在 Firepower 1010 上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 在 1010上，以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 在 1210 上，以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 在 1220 上，以太网 1/2 至以太网 1/10 交换机端口会被分配给 VLAN 1。
- 在 220 上，以太网 1/2 至以太网 1/10 交换机端口会被分配给 VLAN 1。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置交换机端口和以太网供电

要配置交换机端口和 PoE，请完成以下任务。

启用或禁用交换机端口模式

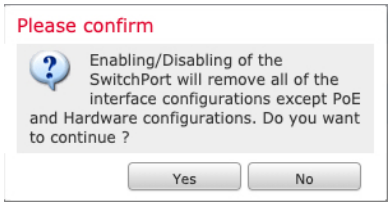
您可以将每个接口单独设置为防火墙接口或交换机端口。默认情况下，以太网 1/1 是防火墙接口，而剩余的以太网接口则配置为交换机端口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**交换机端口 (SwitchPort)** 列中的滑块，设置交换机端口模式，使其显示为 **滑块已启用** (🔵) 或 **滑块已禁用** (⚫)。

默认情况下，交换机端口在 VLAN 1 中会被设为访问模式。您必须手动添加逻辑 VLAN 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 Firewall Threat Defense 安全策略（请参阅配置 VLAN 接口，第 757 页）。您无法将管理接口设置为交换机端口模式。更改交换机端口模式时，会删除所有不支持的配置：



此外，如果该接口已经启用，系统也会将其禁用。请确保重新启用该接口。

配置 VLAN 接口

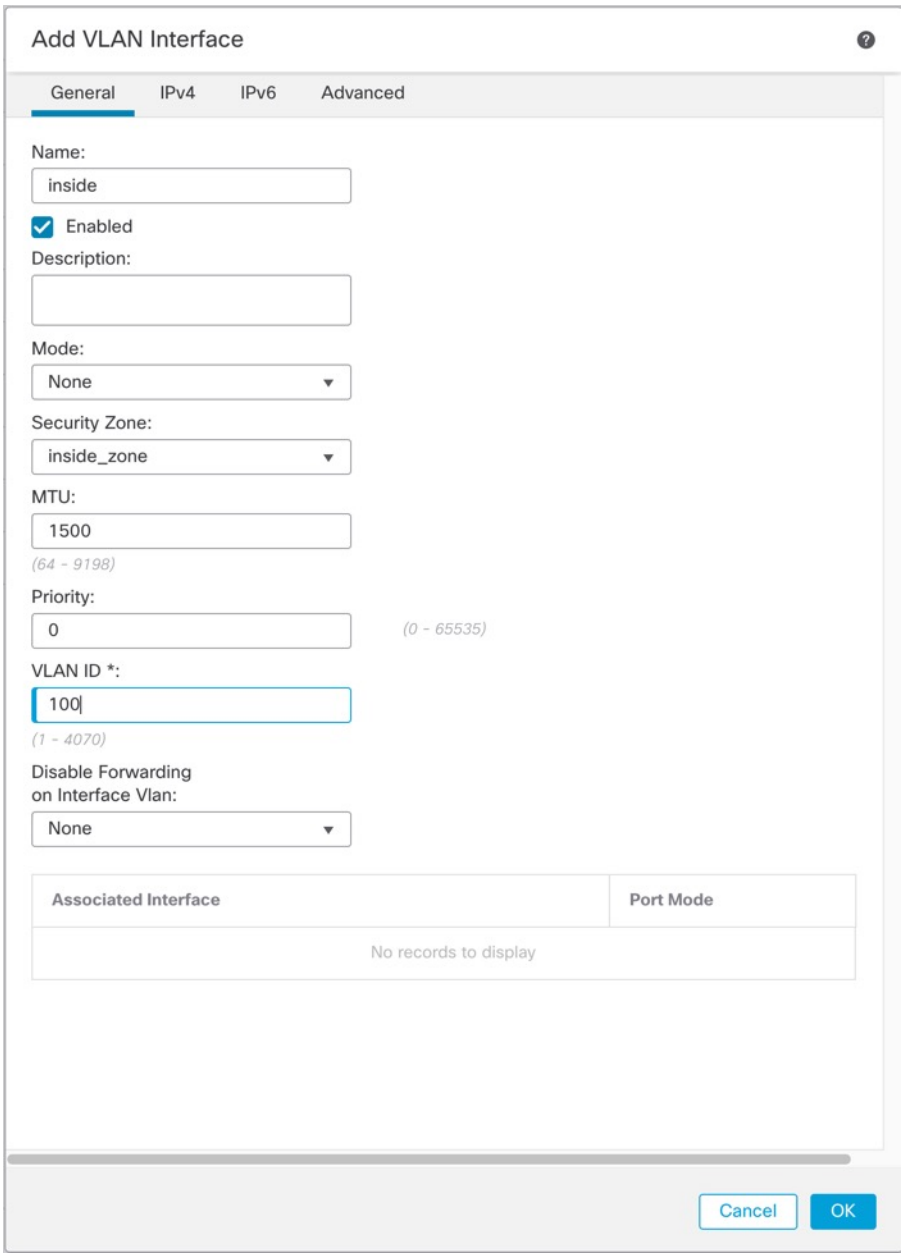
本节介绍如何配置 VLAN 接口以用于关联交换机端口。默认情况下，交换机端口分配给 VLAN1；但是，您必须手动添加逻辑 1 接口（或为这些交换机端口设置的任何 VLAN），以便路由流量并参与 Firewall Threat Defense 安全策略。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**。

步骤 3 在 **常规**上，设置以下 VLAN 特定参数：



如果编辑的是现有 VLAN 接口，则 **关联接口** 表会显示此 VLAN 上的交换机端口。

a) 设置 **VLAN ID**，介于 1 和 4070 之间，不包括 3968 到 4047 范围内的ID（保留供内部使用）。

保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

b) （可选） 为 **接口 VLAN 上的禁用转发** 选择 VLAN ID，以禁用转发到另一个 VLAN。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以禁用家庭 VLAN 上的转发；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

步骤 4 要完成接口配置，请参阅以下过程之一：

- 配置路由模式接口，第 792 页
- 配置常规网桥组成员接口参数，第 797 页

步骤 5 点击**确定**。

步骤 6 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。接入端口仅接受未标记流量。启用交换机端口并分配给 VLAN1 的接口如下：

设备型号	交换机端口接口
Cisco Secure Firewall 220	以太网 1/2 至以太网 1/5
Firepower 1010	以太网 1/2 至以太网 1/8
Cisco Secure Firewall 1210	以太网 1/2 至以太网 1/8
Cisco Secure Firewall 1220	以太网 1/2 至以太网 1/10

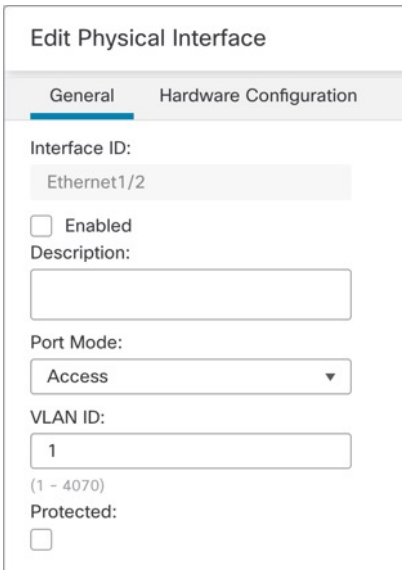
注释 设备不支持在网络中进行环路检测的生成树协议。因此，您必须确保与 Firewall Threat Defense 的任何连接均不会在网络环路中结束。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

图 *294:* 编辑物理接口



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**访问 (Access)**。

步骤 6 在 **VLAN ID** 字段中，设置此交换机端口的 VLAN，范围介于 1 和 4070 之间。

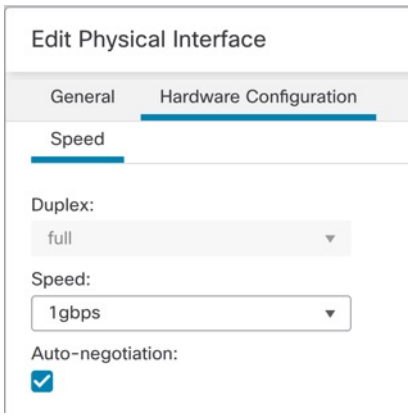
默认的 VLAN ID 为 1。

步骤 7 （可选） 选中**受保护 (Protected)** 复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，当您在交换机端口上启用**受保护 (Protected)** 后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

步骤 8 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

图 *295:* 硬件配置



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

注释
如果通过 50G 电缆连接到该端口的对等交换机不支持自动协商，请确保也在该交换机和威胁防御接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持通过 50G 电缆进行自动协商。因此，要连接该端口，您必须在平台和交换机上禁用默认的自动协商。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将交换机端口配置为中继端口

此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

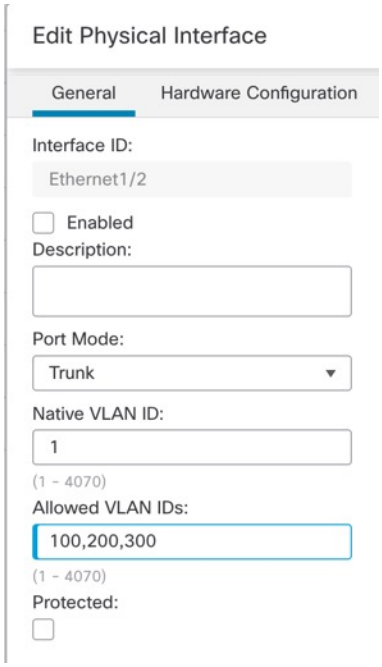
中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 Firewall Threat Defense 设备可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 Firewall Threat Defense 设备从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

图 ***296:*** 设置中继端口模式



步骤 3 选中**启用**复选框以启用此接口。

步骤 4 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 5 将**端口模式 (Port Mode)** 设为**干线 (Trunk)**。

步骤 6 在**本地 VLAN ID (Native VLAN ID)** 字段中，设置此交换机端口的本地 VLAN，范围介于 1 和 4070 之间。

默认的本地 VLAN ID 为 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

步骤 7 在**允许的 VLAN ID (Allowed VLAN IDs)** 字段中，输入此中继端口的 VLAN，范围介于 1 和 4070 之间。

您可以通过以下方式之一识别最多 20 个ID：

- 单一编号 (n)
- 范围 (n-x)
- 用逗号将编号和范围隔开，例如：

  5,7-10,13,45-100

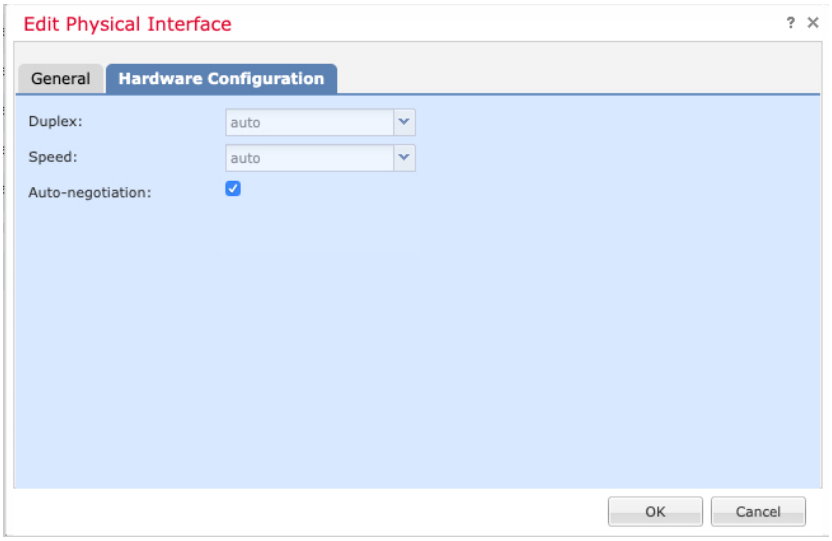
  您可以输入空格而不是逗号。

如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

步骤 8 （可选） 选中**受保护 (Protected)** 复选框以将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，当您在交换机端口上启用**受保护 (Protected)** 后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

步骤 9 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。



选中**自动协商 (Auto-negotiation)** 复选框（默认）以自动检测速度和双工。如果取消选中，您可以手动设置速度和双工：

- **复用**—选择 **全** 或 **半**。
- **速度 (Speed)** - 选择 **10mbps**、**100mbps** 或 **1gbps**。

如果通过 50G 电缆连接到该端口的对等交换机不支持自动协商，请确保也在该交换机和威胁防御接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持通过 50G 电缆进行自动协商。因此，要连接该端口，您必须在平台和交换机上禁用默认的自动协商。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置以太网供电

以太网供电 (PoE) 端口为 IP 电话或无线接入点等设备供电。默认情况下，PoE 处于启用状态。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

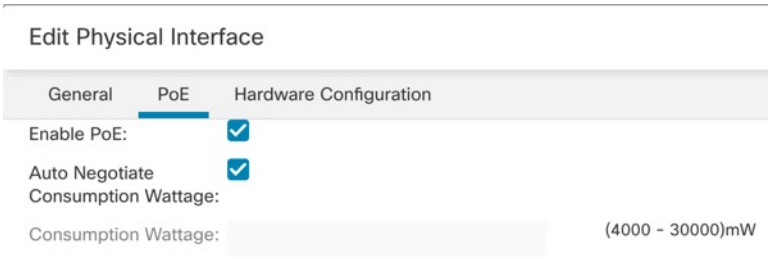
过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击 Firepower 1010 上 Ethernet1/7 或 1/8 的 **编辑** (✎)，或 Secure Firewall 1210CP 。

步骤 3 点击 **PoE**。

图 *297: PoE*



步骤 4 选中**启用 PoE (Enable PoE)** 复选框。

默认情况下，PoE 处于启用状态。

步骤 5 选择自动协商或手动电源。

- **自动协商功耗功率 (Auto Negotiate Consumption Wattage)** - PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。防火墙使用 LLDP 进一步协商正确的瓦数。当连接某个类别的设备时，它会被调配到该等级的最大功率，以防需要使用更多电能。例如，如果您添加请求的功率为 12.95W 的 4 类设备，即使它当前没有使用该功率，系统也会为其分配 30W。某些设备可以重新协商电源需求。如果您知道设备需要的电量少于所分配的电量，则可以手动设置**功耗瓦数**，将电量释放给其他设备。
- **功耗瓦数 (Consumption Wattage)** - 取消选中**自动协商功耗功率 (Auto Negotiate Consumption Wattage)** 复选框以手动设置瓦数，从而以毫瓦为单位手动指定范围从 4000 至 30000 (1010) 或 90000 (1210CP) 的瓦数。如果要手动设置瓦数并禁用 LLDP 协商，请使用此选项。对于手动分配，该类别将在 **show power inline** 输出中显示为**不适用 (n/a)**，因为该类别不用于决定功耗。

  使用 **show power inline** 命令查看当前 PoE 状态。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置环回接口

本节介绍如何配置环回接口。

关于环回接口

环回接口是一种会模拟物理接口的纯软件接口。此接口可通过多个物理接口在IPv4和IPv6上访问。环回接口有助于克服路径故障；它可以从任何物理接口访问，因此，如果其中一个接口发生故障，您可以从另一个接口访问环回接口。

环回接口可用于：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- IPsec 流量分流 - 仅限 Cisco Secure Firewall 1200/3100 /4200 /6100
- NetFlow
- SNMP
- SSH
- 静态和动态 VTI 隧道
- 系统日志

Firewall Threat Defense 可以使用动态路由协议分发环回地址，也可以在对等设备上配置静态路由，以通过 Firewall Threat Defense的物理接口之一到达环回 IP 地址。不能在指定环回接口的 Firewall Threat Defense 上配置静态路由。

相关主题

环回接口的准则和限制，第 766 页
配置环回接口，第 766 页

环回接口的准则和限制

防火墙模式

- 仅在路由模式中受支持。

和集群

- 无集群支持。

其他准则和限制

- 对于从物理接口到环回接口的流量，TCP 序列随机化始终处于禁用状态。

配置环回接口

要为设备添加环回接口：

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 从**添加接口 (Add Interfaces)** 下拉列表中，选择**环回接口 (Loopback Interface)**。

步骤 3 在**常规 (General)** 选项卡中，配置以下参数：

a) **名称 (Name)** - 输入环回接口的名称。

b) **启用 (Enabled)** - 选中此复选框可启用环回接口。

c) **环回 ID (Loopback ID)** - 输入介于 1 和 1024 之间的环回 ID。

d) **说明 (Description)** - 输入环回接口的说明。

步骤 4 配置已路由模式的接口参数。请参阅配置路由模式接口，第 792 页。

对流向环回接口的流量进行速率限制

开始之前

您应该对流向环回接口 IP 地址的流量进行速率限制，以防止系统负载过大。您可以向全局服务策略添加连接限制规则。

过程

步骤 1 创建用于标识流向环回接口 IP 地址的流量的扩展访问列表。

a) 选择**对象** > **访问列表** > **扩展**。

b) 点击 **添加扩展访问列表** 以创建新 ACL。

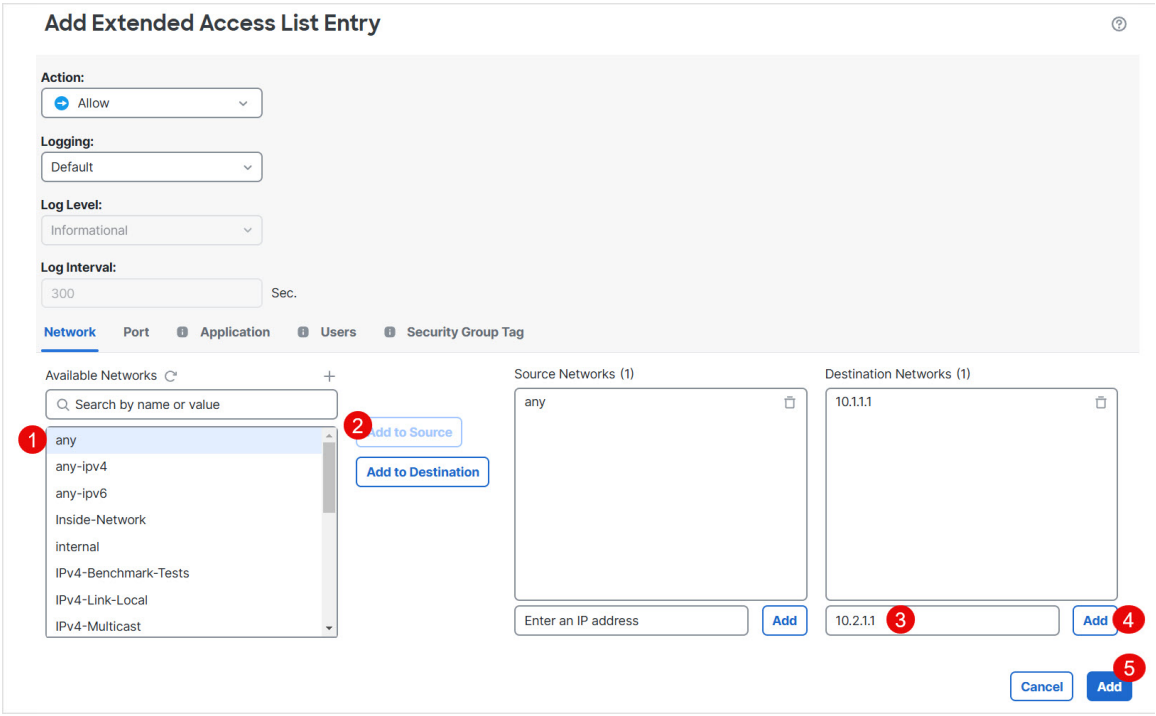
c) 在 **新建扩展访问列表对象** 对话框中，输入 ACL 的名称（不允许使用空格），然后点击 **添加** 以创建新条目。

图 *298:* 命名 *ACL* 并添加条目



d) 在 **网络** 选项卡上配置源地址（任意）和目的地址（环回 IP 地址）。

图 *299:* 源和目标网络



注释

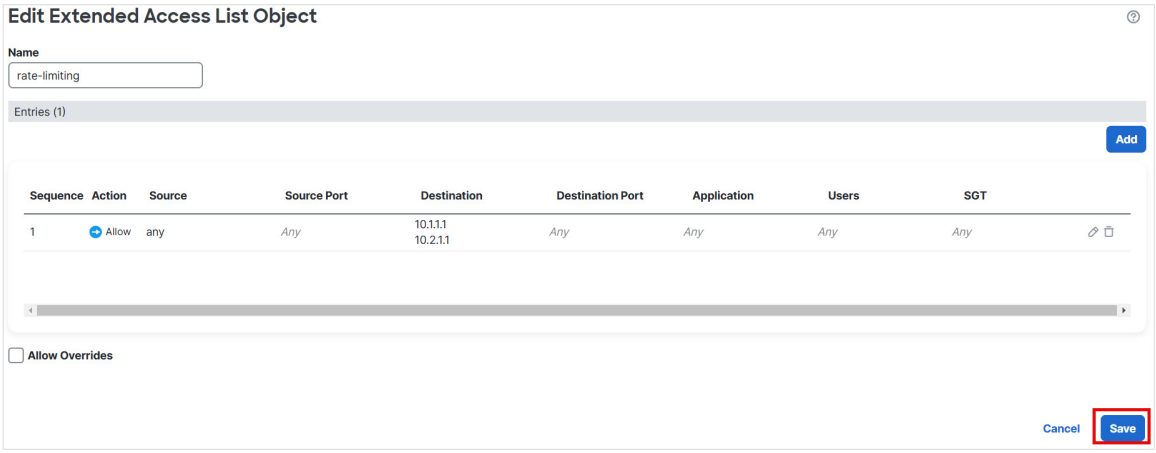
保持默认 **操作** 为 **允许** （匹配），其他设置保持原样。

- 源-从 **可用网络** 列表中选择 **任何**，然后点击 **添加至源**。您还可以通过指定源 IP 地址而不是 **任何**来缩小此访问列表的范围。

- 目标-在 **目标网络** 列表下面的编辑框中输入地址并点击 **添加**。对每个环回接口重复上述操作。

e) 点击 **添加** 以将条目添加至 ACL。
f) 点击 **保存** 以保存 ACL。

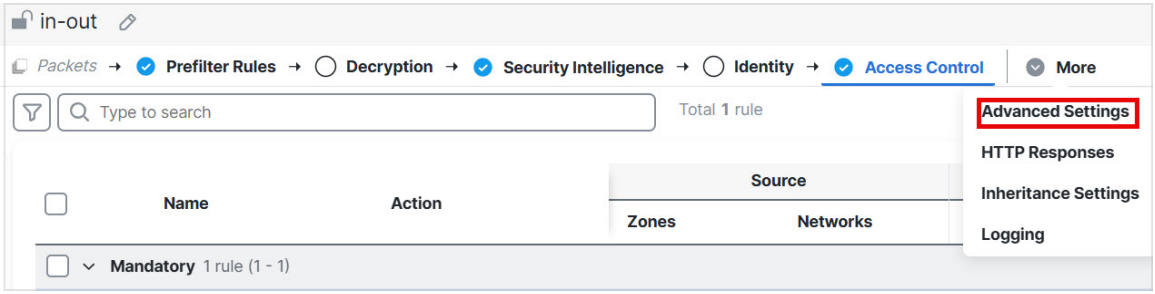
图 ***300:*** 保存 ***ACL***



步骤 2 选择 **策略** > **安全策略** > **访问控制**，然后点击分配给设备的访问控制策略对应的 **编辑** ()。

步骤 3 从数据包流末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

图 ***301:*** 高级设置



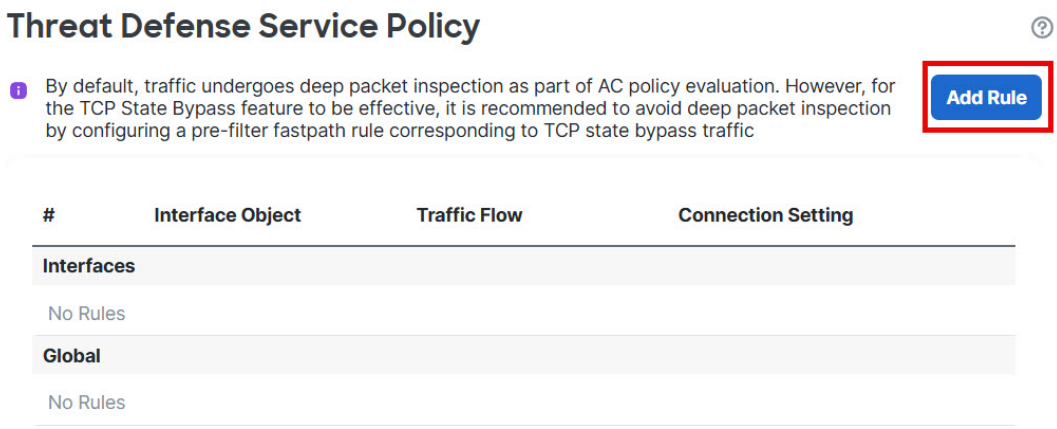
步骤 4 点击**威胁防御服务策略 (Threat Defense Service Policy)** 组中的 **编辑** ()。

图 ***302:*** 威胁防御服务策略



步骤 5 点击**添加规则**以创建新规则。

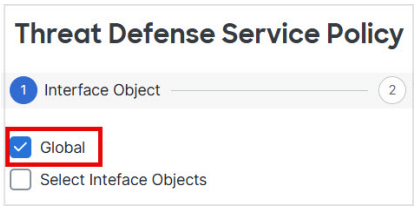
图 *303:* 添加规则



系统将打开服务策略规则向导，逐步指导您完成配置规则的流程。

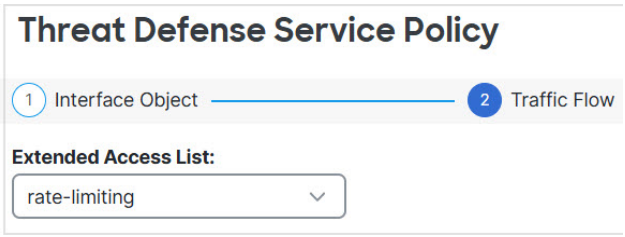
步骤 6 在 **接口对象** 步骤中，点击 **全局** 以创建适用于所有接口的全局规则，然后点击 **下一步**。

图 *304:* 全局策略



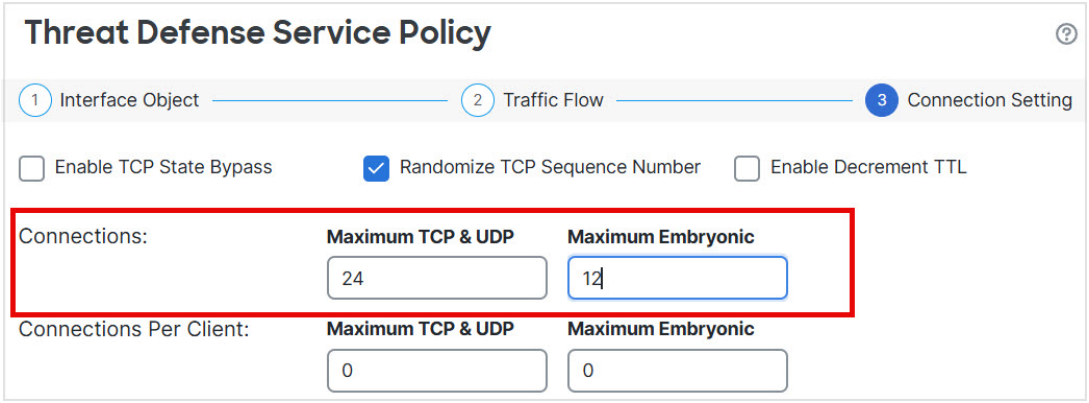
步骤 7 在 **流量** 步骤中，选择您在 步骤 1，第 767 页中创建的扩展访问列表对象，然后点击 **下一步**。

图 *305:* 选择扩展访问列表



步骤 8 在 **连接设置** 步骤中，设置 **连接** 限制。

图 *306:* 设置连接限制



将 **最大 TCP 和 UDP** 连接数设置为环回接口的预期连接数，将 **最大初期** 连接数设置为较低的数字。例如，您可以将其设置为 5/2、10/5 或 1024/512，具体取决于所需的预期环回接口会话。

设置初期连接限制触发 TCP 拦截，从而防止系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

步骤 9 点击**完成**以保存所做的更改。

步骤 10 点击**确定**。

步骤 11 点击 **高级设置** 窗口中的 **保存** 。

步骤 12 现在您可以将更改部署到受影响的设备。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，您可以将物理接口、冗余接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

VLAN 子接口准则

型号支持

- 1010/200/1210/1220 - 交换机端口或 VLAN 接口上不支持 VLAN 子接口。

高可用性和集群

不能将子接口用于故障切换或状态链路，或用于集群控制链路。多实例模式例外：您可以为这些链路使用 机箱 定义的子接口。

其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。此属性对冗余接口对中的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口、冗余接口或 EtherChannel 接口才能使子接口传递流量，请通过不为接口配置名称来确保物理接口、冗余接口或 EtherChannel 接口不传递流量。如果要使物理接口、冗余接口或 EtherChannel 接口传递未标记的数据包，可以照常配置名称。
- 不能在管理接口上配置子接口，无论是在 CLI 中配置的专用管理接口，还是用于管理器访问的数据接口。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- Firewall 威胁防御不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 Firewall 威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 Firewall 威胁防御 上特定实例内发生流量中断。

注释 如果手动分配 MAC 地址，请确保为同一物理接口上的所有子接口分配 MAC 地址，以避免意外行为和中断。

各设备型号的最大 VLAN 子接口数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。

下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Secure Firewall 200	1024
Firepower 1010	60
Firepower 1120	512
Firepower 1140 和 1150	1024
Cisco Secure Firewall 1200	1024
Cisco Secure Firewall 3100	1024
Cisco Secure Firewall 4200	1024
Cisco Secure Firewall 6100	1024

型号	最大 VLAN 子接口数量
Firepower 4100	1024
Firepower 9300	1024
Firewall Threat Defense Virtual	50
ISA 3000	100

添加子接口

向物理接口、冗余接口或 port-channel 接口添加一个或多个子接口。

对于 Firepower 4100/9300，您可以在 FXOS 中配置子接口用于容器实例；请参阅为容器实例添加 VLAN 子接口，第 313 页。这些子接口显示在 防火墙管理中心 接口列表中。您还可以在 防火墙管理中心 中添加子接口，但仅可在未于 FXOS 中定义子接口的父接口上进行操作。

注释 父物理接口会传递未标记的数据包。您可能不想传递未标记的数据包，因此请确保未在安全策略中包括父接口。

过程

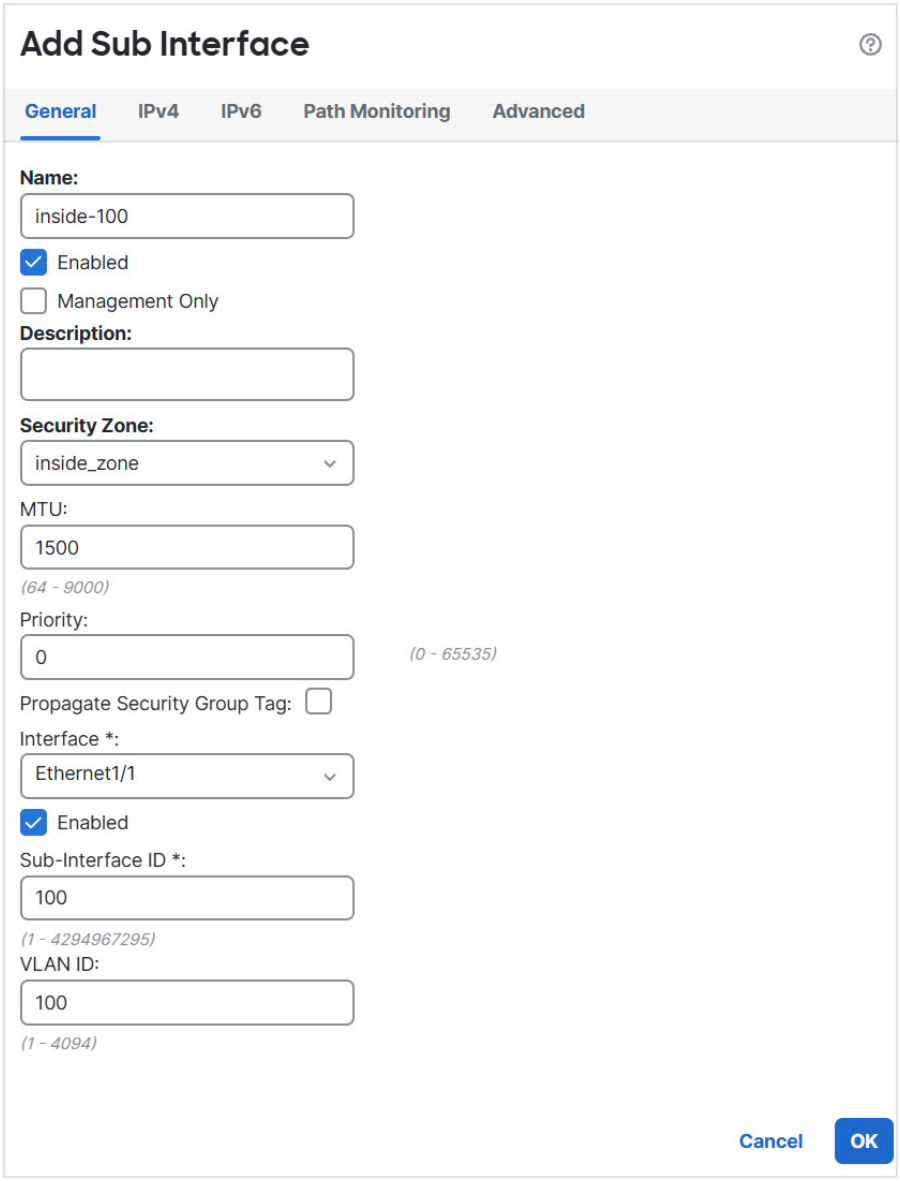
步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** ()。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 根据启用物理接口并配置以太网参数，第 716 页启用父接口。

步骤 3 点击 **添加接口** > **子接口**。

步骤 4 在 **常规**上，设置以下参数：

图 *307:* 添加子接口



a) **接口** - 选择要将子接口添加到的物理、冗余或端口通道接口。

b) **子接口 ID** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

c) **VLAN ID** - 输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。

此 VLAN ID 对父接口必须为唯一。 对于 1010/200/1210/1220，您不能使用 VLAN 1。VLAN 1 保留用于交换机端口的逻辑 VLAN 接口。

步骤 5 点击**确定**。

步骤 6 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 7 配置路由或透明模式接口参数。请参阅配置路由模式接口，第 792 页或配置网桥组接口，第 797 页。

配置 VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 接口作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关 VXLAN 的详细信息，请参阅 RFC 7348。有关 Geneve 的详细信息，请参阅 RFC 8926。

封装

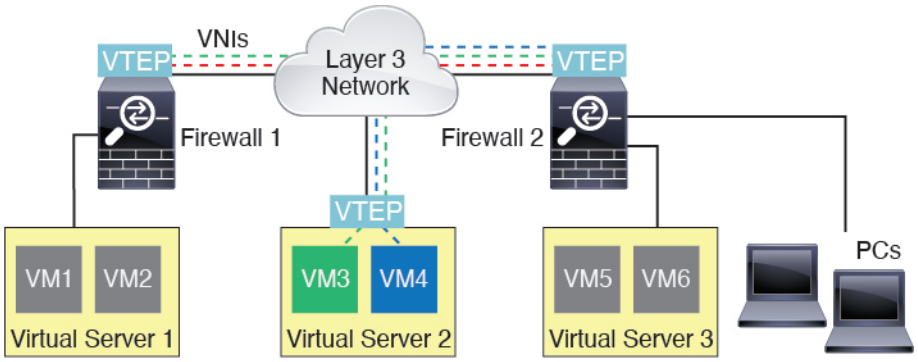
Firewall Threat Defense 支持两种类型的 VXLAN 封装：

- VXLAN（所有型号）- VXLAN 使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。
- Geneve（仅限 Firewall Threat Defense Virtual）- Geneve 具有不限于 MAC 地址的灵活内部报头。要在 Amazon Web 服务 (AWS) 网关负载均衡器和设备之间透明路由数据包，以及发送额外信息，则需要使用 Geneve 封装。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示两个 Firewall Threat Defense 和充当第 3 层网络中的 VTEP 的虚拟服务器 2，用于在站点之间扩展 VNI 1、2 和 3 网络。Firewall Threat Defense 充当 VXLAN 和非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。对于 VXLAN 封装：当远程 VTEP 未知时，目标 IP 地址可以是组播组。在使用 Geneve 时，Firewall Threat Defense 仅支持静态对等体。默认情况下，VXLAN 的目标端口是 UDP 端口 4789（用户可配置）。Geneve 的目的端口是 6081。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 接口（物理、EtherChannel 接口，甚至 VLAN 接口）。每个 Firewall Threat Defense Virtual 设备可以配置一个 VTEP 源接口。 由于只能配置一个 VTEP 源接口，因此不能在同一设备上同时配置 VXLAN 和 Geneve 接口。AWS 或 Azure 上的 Firewall Threat Defense Virtual 集群有一个例外，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve (AWS) 或 VXLAN (Azure) 接口可用于 AWS 网关负载均衡器。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下，VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

您智能添加一个 VTEP 接口，并且所有 VNI 接口都与同一 VTEP 接口相关联。AWS 或 Azure上的 Firewall Threat Defense Virtual 集群例外。对于 AWS 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。对于 Azure 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，第二个 VXLAN 接口可用于 Azure 网关负载均衡器。

VXLAN 数据包处理

VXLAN

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封；Firewall Threat Defense 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

日内瓦

进出 VTEP 源接口的流量取决于 Geneve 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 Geneve 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 会被设置为您配置的对等体 IP 地址。

解封；Firewall Threat Defense 仅在以下条件下解封 Geneve 数据包：

- VXLAN 数据包是目标端口设置为 6081（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- Geneve 数据包格式符合标准。

对等体 VTEP

当 Firewall Threat Defense 将数据包发送到对等体 VTEP 之后的设备时，Firewall Threat Defense 需要两条重要的信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

Firewall Threat Defense 会维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 对等体

有两种方法使 Firewall Threat Defense 可以找到此信息：

- 可以在 Firewall Threat Defense 上静态配置单个对等体 VTEP IP 地址。

  对于 IPv4: 然后， Firewall Threat Defense 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

  对于 IPv6： Firewall Threat Defense 然后向 IPv6 被请求节点的组播地址发送 IPv6 邻居请求消息。对等体 VTEP 以具有其链路本地地址的 IPv6 邻居通告消息作为响应。

- 可以在 Firewall Threat Defense 上静态配置一组对等体 VTEP IP 地址。

  对于 IPv4: 然后， Firewall Threat Defense 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

  对于 IPv6： Firewall Threat Defense 然后向 IPv6 被请求节点的组播地址发送 IPv6 邻居请求消息。对等体 VTEP 以具有其链路本地地址的 IPv6 邻居通告消息作为响应。

- 可以在每个 VNI 接口（或者总的来说，在 VTEP 上）配置组播组。

  对于 IPv4： Firewall Threat Defense 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 Firewall Threat Defense 可以获取远程终端节点的远程 VTEP IP 地址和目标 MAC 地址。

  对于 IPv6： Firewall Threat Defense 通过 VTEP 源接口发送组播侦听程序发现 (MLD) 报告消息，以指示 Firewall Threat Defense 正在 VTEP 接口上侦听组播地址流量。

  Geneve 不支持此选项。

Geneve 对等体

Firewall Threat Defense Virtual 仅支持静态定义的对等设备。您可以在 AWS 网关负载均衡器上定义 Firewall Threat Defense Virtual 对等体 IP 地址。由于 Firewall Threat Defense Virtual 绝不会向网关负载均衡器发起流量，因此您也不必在 Firewall Threat Defense Virtual 上指定网关负载均衡器 IP 地址；它会在收到 Geneve 流量时获知对等体 IP 地址。Geneve 不支持组播组。

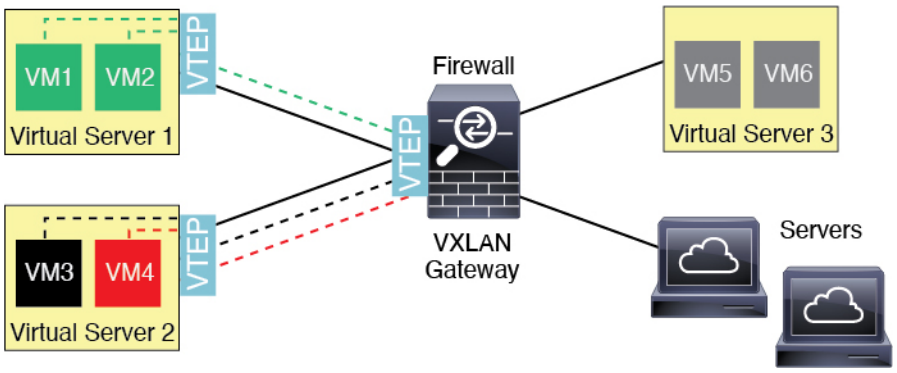
VXLAN 使用案例

本节介绍在 Firewall Threat Defense 上实施 VXLAN 的使用案例。

VXLAN 网桥或网关概述

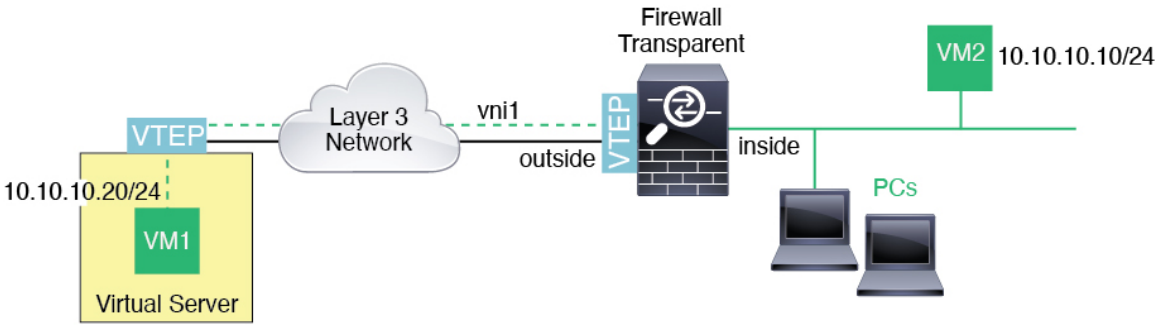
每个 Firewall Threat Defense VTEP 都可作为终端节点（例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，Firewall Threat Defense 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

Firewall Threat Defense 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



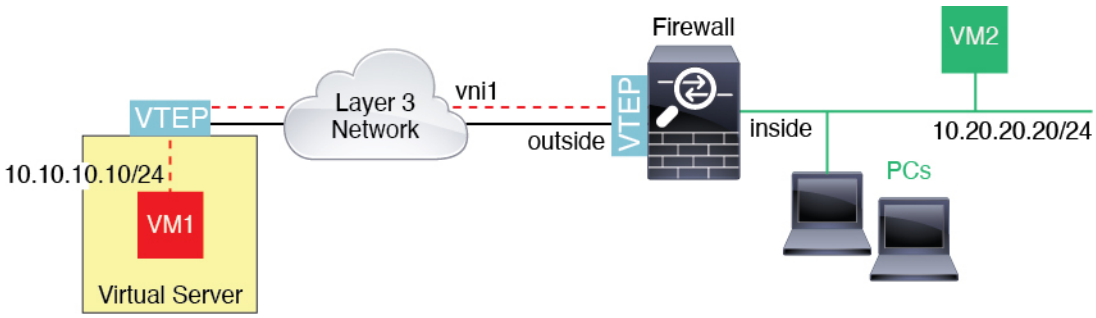
VXLAN 网桥

在使用网桥组（透明防火墙模式或可选的路由模式）时，Firewall Threat Defense 可以用作 VXLAN 网段与本地网段之间的 VXLAN 网桥（远程），其中二者均位于同一网络中。在这种情况下，网桥组的一个成员是常规接口，而另一个成员是 VNI 接口。



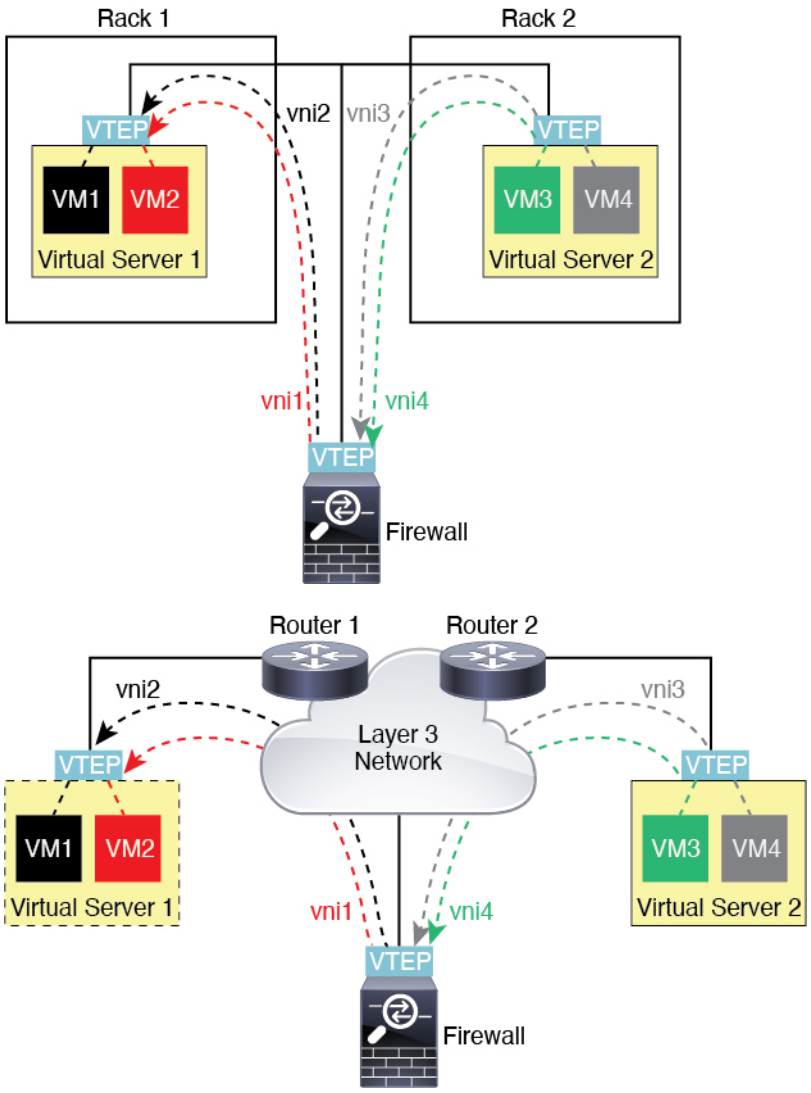
VXLAN 网关（路由模式）

Firewall Threat Defense 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 Firewall Threat Defense 作为其网关，即使 Firewall Threat Defense 位于不同机架中，甚至当 Firewall Threat Defense 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 Firewall Threat Defense MAC 地址，因为 Firewall Threat Defense 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标记封装数据包，并将数据包发送到 Firewall Threat Defense。
3. 当 Firewall Threat Defense 接收数据包时，会解封数据包以获得内部帧。
4. Firewall Threat Defense 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，Firewall Threat Defense 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注释 Firewall Threat Defense 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

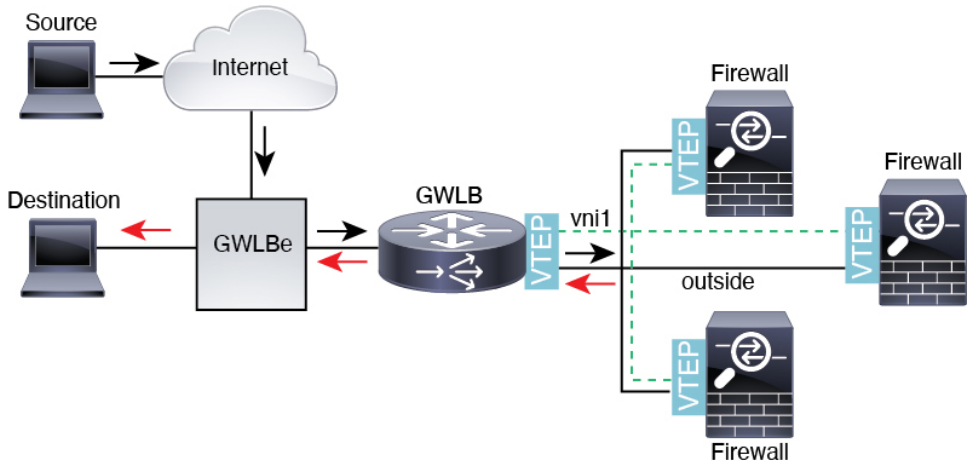
5. Firewall Threat Defense 再次使用 VXLAN 标记为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前，Firewall Threat Defense 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址（Firewall Threat Defense 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Firewall Threat Defense Virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。Firewall Threat Defense Virtual然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *308: Geneve* 单臂代理



AWS 网关负载均衡器和 Geneve 双臂代理

注释 这是 Geneve 接口唯一支持的使用案例。

Firewall Threat Defense Virtual 在单臂和双臂模式下，支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示直接转发到目标（互联网）的出站流量（由 Firewall Threat Defense Virtual检查的流量），无需流量跃点到 GWLB 和 GWLB 终端。Firewall Threat Defense Virtual 检查出站流量并执行 NAT，然后丢弃流量或通过 NAT 网关将流量发送回互联网。双臂代理为多 VPC 部署提供通用出口路径。防火墙检查来自多个 VPC 的出站流量，并从单点退出到互联网，使其成为具有成本效益的基础设施解决方案。

图 *309: Geneve* 双臂代理：来自单 *VPC* 的出口流量

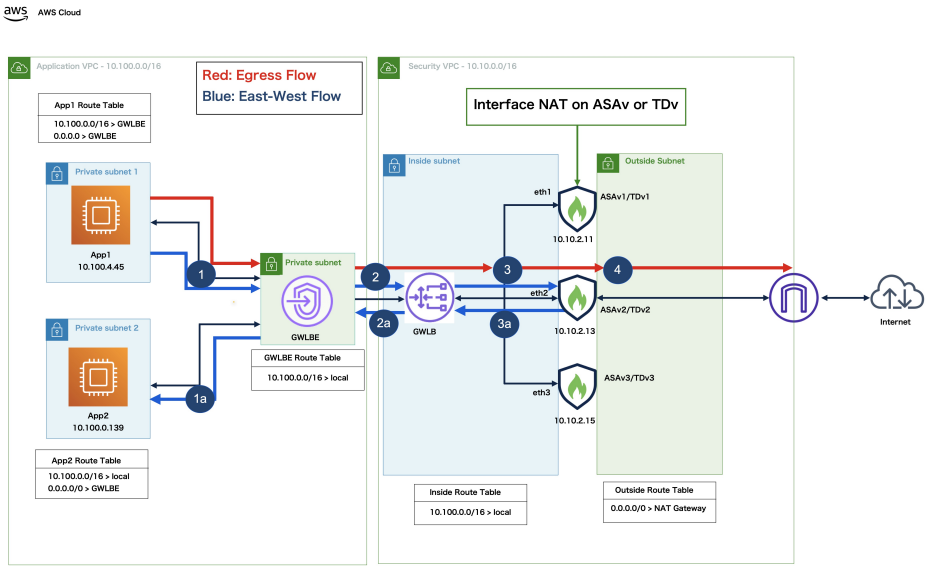
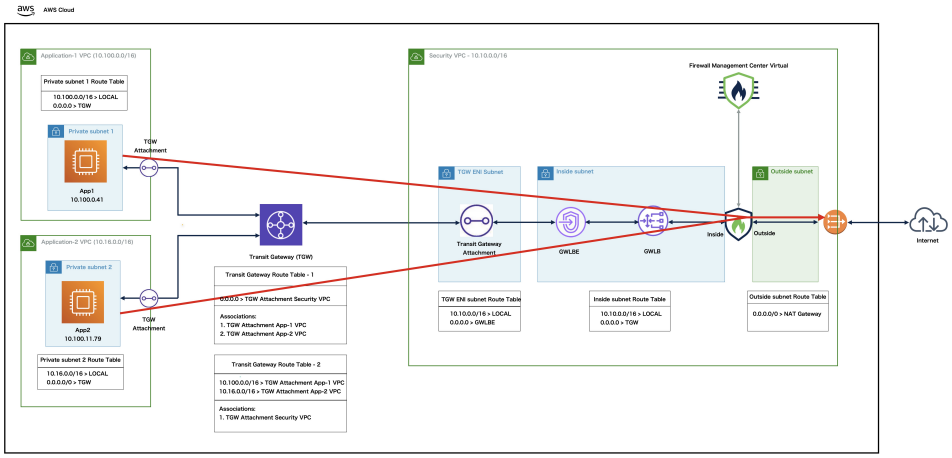


图 *310: Geneve* 双臂代理：来自多个 *VPC* 的出口流量

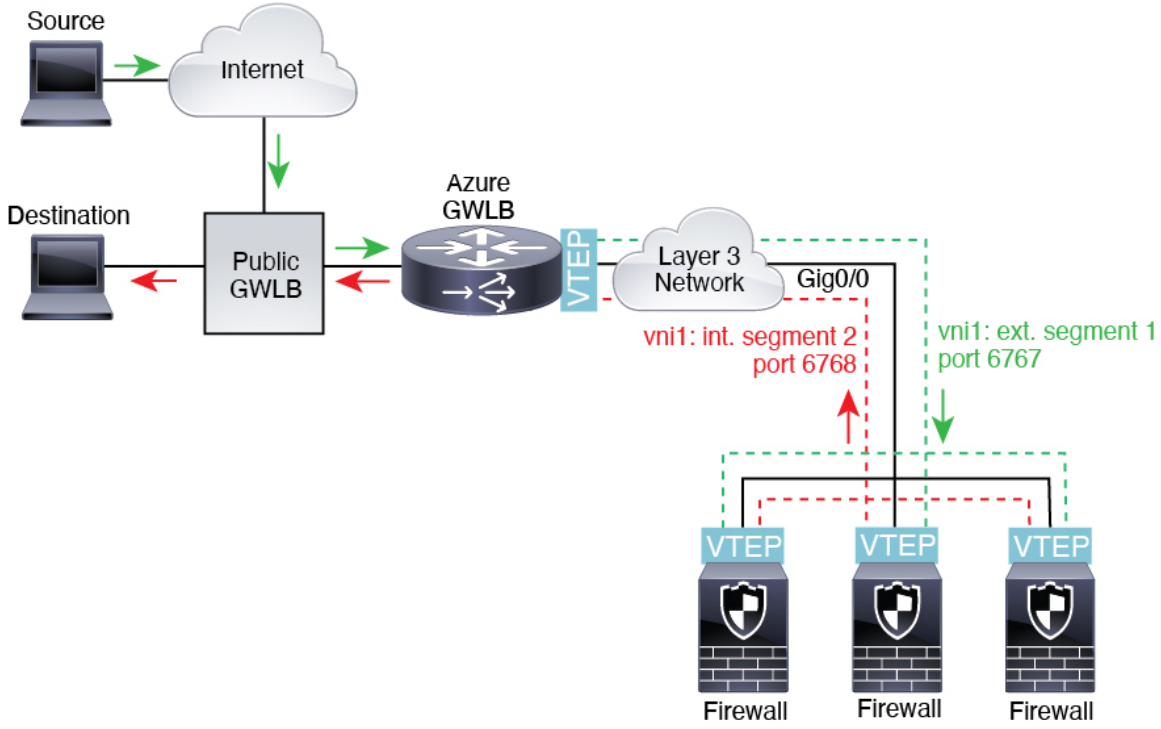


Azure 网关负载均衡器和配对代理

在 Azure 服务链中， Firewall Threat Defense Virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 Firewall Threat Defense Virtual流量之间进行均衡 ， 这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *311: Azure* 网关负载均衡器和配对代理



VXLAN 接口的要求和前提条件

型号要求

- 所有型号均支持 VXLAN 封装。
- 以下型号支持 Geneve 封装：
  - Amazon Web 服务 (AWS) 中的 Firewall Threat Defense Virtual
- 以下型号支持 配对代理模式 下的 VXLAN：
  - Firewall Threat Defense Virtual 在 Azure 中
- 不支持将 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口和 VLAN 接口用作 VTEP 接口。

VXLAN 接口准则

防火墙模式

- Geneve 接口仅在路由防火墙模式下支持。

- 配对代理 VXLAN 接口仅在路由防火墙模式下支持。

IPv6

- VNI 接口支持 IPv4 和 IPv6 流量。
- 对于 VXLAN 封装，VTEP 源接口同时支持 IPv4 和 IPv6。 Firewall Threat Defense Virtual 集群控制链路 VTEP 源接口仅支持 IPv4。

  对于 Geneve，VTEP 源接口仅支持 IPv4。

集群

- 集群在单个接口模式下不支持 VXLAN，但集群控制链路除外（仅限Firewall Threat Defense Virtual）仅跨区以太网通道模式支持 VXLAN。

  例外情况是，AWS 可以使用额外的 Geneve 接口与 GWLB 配合使用，而 Azure 可以使用额外的配对代理 VXLAN 接口与 GWLB 配合使用。

路由

- VNI 接口上仅支持静态路由或策略型路由；动态路由协议不受支持。

VPN

不能为 VPN 配置 VTEP 源接口或将其用作 VTI。

MTU

- VXLAN 封装-如果源接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 Firewall Threat Defense 会自动将 MTU 提高到 1554 个字节 或 1574 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。如果其他设备使用的 MTU 更大，则您应 为 IPv4 将源接口 MTU 设置为网络 MTU + 54 个字节，或者为 IPv6 设置为 +64 个字节。对于 Firewall Threat Defense Virtual，此 MTU 需要您重新启动以启用巨帧保留。
- Geneve 封装 (Geneve encapsulation) - 如果源接口 MTU 少于 1806 个字节，Firewall Threat Defense 会自动将 MTU 提高到 1806 个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。如果其他设备使用的 MTU 更大，您应将源接口 MTU 设置为网络 MTU + 306 个字节。此 MTU 需要您重新启动以启用巨帧保留。

配置 VXLAN 或 Geneve 接口

您可以配置 VXLAN 或 Geneve 接口。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

注释 您可以配置 VXLAN 或 Geneve（仅限 Firewall Threat Defense Virtual）。有关 Geneve 接口，请参阅配置 Geneve 接口，第 786 页。

注释 对于 Azure GWLB，在使用 ARM 模板部署 VM 时会配置 VXLAN 接口。您可以在此部分中更改配置。

1. 配置 VTEP 源接口，第 784 页。
2. 配置 VNI 接口，第 785 页。
3. (Azure GWLB) 允许网关负载均衡器运行状况检查，第 788 页。

配置 VTEP 源接口

每个 Firewall Threat Defense 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。VXLAN 是默认的封装类型。在 Azure 中，Firewall Threat Defense Virtual 上的集群是个例外，您可以使用一个 VTEP 源接口作为集群控制链路，将另一个 VTEP 源接口用于连接到 Azure GWLB 的数据接口。

过程

步骤 1 如果要指定一组对等 VTEP，请添加具有对等体 IP 地址的网络对象。请参阅创建网络对象，第 2660 页。

步骤 2 选择**设备** > **设备管理**。

步骤 3 点击要配置 VXLAN 的设备旁边的 **编辑** ()。

步骤 4 （可选） 将源接口指定为仅限 NVE。

在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此设置是可选的。对于透明防火墙模式，系统会自动启用此设置。

a) 点击**接口 (Interfaces)**。
b) 点击 VTEP 源接口的 **编辑** ()。
c) 在**常规 (General)** 页面上，选中**仅限 NVE (NVE Only)** 复选框。

步骤 5 如果尚未显示，点击 **VTEP**。

步骤 6 选中**启用 NVE (Enable NVE)**。

步骤 7 点击**添加 VTEP (Add VTEP)**。

步骤 8 对于**封装类型 (Encapsulation Type)**，请选择 **VxLAN**。

对于 AWS，您可以在 **VxLAN** 和 **Geneve** 之间进行选择。其他平台会自动选择 **VxLAN**。

步骤 9 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

默认值为 4789。

步骤 10 选择 **VTEP 源接口 (VTEP Source Interface)**。

从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 防火墙管理中心 会自动将 MTU 提高到 1554 个字节或 1574 字节。

步骤 11 选择**邻居地址 (Neighbor Address)**。可用选项包括：

- **无 (None)** - 未指定邻居地址。
- **对等体 VTEP (Peer VTEP)** - 指定对等体 VTP 地址。
- **对等体组 (Peer Group)** - 指定具有对等体 IP 地址的网络对象。
- **默认组播 (Default Multicast)** - 指定所有相关 VNI 接口的默认组播组。如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

步骤 12 点击**确定**。

步骤 13 点击**保存**。

步骤 14 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

对于 Azure 中的 Firewall Threat Defense Virtual，您可以配置常规 VXLAN 接口，也可以配置配对代理模式 VXLAN 接口，以便与 Azure GWLB 配合使用。配对代理模式是唯一支持的集群模式。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 VXLAN 的设备旁边的 **编辑** ()。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 输入接口**名称 (Name)** 和**说明 (Description)**。

步骤 6 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

步骤 7 在指定范围内为**优先级 (Priority)** 字段输入值。默认情况下会选择 0。

步骤 8 输入值介于 1 和 10000 之间的 **VNI ID**。

此 ID 仅为内部接口标识符。

步骤 9 （Azure GWLB 的已配对代理 VXLAN）启用代理配对模式并设置所需的参数。

a) 选中**已配对代理 (Proxy Paired)**。

b) 将**内部端口 (Internal Port)** 设置为 1024 和 65535 之间的值。
c) 将**内部网段 ID (Internal Segment ID)** 设置为 1 和 16777215 之间的值。
d) 将**外部端口 (External Port)** 设置为 1024 和 65535 之间的值。
e) 将**外部网段 ID (External Segment ID)** 设置为 1 和 16777215 之间的值。

步骤 10 （常规 VXLAN）为 **VNI 网段 ID (VNI Segment ID)** 设置为 1 和 16777215 之间值。

网段 ID 用于 VXLAN 标记。

步骤 11 输入**多播组 IP 地址 (Multicast Group IP Address)**。

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组（如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。

步骤 12 选中 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 13 点击**确定**。
步骤 14 点击**保存**以保存接口配置。
步骤 15 配置路由或透明接口参数。请参阅配置路由和透明模式接口，第 789 页。

配置 Geneve 接口

要为 Firewall Threat Defense Virtual 配置 Geneve 接口，请执行以下步骤：

注释 您可以配置 VXLAN 或 Geneve。有关 VXLAN 接口的信息，请参阅配置 VXLAN 接口，第 783 页。

1. 配置 VTEP 源接口，第 786 页。
2. 配置 VNI，第 787 页。
3. 允许网关负载均衡器运行状况检查，第 788 页。

配置 VTEP 源接口

每个 Firewall Threat Defense Virtual 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

过程

步骤 1 选择**设备** > **设备管理**。
步骤 2 点击要配置 Geneve 的设备旁边的 **编辑** (✎) 。
步骤 3 点击 **VTEP**。

步骤 4 选中**启用 NVE (Enable NVE)**。

步骤 5 点击**添加 VTEP (Add VTEP)**。

步骤 6 对于**封装类型 (Encapsulation Type)**，请选择 **Geneve**。

步骤 7 在**封装端口 (Encapsulation port)** 中输入指定范围内的值。

我们不建议更改 Geneve 端口；AWS 需要使用端口 6081。

步骤 8 选择 **VTEP 源接口 (VTEP Source Interface)**。

您可以从设备上的可用物理接口列表中进行选择。如果源接口 MTU 少于 1806 个字节，防火墙管理中心 会自动将 MTU 提高到 1806 个字节。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

步骤 11 配置已路由的接口参数。请参阅配置路由模式接口。

配置 VNI

添加 VNI，将其与 (VTEP) 源接口相关联，并配置基本的接口参数。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要配置 Geneve 的设备旁边的 **编辑** (✎) 。

步骤 3 点击**接口 (Interfaces)**。

步骤 4 点击**添加接口 (Add Interfaces)**，然后选择 **VNI 接口 (VNI Interface)**。

步骤 5 在**名称 (Name)** 和**说明 (Description)** 字段中提供相关信息。

步骤 6 在 **VNI ID** 字段中，输入介于 1 和 10000 之间的值。

注释
此 ID 仅为内部接口标识符。

步骤 7 选中**启用代理 (Enable Proxy)** 复选框。

注释
当设备的 VNI 接口启用 AWS 代理时，不允许配置 NAT。

该选项可启用单臂代理模式或双臂代理模式。单臂代理模式允许流量从进入的同一接口流出（U-turn 流量），而双臂代理模式则使虚拟设备能够对检查到的流量执行 NAT，然后直接将出站流量转发到互联网，而不返回到 GWLB 和 GWLB 端点。如果以后编辑接口，则无法禁用单臂代理模式或双臂代理模式。为此，您需要删除现有接口并创建一个新的 VNI。

此选项仅适用于 Geneve VTEP。

步骤 8 从**代理类型 (Proxy type)** 下拉列表中，选择要为接口启用的代理模式。如果没有为接口指定代理模式，则默认情况下会考虑单臂代理模式。

步骤 9 选择 **NVE 已映射到 VTEP 接口 (NVE Mapped to VTEP Interface)**。

此选项会将该接口与 VTEP 源接口相关联。

步骤 10 点击**确定**。

步骤 11 点击**保存**。

下一步做什么

配置已路由的接口参数。请参阅配置路由模式接口。

允许网关负载均衡器运行状况检查

AWS 或 Azure GWLB 要求设备对运行状况检查进行正确应答。GWLB 只会将流量发送到被视为正常的设备。您必须将 Firewall Threat Defense Virtual 配置为响应 SSH、HTTP 或 HTTPS 运行状况检查。

配置以下方法之一。

过程

步骤 1 配置 SSH。请参阅配置安全外壳

允许来自 GWLB IP 地址的 SSH。GWLB 将尝试与 Firewall Threat Defense Virtual 建立连接，而 Firewall Threat Defense Virtual 的登录提示将被视为运行状况的证明。SSH 登录尝试会在 1 分钟后超时。为了适应此超时，您需要在 GWLB 上配置更长的运行状况检查间隔。

步骤 2 使用支持端口转换的静态接口 NAT 来配置 HTTP(S) 重定向。

您可以将 Firewall Threat Defense Virtual 配置为将运行状况检查重定向到元数据 HTTP(S) 服务器。对于 HTTP(S) 运行状况检查，HTTP(S) 服务器必须使用 200 到 399 范围内的状态代码来回复 GWLB。由于 Firewall Threat Defense Virtual 对同时管理连接的数量存在限制，因此您可以选择将运行状况检查分流到外部服务器。

支持端口转换的静态接口 NAT 允许您将某个端口（例如端口 80）的连接重定向到其他 IP 地址。例如，将来自 GWLB 的 HTTP 数据包转换为 Firewall Threat Defense Virtual 外部接口的目标，使其看起来像是来自目标为 HTTP 服务器的 Firewall Threat Defense Virtual 外部接口。Firewall Threat Defense Virtual 随后会将数据包转发到映射的目标地址。HTTP 服务器会响应 Firewall Threat Defense Virtual 外部接口，然后 Firewall Threat Defense Virtual 会将响应转发回 GWLB。您需要允许从 GWLB 到 HTTP 服务器的流量的访问规则。

a) 在访问规则中允许来自 GWLB 网络的外部接口上的 HTTP(S) 流量。请参阅访问控制规则，第 1743 页。

b) 对于 HTTP(S)，请将源 GWLB IP 地址转换为 Firewall Threat Defense Virtual 外部接口 IP 地址；然后将外部接口 IP 地址的目的地转换为 HTTP(S) 服务器 IP 地址。请参阅配置静态手动 NAT，第 1336 页。

配置路由和透明模式接口

本部分介绍在路由或透明防火墙模式下为所有型号完成常规接口配置的相关任务。

关于路由和透明模式接口

防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅透明或路由防火墙模式，第 123 页。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。
- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。 在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

双 IP 堆栈（IPv4 和 IPv6）

Firewall 威胁防御设备在接口上同时支持 IPv6 和 IPv4 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

31 位子网掩码

对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 Firewall 威胁防御 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

31 位子网和集群

您可以在跨集群模式，但管理接口和集群控制链路除外。

31 位子网和故障转移

进行故障转移时，如果为 Firewall 威胁防御 接口 IP 地址使用 31 位子网，则无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障转移的接口应有一个备用 IP 地址，以便主设备

可以执行接口测试来确保备用接口正常运行。如果没有备用 IP 地址，Firewall 威胁防御 无法执行任何网络测试；只能跟踪链路状态。

对于故障转移和可选的独立状态链路（点对点连接），也可以使用 31 位子网。

31 位子网和管理

如果您有直接连接的管理工作站，则对于 Firewall 威胁防御 的 SSH 或 HTTP，或管理工作站上的 SNMP 或 Syslog，可使用点对点连接。

31 位子网不支持的功能

以下功能不支持 31 位子网：

- 网桥组的 BVI 接口 - 网桥组需要至少 3 个主机地址：BVI 和连接到两个网桥组成员接口的两台主机。您必须使用 /29 子网或更小的子网。
- 组播路由

路由和透明模式接口准则和限制

、集群和多实例

- 请勿采用本章中的程序配置故障转移接口。有关详细信息，请参阅。
- 对于集群接口，请参阅“集群”一章了解要求。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 在使用时，则必须为数据接口手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。在**监控接口**区域中的**设备** > **设备管理** > **高可用性**选项卡上设置备用 IP 地址。有关详细信息，请参阅章节。

IPv6

- 所有接口上都支持 IPv6。
- 只能在透明模式下手动配置 IPv6 地址。
- Firewall 威胁防御设备 不支持 IPv6 任播地址。
- 透明模式、集群或不支持 DHCPv6 和前缀委派选项。

型号准则

- 对于具有桥接 ixgbevf 接口的 VMware 上的Firewall Threat Defense Virtual，桥接组不受支持。

透明模式和网桥组准则

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。

- 各个直连网络必须在同一子网上。
- Firewall 威胁防御设备不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 Firewall 威胁防御设备。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于多实例模式，共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 Firewall Threat Defense Virtual ，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。20012101220
- 对于 Firepower 4100/9300，不支持将数据共享接口作为网桥组成员。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 Firewall 威胁防御另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- Amazon Web 服务、Microsoft Azure、Google Cloud Platform 和 Oracle Cloud Infrastructure 上部署的 Threat Defense Virtual 实例不支持透明模式。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，Firewall 威胁防御 - 不支持将 EtherChannel 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 Firewall 威胁防御。如果 Firewall 威胁防御 的一端有两个邻居运行 BFD，则 Firewall 威胁防御 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

其他准则和要求

- Firewall 威胁防御 仅支持数据包中的一个 802.1Q 报头，不支持防火墙接口的多个报头（称为 QinQ 支持）。**注意**：对于内联集和被动接口，FTD 在数据包中最多支持 Q-in-Q 两个 802.1Q 报头，但 Firepower 4100/9300 仅支持一个 802.1Q 报头。

- 接口问题（例如频繁的启动/关闭状态更改）会导致浮动连接计时器无法正确应用于通过接口的连接。如果接口状态有问题，可考虑在状态稳定后清除所有连接，以清除无效连接。

配置路由模式接口

此程序介绍如何设置名称、安全区域和 IPv4 地址。



注释 并非所有接口类型都支持所有的字段。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口，第 310 页
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道），第 311 页
     - 为容器实例添加 VLAN 子接口，第 313 页 在 FXOS 中
     - 配置环回接口，第 766 页
     - 添加子接口，第 772 页 在 防火墙管理中心
     - 配置 VXLAN 接口，第 783 页
- （可选） **所有其他型号**：
  - 配置 EtherChannel，第 724 页
  - 配置环回接口，第 766 页
  - 添加子接口，第 772 页
  - 配置 VXLAN 接口，第 783 页
  - AWS 上的 Firewall Threat Defense Virtual：配置 Geneve 接口，第 786 页
  - Firepower 1010 和 Cisco Secure Firewall 1210/1220：配置 VLAN 接口，第 757 页

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

名称不能以短语“cluster”开头。它保留供内部使用。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选） 将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

常规防火墙接口的模式设置为“无”。其他模式用于仅 IPS 接口类型。

步骤 8 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

路由接口是路由类型的接口，只能属于路由类型的区域。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 819 页。

步骤 10 在 **优先级** 字段中，输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口路由流量。有关详细信息，请参阅配置策略型路由策略，第 1266 页。

步骤 11 点击 **Ipv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性、集群和环回接口仅支持静态 IP 地址配置；不支持 DHCP 和 PPPoE。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于点对点连接，可以指定 31 位子网掩码（255.255.255.254 或 /31）。在这种情况下，不会为网络或广播地址预留 IP 地址。在此情况下，无法设置备用 IP 地址。对于高可用性，只能使用静态 IP 地址。在 监控接口 区域中的 **设备 设备管理** 高可用性选项卡上设置备用 IP 地址。**设备 > 设备管理**如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。
- **使用 PPPoE** - 如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，请配置以下参数：
  - **VPDN 组名称** - 指定您选择的组名称来表示此连接。
  - **PPPoE 用户名** - 指定 ISP 提供的用户名。
  - **PPPoE 密码/确认密码** - 指定并确认 ISP 提供的密码。
  - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 路由指标** - 向获悉的路由分配管理距离。有效值范围为 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **启用路由设置** - 要手动配置 PPPoE IP 地址，请选中此框，然后输入 **IP 地址**。

  如果选中 **启用路由设置** 复选框并将 **IP 地址** 留空，则会应用 **ip address pppoe setroute** 命令，如下例所示：

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- **在闪存中存储用户名和密码** - 在闪存中存储用户名和密码。

  Firewall Threat Defense 设备将用户名和密码存储在 NVRAM 中的专用位置。

步骤 12 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址，第 801 页。

步骤 13 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址，第 820 页。

步骤 14 （可选） 通过点击 **硬件配置 (Hardware Configuration)** > **速度 (Speed)**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。但是，Cisco Secure Firewall 220 的 SFP 接口 (Ethernet 1/5) 支持**全双工**和**半双工**。
- **速度**-选择速度（因型号而异）。对于 SFP，选择 **检测 SFP** 以检测已安装 SFP 模块的速度，并使用相应的速度。双工模式始终为全双工，自动协商始终启用，且 FEC 设置为自动。对于双速收发器，将使用较低速度。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。某些交换机和收发器不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。例如，Cisco Secure Firewall 6100 上的 SFP-H25GB-CU1M 不支持自动协商或 FEC，因此您必须手动设置速度、禁用**自动协商**并禁用**前向纠错模式**。

  注释
  您无法修改高可用性或集群控制链路接口的速度。
- **自动协商** - 设置接口以协商速度、链路状态和流量控制。

  1100除外，自动协商与速度分开设置。某些交换机不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。
- **前向纠错模式** - 对于 25 Gbps 及更高速率的接口，请启用前向纠错 (FEC)。

对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。如果从 EtherChannel 中删除接口，则重新启动后可能需要为该接口重新配置 FEC。

有些交换机不支持 FEC 自动模式，尤其是较大的接口。请根据交换机支持情况确保手动配置该设置。不建议禁用 FEC；如果禁用，EtherChannel 可能无法正常启用。

使用 **自动** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *55:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

注释
从版本 7.4.2 开始，防火墙威胁防御支持 SFP 10G_25G_CSR_S 模块。为避免重启后出现链路断开问题，必须在这些接口上启用前向纠错 (FEC)。

步骤 15 （可选） 在**管理访问 (Manager Access)** 页面上启用数据接口上的 防火墙管理中心 管理器访问。

首次设置 Firewall Threat Defense 时，您可以从数据接口启用管理器访问。如果要在将 Firewall Threat Defense 添加到 防火墙管理中心 后启用或禁用管理器访问，请参阅：

- 启用管理器访问：将管理器访问接口从管理更改为数据

  注释
  除非先启动管理器接口从管理到数据接口的迁移，否则无法启用管理器访问。启动迁移后，您可以在**管理器访问 (Manager Access)** 页面上启用管理器访问并成功保存配置。

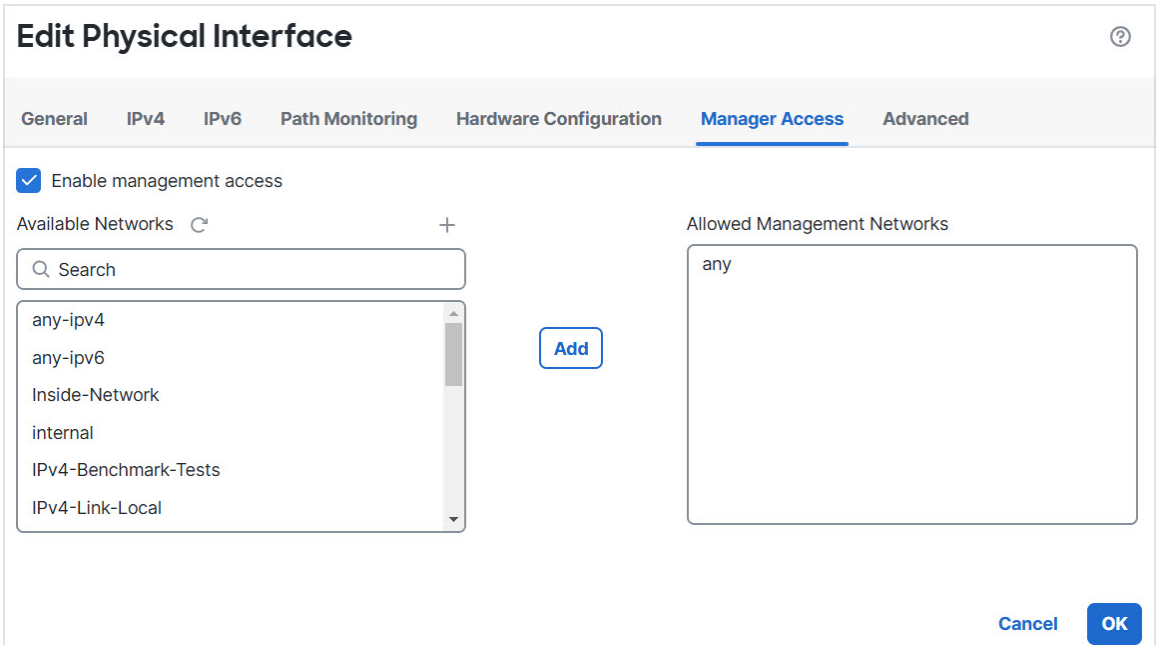
- 禁用管理器访问：将管理器访问接口从数据更改为管理

如果要将管理器访问接口从一个数据接口更改为另一个数据接口，必须在原始数据接口上禁用管理器访问，但不要禁用接口本身；必须使用原始数据接口执行部署。如果要在新管理器访问接口上使用相同的 IP 地址，可以删除或更改原始接口上的 IP 配置；此更改不应影响部署。如果为新接口使用不同的 IP 地址，则还要更改 防火墙管理中心 中显示的设备 IP 地址；请参阅更新防火墙管理中心中的主机名或 IP 地址。请务必同时更新相关配置，以使用新接口，例如静态路由、DDNS 和 DNS 设置。

从数据接口进行管理器访问具有以下限制：

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel，也不能在管理器访问接口上创建子接口。您还可以使用 防火墙管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 Firewall Threat Defense 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 防火墙管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 Firewall Threat Defense Virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。

图 *312:* 管理器访问



- 选中**在此接口上为管理器启用管理 (Enable management on this interface for the manager)** 以便使用此数据接口进行管理，而不是专用管理接口。
- （可选）在**允许的管理网络 (Allowed Management Networks)** 框中，添加要允许管理器访问的网络。默认情况下，允许任何网络。

步骤 16 点击**确定**。

步骤 17 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置网桥组接口

网桥组是指 Cisco Secure Firewall Threat Defense 设备网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。有关网桥组的详细信息，请参阅 关于网桥组 ，第 125 页。

要配置网桥组和关联接口，请执行以下步骤。

配置常规网桥组成员接口参数

此程序描述如何为每个网桥组成员接口设置名称和安全区域。同一网桥组可以包括不同类型的接口：物理接口、子接口、 Firepower 1010 和 Cisco Secure Firewall 1210/1220 VLAN 接口、EtherChannel 接口和冗余接口 。管理接口不受支持。 在路由模式中，不支持 EtherChannels。对于 Firepower 4100/9300，不支持数据共享类型的接口。

开始之前

- **Firepower 4100/9300**
  1. 配置物理接口 ，第 310 页
  2. （可选）配置任何特殊接口。
     - 添加 EtherChannel（端口通道） ，第 311 页
     - 为容器实例添加 VLAN 子接口 ，第 313 页 在 FXOS 中
     - 添加子接口 ，第 772 页 在 防火墙管理中心
- （可选） **所有其他型号**：
  - 配置 EtherChannel ，第 724 页
  - 添加子接口 ，第 772 页
  - Firepower 1010 和 Cisco Secure Firewall 1210/1220：配置 VLAN 接口 ，第 757 页

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在**名称**字段中，输入长度最大为 48 个字符的名称。

名称不能以短语“cluster”开头。它保留供内部使用。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 （可选） 将此接口设置为**管理专用**以限制到管理流量的流量；不允许通过设备的流量。

步骤 6 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 7 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

常规防火墙接口的模式设置为“无”。其他模式用于仅IPS接口类型。在将此接口分配到网桥组后，该模式将显示为**交换**。

步骤 8 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

桥接组成员接口是交换类型的接口，只能属于交换类型的区域。请勿为此接口设置任何 IP 地址设置。您将只设置桥接虚拟接口 (BVI) 的 IP 地址。请注意，BVI 不属于某个区域，您不能将访问控制策略应用到 BVI。

步骤 9 有关 **MTU** 的详细信息，请参阅配置 MTU，第 819 页。

步骤 10 （可选） 通过点击 **硬件配置 (Hardware Configuration)** > **速度 (Speed)**，设置复用和速度。

- **复用**—选择 **全** 或 **半**。SFP 接口仅支持 **全** 复用。但是，Cisco Secure Firewall 220 的 SFP 接口 (Ethernet 1/5) 支持**全双工**和**半双工**。
- **速度**-选择速度（因型号而异）。对于 SFP，选择 **检测 SFP** 以检测已安装 SFP 模块的速度，并使用相应的速度。双工模式始终为全双工，自动协商始终启用，且FEC设置为自动。对于双速收发器，将使用较低速度。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。某些交换机和收发器不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。例如，Cisco Secure Firewall 6100 上的 SFP-H25GB-CU1M 不支持自动协商或 FEC，因此您必须手动设置速度、禁用**自动协商**并禁用**前向纠错模式**。

  注释
  您无法修改高可用性或集群控制链路接口的速度。

- **自动协商** - 设置接口以协商速度、链路状态和流量控制。

  1100除外，自动协商与速度分开设置。某些交换机不支持自动协商，尤其是高速接口。在这种情况下，请将Firewall Threat Defense的接口设置为手动速度，并禁用**自动协商**，以便建立链路。

- **前向纠错模式** - 对于 25 Gbps 及更高速率的接口，请启用前向纠错 (FEC)。

  对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。如果从 EtherChannel 中删除接口，则重新启动后可能需要为该接口重新配置 FEC。

  有些交换机不支持 FEC 自动模式，尤其是较大的接口。请根据交换机支持情况确保手动配置该设置。不建议禁用 FEC；如果禁用，EtherChannel 可能无法正常启用。

  使用 **自动** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 *56:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

注释
从版本 7.4.2 开始，防火墙威胁防御支持 SFP 10G_25G_CSR_S 模块。为避免重启后出现链路断开问题，必须在这些接口上启用前向纠错 (FEC)。

步骤 11 （可选） 要在 **IPv6** 选项卡上配置 IPv6 寻址，请参阅配置 IPv6 寻址，第 801 页。

步骤 12 （可选） 要在**高级**选项卡上手动配置 MAC 地址，请参阅配置 MAC 地址，第 820 页。

步骤 13 点击**确定**。

步骤 14 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置网桥虚拟接口 (BVI)

每个网桥组都需要一个您应为其配置 IP 地址的 BVI。Firewall Threat Defense 使用此 IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与所连接的网络位于同一子网。对于 IPv4 流量，任何流量的传递都需要使用 BVI IP。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。

对于路由模式，如果为 BVI 提供一个名称，则 BVI 将参与路由。如果不提供名称，网桥组在透明防火墙模式下将保持隔离状态。

开始之前

您不能将 BVI 添加到安全区域；因此，不能将访问控制策略应用到 BVI。必须根据其区域将策略应用于网桥组成员接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 选择**添加接口** > **网桥组接口**。

步骤 3 （路由模式）在**名称**字段中，输入长度最大为 48 个字符的名称。

如果要在网桥组成员之外路由流量，例如路由到外部接口或其他网桥组的成员，则必须为 BVI 命名。该名称不区分大小写。

步骤 4 在**网桥组 ID** 字段中，输入 1 和 250 之间的网桥组 ID。

步骤 5 在**说明**字段中，输入此网桥组的说明。

步骤 6 在**接口**选项卡上，点击某个接口对，然后点击**添加**，以将其移动至**选定的接口**区域。对要使其成为网桥组成员的所有接口重复此步骤。

步骤 7 （透明模式）点击 **IPv4** 选项卡。在 **IP 地址**字段中，输入 IPv4 地址和子网掩码。

请勿为 BVI 分配主机地址（/32 或 255.255.255.255）。此外，请勿使用主机地址不足 3 个（分别用于上游路由器、下游路由器和透明防火墙）的其他子网，例如 /30 子网 (255.255.255.252)。Firewall Threat Defense 设备会丢弃传入子网中第一个和最后一个地址或从其传出的所有 ARP 数据包。例如，如果您使用 /30 子网，并从该子网中为上游路由器分配了一个预留地址，那么 Firewall Threat Defense 设备将丢弃从下游路由器发送至上游路由器的 ARP 请求。

对于高可用性，请在 **设备** > **设备管理** 页面上设置备用 IP 地址，然后点击**监控接口**区域中的**高可用性**选项卡。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 8 （路由模式）点击 **IPv4** 选项卡。要设置 IP 地址，请使用 **IP 类型**下拉列表中的下列选项之一。

高可用性和集群接口仅支持静态 IP 地址配置；不支持 DHCP。

- **使用静态 IP** - 输入 IP 地址和子网掩码。对于高可用性，只能使用静态 IP 地址。在 **设备** > **设备管理** 上设置备用 IP 地址，然后在**监控接口**区域中点击**高可用性**选项卡。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **使用 DHCP** - 配置以下可选参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

步骤 9 （可选） 请参阅配置 IPv6 寻址，第 801 页配置 Ipv6 寻址。

步骤 10 （可选） 要配置 **ARP** 和 **MAC** 设置，请参阅添加静态 ARP 条目，第 821 页和添加静态 MAC 地址并为网桥组禁用 MAC 学习，第 821 页（仅对于透明模式）。

步骤 11 点击**确定**。

步骤 12 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 IPv6 寻址

本节介绍如何在路由模式和透明模式下配置 IPv6 寻址。

关于 IPv6

本节包括关于 IPv6 的信息。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要为 BVI（而不必为每个成员接口）配置此地址。还可以为透明模式下的管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或邻居发现功能，例如地址解析。在网桥组中，只有成员接口具有链路本地地址；BVI 没有链路本地地址。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。对于网桥组成员接口，在 BVI 上配置全局地址时，Firewall 威胁防御设备 将为成员接口自动生成链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

修改的 EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址（以二进制值 000 开头的地址除外）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。Firewall 威胁防御设备可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。

配置 IPv6 前缀代理客户端

Firewall Threat Defense 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 Firewall Threat Defense 可以将这些前缀通过子网分配到其内部接口。

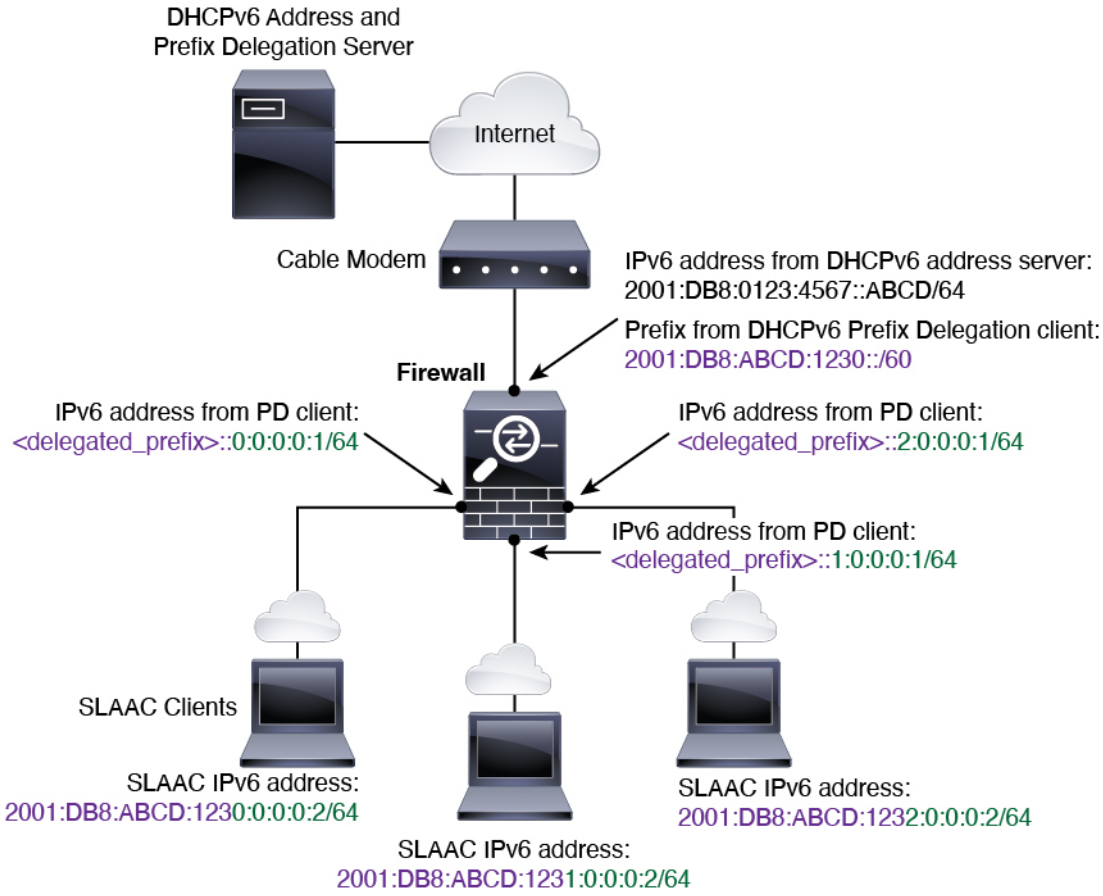
关于 IPv6 前缀授权

Firewall Threat Defense 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 Firewall Threat Defense 可以将这些前缀通过子网分配到其内部接口。然后，连接到内部接口的主机可以使用无状态地址自动配置 (SLAAC) 获取全局 IPv6 地址。请注意，内部 Firewall Threat Defense 接口不会依次充当前缀授权服务器；Firewall Threat Defense 只能向 SLAAC 客户端提供全局 IP 地址。例如，如果路由器连接到 Firewall Threat Defense，它可以作为 SLAAC 客户端获取其 IP 地址。但是，如果您要为路由器后的网络使用授权的前缀的子网，则必须在路由器的内部接口上手动配置这些地址。

Firewall Threat Defense 中包括一个轻型 DHCPv6 服务器，以便 SLAAC 客户端在向 Firewall Threat Defense 发送信息请求 (IR) 数据包时，Firewall Threat Defense 可以向这些客户端提供 DNS 服务器和域名等信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 Firewall Threat Defense 的前缀。

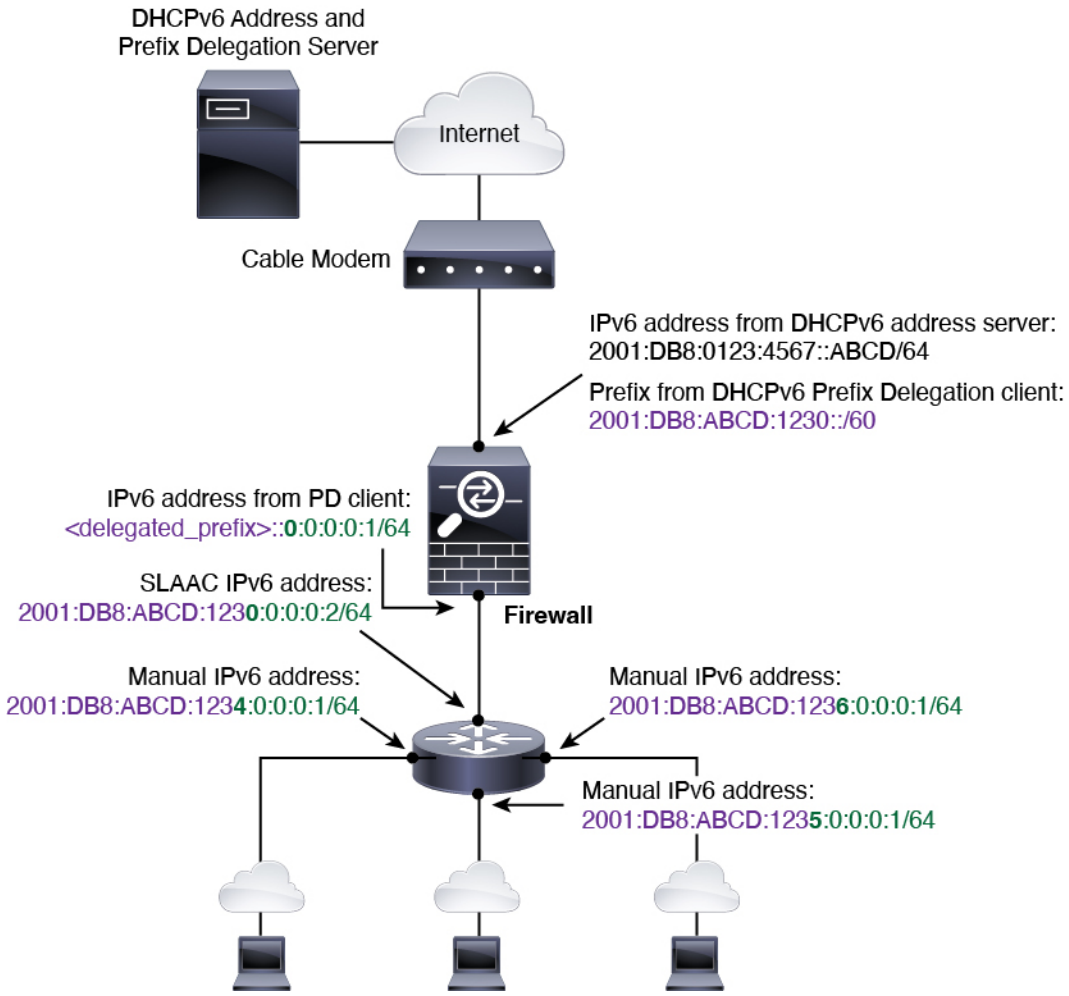
IPv6 前缀授权 */64* 子网示例

以下示例显示使用 DHCPv6 地址客户端在外部接口上接收 IP 地址的 Firewall Threat Defense。此外，它还会使用 DHCPv6 前缀授权客户端获得一个授权的前缀。Firewall Threat Defense 将授权的前缀编入 /64 网络的子网，并使用授权的前缀以及手动配置的子网（::0、::1 或 ::2）和每个接口上的 IPv6 地址 (0:0:0:1) 为其内部接口动态分配全局 IPv6 地址。连接至这些内部接口的 SLAAC 客户端将获得每个 /64 子网上的 IPv6 地址。



IPv6 前缀委派 */62* 子网示例

以下示例显示了 Firewall Threat Defense 将前缀子网划分到 4 个 /62 子网中:2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62 和 2001:DB8:ABCD:123**C**::/62。Firewall Threat Defense 将 2001:DB8:ABCD:1230::/62 上 4 个可用 /64 子网之一用于其内部网络 (::0)。随后您可以手动将其他 /62 子网用于下游路由器。所示的路由器将 2001:DB8:ABCD:1234::/62 上 4 个可用 /64 子网中的 3 个用于其内部接口（::4、::5 和 ::6）。在此情况下，内部路由器接口无法动态获取委派的前缀，因此您需要在 Firewall Threat Defense 上查看委派的前缀，然后将该前缀用于您的路由器配置。通常，当租约到期时，ISP 会将同一前缀委派给指定客户端，但如果 Firewall Threat Defense 收到新前缀，则您必须修改路由器配置以使用该新前缀。DHCP 唯一标识符 (DUID) 在重新启动时会保持不变。



启用 IPv6 前缀授权客户端

在一个或多个接口上启用 DHCPv6 前缀代理客户端。Firewall Threat Defense 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 Firewall Threat Defense 接口才能使用代理前缀衍生的地址。

此功能仅支持路由模式。此功能不支持集群或高可用性。

开始之前

当您使用前缀代理时，必须将 Firewall Threat Defense IPv6 邻居发现路由器通告间隔设置为远低于 DHCPv6 服务器分配的前缀的首选有效期，以防 IPv6 流量中断。例如，如果 DHCPv6 服务器将首选前缀代理有效期设置为 300 秒，则您应将 Firewall Threat Defense RA 间隔设置为 150 秒。要设置首选有效期，请使用 **show ipv6 general-prefix** 命令。要设置 Firewall Threat Defense RA 间隔，请参阅配置 IPv6 邻居发现，第 810 页；默认值为 200 秒。

过程

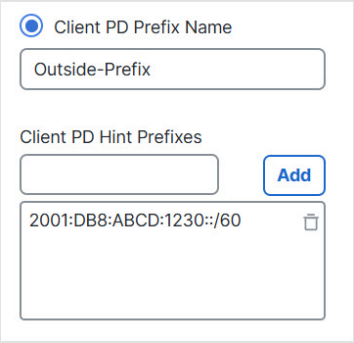
步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6** 页面，然后点击 **DHCP**。

步骤 4 点击**客户端 PD 前缀名称 (Client PD Prefix Name)**，然后输入此前缀的名称。

图 *313:* 启用前缀授权客户端



name 最长为 200 个字符。

步骤 5 （可选）在**客户端 PD 提示前缀 (Client PD Hint Prefixes)** 字段中输入前缀和前缀长度，以便向 DHCP 服务器提供有关要接收的委派前缀的一个或多个提示，然后点击**添加 (Add)**。

通常，您需要请求特定的前缀长度（例如 ::/60），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置全局 IPv6 地址

要为任何路由模式接口和透明或路由模式 BVI 配置全局 IPv6 地址，请执行以下步骤。

注释 配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。对于网桥组，在 BVI 上配置全局地址会自动在所有成员接口上配置链路本地地址。

对于在 Firewall 威胁防御 上定义的子接口，建议您同样手动设置 MAC 地址，这是因为它们使用父接口上相同的固化 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址，这能够避免 Firewall 威胁防御 上特定实例内发生流量中断。请参阅配置 MAC 地址，第 820 页。

开始之前

对于网桥组的 IPv6 邻居发现，您必须使用双向访问规则明确允许邻居请求（ICMPv6 类型 135）和邻居通告（ICMPv6 类型 136）数据包通过 Firewall Threat Defense 网桥组成员接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6** 页面。

对于路由模式，**基本 (Basic)** 页面默认处于选中状态。对于透明模式，**地址 (Address)** 页面默认处于选中状态。

步骤 4 （可选） 在**基本 (Basic)** 页面上，选中**启用 IPv6 (Enable IPv6)**。

如果您只想配置链路本地地址，请使用此选项。否则，配置 IPv6 地址将自动启用 IPv6 处理。

步骤 5 使用以下其中一种方法配置全局 IPv6 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址。对于集群，也不支持手动配置链路本地地址。

- （路由接口）无状态自动配置 - 选中**自动配置**复选框。

  在接口上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID 自动生成接口的链路本地地址。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 Firewall Threat Defense 设备在这种情况下确实会发送路由器通告消息。依次点击 **Settings** 选项卡和 **IPv6** 选项卡，然后取消选中 **启用 RA** 复选框以抑制消息。

- 手动配置 - 要手动配置全局 IPv6 地址，请执行以下操作：

  1. 点击**地址 (Address)** 页面并点击 (+)**添加地址 (Add Address)**。

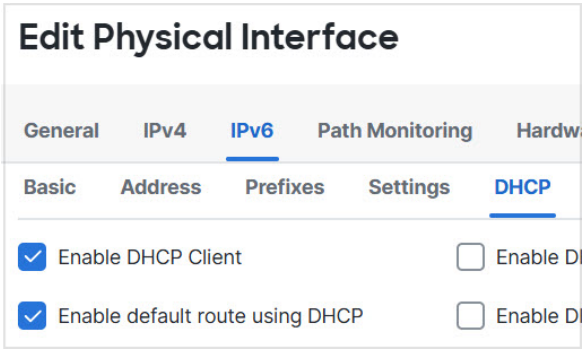
     系统将显示**添加接口**对话框。

2. 在**地址**字段中，输入完整全局 IPv6 地址（包括接口 ID），或输入 IPv6 前缀以及 IPv6 前缀长度。（路由模式）如果仅输入前缀，请务必选中**强制 EUI 64** 复选框，以使用修改的 EUI-64 格式生成接口 ID。例如，2001:0DB8::BA98:0:3210/48（完整地址）或 2001:0DB8::/48（前缀，且选中 EUI 64）。

   对于高可用性（如果您没有设置 **强制执行 EUI 64**，请在 **设备** > **设备管理** 页面上设置备用 IP 地址，然后在 **受监控接口** 区域中单击 **高可用性**。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

- （路由接口）使用 DHCPv6 获取地址 - 要使用 DHCPv6，请执行以下操作：

图 *314:* 启用 *DHCPv6* 客户端



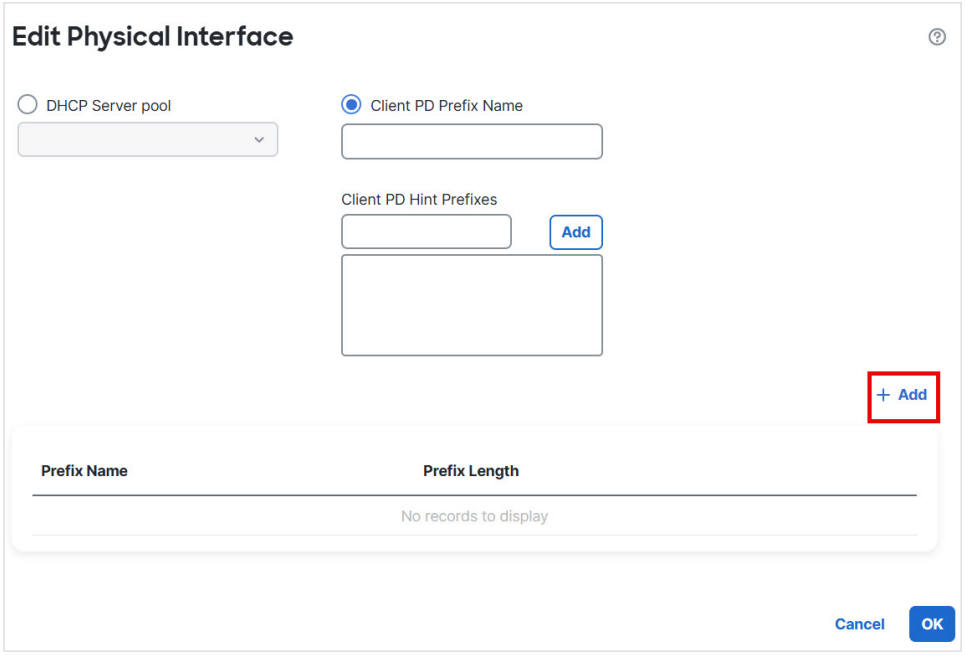
1. 点击 **DHCP** 页面。
2. 选中**启用 DHCP 客户端 (Enable DHCP Client)** 的复选框。
3. （可选）选中**使用 DHCP 启用默认路由 (Enable default route using DHCP)** 复选框，从路由器通告中获取默认路由。

- （路由接口）使用授权前缀 - 要使用授权前缀分配 IPv6 地址，请执行以下操作：

  此功能要求 Firewall Threat Defense 在不同接口上启用 DHCPv6 前缀授权客户端。请参阅启用 IPv6 前缀授权客户端，第 804 页。

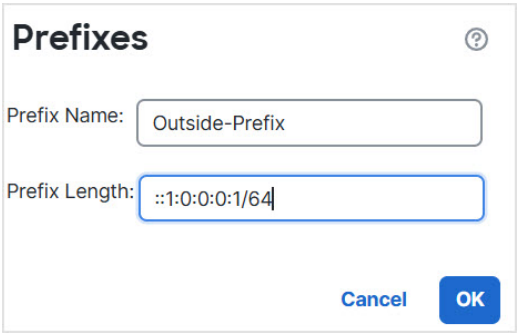
1. 点击 **DHCP** 页面。
2. 请点击 (+)。

图 *315:* 使用授权的前缀



3. 输入您在另一个接口上为前缀委派客户端指定的**前缀名称**（请参阅启用 IPv6 前缀授权客户端，第 804 页）。

图 *316:* 指定前缀名称和地址

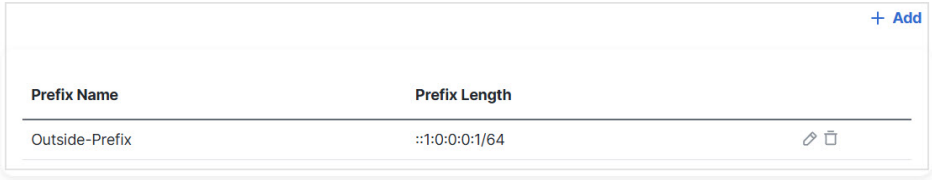


4. 输入 IPv6 地址和**前缀长度**。

   通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:Db8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。

5. 点击**确定**。

图 *317:* 前缀授权表



6. 或者，在此接口上启用 DHCPv6 无状态服务器（请参阅启用 DHCPv6 无状态服务器，第 963 页）。如果执行此操作，我们建议您同时选中**为非地址配置启用 DHCP (Enable DHCP for non-address config)** 选项。

步骤 6 对于路由接口，您可以选择在**基本 (Basic)** 页面上设置下列值：

- 要在本地链路上的 IPv6 地址中强制使用修改的 EUI-64 格式的接口标识符，请选中**强制 EUI-64** 复选框。
- 要手动设置链路本地地址，请在**链路本地地址**字段中输入地址。

  链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。如果您不想配置全局地址，且只需配置链路本地地址，则可以选择手动定义链路本地地址。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

  集群不支持手动链路本地地址。

步骤 7 对于路由接口，您可以选择在 **DHCP** 页面上设置下列值：

- 选中**为地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置托管地址配置标志。

  IPv6 路由器通告中的此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。

- 选中**为非地址配置启用 DHCP** 复选框以在 IPv6 路由器通告数据包中设置其他地址配置标志。

  IPv6 路由器通告中的此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。在使用具有 DHCPv6 前缀委派的 DHCPv6 无状态服务器时使用此选项。

步骤 8 对于路由接口，请参阅配置 IPv6 邻居发现，第 810 页以配置**前缀 (Prefixes)** 和**设置 (Settings)** 页面上的设置。对于 BVI 接口，请参阅**设置 (Settings)** 页面上的以下参数：

- **DAD 尝试次数** - DAD 尝试的最大数，介于 1 和 600 之间。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。默认值为 1 次尝试。
- **NS 间隔** - 接口上 Ipv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。默认值为 1000 毫秒。
- **可达时间** - 可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪

可访问时间的值。邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 9 点击**确定**。

步骤 10 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 IPv6 邻居发现

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络（本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点（主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可访问及哪些邻居不可访问，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

开始之前

仅在路由模式下受支持。有关透明模式下支持的 IPv6 邻居设置，请参阅配置全局 IPv6 地址，第 805 页。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6**，然后点击**前缀 (Prefixes)**。

步骤 4 （可选） 要配置包含在 IPv6 路由器通告中的 IPv6 前缀，请执行以下步骤：

a) 点击 (＋)**添加前缀**。

b) 在**地址**字段中，输入带有前缀长度的 IPv6 地址，或选中**默认**复选框以使用默认前缀。

c) （可选）取消选中**通告**复选框，以指示未通告 IPv6 前缀。对于**默认**前缀，此设置仅适用于 on-link 前缀。除非您取消选中特定 Off-link 前缀的**通告**，否则仍将通告 Off-link 前缀。

d) 选中**关闭链路**复选框以指示指定的前缀已分配给链路。向包含指定前缀的地址发送流量的节点会将目标视为在链路上本地可访问。此前缀不得用于链路上确定。

e) 要使用指定的前缀进行自动配置，请选中**自动配置**复选框。

f) 对于**前缀有效期**，请点击**持续时间**或**到期日期**。

- **持续时间** - 以秒为单位输入前缀的**首选有效期**。此设置是将指定的 IPv6 前缀通告为有效的时间。最大值代表无穷大。有效值为 0 到 4294967295。默认值为 2592000 秒（30 天）。以秒为单位输入前缀的**有效期**。此设置是将指定的 IPv6 前缀通告为首选时间。最大值代表无

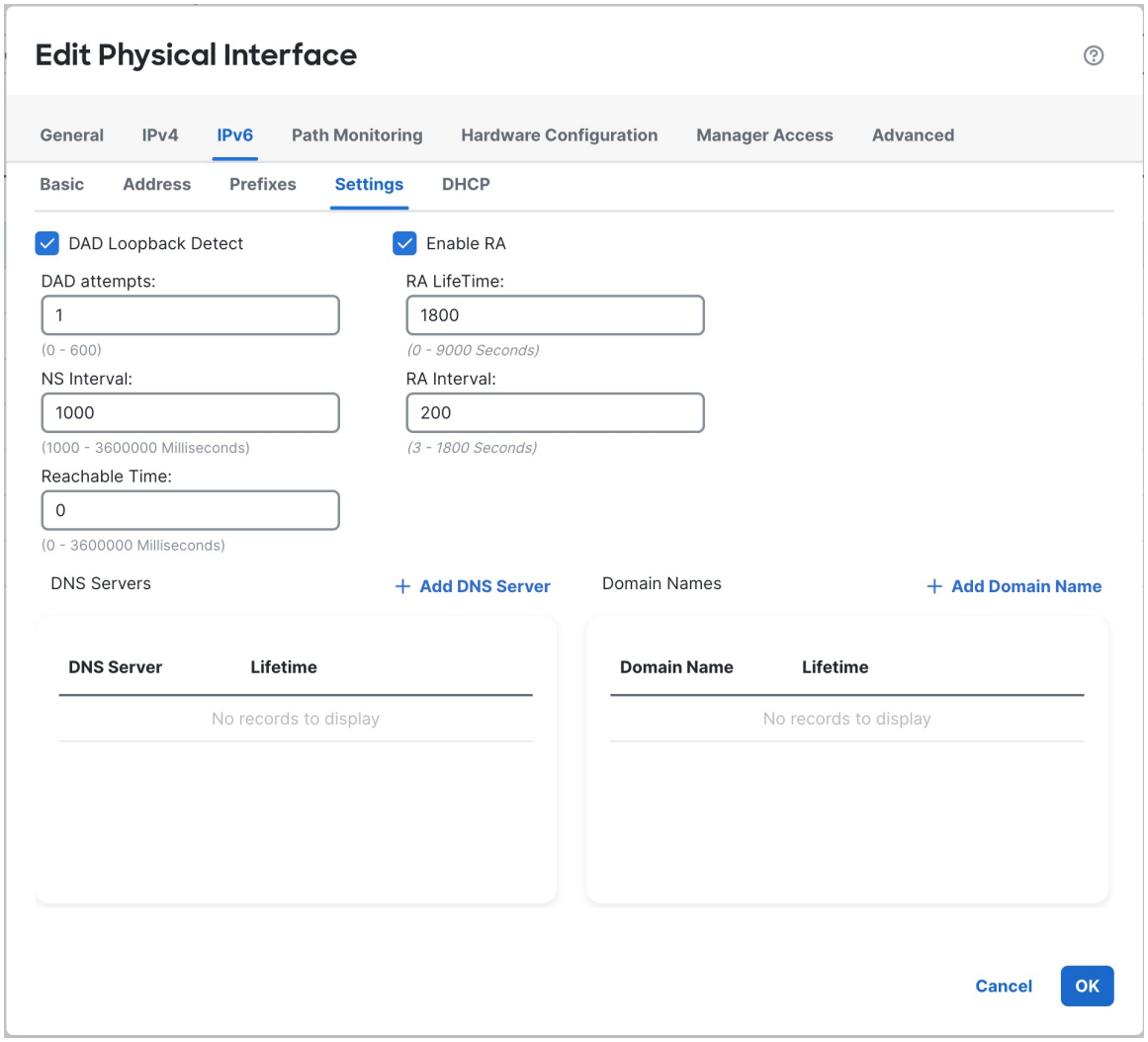
穷大。有效值为 0 到 4294967295。默认设置为 604800 秒（七天）。或者，选中**无限 (Infinite)**复选框以设置不受限制的持续时间。

- **到期日期** - 选择**有效**和**首选**日期和时间。

g) 点击**确定**。

步骤 5 点击**设置**。

图 *318: BGP IPv6* 设置



步骤 6 （可选） 设置介于 1 和 600 之间的 **DAD 尝试次数**最大值。默认值为 1 次尝试。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

此设置可配置当对 IPv6 地址执行 DAD 时，接口上发送的连续邻居请求消息的数量。

在无状态自动配置过程中，重复地址检测会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。

步骤 7 （可选） 在 **NS 间隔**字段中配置 IPv6 邻居请求重新传输之间的间隔，介于 1000 和 3600000 毫秒之间。

默认值为 1000 毫秒。

邻居请求消息（ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息（ICPMv6 类型 136）作出应答。

源节点接收邻居通告后，源节点与目标节点即可通信。识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可访问性。当节点要验证邻居的可访问性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。

步骤 8 （可选） 在**可达时间**字段中，配置可达性确认事件发生后远程 IPv6 节点被视为可达的时长，介于 0 和 3600000 毫米之间。

默认值为 0 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

步骤 9 （可选） 要禁用路由器通告传输，请取消选中**启用 RA** 复选框。如果启用路由器通告传输，则可以设置 RA 的有效期和间隔。

路由器通告消息（ICMPv6 类型 134）会自动发送，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

在不希望 Firewall Threat Defense 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

- **RA 有效期** - 在 IPv6 路由器通告中配置路由器有效期的值，介于 0 和 9000 秒之间。

  默认值为 1800 秒。

- **RA 间隔** - 配置 IPv6 路由器通告传输之间的间隔，介于 3 和 1800 秒之间。

  默认值为 200 秒。

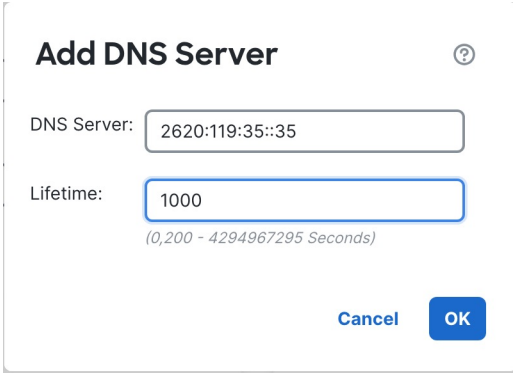
  为防止与其他 IPv6 节点同步，防火墙会随机调整您设置的值（抖动）。

步骤 10 （可选） 配置递归 DNS 服务器 (RDNSS) 选项，以向 IPv6 客户端通告 DNS 服务器列表。

对于使用 SLAAC 而不是 DHCPv6 进行寻址的客户端，此选项非常有用。请注意，如果在 Firewall Threat Defense上启用了前缀委派客户端，也可以使用 Firewall Threat Defense的 DHCPv6 无状态服务器传递 Firewall Threat Defense 接收到的 DNS 服务器信息。 如果两种方法都配置，则客户端将同时接收两组服务器。

a) 在 **DNS 服务器**区域中，点击**添加 DNS 服务器**。

图 *319:* 添加 *DNS* 服务器



b) 输入 **DNS 服务器** IPv6 地址。

c) 输入 DNS 服务器用于域名解析的最长**生命周期**（以秒为单位），范围为 200 到 4294967295。如果将该值设置为 0，将不使用该条目。如果将该值设置为 4294967295，则该条目永不过期。默认值为最大 RA 间隔的 3 倍。值必须大于或等于**RA 间隔**

d) 点击**确定**。

e) 最多可为 8 个站点重复该过程。

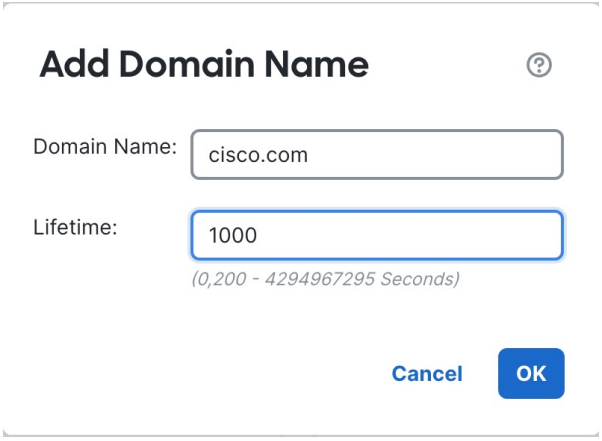
服务器按照添加顺序进行通告。

步骤 11 （可选） 配置 DNS 搜索列表 (DNSSL) 选项，向 IPv6 客户端通告搜索域列表。

对于使用 SLAAC 而不是 DHCPv6 进行寻址的客户端，此选项非常有用。请注意，如果您在Firewall Threat Defense上启用了前缀委派客户端，也可以使用Firewall Threat Defense 的 DHCPv6 无状态服务器传递Firewall Threat Defense 接收到的 DNS 域。 如果同时配置这两种方法，则客户端将接收两套域。

a) 在**路由器通告 DNS 搜索列表**区域中，点击**添加**。

图 *320:* 添加域进行搜索



b) 输入**域名**。

c) 输入域使用的最长**生命周期**持续时间（以秒为单位），范围为 200 到 4294967295。如果将该值设置为 0，将不使用该条目。如果将该值设置为 4294967295，则该条目永不过期。默认值为最大 RA 间隔的 3 倍。值必须大于或等于**RA 间隔**

d) 点击**确定**。

e) 最多可对 5 个域重复此步骤。

域按添加顺序进行通告。

步骤 12 点击**确定**。

步骤 13 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置高级接口设置

本部分介绍如何为常规防火墙模式接口配置 MAC 地址，如何设置最大传输单元 (MTU) 以及如何设置其他高级参数。

关于高级接口配置

本节介绍高级接口设置。

关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。 对于容器实例，FXOS 机箱会自动为所有接口生成唯一 MAC 地址。

注释 您可能想要为 Firewall 威胁防御 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 Firewall 威胁防御 上特定实例内发生流量中断。

注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- VLAN 接口 (Firepower 1010 和 Cisco Secure Firewall 1210/1220) -路由防火墙模式： 所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅配置 MAC 地址，第 820 页。

  透明防火墙模式：各 VLAN 接口均有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅配置 MAC 地址，第 820 页。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。
- EtherChannel（ASA 型号）- 端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口配置 MAC 地址。我们建议在组通道接口成员身份更改时，配置唯一的 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。
- 子接口（Firewall Threat Defense 定义）- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 Firewall Threat Defense 上特定实例内发生流量中断。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址，第 298 页。

关于 MTU

MTU 指定 Firewall Threat Defense 在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

对于 Geneve，帧中会封装整个以太网数据报，因此新的 IP 数据包更大，需要更大的 MTU：您应该将 ASA VTEP 源接口 MTU 设置为网络 MTU + 306 字节。Firewall Threat Defense

路径 MTU 发现

Firewall Threat Defense 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

默认 MTU

Firewall 威胁防御设备 上的默认 MTU 为 1500 字节。该值不包括 18-22 字节的以太网报头、VLAN 标记和其他开销。

MTU 和分段

对于IPv4，如果传出IP数据包大于指定MTU，则该数据包将分为2帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 TCP 数据包，终端通常使用它们的 MTU 来确定 TCP 最大报文段长度（例如，MTU-40）。如果之后添加额外的 TCP 报头，例如对于站点间的 VPN 隧道，则 TCP MSS 可能需要由隧道传输实体向下调整。请参阅关于 TCP MSS，第 816 页。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，Firewall Threat Defense 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 Firewall Threat Defense接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 在启用巨型帧时，MTU 可设置为 9000 字节或更高。最大值取决于型号。

关于 TCP MSS

TCP 最大报文段长度 (MSS) 是 TCP 负载在添加任何 TCP 和 IP 报头前的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

您可以使用 FlexConfigFlexConfig 策略，第 1041 页；默认情况下，最大 TCP MSS 设置为 1380 字节。当 Firewall 威胁防御设备 需要增加数据包长度以执行 IPsec VPN 封装时，此设置非常有用。不过，对于非 IPsec 终端，应在 Firewall 威胁防御设备 上禁用最大 TCP MSS。

如果设置了 TCP MSS 的最大值，当连接的任一终端请求的 TCP MSS 大于 Firewall 威胁防御设备 中设定的值时，Firewall 威胁防御设备 会使用 Firewall 威胁防御设备 最大值覆盖请求数据包中的 TCP MSS。如果主机或服务器没有请求 TCP MSS，Firewall 威胁防御设备 会假定采用 RFC 793 的默认值 536 字节 (IPv4) 或 1220 字节 (IPv6)，但不会修改数据包。例如，可以将默认 MTU 保留为 1500 字节。如果主机请求的 MSS 为 1500 减去 TCP 和 IP 报头长度，这会将 MSS 设置为 1460。如果 Firewall 威胁防御设备 上的最大 TCP MSS 为 1380（默认值），Firewall 威胁防御设备 会将 TCP 请求数据包中的 MSS 值改为 1380。然后，服务器会发送 1380 字节负载的数据包。然后，Firewall 威胁防御设备 可向数据包中增加最多 120 字节的报头，并且仍然符合 1500 的 MTU 大小。

您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 Firewall 威胁防御设备 可将该值调高。默认情况下，最小 TCP MSS 未启用。

对于流向设备的流量，包括用于 SSL VPN 连接的流量，此设置不适用。Firewall 威胁防御设备 使用 MTU 来推导 TCP MSS：MTU - 40 (IPv4) 或 MTU - 60 (IPv6)。

默认 TCP MSS

默认情况下，Firewall 威胁防御设备 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可达到 120 字节）；此值在默认 MTU（1500 字节）范围内。

建议的最大 TCP MSS 设置

默认 TCP MSS 假定 Firewall 威胁防御设备作为 IPv4 IPsec VPN 终端，并且 MTU 为 1500。当 Firewall 威胁防御设备用作 IPv4 IPsec VPN 终端时，它需要为 TCP 和 IP 报头容纳最多 120 个字节。

如果您要更改 MTU 值、使用 IPv6 或不将Firewall 威胁防御设备设备用作 IPsec VPN 端点，则应更改 TCP MSS 设置使用 FlexConfig 中的 Sysopt_Basic 对象。

注释 即使您明确设置了 MSS，如果 TLS/SSL 解密或服务器发现等组件需要某个特定 MSS，它也会根据接口 MTU 设置该 MSS 并忽略您设置的 MSS。

请参阅以下准则：

- 正常流量 - 禁用 TCP MSS 限制，并接受在连接终端之间建立的值。由于连接终端一般是从 MTU 获得 TCP MSS，因此非 IPsec 数据包通常符合此 TCP MSS。
- IPv4 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨帧并将 MTU 设置为 9000，则需要将 TCP MSS 设置为 8880，以利用新 MTU。
- IPv6 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 140。

网桥组流量的 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，Firewall 威胁防御设备 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 Firewall 威胁防御设备 会丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 Firewall 威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。



注释 即使此参数设置为 flood，专用管理接口也绝不会以泛洪方式传输数据包。

MAC 地址表

当你使用网桥组时，Firewall 威胁防御 以与一般网桥或交换机相似的方式获悉和构建 MAC 地址表：当某个设备通过网桥组发送数据包时，Firewall 威胁防御 将在其表中添加 MAC 地址。此表将 MAC 地址与源接口相关联，以便 Firewall 威胁防御 可了解如何将要发送到设备的任何数据包从正确的接口发出。由于网桥组成员之间的流量须遵守 Firewall 威胁防御 安全策略，因此如果数据包的目标 MAC 地址不在此表中，则 Firewall 威胁防御 不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - Firewall 威胁防御 将生成针对目标 IP 地址的 ARP 请求，以使它能了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - Firewall 威胁防御将生成一个针对目标 IP 地址的 ping，以使它能了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

默认设置

- 如果启用 ARP 检测，则默认情况下会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 Firewall 威胁防御设备 会将对应的条目添加到 MAC 地址表中。

注释 Cisco Secure Firewall Threat Defense 设备 生成重置数据包以重置状态检测引擎拒绝的连接。在这里，数据包的目标 MAC 地址不是根据 ARP 表查找确定的，而是直接从被拒绝的数据包（连接）中获取的。

ARP 检测和 MAC 地址表准则

- ARP 检测仅支持网桥组。
- MAC 地址表配置仅支持网桥组。

配置 MTU

自定义接口上的 MTU，以便实现允许巨型帧等目的。

对于 ISA 3000 和 Firewall Threat Defense Virtual：将 MTU 更改为 1500 字节以上会自动启用巨帧预留。您必须重新启动系统，然后才能使用巨帧。 对于支持集群的 Firewall Threat Defense Virtual，您可以在 Day0 配置中启用巨帧预留，因此在这种情况下无需重新启动。重新启动后，您将无法禁用巨帧预留。Firewall Threat Defense Virtual 的例外情况是，您可以在 Day0 配置中禁用巨帧预留（如果支持）。如果在内联集中使用接口，则不使用 MTU 设置。但是，巨帧预留设置与内联集相关；巨帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨帧预留，您必须将任何接口的 MTU 设置为 1500 字节以上。

默认情况下，其他平台上会启用巨帧。

注意 当部署配置更改时，为数据接口更改设备上的最高 MTU 值会重新启动 Snort 进程，从而暂时中断流量检测。所有数据接口上的检测都会中断，而不只是在已修改的接口上中断。此中断是丢弃流量还是使其通过而不进一步检测取决于托管设备的型号和接口类型。此警告不适用于 仅管理接口。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在 **常规** 选项卡上，设置 **MTU**。最小值和最大值取决于您的平台。

默认值为 1500 字节。

步骤 4 点击**确定**。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 6 对于 ISA 3000 和 Firewall Threat Defense Virtual，如果您将 MTU 设置为 1500 字节以上，则请重新启动系统以启用巨帧预留。请参阅关闭或重新启动设备，第 64 页。

配置 MAC 地址

可能需要手动分配 MAC 地址。您还可以通过从添加 **设备** > **设备管理** (**Add**) 下拉列表中选择 **高可用性** 来设置主用和备用 MAC 地址。如果您在两个屏幕中均设置某个接口的 MAC 地址，则**接口** > **高级**选项卡上的地址具有较高优先级。



注释 对于容器实例，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级 (Advanced)** 选项卡。
将选择**信息 (Information)** 选项卡。

步骤 4 （对于单个接口模式下的集群）从下拉列表中选择 MAC 地址池。

您可以根据地址池，第 2630 页添加 MAC 地址池。

步骤 5 （对于其他模式）设置主用和备用 MAC 地址。

a) 在**主用 MAC 地址 (Active MAC Address)** 字段中，输入 H.H.H 格式的 MAC 地址，其中 H 表示 16 位的十六进制数字。

例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

b) 在**备用 MAC 地址 (Standby MAC Address)** 字段中，输入用于高可用性的 MAC 地址。

如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加静态 ARP 条目

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量（请参阅ARP 检测，第 975 页）。ARP 检测会对比 ARP 数据包与 ARP 表中的静态 ARP 条目。

对于路由接口，可以输入静态 ARP 条目，但通常动态条目就足够了。对于路由接口，使用 ARP 表向直连主机交付数据包。虽然发件人可根据 IP 地址识别数据包目标，但在以太网上实际交付数据包依赖于以太网 MAC 地址。当路由器或主机希望在直连网络上交付数据包时，它会发送 ARP 请求来寻求与该 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器可保留 ARP 表，所以不必对需要交付的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果某个条目错误（例如给定 IP 地址的 MAC 地址改变），该条目需要超时后，才能为其更新新信息。

对于透明模式，Firewall Threat Defense 仅对进出 Firewall Threat Defense 的流量（例如管理流量）使用 ARP 表中的动态 ARP 条目。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级**选项卡，然后点击 **ARP** 选项卡（在透明模式下，称为 **ARP 和 MAC**）。

步骤 4 点击 (+)**添加 ARP 配置**。
屏幕上随即会显示**添加 ARP 配置**对话框。

步骤 5 在 **IP 地址**字段中，输入主机的 IP 地址。

步骤 6 在 **MAC 地址**字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。

步骤 7 要对该地址执行代理 ARP，请选中**启用别名**复选框。

如果 Firewall Threat Defense 设备收到指定 IP 地址的 ARP 请求，则会使用指定 MAC 地址做出响应。

步骤 8 点击**确定**，然后再次点击**确定**退出“高级”设置。

步骤 9 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加静态 MAC 地址并为网桥组禁用 MAC 学习

通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。可以禁用 MAC 地址获悉；然而除非将 MAC 地址静态添加到表中，否则没有流量可以通过 Firewall

Threat Defense 设备。还可以向 MAC 地址表中添加静态 MAC 地址。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向与静态条目不匹配的接口发送流量，则 Firewall Threat Defense 设备会丢弃这些流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目，第 821 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

开始之前

此屏幕仅适用于透明模式下的命名 BVI。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级 (Advanced)**选项卡，然后点击 **ARP 和 MAC (ARP and MAC)** 选项卡。

步骤 4 （可选） 通过取消选中**启用 MAC 学习**复选框来禁用 MAC 学习。

步骤 5 要添加静态 MAC 地址，请点击**添加 MAC 配置 (Add MAC Config)**。
此时将显示**添加 MAC 配置**对话框。

步骤 6 在 **MAC 地址 (MAC Address)** 字段中，输入主机的 MAC 地址；例如，00e0.1e4e.3d8b。点击**确定 (OK)**。

步骤 7 点击**确定 (OK)** 以退出高级设置。

步骤 8 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

设置安全配置参数

本部分介绍如何防止 IP 欺骗、允许完整分段重组以及覆盖在**平台设置**中的设备级别设置的默认分段设置。

反欺骗

本部分使您可以在接口上启用单播反向路径转发。单播 RPF 根据路由表来确保所有数据包均有与正确的源接口匹配的源 IP 地址，从而避免 IP 欺骗（即数据包使用不正确的源 IP 地址以掩盖其真正来源）。

通常情况下，Firewall Threat Defense 设备在确定向何处转发数据包时只查看目标地址。单播 RPF 会指示设备还查找源地址；其因此被称为“反向路径转发”。对于您要允许通过 Firewall Threat Defense 设备的任何流量，设备路由表必须包括回到源地址的路由。有关详细信息，请参阅 RFC 2267。

例如，对于外部流量，Firewall Threat Defense 设备可使用默认路由来满足单播 RPF 保护。如果流量从外部接口进入，则路由表不知道源地址，而设备使用默认路由将外部接口正确识别为源接口。

如果流量从路由表中包含的已知地址进入外部接口，但与内部接口关联，则 Firewall Threat Defense 设备会丢弃该数据包。同样，如果流量从未知源地址进入内部接口，则设备会丢弃数据包，因为匹配的路由（默认路由）指示外部接口。

单播 RPF 的实施过程如下：

- ICMP 数据包没有会话，因此要检查每个数据包。
- UDP 和 TCP 有会话，因此初始数据包要求反向路由查找。对于在会话期间到达的后续数据包，使用作为部分会话来维护的现有状态进行检查。系统会检查非初始数据包，以确保它们到达初始数据包使用的同一接口。

每个数据包的分段数

默认情况下，Firewall Threat Defense设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但是，如果没有对流量分段的应用，则我们建议您不要允许分段通过 Firewall Threat Defense 设备。分段的数据包通常用作 DoS 攻击。

分段重组

Firewall Threat Defense 设备执行以下分段重组过程：

- 系统会收集 IP 分段，直到形成分段集或达到超时间隔。
- 如果分段集形成，则对片段集执行完整性检查。这些检查包括无重叠、无尾部溢出和无链溢出。
- 在 Firewall Threat Defense 设备处终止的 IP 分段始终会完全重组。
- 如果禁用了**完全分段重组**（默认设置），则分段集会转发到传输层以进一步处理。
- 如果启用了**完全分段重组**，则分段集首先会合并为单个 IP 数据包。然后，该单个 IP 数据包被转发到传输层，以供进一步处理。

开始之前

此屏幕仅适用于指定的接口。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击**高级**选项卡，然后点击**安全配置**选项卡。

步骤 4 要启用单播反向路径转发，请选中 **启用反欺骗** 复选框。

步骤 5 要启用完整分段重组，请选中 **允许完整分段重组** 复选框。

步骤 6 要更改每个数据包所允许的分段数，请选中**覆盖默认分段设置**复选框，并设置以下值：

- **大小** - 设置 IP 重组数据库中等待重组的最大数据包数。默认值为 200。将该值设置为 1 会禁用分段。
- **链** - 设置完整 IP 数据包可分成的最大数据包数。默认值为 24 个数据包。
- **超时** - 设置等待整个分段数据包到达的最大秒数。在数据包的第一个分段到达后计时器启动。如果在指定秒数后数据包的分段没有全部抵达，则已收到的数据包的所有分段将被丢弃。默认值为 5 秒。

步骤 7 点击**确定**。

步骤 8 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

常规防火墙接口的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
递归 DNS 服务器 (RDNSS) 和 DNS 搜索列表 (DNSSL) 选项，用于向 IPv6 客户端通告 DNS 服务器和域列表	10.0.0	10.0.0	现在，您可以配置递归 DNS 服务器 (RDNSS) 和 DNS 搜索列表 (DNSSL) 选项，以便为使用路由器通告的 SLAAC 客户端提供 DNS 服务器和域。 新增/修改的屏幕： **设备** > **设备管理** > **接口** > **添加/编辑接口** > **IPv6** > **设置** 新增/修改的命令： **show ipv6 nd detail**, **show ipv6 nd ra dns-search-list**, **show ipv6 nd ra dns server**, **show ipv6 nd summary**
Secure Firewall 200 硬件交换机支持	10.0.0	10.0.0	Secure Firewall 200 支持将各以太网接口设置为交换机端口或防火墙接口。
Cisco Secure Firewall 1210CP IEEE 802.3bt 支持（PoE++ 和 Hi-PoE）	7.7.0	7.7.0	请参阅以下与 IEEE 802.3bt 支持相关的改进： • PoE++ 和 Hi-PoE - 每个端口最高 90W。 • 单签名和双签名受电设备 (PD)。 • 电源预算遵循先到先得的原则。 • 功率预算字段已被添加到 **show power inline**。 新增/修改的屏幕：**设备** > **设备管理** > **接口** > **编辑物理接口** > **PoE** 新增/修改的命令：**show power inline**

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
对于带有内置交换机的型号，子接口不能使用 VLAN 1	7.6	7.6	对于带有内置交换机的型号，您无法使用 VLAN 1 创建子接口。VLAN 1 保留用于交换机端口的逻辑 VLAN 接口。 若将 1010 升级至 7.6 或以上版本，且已为子接口分配 VLAN 1，您必须将子接口的 VLAN ID 改为新 VLAN ID。将无法使用 VLAN 1 部署配置。
Cisco Secure Firewall 通过 GWLB 支持 AWS 上的双臂部署模式	7.6	7.6	Cisco Secure Firewall 支持在 AWS 上使用 GWLB 的双臂部署模式。此模式可使防火墙在进行流量检查后，通过互联网网关直接将互联网流量转发到互联网，同时还可执行网络地址转换 (NAT)。
Cisco Secure Firewall 1210/1220 硬件交换机支持	7.6	7.6	Cisco Secure Firewall 1210/1220 支持将各以太网接口设置为交换机端口或防火墙接口
以太网端口 1/5-1/8 上的 Cisco Secure Firewall 1210CP PoE+ 支持	7.6	7.6	Cisco Secure Firewall 1210CP 在以太网端口 1/5-1/8 上支持以太网供电+ (PoE+)。
VXLAN VTEP IPv6 支持	7.4	任意	现在，您可以为 VXLAN VTEP 接口指定 IPv6 地址。Threat Defense Virtual 集群控制链路或 Geneve 封装不支持 IPv6。 新增/修改的屏幕： • **设备** > **设备管理** > **编辑** > **VTEP** > **添加 VTEP** **设备** > **设备管理** > **编辑** > **接口** > **添加接口** > **VNI 接口** 需要 Firewall Threat Defense 7.4 版本。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
环回接口支持 BGP 和管理流量	7.4	任意	您可以将环回接口用于： • AAA • BGP • DNS • HTTP • ICMP • IPsec 流分流 • NetFlow • SNMP • SSH • 系统日志 需要 Firewall Threat Defense 7.4 版本。
VTI 的环回接口支持。	7.3	任意	您现在可以添加环回接口。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。对于 VTI，除了将环回接口设置为源接口外，还添加了支持以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **添加环回接口 (Add Loopback Interface)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
IPv6 DHCP	7.3	任意	Firewall Threat Defense 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - Firewall Threat Defense 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - Firewall Threat Defense 从 DHCPv6 服务器获取指定的前缀。然后，Firewall Threat Defense 可以使用这些前缀来配置其他 Firewall Threat Defense 接口地址，以便无状态地址自动配置 (SLAAC) 客户端可以自动配置同一网络上的 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 Firewall Threat Defense 发送信息请求 (IR) 数据包时，Firewall Threat Defense 会向它们提供域名等其他信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加/编辑接口 (Add/Edit Interfaces)** > **IPv6** > **DHCP** • **对象 (Objects)** > **对象管理 (Object Management)** > **DHCP IPv6 池 (DHCP IPv6 Pool)** 新增/修改的命令：**show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix**
Firewall Threat Defense Virtual 用于 Azure 网关负载均衡器的已配对代理 VXLAN	7.3	任意	您可以为 Azure 中的 Firewall Threat Defense Virtual 配置配对代理模式 VXLAN 接口，以便与 Azure 网关负载均衡器 (GWLB) 配合使用。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** 支持的平台：Azure 中的 Firewall Threat Defense Virtual

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
VXLAN 支持	7.2	任意	添加了 VXLAN 封装支持。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **VTEP** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** 编辑物理接口 > **General** 支持的平台：全部
Geneve 支持 Firewall Threat Defense Virtual	7.1	任意	为 Firewall Threat Defense Virtual 增加了 Geneve 封装支持，以支持 Amazon Web 服务 (AWS) 网关负载均衡器的单臂代理。AWS 网关负载均衡器将透明网络网关（所有流量都有一个入口和出口点）与负载均衡器相结合，该负载均衡器可分配流量并扩展 Firewall Threat Defense Virtual 以匹配流量需求。 此功能需要使用 Snort 3。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **VTEP** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **添加接口 (Add Interfaces)** > **VNI 接口 (VNI Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** 编辑物理接口 > **General** 支持的平台：AWS 中的 Firewall Threat Defense Virtual

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
31 位子网掩码	7.0	任意	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 FTD 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行SNMP或系统日志的一个直连管理站。网桥组或组播路由的 BVI 不支持此功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)**
Firepower 4100/9300 的 Firewall Threat Defense 运行链路状态与物理链路状态之间的同步	6.7	任意	Firepower 4100/9300 机箱现在可以将 Firewall Threat Defense 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 Firewall Threat Defense 应用接口管理状态。如果没有从 Firewall Threat Defense同步，数据接口可能在 Firewall Threat Defense 应用完全上线之前处于“Up”物理状态，或者在您启动 Firewall Threat Defense 关闭后的一段时间内保持 “Up” 状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 Firewall Threat Defense 可以处理流量之前开始向 Firewall Threat Defense 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 Firewall Threat Defense 不支持此功能。ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail** 支持的平台：Firepower 4100/9300
Firepower 1010 硬件交换机支持	6.5	任意	Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加 VLAN 接口 (Add VLAN Interface)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8	6.5	任意	在被配置为交换机端口时，Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **PoE**
用于容器实例的VLAN子接口	6.3.0	任意	要确保灵活使用物理接口，可以在FXOS中创建VLAN子接口，还可以在多个实例之间共享接口。 新增/修改的 Secure Firewall Management Center菜单项： **设备** > **设备管理** > **编辑** 图标 > **接口** 选项卡 新增/修改的 Cisco Secure Firewall 机箱管理器菜单项： **接口** > **所有接口** > **新增**下拉菜单**子接口** 新增/修改的FXOS 命令：**create subinterface**、**set vlan**、**show interface**、**show subinterface** 支持的平台：Firepower 4100/9300
用于容器实例的数据共享接口	6.3.0	任意	要确保灵活使用物理接口，可以在多个实例之间共享接口。 新增/修改的 Cisco Secure Firewall 机箱管理器菜单项： **接口** > **所有接口** > **类型** 新增/修改的 FXOS 命令：**set port-type data-sharing**、**show interface** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
集成路由和桥接	6.2.0	任意	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组是指 Firewall Threat Defense 网桥（而非路由）的接口组。Firewall Threat Defense 并非真正的网桥，因为 Firewall Threat Defense 仍将继续充当防火墙：接口之间实施访问控制，并且部署所有常用防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 Firewall Threat Defense 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 以下功能在透明模式下受支持，但在路由模式下不受支持：集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** • 设备 > 设备管理 > 接口 > 添加接口 > 网桥组接口 支持的平台：Firepower 2100 和 Firewall Threat Defense Virtual 以外的所有平台



第 16 章

内联集和被动接口

您可以配置仅限 IPS 被动接口、被动 ERSPAN 接口和内联集。

- 关于 IPS 接口，第 833 页
- 内联集的要求和前提条件，第 836 页
- 内联集和被动接口的准则，第 838 页
- 配置被动接口，第 840 页
- 配置内联集，第 841 页
- 内联集和被动接口的历史记录，第 844 页

关于 IPS 接口

IPS 接口包括无源接口、无源 ERSPAN 接口和内联集。IPS-only 模式接口可以绕过许多防火墙检查，只支持 IPS 安全策略 (Snort)。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。

IPS-only 模式接口可以绕过许多防火墙检查，只支持 IPS 安全策略 (Snort)。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。



注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。

内联集

内联集就像导线上的凸起，用于将一个或多个接口对绑定在一起，以便插入到现有网络中。此功能使 Firewall Threat Defense 可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但除非已明确丢弃，否则这些接口上接收的所有流量都会从内联接口对中的另一个接口重传出去。当当一个内联集中有多个内联对时，流量只能在内联对中的接口间传输，而无法在不同内联对的接口间传输。

在分流模式下，Firewall Threat Defense 会进行内联部署，但网络流量不受干扰。相反，Firewall Threat Defense 会复制每个数据包，这样它就可以对数据包进行分析。请注意，这些类型的规则在触发时会

生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。在已部署内联的FTD上使用分流模式有很多优点。例如，您可以设置 Firewall Threat Defense 和网络之间的布线，就像 Firewall Threat Defense 是内联，并分析 Firewall Threat Defense 生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署Firewall Threat Defense内联时，您可以禁用分流模式，并开始丢弃可疑流量，而无需重新配置Firewall Threat Defense和网络之间的走线。

注释 分流模式 显著 影响 Firewall Threat Defense 性能，具体取决于流量。

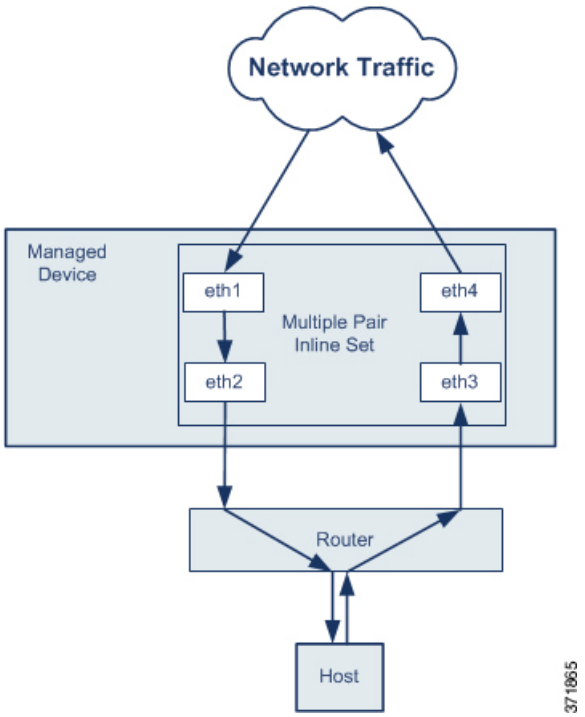
注释 内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与透明防火墙模式或防火墙类型接口无关。

多个内联对和异步路由

您可以配置接口通过不同的内联对路由网络上的主机和外部主机之间的流量，具体取决于流量是入站还是出站。这是异步路由配置。如果您部署的是异步路由，但一个内联集只包含一个内联对，则设备可能无法正确分析网络流量，因为它可能只会发现一半的流量。

在同一内联集中添加多个内联对，可让系统将入站和出站流量识别为同一流量的一部分。您也可以通过将接口对包括在同一安全区域中来实现此目的，但这种方法仅适用于被动接口。

图 *321:* 异步路由



注释 如果将多个内联对分配给一个内联集，但遇到重复流量问题，则可能需要将内联对重新分配给不同的内联集或修改安全区。

如果在不同的接口对上收到数据包的分片，它们不会重组，而是会被丢弃。确保在同一接口对上接收和发送数据包的所有分片。

被动接口

被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置 Firewall Threat Defense，Firewall Threat Defense 将无法执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。封装远程交换端口分析器 (ERSPAN) 接口允许您监控分布于多个交换机的源端口流量，并使用 GRE 来封装流量。仅当 Firewall Threat Defense 处于路由防火墙模式时，才允许 ERSPAN 接口。

注释 由于混杂模式限制，某些使用 SR-IOV 驱动程序的 Intel 网络适配器（例如 Intel X710 或 82599）不支持在 NGFWv 上将 SR-IOV 接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅英特尔以太网产品。

关于内联集的硬件旁路

对于支持的型号上的某些接口模块（请参阅内联集的要求和前提条件，第 836 页），您可以启用 硬件旁路 功能。硬件旁路 可确保流量在停电期间继续在内联接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

硬件旁路触发器

硬件旁路可以在以下情况下触发：

- Firewall Threat Defense崩溃
- Firewall Threat Defense 重新启动
- 安全模块重新启动
- 机箱崩溃
- 重新引导机箱
- 手动触发
- 机箱断电
- 安全模块断电

注释 硬件旁路适用于计划外/意外故障情况，并且在计划的软件升级期间不会自动触发。硬件旁路仅在计划的升级过程结束时，当 Firewall Threat Defense 应用重新启动时才会启用。

硬件旁路切换

当从正常操作切换到硬件旁路或从硬件旁路切换回正常操作时，流量可能会中断几秒钟。中断时长可能受许多因素影响；例如，铜缆端口自动协商、光纤链路合作伙伴的行为（比如如何处理链路故障和去抖时间）、生成树协议汇聚、动态路由协议汇聚等等。在此期间，您可能会遇到连接中断。

还有可能在恢复正常运行后分析连接中游时由于应用识别错误而遇到连接中断。

Snort 故障开启与硬件旁路

对于不是分路模式下的内联集的内联集，您可以使用“Snort 故障开启”选项，在不检查 Snort 进程何时繁忙或关闭的情况下丢弃流量或允许流量通过。除了分路模式下的内联集，其他所有内联集上都支持“Snort 故障开启”，而不仅仅是支持硬件旁路的接口。

硬件旁路功能允许流量在硬件故障（包括完全断电以及有限的一些软件故障）期间流动。触发 Snort 故障开启的软件故障不会触发硬件旁路。

硬件旁路 状态

如果系统通电，则旁路 LED 指示灯指示硬件旁路状态。请参阅 Firepower 机箱硬件安装指南中有关 LED 的说明。

内联集的要求和前提条件

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件旁路 支持

对于以下型号上特定网络模块的接口对，Firewall Threat Defense 支持 硬件旁路：

- Cisco Secure Firewall 3100
- Firepower 4100
- Cisco Secure Firewall 4200
- Firepower 9300

- Cisco Secure Firewall 6100



注释 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

这些型号的受支持 硬件旁路 网络包括：

- Cisco Secure Firewall 3100：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR3K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X10LRF)
  - 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-X25SRF)
  - 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X25LRF)
  - 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR3K-XNM-8X1GF)
- Cisco Secure Firewall 4200：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR4K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X10LRF)
  - 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-X25SRF)
  - 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X25LRF)
  - 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR4K-XNM-8X1GF)
- Firepower 4100：
  - Firepower 6-端口 1G SX FTW 单位宽网络模块 (FPR4K-NM-6X1SX-F)
  - Firepower 6-端口 10G SR FTW 单位宽网络模块 (FPR4K-NM-6X10SR-F)
  - Firepower 6-端口 10G LR FTW 单位宽网络模块 (FPR4K-NM-6X10LR-F)
  - Firepower 2-端口 40G SR FTW 单位宽网络模块 (FPR4K-NM-2X40G-F)
  - Firepower 8-端口 1G 铜 FTW 单位宽网络模块 (FPR-NM-8X1G-F)
- Cisco Secure Firewall 6100：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR4K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X10LRF)

- 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-X25SRF)
- 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X25LRF)
- 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR4K-XNM-8X1GF)

- Firepower 9300：
  - Firepower 6-端口 10G SR FTW 单位宽网络模块 (FPR9K-NM-6X10SR-F)
  - Firepower 6-端口 10G LR FTW 单位宽网络模块 (FPR9K-NM-6X10LR-F)
  - Firepower 2-端口 40G SR FTW 单位宽网络模块 (FPR9K-NM-2X40G-F)

硬件旁路 仅可使用以下端口对：

- 1、2
- 3、4
- 5、6
- 7、8

内联集和被动接口的准则

防火墙模式

- 仅当设备处于路由防火墙模式时，才允许 ERSPAN 接口。

集群

- 集群不支持内联集的链路状态传播。
- 单个接口模式不支持仅 IPS 接口。

多实例模式

- 不支持多实例共享接口。您必须使用非共享接口。
- 不支持多实例机箱定义的子接口。必须使用物理接口或 EtherChannel 接口。

一般准则

- 内联集和被动接口仅支持物理接口和 EtherChannel，并且不能使用 VLAN 或其他虚拟接口，包括多实例机箱定义的子接口。
- 由于 IPS 接口不支持常规防火墙保护，因此 IPS 安全策略 (Snort) 要求流量通过同一个 Firewall Threat Defense ，以便检测所有流量。

- 使用内联集时，不允许双向转发检测 (BFD) 回应数据包通过 Firewall Threat Defense。如果 Firewall Threat Defense 的一端有两个邻居运行 BFD，则 Firewall Threat Defense 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。
- 对于内联集和被动接口， Firewall Threat Defense 在数据包中最多支持两个 802.1Q 报头（也称为 Q-in-Q 支持），但 Firepower 4100/9300 仅支持一个 802.1Q 报头。**注意**：防火墙类型的接口不支持 Q-in-Q，并且仅支持一个 802.1Q 报头。

硬件旁路 准则

- 硬件旁路 端口仅对内联集支持。
- 硬件旁路 端口不能是 EtherChannel 的一部分。
- 硬件旁路 在高可用性模式下不受支持。
- Firepower 9300 支持使用机箱内集群的硬件旁路 端口。当机箱中的最后一个设备出现故障时，将端口置于硬件旁路模式。不支持机箱间集群，因为机箱间集群仅支持跨网络 EtherChannel；硬件旁路 端口不能是 EtherChannel 的一部分。
- 如果 Firepower 9300 上机箱内群集中的所有模块都发生故障，则在最后一个设备上触发硬件旁路，使流量继续通过。当设备重新恢复时，硬件旁路将恢复为备用模式。但是，当您使用匹配应用流量的规则时，这些连接可能会被丢弃，且需要重新建立。由于在集群设备上未保留状态信息，并且设备无法将流量标识为属于允许的应用，连接会被丢弃。若要避免流量被丢弃，请使用基于端口的规则，而不是基于应用的规则（如果适合您的部署）。
- 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

IPS 接口上不支持的防火墙功能

- DHCP 服务器
- DHCP 中继
- DHCP 客户端
- TCP 拦截
- 路由
- NAT
- VPN
- 应用检测
- QoS
- NetFlow
- VXLAN

配置被动接口

本节介绍如何执行以下操作：

- 启用接口。默认情况下，接口处于禁用状态。
- 将接口模式设为被动或 ERSPAN。对于 ERSPAN 接口，需要设置 ERSPAN 参数和 IP 地址。
- 更改 MTU。默认情况下，MTU 设置为 1500 字节。有关 MTU 的详细信息，请参阅关于 MTU，第 816 页。
- 设置特定的速度和双工（如有）。默认情况下，速度和双工均设置为“自动”。



注释 对于 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，可在 Firepower 4100/9300上配置基本接口设置。有关详细信息，请参阅配置物理接口，第 310 页。

开始之前

- 如果您使用的是 EtherChannel，请根据 配置 EtherChannel，第 724 页添加它们。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 在**模式**下拉列表中，选择**被动**或 **Erspan**。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 在**名称**字段中，输入长度最大为 48 个字符的名称。

步骤 6 从**安全区域**下拉列表中选择一个安全区域，或者点击**新建**添加一个新的安全区域。

步骤 7 （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 8 （可选） 在**常规 (General)** 中，将 **MTU** 设置为介于 64 和 9198 字节之间；对于 Secure Firewall Threat Defense Virtual 和 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，最大值为 9000 字节。

默认值为 1500 字节。

步骤 9 对于 ERSPAN 接口，请设置以下参数：

- **流 ID** - 配置源和目标会话使用的 ID 来标识 ERSPAN 流量，介于 1 和 1023 之间。在 ERSPAN 目标会话配置中也必须输入此 ID。

- **源 IP** - 配置用作 ERSPAN 流量的源的 IP 地址。

步骤 10 对于 ERSPAN 接口，请在 **IPv4** 上设置 IPv4 地址和掩码。

步骤 11 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

步骤 12 点击**确定**。

步骤 13 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置内联集

本节启用并命名可以添加到内联集的每个内联对的两个物理接口或 EtherChannels。您可以为每个内联集添加多个内联对。您也可以选择为支持的内联对启用 硬件旁路 。

注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。有关详细信息，请参阅配置物理接口，第 310 页。

开始之前

- 如果您使用的是 EtherChannel，请根据 配置 EtherChannel，第 724 页 添加它们。
- 我们建议您为连接到 Firewall Threat Defense 内联接口对且启用 STP 的交换机设置 STP PortFast。此设置对硬件旁路配置尤其有用，可以减少绕行时间。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 为该内联对中的每个接口命名并启用该接口。您还可以配置其他硬件设置。对于内联对中的每个接口，请务必使其硬件设置相匹配。可以配置多对接口。

a) 点击要编辑的接口的 **编辑** (✎)。

b) 在**名称**字段中，输入长度最大为 48 个字符的名称。

c) 选中**启用**复选框以启用此接口。

d) （可选） 在**说明**字段中添加说明。

一行说明最多可包含 200 个字符（不包括回车符）。

e) 将 **模式** 保留为 **无**。

在将此接口添加到内联集后，此字段将显示的模式为“内联”。

f) 暂时不要设置安全区域；此过程中，必须在稍后创建好内联集后，再设置它。

g) （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

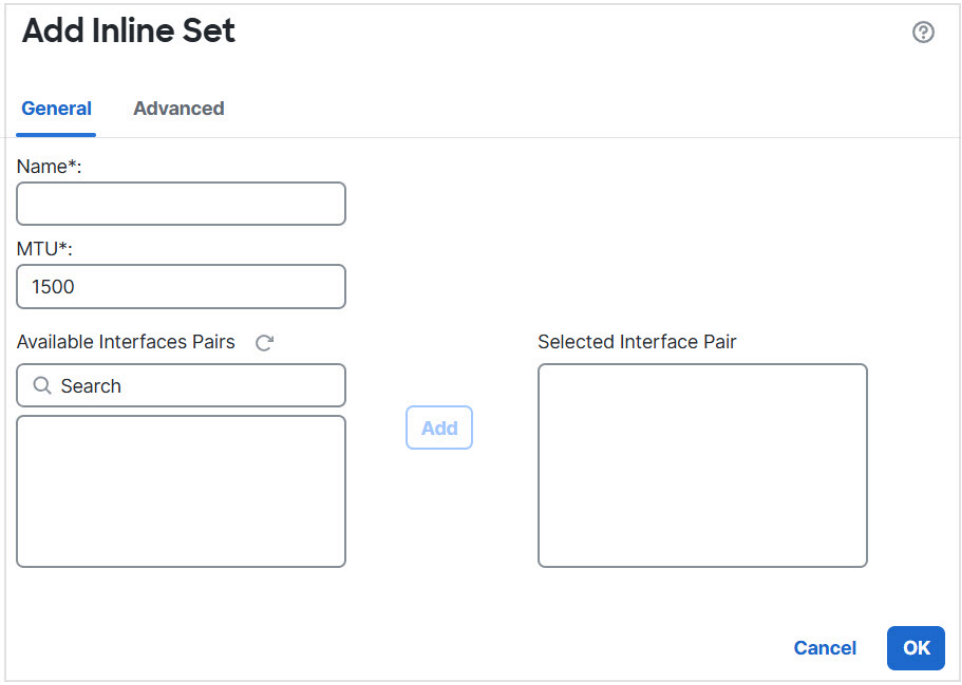
h) 点击**确定**。

请勿为此接口设置任何其他设置。

步骤 3 点击**内联集 (Inline Sets)**。

步骤 4 点击**添加内联集 (Add Inline Set)**。

图 *322:* 添加内联集



此时将显示**添加内联集 (Add Inline Set)** 对话框，其中**常规 (General)** 处于选中状态。

步骤 5 在**名称**字段中，输入内联集的名称。

步骤 6 （可选） 更改 **MTU** 以启用巨帧。

对于内联集，不使用 MTU 设置。但是，巨型帧设置与内联集相关；巨型帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨型帧，必须将设备上的任意接口的 MTU 设置为 1500 字节以上。

步骤 7 配置 硬件旁路。

a) 对于**绕行 (Bypass)** 模式，请选择以下其中一个选项：

- **禁用** - 对支持硬件旁路的接口，将硬件旁路设置为禁用，或使用不支持硬件旁路的接口。
- **备用** - 在支持硬件旁路的接口上，将硬件绕行设为备用状态。只有成对的硬件旁路接口才会显示出来。在“备用”状态下，接口可以保持正常运行，直至发生触发事件。
- **强制绕行** - 手动强制接口对进入绕行状态。对于处于“强制绕行”模式的任何接口对，**内联集**均显示**是**。

b) 在**可用接口对 (Available Interfaces Pairs)** 区域中，点击某个接口对，然后点击**添加 (Add)**，以将其移动至**选定的接口对 (Selected Interface Pair)** 区域。

此区域中会显示模式设置为“无”的已命名接口和已启用接口之间所有可能的配对。

步骤 8 （可选） 点击**高级 (Advanced)** 设置以下可选参数：

- **分流模式** - 设置为内联分流模式。

  请注意，您不能在同一内联集中启用此选项和严格 TCP 执行选项。

  注释
  如果需要启用或禁用分流模式，应在维护窗口期间执行此操作。在设备传递流量时更改模式可能会导致流量中断。

  注释
  分流模式 显著 影响 Firewall Threat Defense 性能，具体取决于流量。

- **传播链路状态** - 配置链路状态传播。

  当内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，设备会感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

  注释
  使用集群时，请勿启用**传播链路状态 (Propagate Link State)**。

- **Snort 故障时自动打开** - 如果您希望在 Snort 进程繁忙或关闭时，新流量和现有流量不检查直接通过（启用）或丢弃（禁用），请启用或禁用**繁忙 (Busy)** 和**关闭 (Down)** 选项之一或两项都启用。

  默认情况下，当Snort进程关闭时，流量会不进行检查就通过，而当进程繁忙时，流量会丢弃。

  当 Snort 进程处于以下状态时：

- “繁忙”- 由于流量缓冲区已满，进程无法足够快速地处理流量，这表明流量超过设备的处理能力，或者存在其他软件资源问题。
- “关闭”- 由于您部署了要求进程重启的配置，因此它会重启。请参阅部署或激活时重启 Snort 进程的配置，第 176 页。

当 Snort 进程关闭并重新启动后，它会检查新的连接。为了防止误报和漏报，此进程不检查内联、路由或透明接口上的现有连接，因为最初的会话信息可能已经在它关闭时丢失。

注释
如果 Snort 无法打开，则依赖 Snort 进程的功能会停止运行，这些功能包括应用控制和深度检查。借助简单、易于确定的传输层和网络层特征，系统仅执行基本访问控制。

注释
不支持**严格 TCP 执行 (Strict TCP Enforcement)** 选项。

步骤 9 设置每个接口的安全区域。

a) 点击**接口 (Interfaces)**。
b) 点击成员接口的 **编辑** ()。
c) 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

只有在将接口添加到内联集之后，才能设置安全区域；将接口添加到内联集可将模式配置为“内联”(Inline)，并且可让您选择内联类型的安全区域。

d) 点击**确定**。

步骤 10 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

内联集和被动接口的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Cisco Secure Firewall 6100 上对所支持网络模块的硬件绕行支持	10.0.0	10.0.0	Cisco Secure Firewall 6100 支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 6100

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Cisco Secure Firewall 4200上对所支持网络模块的硬件绕行支持	7.4.0	7.4.0	Cisco Secure Firewall 4200 支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 4200
Cisco Secure Firewall 3100上对所支持网络模块的硬件绕行支持	7.2	任意	Cisco Secure Firewall 3100 现在支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 3100
Firepower 4100/9300 的 Firewall Threat Defense 运行链路状态与物理链路状态之间的同步	6.7	任意	Firepower 4100/9300 机箱现在可以将 Firewall Threat Defense 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 Firewall Threat Defense 应用接口管理状态。如果没有从 Firewall Threat Defense同步，数据接口可能在 Firewall Threat Defense 应用完全上线之前处于“Up”物理状态，或者在您启动关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 Firewall Threat Defense 可以处理流量之前开始向 Firewall Threat Defense 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 Firewall Threat Defense 不支持此功能。ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 2130 和 2140 上对所支持网络模块的硬件绕行支持	6.3.0	任意	Firepower 2130 和 2140 现在支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 2130 和 2140
支持 Firewall Threat Defense 内联集中的 Etherchannel 或被动接口	6.2.0	任意	现在，您可以在 Firewall Threat Defense 内联集或被动接口中使用 EtherChannel。
Firepower 4100/9300 上对所支持网络模块的硬件旁路支持	6.1.0	任意	硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 4100/9300
内联集链路状态传播支持 Firewall Threat Defense	6.1.0	任意	当您在 Firewall Threat Defense 应用中配置内联集并启用链路状态传播时，Firewall Threat Defense 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的 FXOS 命令：**show fault |grep link-down**、**show interface detail**



第 17 章

设备设置

添加设备后，您可以在**设备 (Device)** 页面上编辑与设备相关的设置。

1. 选择**设备** > **设备管理**。
2. 在要修改的设备名单旁，点击 **编辑** ()。
3. 点击**设备 (Device)**。

- 编辑常规设置， 第 847 页
- 编辑许可证设置， 第 861 页
- 查看系统信息， 第 862 页
- 查看检测引擎， 第 863 页
- 编辑运行状况设置， 第 864 页
- 编辑管理设置， 第 874 页
- 查看清单详细信息， 第 915 页
- 编辑应用的策略， 第 916 页
- 编辑高级设置， 第 917 页
- 编辑部署设置， 第 921 页
- 编辑集群运行状况监控设置， 第 923 页
- 热插拔 SSD， 第 928 页
- 禁用 USB 端口， 第 930 页
- 为 FXOS 配置 SNMP， 第 933 页
- 配置 ISA 3000 的报警， 第 937 页
- 设备设置历史记录， 第 950 页

编辑常规设置

设备 (Device) 页面上的 **常规 (General)** 部分会显示下表所述信息。

图 *323:* 常规

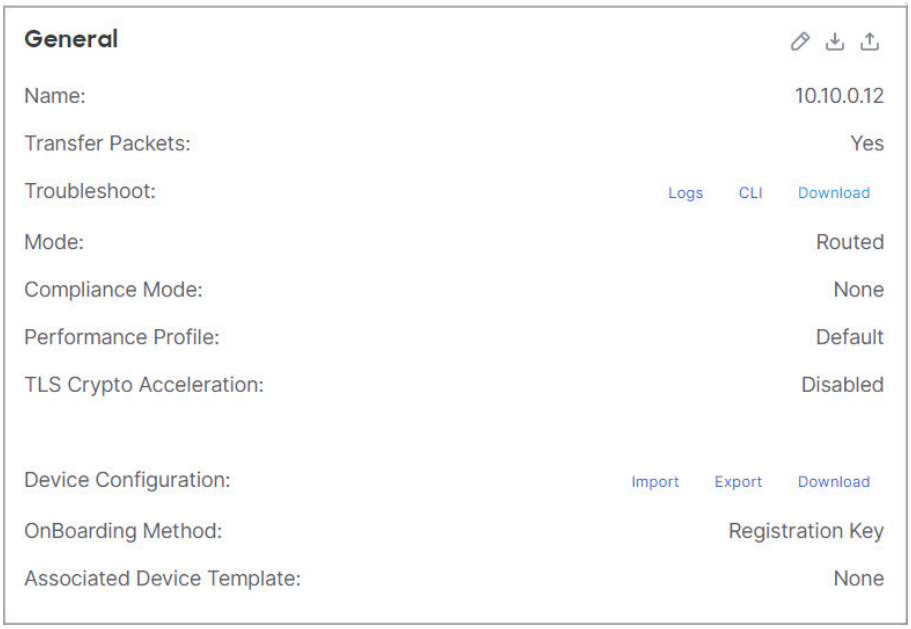


表 *57:* “常规” *(General)* 部分表字段

字段	说明
名称	防火墙管理中心上的设备的显示名称。
传输数据包	显示托管设备是否将数据包数据随事件一起发送到 防火墙管理中心 。
故障排除	可用于生成和下载故障排除文件，还可查看CLI命令输出。请参阅生成故障排除文件，第 849 页和查看 CLI 输出，第 852 页。
模式	显示设备的管理接口的模式：**路由**或**透明**。
合规模式	显示设备的安全认证合规性。有效值为 CC、UCAPL 和 None。
性能配置文件	这将显示设备的核心分配性能配置文件，如平台设置策略中所配置。
TLS 加密加速：	显示 TLS 加密加速是已启用还是已禁用。
设备配置	允许您复制、导出或导入配置。请参阅将配置复制到另一台设备，第 855 页和导出和导入设备配置，第 856 页。
载入方法	显示设备是使用注册密钥还是使用序列号注册的 (零接触调配)。

您可以在此部分编辑其中一些设置。

过程

步骤 1 选择 设备 > 设备管理。

步骤 2 在要修改的设备名单旁，点击 编辑 ()。

步骤 3 点击设备 (Device)。

步骤 4 在常规 (General) 部分中，点击 编辑 ()。

a) 输入托管设备的名称 (Name)。

b) 选择转换数据包 (Transfer Packets) 复选框以允许数据包数据随事件一起存储在 防火墙管理中心 上。

c) 点击强制部署 (Force Deploy) 以强制将当前策略和设备配置部署到设备。

注释
强制部署比常规部署需要更多时间，因为它涉及要在Firewall Threat Defense上部署的策略规则的完整生成。

步骤 5 有关 故障排除 操作，请参阅 生成故障排除文件，第 849 页 和 查看 CLI 输出，第 852 页。

步骤 6 有关设备配置 操作，请参阅将配置复制到另一台设备，第855页和导出和导入设备配置，第856页。

步骤 7 点击部署 (Deploy)。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

生成故障排除文件

您可以在每个设备以及所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。

您也可以从 设备 > 设备管理 触发文件生成，从 更多 () 下拉列表选择故障排除文件。

过程

步骤 1 选择 设备 > 设备管理。

步骤 2 点击要查看的设备旁边的 编辑 ()。

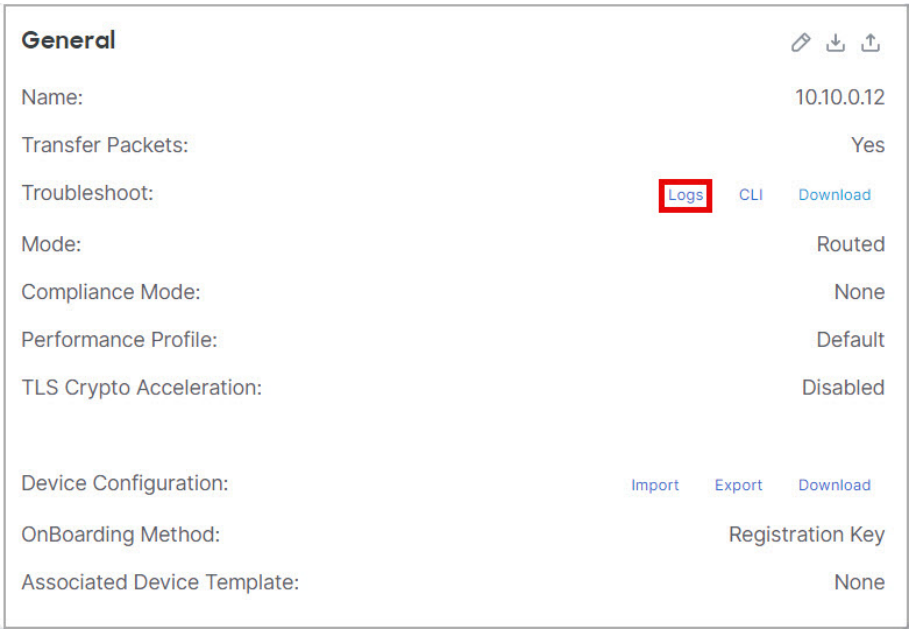
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 设备 或 集群。

步骤 4 为设备或所有集群节点生成日志。

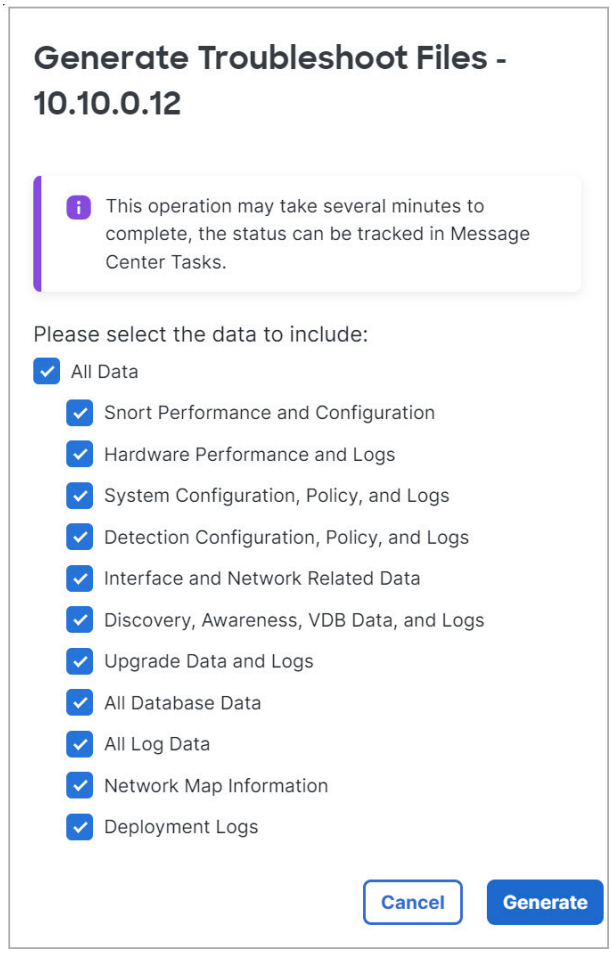
a) 在常规区域的故障排除部分中，点击日志。

图 *324:* 日志



b) 系统会提示您选择要包括的日志。对于集群，在 **设备**下，您可以选择 **所有设备** 或单个节点。集群还具有可用的 **集群日志** 。

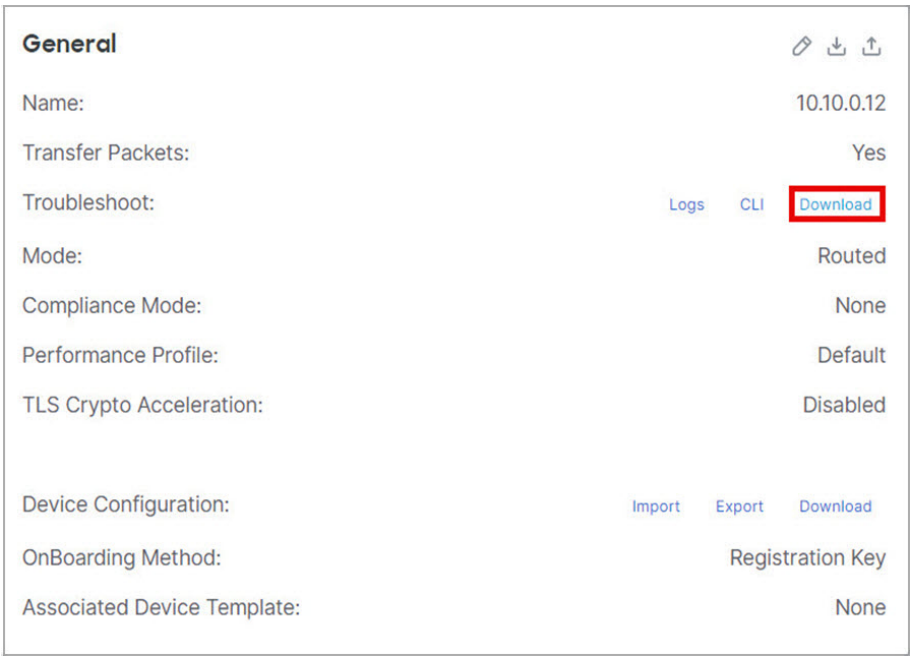
图 *325:* 生成故障排除文件



c) 点击**生成 (Generate)**。

步骤 5 要下载生成的日志，请在**常规**区域**故障排除**部分中，点击**下载**。

图 *326:* 下载



日志将下载到您的计算机。

查看 CLI 输出

您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。

对于设备，执行以下命令：

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

对于集群或集群节点：

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**

- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

过程

步骤 1 选择 **设备** > **设备管理**。

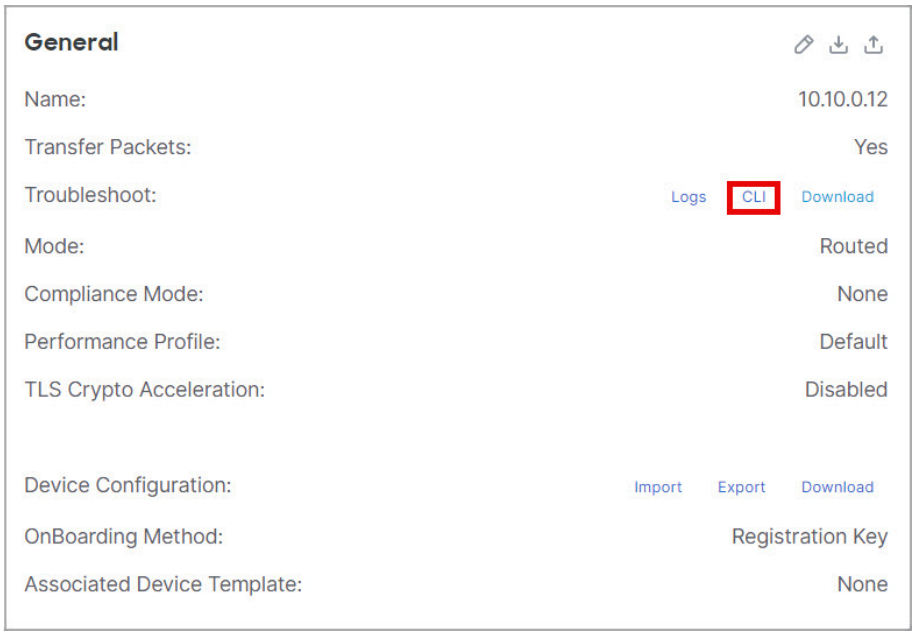
步骤 2 点击要查看的设备旁边的 **编辑** ()。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备** 或 **集群**。

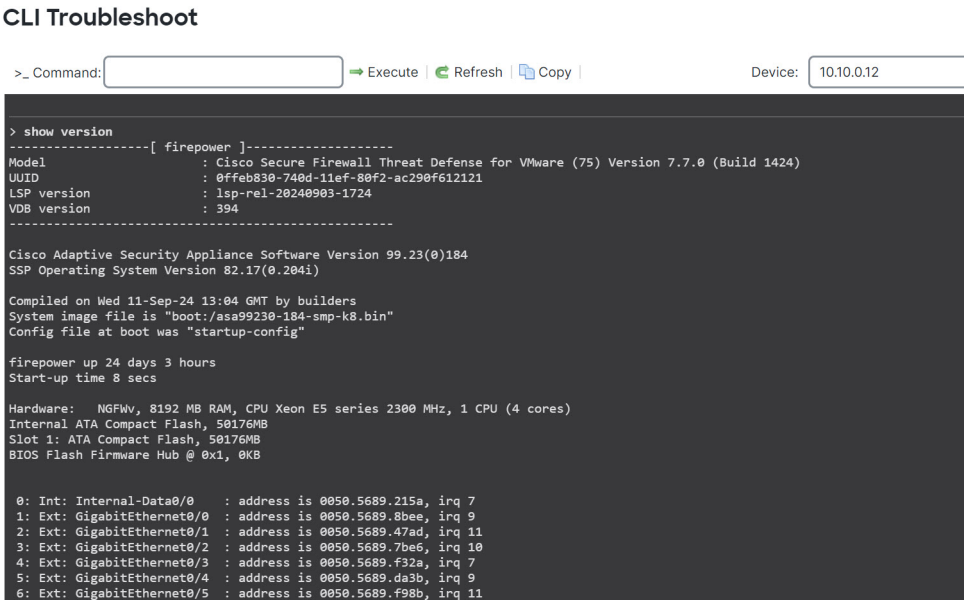
步骤 4 在**常规**区域的**故障排除**部分中，点击 **CLI**。

图 *327: CLI*



系统将显示 **CLI 故障排除** 对话框，其中包含已执行的预定义 CLI。

图 *328: CLI* 故障排除



步骤 5 在 **CLI 故障排除** 对话框中，您可以执行以下任务。

- 在 **命令** 字段中输入 **show** 命令，然后点击 **执行**。新的命令输出将添加到窗口中。
- 点击 **刷新** 以重新运行预定义的 CLI。

- 点击 **复制** 以将输出复制到剪贴板上。
- 对于集群，请从**设备**下拉列表中选择其他节点。

步骤 6 点击**关闭 (Close)**。

将配置复制到另一台设备

在网络中部署新设备时，可以直接复制预配置设备上的配置和策略，而无需手动重新配置新设备。

开始之前

确认：

- 源设备和目标设备是相同型号，并且运行相同版本的软件。
- 源是独立设备或高可用性对。
- 目标设备是独立设备。
- 源设备和目标设备具有相同数量的物理接口。
- 源设备和目标设备处于相同的防火墙模式：路由或透明。
- 源设备和目标设备处于相同的安全认证合规模式。
- 源设备和目标设备处于相同的域。
- 源设备或目标设备上均未进行配置部署。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑** (✎)。

步骤 3 点击 **设备**。

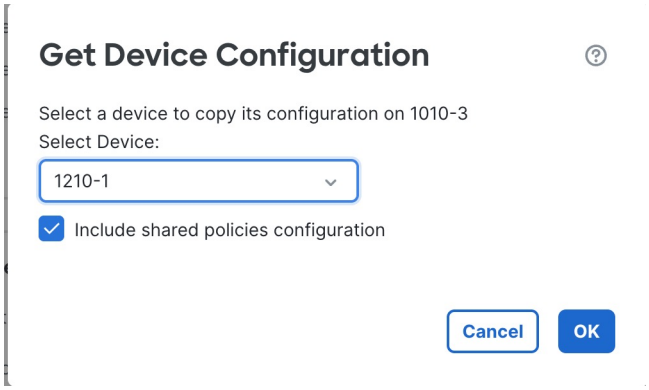
步骤 4 在**常规**部分中，执行以下操作之一：

图 ***329:*** 复制或推送设备配置



- 点击 **获取设备配置** (⬇) 以将设备配置从其他设备复制到新设备。在**获取设备配置**页面中，从**选择设备**下拉列表中选择源设备。

图 *330:* 选择设备



- 点击 **推送设备配置** (⬆) 以将设备配置从当前设备复制到新设备。在 **推送设备配置** 页面上，从 **目标设备**下拉列表中选择复制配置的目标设备。

步骤 5 （可选）选中**包括共享策略配置 (Include shared policies configuration)** 复选框以复制策略。

共享策略（例如访问控制策略、NAT、平台设置和 FlexConfig 策略）可在多个设备之间共享。

步骤 6 点击**确定 (OK)**。

您可以在消息中心中的 **任务 (Tasks)** 监控复制设备配置任务的状态。

复制设备配置任务发起后，便会擦除目标设备上的配置，并将源设备的配置复制到目标设备。

警告 完成复制设备配置任务后，无法将目标设备还原为其原始配置。

导出和导入设备配置

注释

- 共享策略和设备策略不支持在本地 防火墙管理中心 和 云交付的防火墙管理中心 (cdFMC) 之间导出和导入设备配置。
- 如果在不同的丢弃中为策略更改了基础模型，则丢弃版本不支持 cdFMC 的导出和导入云交付的防火墙管理中心。
- 只有当设备 UUID、型号和版本相同时，才支持导出和导入设备配置。

您可以导出设备页面上可配置的所有设备特定配置，包括：

- 接口
- 内联集

- 路由
- DHCP
- VTEP
- 关联对象

然后，您可以在以下使用案例中为同一设备导入已保存的配置：

- 将设备移动到其他 防火墙管理中心 — 首先从原始 防火墙管理中心 取消注册设备，然后将设备添加到新的 防火墙管理中心。然后，您可以导入保存的配置。
- 在域之间移动设备 - 在域之间移动设备时，不会保留某些设备特定的配置，因为新域中不存在支持对象（例如安全区域的接口组）。通过在域移动后导入配置，将为该域创建任何必要的对象，并恢复设备配置。
- 恢复旧配置 - 如果部署的更改会对设备的运行产生负面影响，则可以导入已知工作配置的备份副本，以恢复以前的运行状态。
- 重新注册设备 - 如果从 防火墙管理中心 中取消注册设备，但随后想要重新添加，则可以导入已保存的配置。

请参阅以下准则：

- 您只能将配置导入到同一设备（UUID 必须匹配）。您无法将配置导入到其他设备，即使是同一型号也是如此。
- 请勿在导出和导入的间隙更改设备上运行的版本；版本必须匹配。
- 如果在导出后更改资产（例如添加或删除网络模块，或配置或加入分支端口）， 防火墙管理中心则设备资产将不匹配 。在这种情况下，当您尝试部署时，系统将维护设备资产，并且系统会提示您同步接口（请参阅 与 防火墙管理中心同步接口更改 ，第 727 页）并丢弃 防火墙管理中心 中不兼容的配置。您必须在 防火墙管理中心中重复执行资产更改和相关配置。
- 如果导出独立配置，则无法将其导入到高可用性对，反之亦然。
- 将设备移至其他 防火墙管理中心 时，目标 防火墙管理中心 版本必须与源版本相同。
- 如果对象不存在，系统将创建该对象。如果对象存在，但值不同，请参阅下文：

表 *58:* 对象导入操作

场景	导入操作
存在具有相同名称的对象。	重用现有对象。

场景	导入操作
存在名称相同但值不同的对象。	网络和端口对象：为此设备创建对象覆盖。请参阅对象覆盖，第 2617 页。 接口对象：创建新对象。例如，如果类型（安全区域或接口组）和接口类型（例如，路由或交换）不匹配，则会创建新对象。 所有其他对象：即使值不同，也可重复使用现有对象。
对象不存在。	创建新对象。

过程

步骤 1 选择**设备** > **设备管理**。

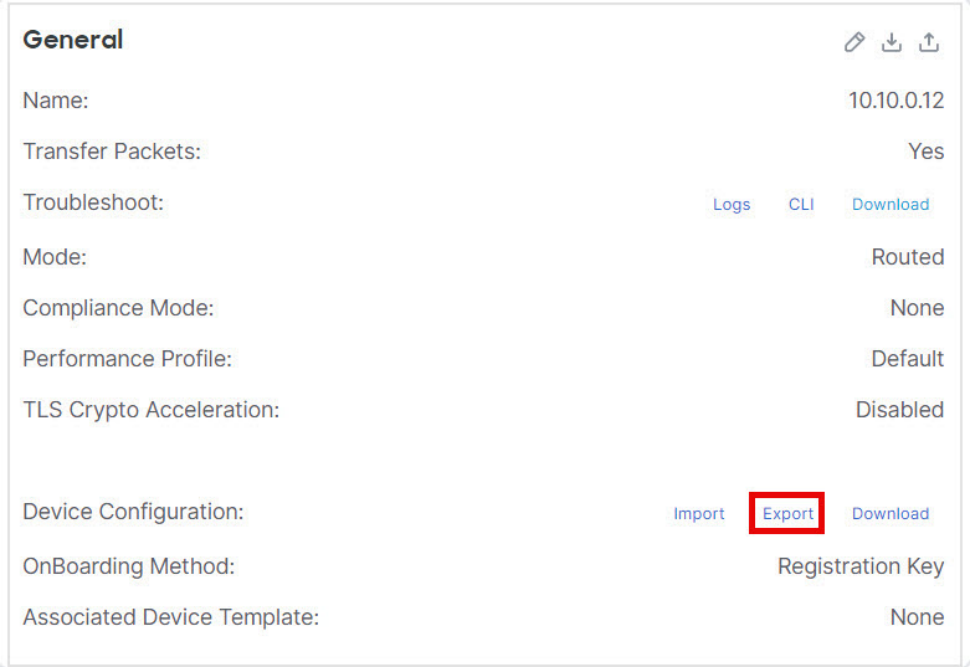
步骤 2 在要编辑的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 导出配置。

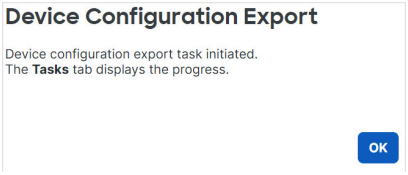
a) 在**常规 (General)** 区域，点击**导出 (Export)**。

图 *331:* 导出设备配置



系统将提示您确认导出；点击**确定**。

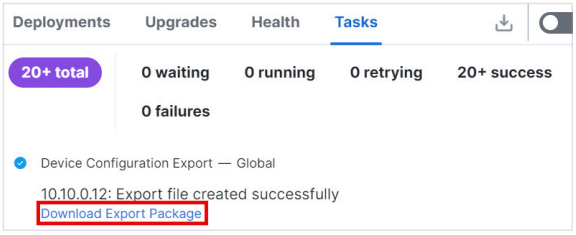
图 *332:* 确认导出



您可以在**任务 (Tasks)** 页面中查看导出进度。

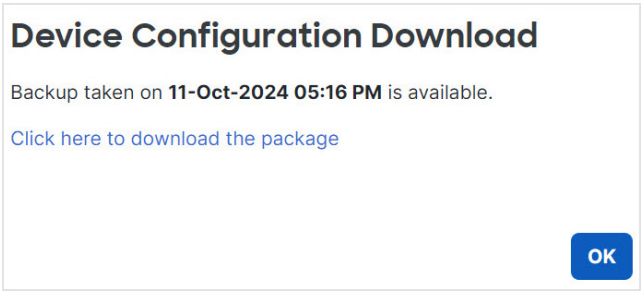
b) 点击 **通知**，然后点击“**任务**”选项卡。验证导出是否已完成，然后点击 **下载导出包 (Download Export Package)**。或者，您可以点击**常规 (General)** 区域中的**下载 (Download)** 按钮。

图 *333:* 导出任务



系统将提示您下载软件包；点击**点击此处下载软件包 (Click here to download the package)** 以本地保存文件，然后点击**确认 (OK)** 以退出对话框。

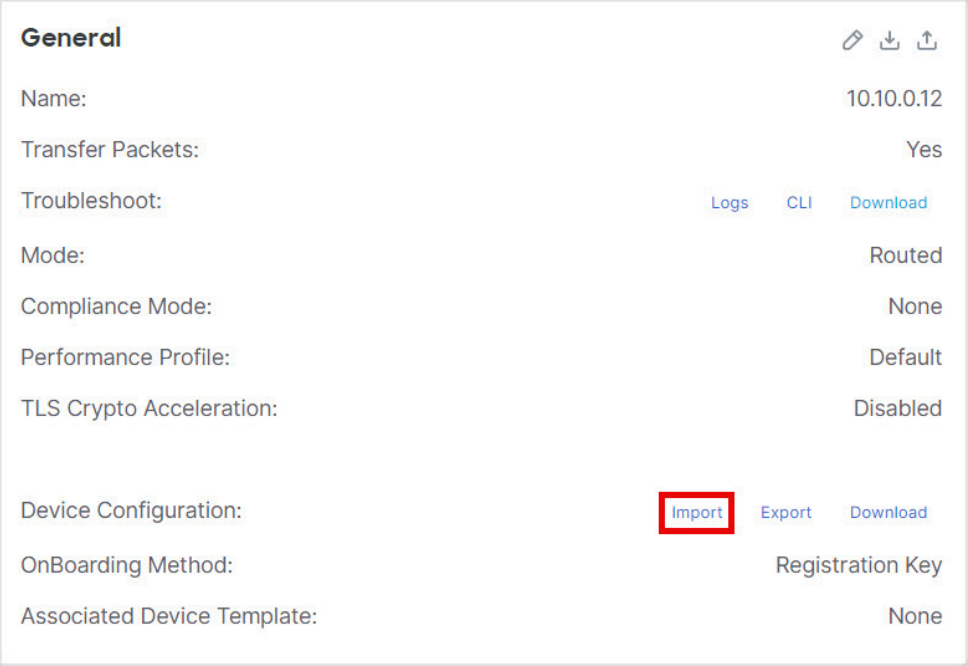
图 *334:* 下载软件包



步骤 5 导入配置。

a) 在**常规 (General)** 区域中，点击**导入 (Import)**。

图 *335:* 导入设备配置



系统将提示您确认将替换当前配置。点击**是 (Yes)**，然后导航到配置包（使用后缀 .sfo；请注意，此文件与备份/恢复文件不同）。

图 *336:* 导入软件包

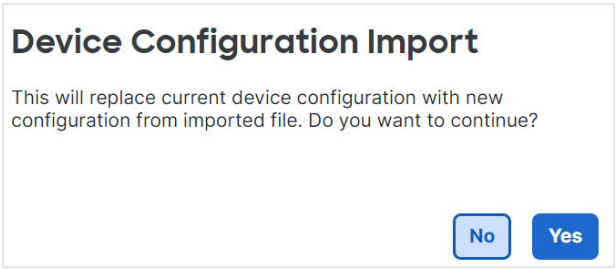
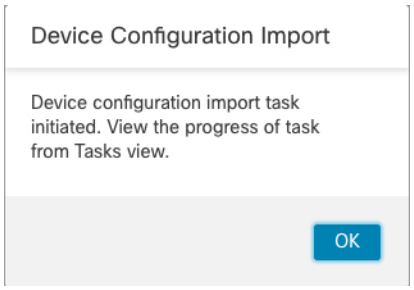


图 *337:* 导航至软件包



系统将提示您确认导入；点击**确认 (OK)**。

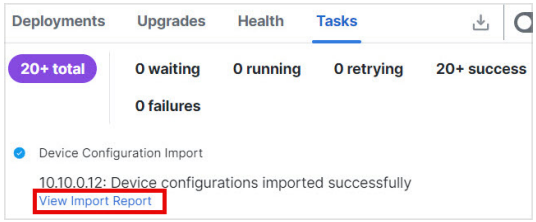
图 *338:* 确认导入



您可以在**任务 (Tasks)** 页面中查看导入进度。

b) 要查看导入报告以便查看导入的内容，请点击 **通知**，然后点击 **任务** 选项卡。点击**查看导入报告**。

图 *339:* 查看导入报告



设备配置导入报告 (Device Configuration Import Reports) 页面提供可用报告的链接。

Device	Shared Policies	Device Configurations
0ffeb830-740d-11ef-80f2-ac290f612121	Report does not exist	Device configurations import report

c) 部署配置更改；请参阅 部署配置更改，第 180 页。

编辑许可证设置

设备 (Device) 页面的**许可证 (License)** 部分显示为设备启用的许可证。

如果在防火墙管理中心上有可用的许可证，则可以启用设备上的许可证。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要启用或禁用许可证的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备**。

步骤 4 在**许可证 (License)** 部分中，点击 **编辑** (✎)。

步骤 5 选中或取消选中要为托管设备启用或禁用的许可证旁边的复选框。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

查看系统信息

设备页面的**系统**部分显示一个只读表格，其中包含系统信息，如下表所述。

您也可以使用右上角的图标从此窗格关闭或重启设备。

图 *340:* 系统

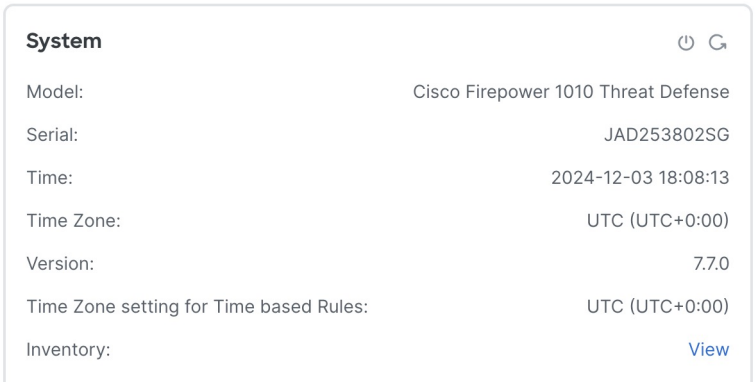


表 *59:* 系统部分表字段

字段	说明
关闭设备 (⏻)	关闭设备。请参阅关闭或重新启动设备。
重启设备 (↻)	重新启动设备。请参阅关闭或重新启动设备。
型号	型号名称和编号。
系列	PCB（电路板）序列号。防火墙包含两个序列号：机箱序列号和PCB序列号。机箱序列号显示在清单部分中。
时间	设备的当前系统时间。
时区	时区。
版本	托管设备上当前安装的软件版本。

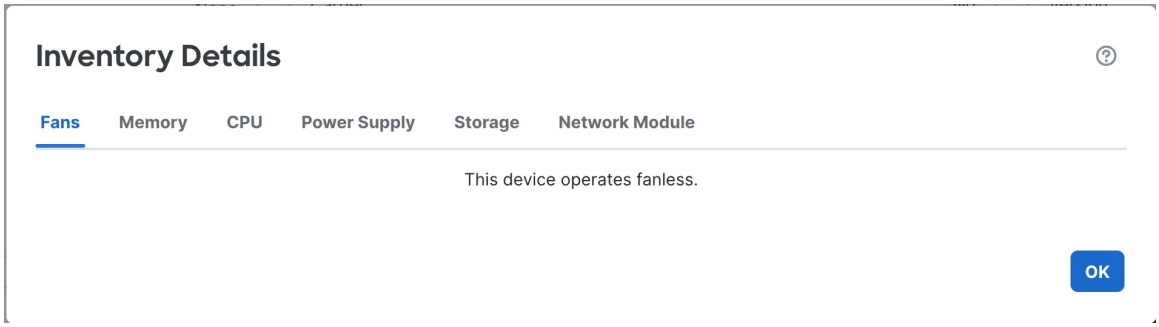
字段	说明
基于时间的规则的时区设置	设备在设备平台设置中指定的时区下的当前系统时间。
设备清单	清单详细信息。请参阅查看设备清单。

查看设备资产

点击**系统**部分中**清单**旁边的**查看**，查看设备清单信息表格，包括风扇、内存、CPU、电源、存储和网络模块。

清单详细信息表格显示分配了产品标识符 (PID) 的 Firewall Threat Defense 设备中安装的所有思科产品的信息。PID 是可用于订购产品的产品名称。

图 *341:* 设备清单详细信息



清单详细信息表格的**内存**选项卡显示受支持 Firewall Threat Defense 设备的现场可更换内存模块信息。它还包括内存模块的运行终端安全评估，这有助于提高其现场可维护性。状态可以是以下其中一项：

- **可操作**：表示现场可更换内存模块已安装在 Firewall Threat Defense 设备中，且容量符合设备平台的预期容量。
- **已降级**：表示已安装内存模块的容量与 Firewall Threat Defense 设备平台的预期容量不匹配，或检测到不可纠正的错误。如需进一步帮助，请联系思科技术支持中心。
- **无法操作**：表示 Firewall Threat Defense 设备无法检测到双列直插内存模块。

查看检测引擎

设备 (Device) 页面的“检测引擎”(Inspection Engine) 部分会显示。Snort 3 是唯一可用于 7.7 及更高版本设备的引擎。

注释 Snort3 是 Cisco Secure Firewall 1200 的默认配置。它不支持 Snort2。

编辑运行状况设置

设备 (Device) 页面上的**运行状况 (Health)** 部分显示下表所述信息。

图 *342:* 运行状况

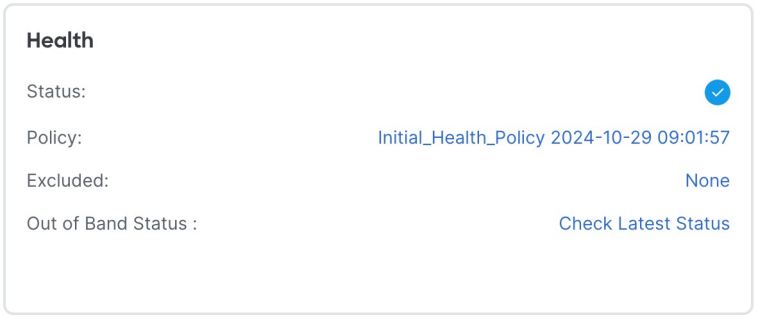


表 *60:* 运行状况部分表字段

字段	说明
状态	一个代表设备当前运行状况的图标。点击该图标将显示设备 的“运行状况监控器”(Health Monitor)。
策略	一个指向当前部署在设备 上的运行状况策略的只读版本的链接。
已排除	一个指向**运行状况排除 (Health Exclude)** 页面 的链接，您可以在该页面上启用和禁用运行状况排除模块。
带外状态	指向**带外配置详细信息 (Out-of-Band configuration details)** 对话框的链接，您可以在其中查看在设备CLI上所做的带外配置更改。在下一次部署之前，您必须确认配置差异，并手动匹配要保留在 防火墙管理中心 中的任何更改。请参阅带外配置检测，第 864 页。

带外配置检测

如果断开了与设备的管理连接，您可以直接通过设备 CLI 选择配置更改：

- 如果使用数据接口进行管理器访问，则恢复管理连接
- 选择无法等到连接恢复后再进行的配置更改

⚠

注意 您应该知道恢复或紧急使用时所需的命令。请勿使用此功能来尝试更改配置。如果您不知道哪些命令是必需的，或者不确定某个命令的作用，建议您联系思科技术支持中心以寻求指导。

在恢复管理连接后，防火墙管理中心 将检测设备上的配置更改。它不会自动更新 防火墙管理中心 中的设备配置；您必须查看配置差异，确认设备配置不同，然后在部署之前在防火墙管理中心 中手动进行相同的更改。

⚠

注意 在确认后部署时，防火墙管理中心 配置中不存在的任何配置将在设备上覆盖。

带外配置准则

恢复配置模式下支持的功能区域

您可以在恢复配置模式下在诊断 CLI 中配置以下功能区域：

- 接口
- 静态路由
- 动态路由：BGP 和 OSPF
- 预过滤器
- 站点间 VPN
- NAT

与其他诊断 CLI 命令一样，有关每个命令的详细信息，请参阅 ASA 命令参考 。

不支持的功能

- 在多实例模式下不支持。
- 不能添加或删除 EtherChannel。

高可用性和群集

- 恢复配置模式仅在主用/控制节点上可用。
- 在集群控制链路或故障转移链路的恢复配置模式下，不支持以下接口命令：
  - **duplex**
  - **fec**
  - **negotiate-auto**
  - **shutdown**
  - **speed**
- 如果在您退出恢复配置模式会话之前发生故障转移或集群切换，防火墙管理中心 将不会检测新的主用/控制节点上的更改。我们建议在新的主用/控制节点上重新进入恢复配置模式，并进行小

幅更改以触发发现功能之前的所有更改。否则，如果您没有手动匹配 防火墙管理中心中的更改，则这些更改将在部署时被覆盖，而不发出任何通知。

- 如果在主用/控制节点上进行带外配置更改，但在配置同步之前，高可用性/集群最终处于“裂脑”模式（在这种情况下，多个节点由于或故障转移/集群控制链路故障时），则当高可用性/集群恢复正常运行且另一个节点变为主用/控制状态时，配置更改将会丢失。
- 如果有活动恢复配置模式会话，则在退出该会话之前，新节点无法加入或重新加入高可用性/集群。

NAT

- 通过恢复配置模式，可以创建如下重叠 PAT 池规则：

  nat (eth_12_subintf_one,any) source dynamic any pat-pool pat_pool_4

  nat (eth_12_subintf_one,any) source dynamic any pat-pool pat_pool_4 include-reserve

  防火墙管理中心 不允许此重叠。如果目的是将 **include-reserve** 添加到现有 NAT 规则中，请首先使用 **no** 命令删除该规则，然后使用 **include-reserve** 选项重新添加该规则。

- 如果在恢复配置模式下创建服务对象以用于如下所示的 NAT 规则中：

  object service obj_mapped_svc

  service tcp source eq www

  object service obj_real_svc

  service tcp source eq 7080

  nat (any,any) source dynamic obj_two obj_dyn_host service obj_real_svc obj_mapped_svc

  然后，当在 防火墙管理中心中重新创建规则时， 防火墙管理中心 会将服务对象名称替换为自动生成的名称。由于 NAT 规则在部署时不匹配，因此系统将在应用新的 防火墙管理中心 规则之前删除 recovery-config 模式规则，从而导致少量流量中断。

其他准则

- 要修改现有的规则或路由，应使用命令的 **no** 形式删除现有命令，然后重新添加已修改的规则。此方法可避免冲突和错误。例如：

  不正确：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
  center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
  or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration changes
  in the
```

```
management center. The management center cannot implement them automatically. When you
 deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
 node join
will be blocked till config CLI session is active, so make sure to exit from the config
 CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: ccfc11a8 4e46d55e 0c99b5ae 3b18a8f1

3939 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

这种情况下会添加第二个路由，而不是替换第一个路由。

正确：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
 center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
 or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration changes
 in the
management center. The management center cannot implement them automatically. When you
 deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
 node join
will be blocked till config CLI session is active, so make sure to exit from the config
 CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# no route outside 10.0.0.0 255.0.0.0 20.1.1.1
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: 81bcc51d 43771bbd 15b6dde6 afeb3442

3945 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

- 如果您启用了自动回滚（请参阅 编辑部署设置，第 921 页），并且由于部署而丢失管理连接，则不应启动带外配置。而是等待 20 分钟，以便自动回滚到先前的部署，或者在 CLI 中使用

configure policy rollback 命令手动回滚（请参阅如果防火墙管理中心断开连接，则手动回滚配置，第 909 页）。如果管理连接仍然关闭，自动回滚将覆盖带外配置更改。

- 对于预过滤器规则，我们不建议添加全新的规则（使用 **access-control advanced** 命令）；将预过滤器规则与入侵策略和日志记录的集成需要 防火墙管理中心，它生成规则 ID 并将其与其他策略集成。
- 所有恢复配置模式会话都将以用户名“enable_15”记录在系统日志中。

访问诊断 CLI 中的恢复配置模式

当管理连接断开时，您可以使用诊断 CLI 恢复配置模式进行带外配置更改。请确保在 防火墙管理中心中进行相同的更改；本地更改将始终被 防火墙管理中心 部署覆盖。

要实现高可用性和集群，请在主用/控制节点上进行更改。在多实例模式下不支持此模式。

过程

步骤 1 通过控制台端口或使用 SSH 连接至设备 CLI。

请参阅登录到设备的命令行界面。

步骤 2 访问诊断 CLI。

system support diagnostic-cli

enable（当系统提示时，请按 Enter 键，无需输入密码。）

示例：

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

步骤 3 显示当前运行配置，以供参考。

show running-config

注释
您不能在恢复配置模式下输入 **show** 命令。

步骤 4 进入恢复配置模式。

configure recovery-config

示例：

```
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
 or
to restore manager access. Do not change management center's auto-generated configurations.
```

```
 After your management center is reachable, manually make the same configuration changes
in the
management center. The management center cannot implement them automatically. When you
deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
node join
will be blocked till config CLI session is active, so make sure to exit from the config CLI
 after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)#
```

步骤 5 您现在可以输入选定的配置命令。

输入 **?** 以查看可用的命令。

有关受支持的功能区域，请参阅带外配置准则，第 865 页。

有关命令的详细信息，请参阅 ASA 配置指南或命令参考。

提示
记录所有更改过的命令。虽然防火墙管理中心将稍后显示差异，但最好记录命令更改，以防需要反复更改来恢复管理连接。

示例：

```
firepower(recovery-config)# ?

  access-list           Configure an access control element
  as-path               BGP autonomous system path filter
  bfd                   BFD configuration commands
  bfd-template          BFD template configuration
  cluster               Cluster configuration
  community-list        Add a community list entry
  crypto                Configure IPSec, ISAKMP, Certification authority, key
  end                   Exit from configure mode
  exit                  Exit from config mode
  extcommunity-list     Add a extended community list entry
  group-policy          Configure or remove a group policy
  interface             Select an interface to configure
  ip                    Configure IP address pools
  ipsec                 Configure transform-set, IPSec SA lifetime and PMTU
                        Aging reset timer
  ipv6                  Configure IPv6 address pools
  ipv6                  Global IPv6 configuration commands
  isakmp                Configure ISAKMP options
  jumbo-frame           Configure jumbo-frame support
  mac-address           MAC address options
  management-interface  Management interface
  mtu                   Specify MTU(Maximum Transmission Unit) for an interface
  nat                   Associate a network with a pool of global IP addresses
  no                    Negate a command or set its defaults
  object                Configure an object
  object-group          Create an object group for use in 'access-list', etc
  policy-list           Define IP Policy list
  prefix-list           Build a prefix list
  route                 Configure a static route for an interface
  route-map             Create route-map or enter route-map configuration mode
```

```
  router                Enable a routing process
  sla                   IP Service Level Agreement
  sysopt                Set system functional options
  time-range            Define time range entries
  tunnel-group          Create and manage the database of connection specific
                        records for IPSec connections
  vpdn                  Configure VPDN feature
  vrf                   Configure a VRF
  zone                  Create or show a Zone
firepower(recovery-config)#
```

步骤 6 退出恢复配置模式，系统将提示您保存更改。输入 **exit** 以退出每个子模式，直到您返回启用模式。

您可以选择将更改保存到启动配置，或不保存，仅将更改保留在运行配置中。重新启动后不会保留运行配置更改。如果您稍后进行其他更改并决定保存配置，则先前的所有更改也会保存，因为会保存整个运行配置。

当恢复配置模式会话打开时，部署将被阻止。

示例：

```
firepower(recovery-config)# interface Ethernet0/1
firepower(config-if)# ip address 10.0.0.2 255.0.0.0
firepower(config-if)# exit
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o: y

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#

Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o:

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#
```

步骤 7 依次键入 Ctrl+a 和 d 返回 Firewall Threat Defense CLI，或者输入 **exit** 退出每种模式。

注释
如果您键入 Ctrl+a，然后键入 d 以返回 Firewall Threat Defense CLI，无需先退出恢复配置模式，恢复配置模式会话将保持打开，并且部署将被阻止。

示例：

```
firepower# exit

Logoff

User enable_1 logged in to firepower
Logins over the last 1 days: 4.  Last login: 20:42:51 UTC Dec 4 2024 from console
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> exit
Console connection detached.
>
```

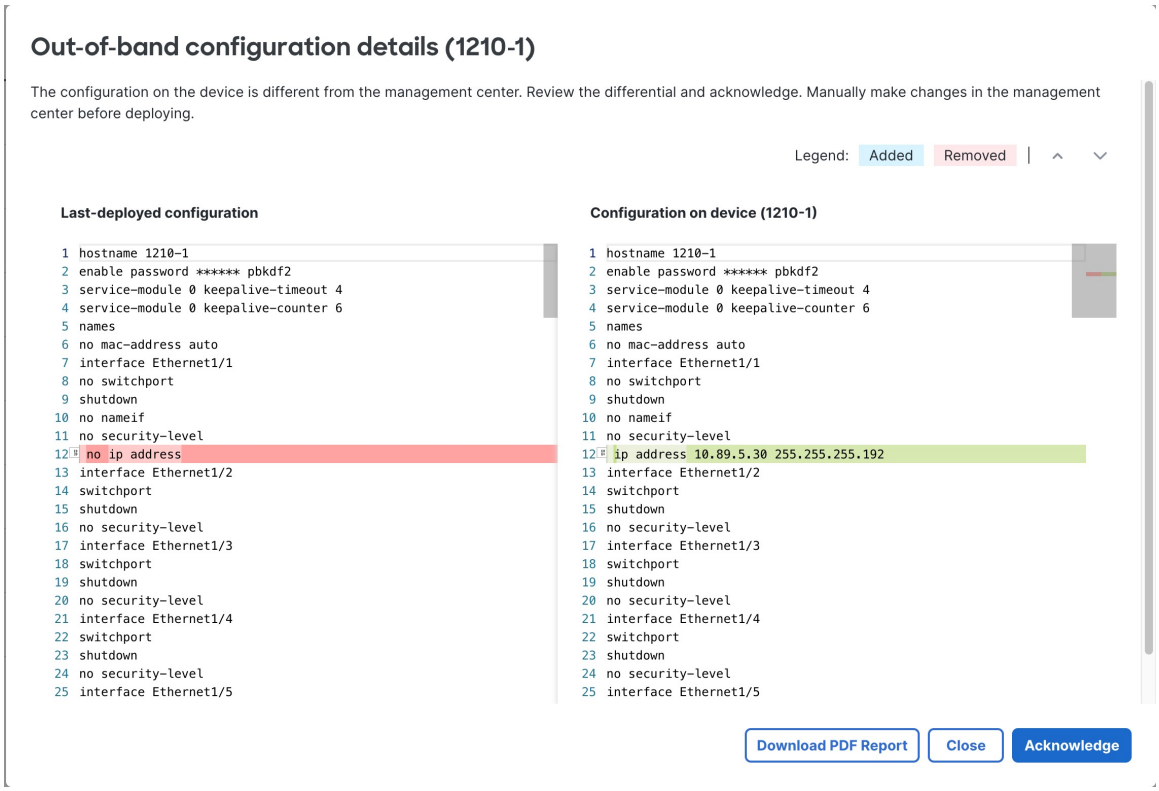
确认带外配置

当 防火墙管理中心 检测到设备上的带外配置更改时，您必须确认更改并与要保留的 防火墙管理中心 中的配置进行匹配。在确认更改之前，部署将被阻止。

过程

步骤 1 打开**带外配置详细信息 (Out-of-Band configuration details)** 对话框。

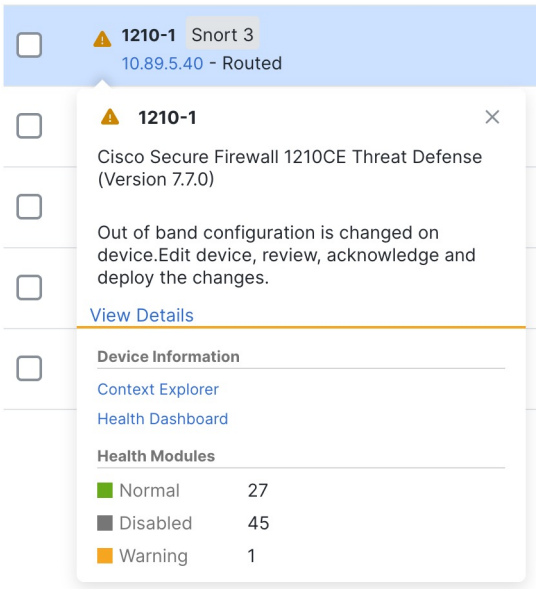
图 *343:* 带外配置详细信息



注释
某些命令在设置为默认值时不会出现在命令输出中。但是，非默认命令会在两侧显示为绿色（添加）或红色（删除）。例如，如果在恢复配置模式下将 **no shutdown** 添加到接口，则 **shutdown** 命令将在左侧 **Last-deployed configuration** 窗格中显示为红色，而右侧 **Configuration on device** 窗格中不会显示 **no shutdown**。在这种情况下，虽然接口的默认设置为 **shutdown**，但解析器会将 **no shutdown** 视为默认设置，并且不会显示它。

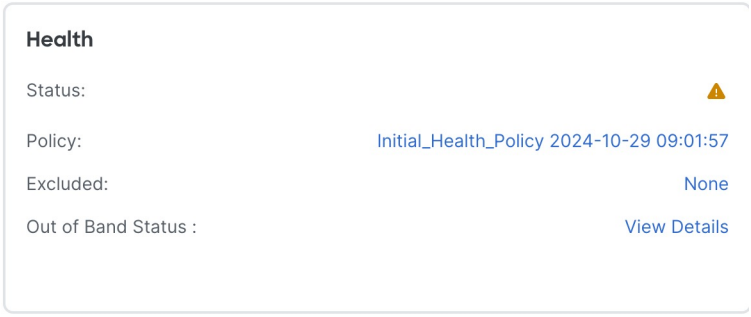
您可以从多个位置打开此对话框。例如，在 **设备 > 设备管理** 页面上，设备将显示一条警告。点击**查看详细信息**。

图 *344:* 设备管理警告



或者，从 **设备** > **设备管理** 导航至**设备**选项卡下的**运行状况**磁贴，您可以点击**查看详细信息**。

图 *345:* 运行状况带外状态



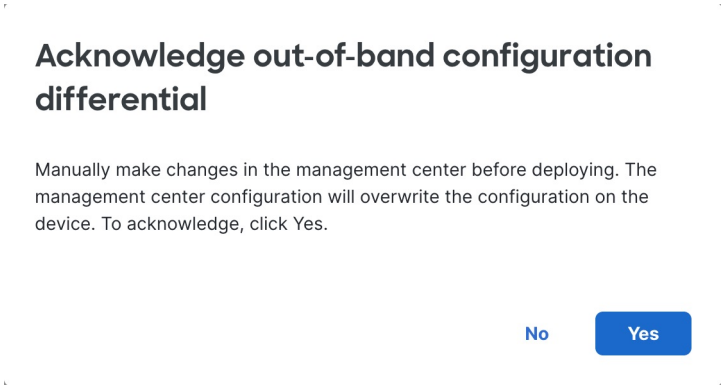
注释
如果带外通知尚未到达 防火墙管理中心，则可以使用**检查最新状态**链接来检查更改。

步骤 2 点击**下载 PDF 报告 (Download PDF Report)**，以便在关闭对话框后参阅需要进行的配置更改。

您也可以随时打开对话框查看更改。

步骤 3 点击**确认**，然后点击**是**。

图 *346:* 确认

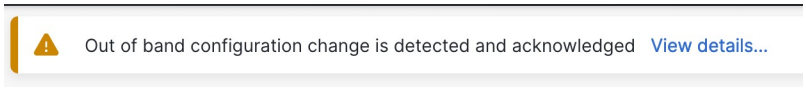


如果要在进行配置更改之前防止意外部署，您可以进行更改，然后返回并点击**确认 (Acknowledge)**。

步骤 4 点击**带外配置详细信息 (Out-of-Band configuration details)** 对话框中的**关闭 (Close)**。

在部署之前，您仍可以重新访问对话框，以便查看需要进行的更改。“设备”(Device) 页面上的状态会发生变化，以显示您已确认带外配置：

图 *347:* 确认状态

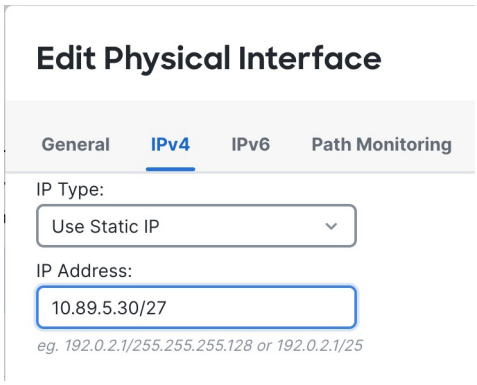


步骤 5 进行您在 CLI 中所做的配置更改。

您需要将配置 CLI 与 防火墙管理中心 屏幕相匹配；CLI 更改不会直接链接到屏幕。

如果不想保留更改，您可以直接部署并覆盖设备配置。您应该进行所有必要的更改，以保持管理连接以及想要保留的任何其他更改。例如，如果在CLI中更改了 IP 地址，则需要转至**接口 (Interfaces)** 页面，编辑接口，并将该 IP 地址设置为匹配：

图 *348:* 匹配 *IP* 地址更改



没有检查机制来确认您是否做了相同的更改；如果需要，您可以设置不同的 IP 地址。

步骤 6 部署配置更改；请参阅 部署配置更改，第 180 页。

在部署后，您可以在 **事件和日志** > **分析** > **审核日志** 页面上查看配置差异，确认是否进行了更改。检查名为设备 *(Device)* > 设备管理 *(Device Management)* > 带外更改 *(Out of band changes)* 的子系统。

编辑管理设置

这些设置控制 防火墙管理中心 与设备建立管理连接的方式。

配置冗余管理器访问数据接口

在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。您只能配置一个辅助接口。设备会使用 SLA 监控来跟踪包含两个接口的静态路由和 ECMP 区域的可行性，以便管理流量可以使用这两个接口。

开始之前

- 辅助接口需要与主接口位于不同的安全区域。
- 适用于辅助接口的所有要求与适用于主接口的要求相同。请参阅使用Firewall Threat Defense数据接口进行管理。

过程

步骤 1 在 **设备** > **设备管理** 页面，点击设备的 **编辑** ()。

步骤 2 启用对辅助接口的管理器访问。

此设置是标准接口设置（例如启用接口、设置名称、设置安全区域和设置静态 IPv4 地址）的补充。

a) 选择**接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)**。
b) 选中**在此接口上为管理器启用管理 (Enable management on this interface for the Manager)**。
c) 点击**确定 (OK)**。

两个接口都会在列表中显示（**管理器访问**）。

图 *349:* 接口列表

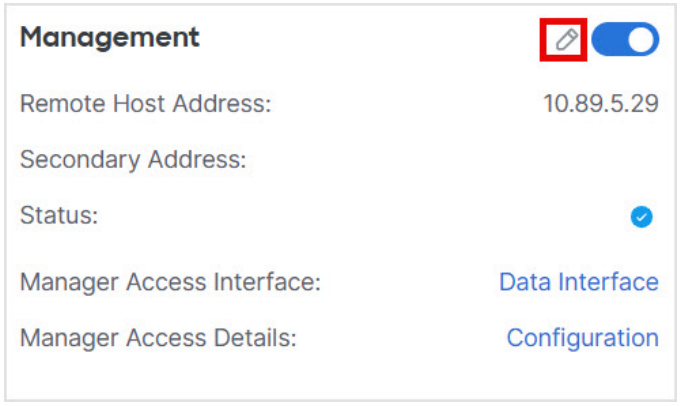
Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

步骤 3 将辅助地址添加到**管理 (Management)** 设置。

a) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

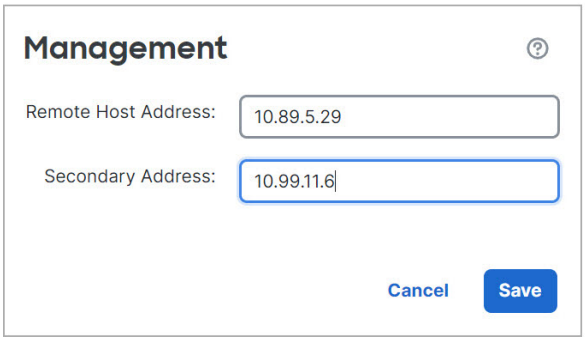
b) 点击**编辑** (✎)。

图 *350:* 编辑管理地址



c) 在**管理 (Management)** 对话框中，在**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址

图 *351:* 管理 *IP* 地址

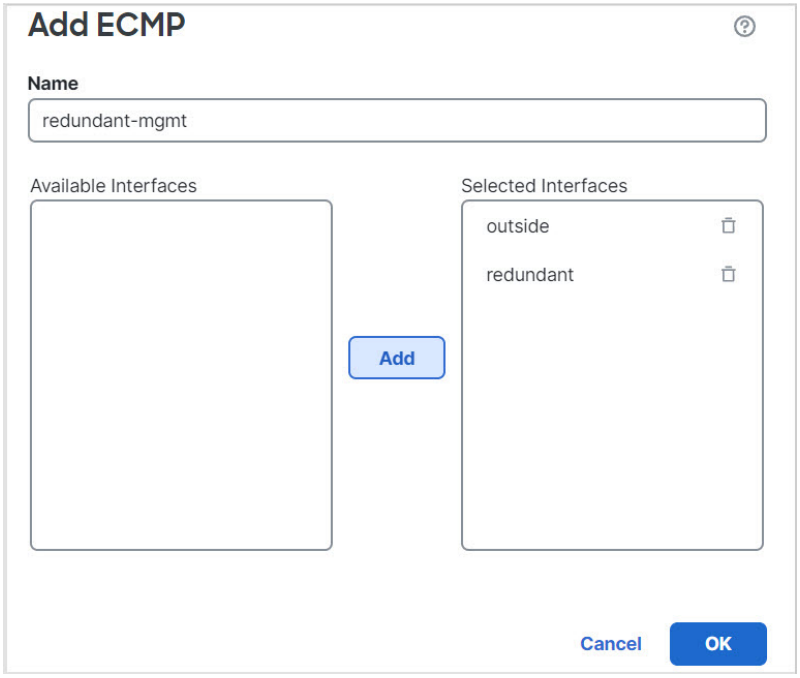


d) 点击**保存 (Save)**。

步骤 4 通过两个接口创建 ECMP 区域。

a) 点击**路由 (Routing)**。
b) 从虚拟路由器下拉列表中，选择主接口和辅助接口所在的虚拟路由器。
c) 点击 **ECMP**，然后点击**添加 (Add)**。
d) 为 ECMP 区域输入一个**名称**。
e) 在**可用接口 (Available Interfaces)** 框下选择主和辅助接口，然后点击**添加 (Add)**。

图 *352:* 添加 *ECMP* 区域

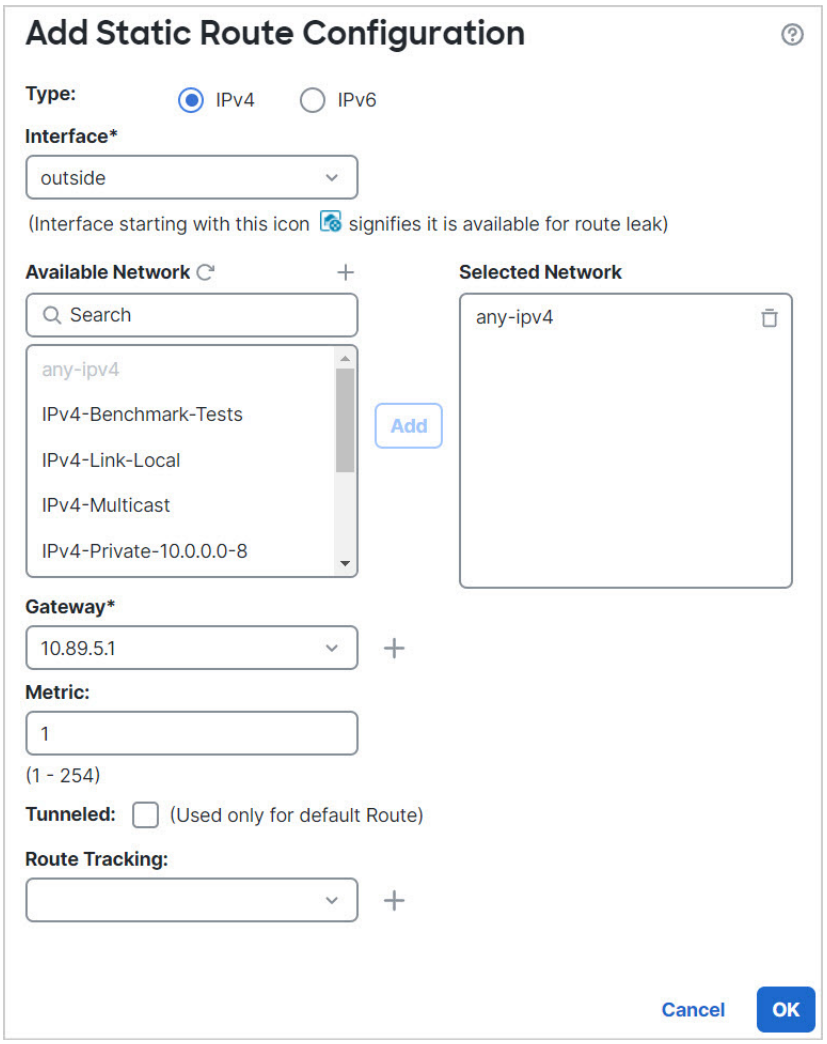


f) 点击**确定 (OK)**，然后点击**保存 (Save)**。

步骤 5 为两个接口添加等价默认静态路由，并在两个接口上启用 SLA 跟踪。

除网关外，路由应完全相同，并且都应具有指标 1。主接口应已具有您可以编辑的默认路由。

图 *353:* 添加/编辑静态路由



a) 点击**静态路由 (Static Route)**。

b) 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑** ()。

c) 从**接口 (Interface)** 下拉列表中选择接口。

d) 对于目标网络，从**可用网络 (Available Networks)** 框中选择 **any-ipv4**，然后点击**添加 (Add)**。

e) 输入默认**网关**。

f) 对于**路由跟踪 (Route Tracking)**，请点击 **添加** () 以添加新的 SLA 监控器对象。

g) 输入以下必需参数：

- 作为 防火墙管理中心 IP 地址的**监控地址**。
- **可用区域 (Available Zones)** 中的主要或辅助管理接口的区域；例如，为主接口对象选择外部区域，为辅助接口对象选择管理区域。

有关详细信息，请参阅SLA 监控器，第 2700 页。

图 *354:* 添加 *SLA* 监控

h) 点击**保存 (Save)**，然后在**路由跟踪 (Route Tracking)** 下拉列表中选择您刚创建的 SLA 对象。
i) 点击**确定 (OK)**，然后点击**保存 (Save)**。
j) 对另一个管理接口的默认路由重复此操作。

步骤 6 部署配置更改；请参阅 部署配置更改，第 180 页。

作为此功能部署的一部分，防火墙管理中心 会为管理流量启用辅助接口，包括用于管理流量的自动生成的策略型路由配置，以到达正确的数据接口。防火墙管理中心 还会部署 **configure network management-data-interface** 命令的第二个实例。请注意，如果在 CLI 中编辑辅助接口，您将无法配置网关或以其他方式更改默认路由，因为只能在 防火墙管理中心 中编辑此接口的静态路由。

更改管理器访问接口设置

在设备或防火墙管理中心上更改任何管理器接口设置都可能中断管理连接。请参阅以下场景，了解如何更改接口设置并重新建立管理连接。

更改设备 IP 地址

更改设备 IP地址，然后在防火墙管理中心中更新地址。

设置设备 IP 地址

使用以下方法之一设置管理器访问接口 IP 地址。

在 *CLI* 中修改 *Firewall Threat Defense* 管理接口

使用 CLI 修改托管设备上的管理接口设置。这些设置中有许多是您在执行初始设置时设置的；此过程允许您更改这些设置，并设置其他设置，例如，启用事件接口（如果您的型号支持）或添加静态路由。

注释 本主题适用于专用管理接口。您也可以为管理配置数据接口。如果要更改该接口的网络设置，则应在 防火墙管理中心 中而不是在CLI中执行此操作。如果您需要对中断的管理连接进行故障排除，并且需要直接在 Firewall Threat Defense 上进行更改，请参阅 修改 CLI 中用于管理的 Firewall Threat Defense 数据接口，第 885 页。

有关 Firewall Threat Defense CLI 的信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*。

注释 使用 SSH 时，在对管理接口进行更改时要小心；如果由于配置错误而无法重新连接，您将需要访问设备控制台端口。

注释 如果更改设备管理 IP 地址，请参阅以下有关 防火墙管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** 命令识别 防火墙管理中心 的方式（请参阅 向新的管理中心注册，第 55 页）：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 防火墙管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 防火墙管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新防火墙管理中心中的主机名或 IP 地址，第 890 页。此操作有助于更快地重新建立连接。**注意**：如果您指定了无法访问的 防火墙管理中心 IP 地址，请参阅下面的 NAT ID 程序。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 防火墙管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新防火墙管理中心中的主机名或 IP 地址，第 890 页 更改 防火墙管理中心 中的设备管理 IP 地址。

注释 在高可用性配置中，当您从设备 CLI 或 防火墙管理中心修改已注册设备的管理 IP 地址时，即使在 HA 同步后，辅助 防火墙管理中心 也不会反映更改。要确保辅助 防火墙管理中心 也更新，请在两个之间切换角色，使辅助 成为主用设备。防火墙管理中心防火墙管理中心, 在备用的 **设备管理** 页面上修改已注册设备的管理IP地址防火墙管理中心。

开始之前

- 您可以使用 **configure user add** 命令创建可登录到 CLI 的用户账号；请参阅 在 CLI 中添加内部用户，第 137 页。您还可以根据外部身份验证，第 980 页配置 AAA 用户。

过程

步骤 1 通过控制台端口或使用 SSH 连接至设备 CLI。

请参阅登录到设备的命令行界面，第 12 页。

步骤 2 使用管理员用户名和密码登录。

步骤 3 (仅限 Firepower 4100/9300/Secure Firewall 4200/6100）将第二个管理接口启用为仅事件接口。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，则可以为仅事件流量启用该接口。

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件通道，设备也会通过管理接口发送事件。

无法同时禁用接口上的事件通道和管理通道。

要使用单独的事件接口，您必须在专用于事件流量的防火墙管理中心上启用一个事件专用接口。请参阅*Cisco Secure Firewall Management Center* 管理指南。

示例：

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

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

>
```

步骤 4 配置管理接口和/或事件接口的 IP 地址：

如果未指定 *management_interface* 参数，则更改默认管理接口的网络设置。配置事件接口时，请确保指定 *management_interface* 参数。事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。如果连接到您正在配置的接口，您将断开连接。您可以重新连接到新 IP 地址。

a) 配置 IPv4 地址：

- 手动配置：

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  请注意，此命令中的 门户*_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 门户*_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您设置 门户*_ip* 以用于管理接口，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

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

  >
  ```

- DHCP（只有默认的管理接口上才支持）：

  configure network ipv4 dhcp

b) 配置 IPv6 地址：

- 无状态自动配置：

  configure network ipv6 router [*management_interface*]

  示例：

  ```
  > configure network ipv6 router management0
  Setting IPv6 network configuration.
  Network settings changed.
  ```

```
>
```

- 手动配置：

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  请注意，此命令中的 *ipv6_gateway_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ipv6_gateway_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ipv6_gateway_ip* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

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

>
```

- DHCPv6（只有默认的管理接口上才支持）：

  configure network ipv6 dhcp

步骤 5 对于IPv6，启用或禁用ICMPv6回应应答和目的地不可达消息。默认情况下，系统会启用这些消息。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

步骤 6 在默认管理接口上启用 DHCP 服务器，以便向已连接的主机提供 IP 地址：

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

示例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

只有手动设置管理接口 IP 地址时，才能配置 DHCP 服务器。Firewall Management Center Virtual上不支持此命令。要显示 DHCP 服务器的状态，请输入 **show network-dhcp-server**：

```
> show network-dhcp-server
```

```
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

步骤 7 如果 防火墙管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

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

对于 默认 路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 步骤 4，第 881 页）。

示例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

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

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

步骤 8 设置主机名：

configure network hostname *name*

示例：

```
> configure network hostname farscape1.cisco.com
```

在重新启动之后，系统日志消息不会反映新的主机名。

步骤 9 选择搜索域：

configure network dns searchdomains *domain_list*

示例：

```
> configure network dns searchdomains example.com,cisco.com
```

为设备设置搜索域，用逗号隔开。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

步骤 10 设置多达 3 个 DNS 服务器，用逗号隔开：

configure network dns servers *dns_ip_list*

示例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

步骤 11 设置与 防火墙管理中心通信的远程管理端口：

configure network management-interface tcpport *number*

示例：

```
> configure network management-interface tcpport 8555
```

防火墙管理中心和托管设备使用双向、TLS-1.3 加密的通信通道（默认情况下在端口 8305 上）进行通信。使用多实例模式时，请勿更改管理端口；仅支持 8305 端口。

注释
思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

步骤 12 （仅限 Firewall Threat Defense）设置管理或事件接口 MTU。默认 MTU 为 1500 字节。

configure network mtu [字节] [*interface_id*]

- 字节-设置 MTU（以字节为单位）。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。对于事件接口，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。
- *interface_id*-指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

示例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

步骤 13 配置 HTTP 代理。该设备配置为直接连接到互联网上的端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP)。您可以通过 HTTP 摘要对代理服务器进行身份验证。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

注释
对于 Firewall Threat Defense 上的代理密码，只能使用 A-Z、a-z 和 0-9 字符。

configure network http-proxy

示例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

步骤 14 如果更改设备管理 IP 地址，请参阅以下有关 防火墙管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** 命令识别 防火墙管理中心 的方式（请参阅 向新的管理中心注册，第 55 页）：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 防火墙管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 防火墙管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新防火墙管理中心中的主机名或 IP 地址，第 890 页。此操作有助于更快地重新建立连接。**注意**：如果指定了无法访问的 防火墙管理中心 IP 地址，则必须使用 更新防火墙管理中心中的主机名或 IP 地址，第 890 页 手动重新建立连接。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 防火墙管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新防火墙管理中心中的主机名或 IP 地址，第 890 页 更改 防火墙管理中心 中的设备管理 IP 地址。

修改 *CLI* 中用于管理的 *Firewall Threat Defense* 数据接口

如果 Firewall Threat Defense 和 防火墙管理中心 之间的管理连接中断，并且您希望指定新的数据接口来替换旧接口，请使用 Firewall Threat Defense CLI 配置新接口。

如果管理连接处于活动状态，则应使用 防火墙管理中心 对现有数据接口进行任何更改（参见修改 GUI 中用于管理的 Firewall Threat Defense 数据接口，第 888 页）。有关数据管理接口的初始设置，请参阅使用 CLI 完成Firewall Threat Defense初始配置中的 **configure network management-data-interface** 命令。

对于高可用性对，在两台设备上执行所有 CLI 步骤。在 防火墙管理中心中，仅对主用设备执行以下步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

注释 本主题适用于为管理配置的数据接口，而不是专用的管理接口。如果要更改管理接口的网络设置，请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口，第 879 页。

有关 Firewall Threat Defense CLI 的信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*。

过程

步骤 1 如果要将数据管理接口更改为新接口，请将当前接口电缆移至新接口。

步骤 2 连接到设备 CLI。

使用这些命令时，应使用控制台端口。如果您正在执行初始设置，则可能会断开与管理接口的连接。如果由于管理连接中断而正在编辑配置，并且您具有专用管理接口的 SSH 访问权限，则可以使用该 SSH 连接。

请参阅登录到设备的命令行界面。

步骤 3 使用**管理员**用户名和密码登录。

步骤 4 禁用接口，以便您重新配置其设置。

configure network management-data-interface disable

注释
如果您只想在同一接口上设置新的 IPv4 地址而不进行任何其他更改，则可以跳过此步骤。其他更改要求您首先禁用该接口。

示例：

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

步骤 5 配置用于管理器访问的新数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

当您将数据管理接口更改为同一网络上的新接口时，请使用与上一个接口相同的设置（接口 ID 除外）。此外，对于 **是否希望在应用之前清除所有设备配置？(y/n) [n]:** 选项，选择 **y**。此选项将清除旧的数据管理接口配置，以便您可以成功地在新接口上重新使用IP地址和接口名称。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 6 （可选） 限制在特定网络上通过数据接口访问 防火墙管理中心。

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

默认情况下，允许所有网络。

步骤 7 更新防火墙管理中心中的主机名或 IP 地址，第 890 页。

连接将自动重新建立，但在防火墙管理中心中禁用和重新启用连接将有助于更快地重新建立连接。或者，您可能需要根据链接的程序更新 防火墙管理中心 中的设备 IP 地址。

步骤 8 检查管理连接是否已重新建立。

sftunnel-status-brief

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

步骤 9 在 防火墙管理中心中，选择 **设备** > **设备管理**，然后点击 **编辑** ()。**在 设备 管理区域中，点击 刷新**。

防火墙管理中心 检测接口和默认路由配置更改，并阻止部署到。当您在设备上本地更改数据接口设置时，必须在 防火墙管理中心 中手动协调这些更改。您可以在**配置 (Configuration)** 选项卡上查看 防火墙管理中心 和 之间的差异。

步骤 10 选择**接口**并进行以下更改。

a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。

b) 使用旧接口（在 CLI 中使用的接口）的配置配置新的数据管理接口，并为其启用管理器访问。

步骤 11 点击**路由**选项卡，点击 **静态路由**，然后将默认路由从旧数据管理界面更改为新界面。

步骤 12 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

下次部署时，防火墙管理中心 配置将覆盖 Firewall Threat Defense 上任何剩余的冲突设置。在您重新部署之前，您有责任在 防火墙管理中心 中手动修复配置。

您将看到“配置已清除”(Config was cleared) 和“管理器 访问已更改并确认 (Manager/FMC access changed and acknowledged)”的预期消息。

修改 *GUI* 中用于管理的 *Firewall Threat Defense* 数据接口

如果管理连接启动，但要更改用于管理器访问的数据接口的 IP 地址，请执行以下步骤。例如，如果使用 零接触调配注册设备，则需要先将 IP 地址更改为静态地址，然后才能启用高可用性。

您也可以在 CLI 中更改接口设置，但我们建议仅在管理连接断开时使用该方法。无论如何，您在 CLI 中所做的任何更改都必须在 GUI 中复制。

过程

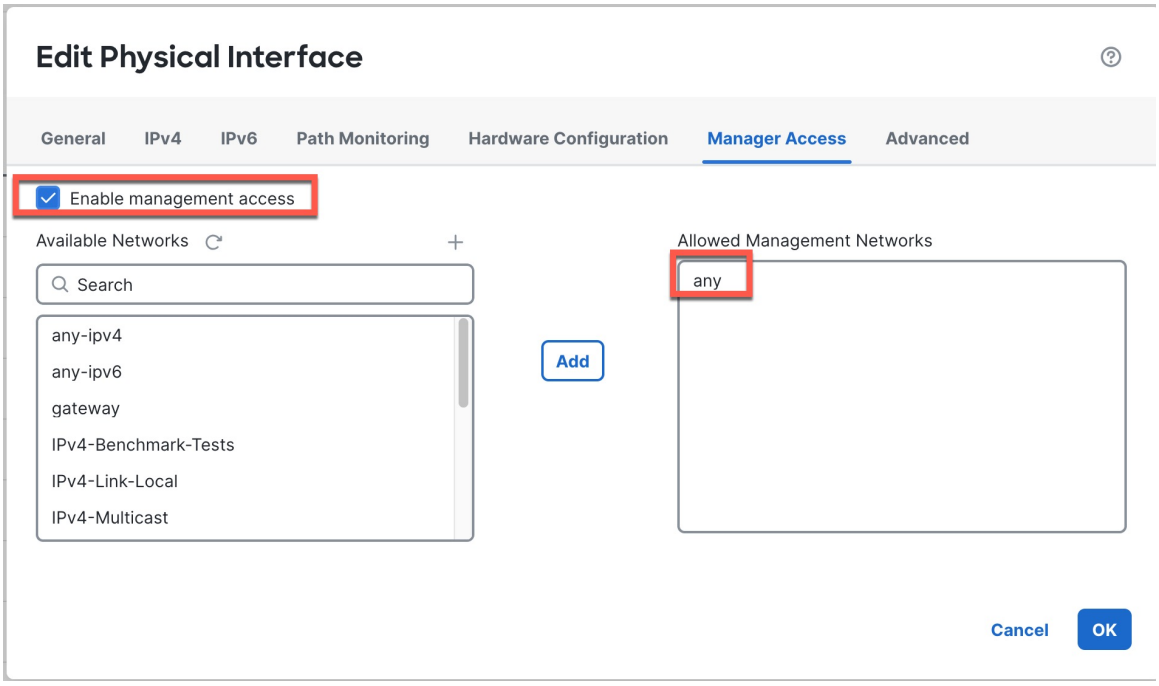
步骤 1 选择 **设备** > **设备管理**，然后点击设备旁边的 **编辑** (✎) 。

步骤 2 选择**接口**。

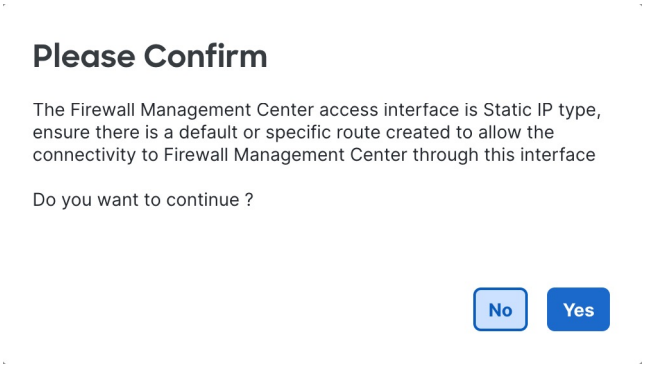
步骤 3 如果要更改用于管理器访问的接口，请执行以下操作：

a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。

b) 使用旧接口的配置配置新的数据管理接口，并为其启用管理器访问。



c) 如果使用静态 IP 地址，系统会提醒您确保具有默认路由。点击**是 (Yes)**。



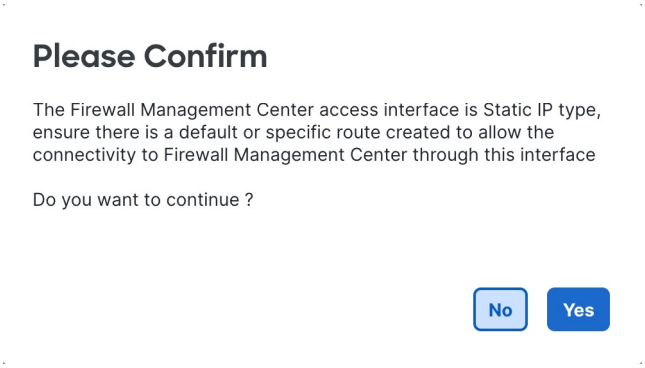
d) 点击 **确定** 退出该界面。

e) 在**接口 (Interfaces)** 页面上点击**保存 (Save)**。

步骤 4 如果只想更改 IP 地址：

a) 请更改 IP 地址。

b) 对于静态 IP 地址，建议您确保具有默认路由。点击**是 (Yes)**。



c) 点击 **确定** 退出该界面。

d) 在**接口 (Interfaces)** 页面上点击**保存 (Save)**。

步骤 5 点击 **路由** 选项卡，点击 **静态路由**，然后添加或更改管理访问接口的默认或静态路由。

步骤 6 部署配置更改；请参阅 部署配置更改，第 180 页。

防火墙管理中心将通过当前连接部署配置更改。在部署后，数据接口将具有新的IP地址，因此需要重新建立管理连接。

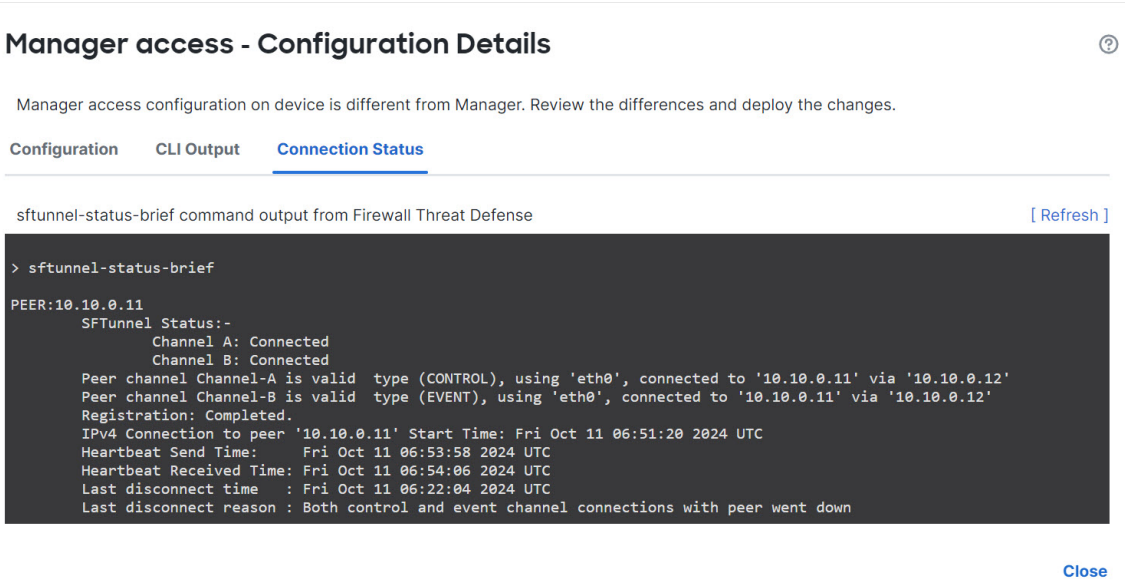
步骤 7 更新防火墙管理中心中的主机名或 IP 地址，第 890 页。

步骤 8 确保管理连接已重新建立。

在**设备** 区域中，在**管理** 字段中，点击 **管理器访问详细信息：配**，然后点击 **连接状态**。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *355:* 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 910 页。

更新防火墙管理中心中的主机名或 IP 地址

如果您在将设备的主机名或 IP 地址添加到 防火墙管理中心 后，对其进行编辑（例如使用设备的 CLI），可能需要使用以下操作步骤手动更新管理 防火墙管理中心 上的主机名或 IP 地址。

更改设备管理 IP 地址的步骤，请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口，第 879 页。

如果您在注册设备时仅使用了 NAT ID，则该 IP 在此页面上显示为 **NO-IP**，您无需更新 IP 地址/主机名。

如果您使用零接触调配在外部接口上注册设备，则会自动生成主机名以及匹配的 DDNS 配置；在这种情况下，您无法编辑主机名。

过程

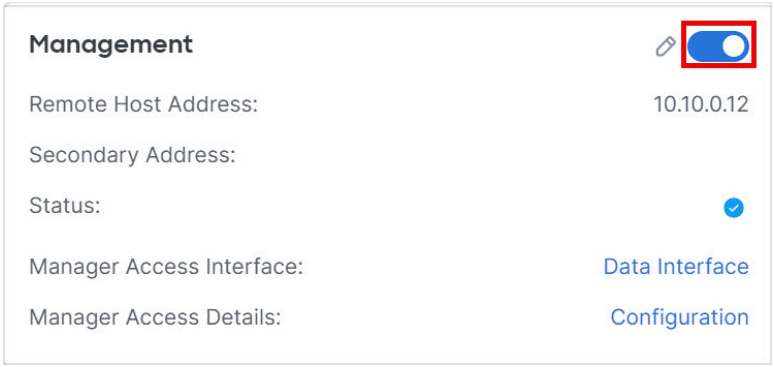
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改管理选项的设备旁边，点击 **编辑** ()。

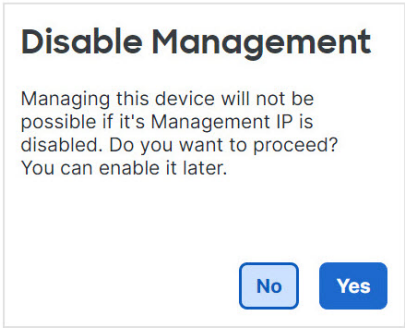
步骤 3 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

步骤 4 点击滑块暂时禁用管理，使其处于禁用状态 **滑块已禁用** ()。

图 *356:* 禁用管理



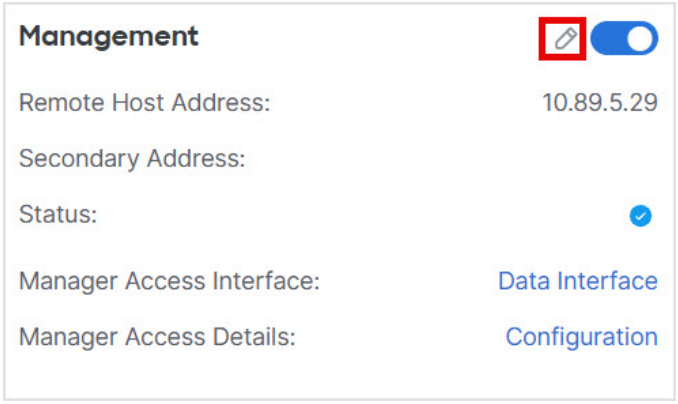
系统将提示您继续禁用管理；点击 **是**。



禁用管理会阻止 防火墙管理中心 和设备之间的连接，但**不会**从 防火墙管理中心 取消注册设备。

步骤 5 通过点击 **编辑** (✎) 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

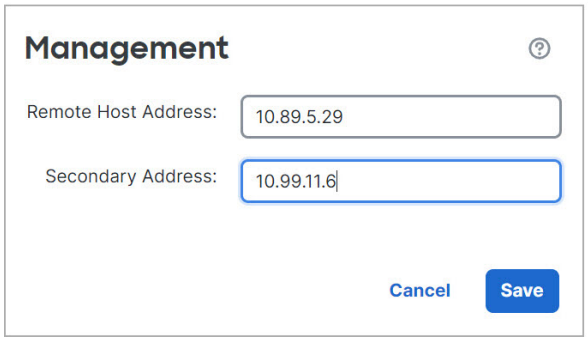
图 *357:* 编辑管理地址



步骤 6 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存**。

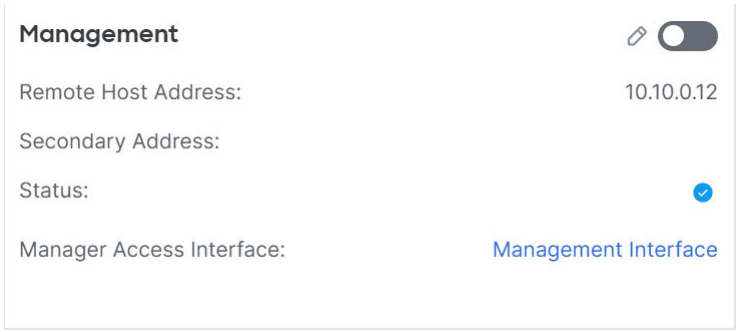
有关使用辅助管理器访问数据接口的信息，请参阅配置冗余管理器访问数据接口，第 874 页。

图 *358:* 管理 *IP* 地址



步骤 7 点击滑块重新启用管理，使其处于启用状态 **滑块已启用** ( )。

图 *359:* 启用管理连接



更改 防火墙管理中心 IP 地址

如果更改 防火墙管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的防火墙管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到防火墙管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持防火墙管理中心IP地址或主机名为最新状态，以实现额外的网络恢复能力。

过程

步骤 1 请更改 防火墙管理中心 IP 地址。

注意
对所连接的防火墙管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 防火墙管理中心 控制台端口以重新配置Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择**管理** > **配置** > **管理接口**。

b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存**。

步骤 2 在 Firewall Threat Defense CLI 中，查看 防火墙管理中心 标识符。

show managers

示例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

步骤 3 在 Firewall Threat Defense CLI 中，编辑 防火墙管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 防火墙管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

管理连接将关闭，然后重新建立。您可以使用 **sftunnel-status** 命令监控连接状态。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

更改防火墙管理中心和威胁防御 IP 地址

如果需要将 防火墙管理中心 和 Firewall Threat Defense IP 地址移至新网络，则可能需要同时更改这些地址。

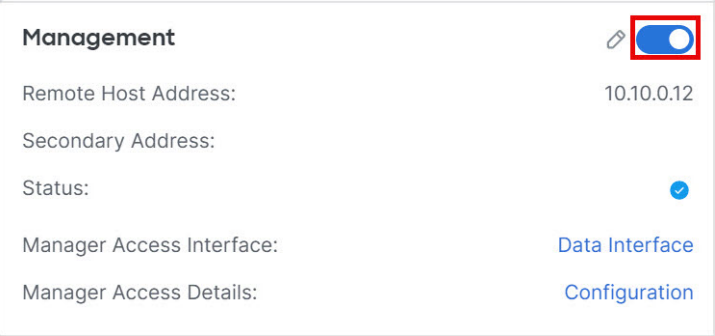
过程

步骤 1 禁用管理连接。

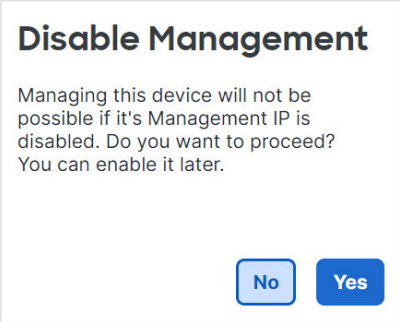
对于高可用性对或集群，在所有设备上执行这些步骤。

a) 选择**设备** > **设备管理**。
b) 点击设备旁边的 **编辑** ( )。
c) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。
d) 点击滑块暂时禁用管理，使其处于禁用状态 ( )。

图 *360:* 禁用管理



系统将提示您继续禁用管理；点击 **是**。



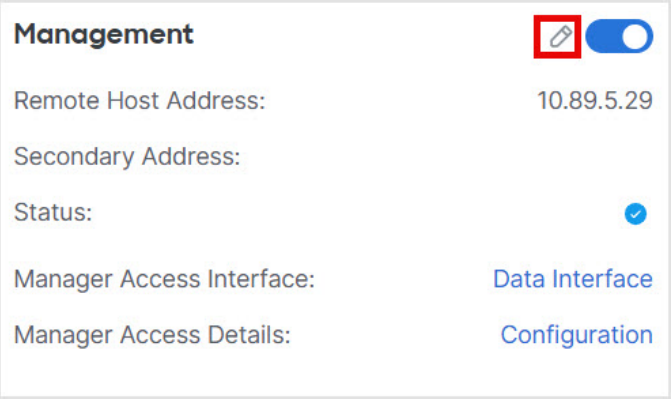
步骤 2 将 防火墙管理中心 中的设备 IP 地址更改为新的设备 IP 地址。

稍后您将更改设备上的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

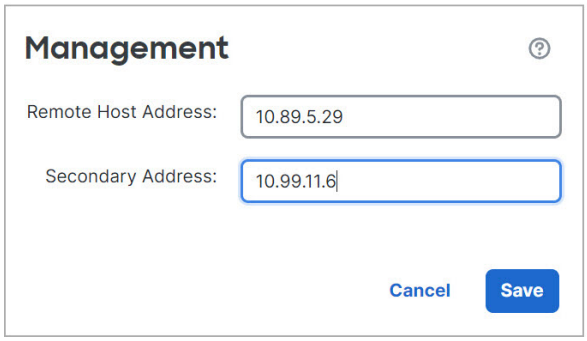
a) 通过点击 **编辑** (✎) 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 *361:* 编辑管理地址



b) 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存**。

图 *362:* 管理 *IP* 地址



步骤 3 请更改 防火墙管理中心 IP 地址。

注意
对所连接的防火墙管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 防火墙管理中心 控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择**管理** > **配置** > **管理接口**。
b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存**。

步骤 4 更改设备上的管理器 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 在 Firewall Threat Defense CLI 中，查看 防火墙管理中心 标识符。

show managers

示例：

```
> show managers
Type                       : Manager
Host                       : 10.10.1.4
Display name               : 10.10.1.4
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
Management type            : Configuration
```

b) 编辑 防火墙管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 防火墙管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

步骤 5 在控制台端口更改管理器访问接口的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

如果您使用专用管理接口：

configure network ipv4

configure network ipv6

如果您使用专用管理接口：

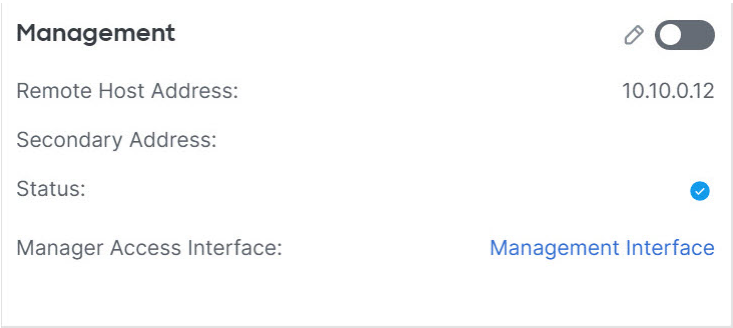
configure network management-data-interface disable

configure network management-data-interface

步骤 6 点击滑块重新启用管理，使其处于启用状态 ( )。

对于高可用性对或集群，在所有设备上执行这些步骤。

图 *363:* 启用管理连接



步骤 7 （如果使用数据接口进行管理器访问）刷新 防火墙管理中心中的数据接口设置。

对于高可用性对，请在两台设备上执行此步骤。

a) 选择**设备** > **设备管理**，点击**管理器访问 - 配置详细信息**，然后点击**刷新**。
b) 选择**设备** > **设备管理**，点击**接口**选项卡，然后设置 IP 地址以便与新地址匹配。
c) 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

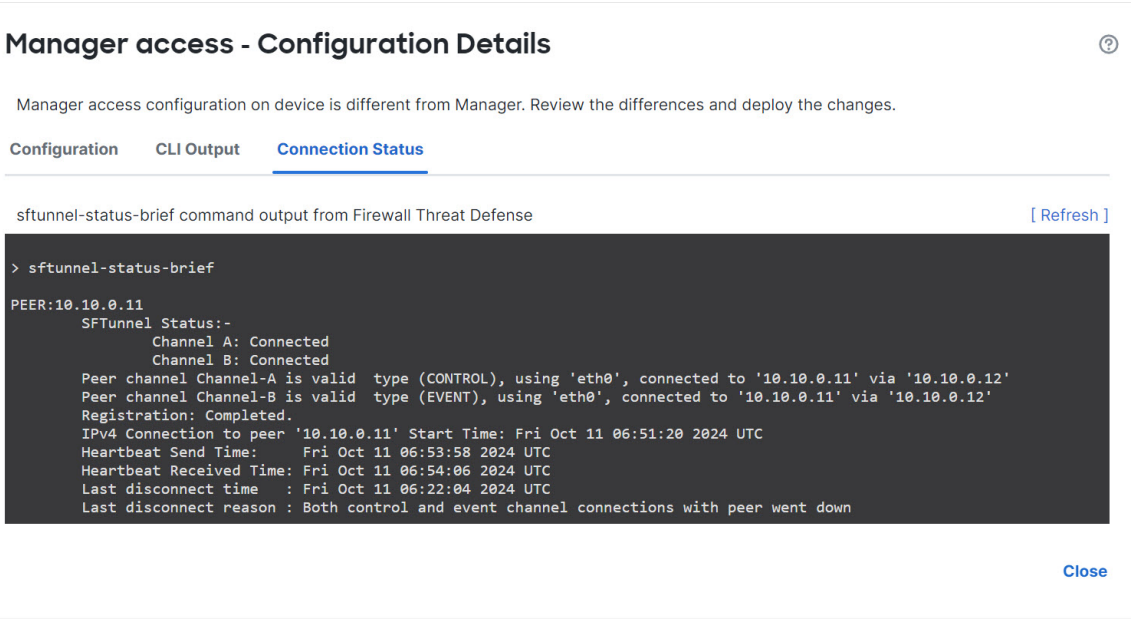
步骤 8 确保管理连接已重新建立。

在防火墙管理中心中，检查管理连接状态。导航到 **设备** > **设备管理**，然后点击**设备**选项卡下的**管理**部分。然后点击**管理器访问 - 配置详细信息**以查看**连接状态**页面。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *364:* 连接状态



步骤 9 （对于高可用性 防火墙管理中心 对）在辅助 防火墙管理中心上重复配置更改。

a) 更改辅助 防火墙管理中心 IP 地址。
b) 在两台设备上指定新的对等地址。
c) 将辅助设备设置为主用设备。
d) 禁用设备管理连接。
e) 更改 防火墙管理中心 中的设备 IP 地址。
f) 重新启用管理连接。

更改管理器访问接口

注册设备后，可以在管理接口和数据接口之间更改管理器访问接口。

将管理器访问接口从管理更改为数据

你可以从专门的管理界面，或从数据界面管理 Firewall Threat Defense。如果要在添加设备转至 防火墙管理中心 后更改管理器访问接口，请按照以下步骤从管理接口迁移到数据接口。要迁移另一个方向，请参阅将管理器访问接口从数据更改为管理，第 902 页。

启动从管理到数据的管理器访问迁移会导致 防火墙管理中心 在部署到 Firewall Threat Defense 时应用阻止。要删除数据块，请在数据接口上启用管理器访问。

请参阅以下步骤以启用数据接口上的管理器访问，并配置其他所需的设置。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

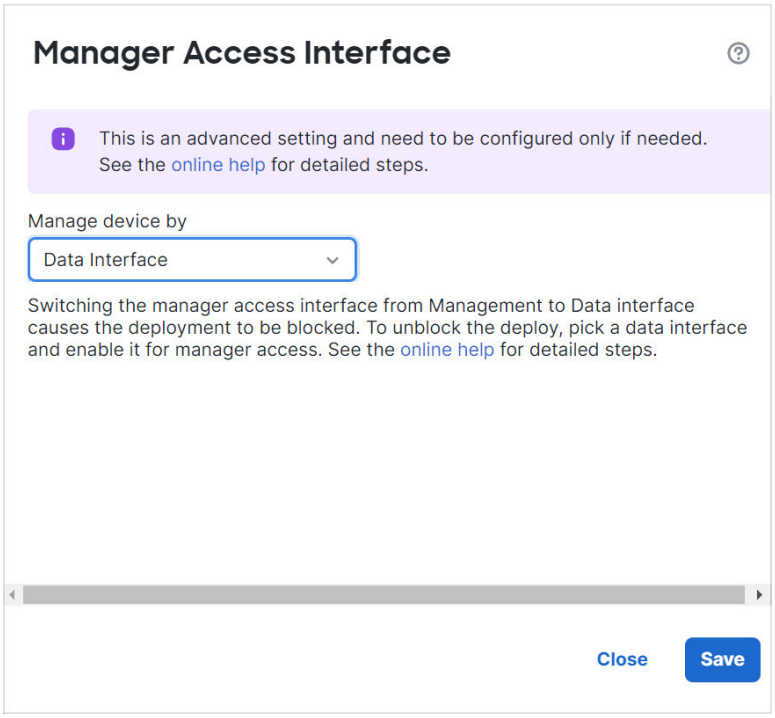
过程

步骤 1 初始化接口迁移。

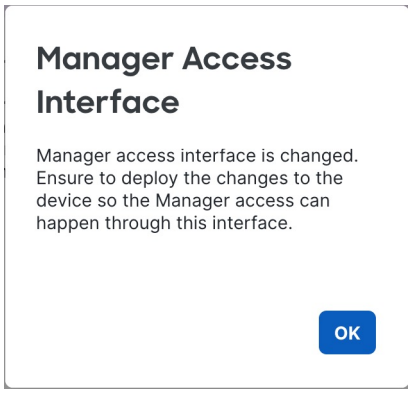
a) 在 设备设备管理 页面，然后点击设备的 **设备** > **设备管理** 。**编辑** (✎)**点击 设备**，然后在**管理**区域中点击FMC 访问接口的链接。

管理器访问接口 (Manager Access Interface) 字段会显示当前管理接口。当您点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型 **数据接口**。

图 ***365:*** 管理器访问接口

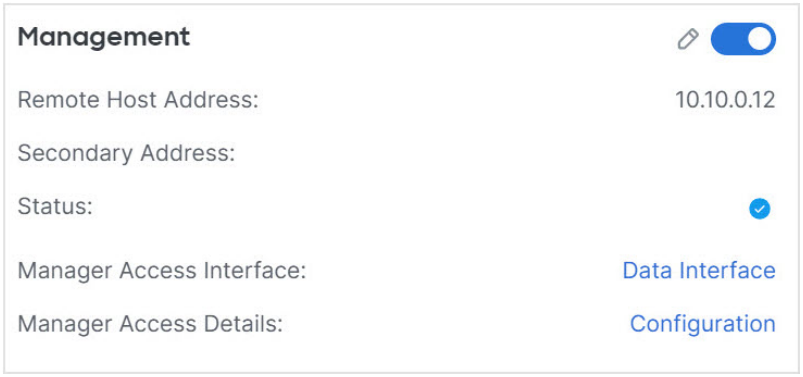


b) 点击 **确定** ，然后点击 **关闭 (Close)**。



您现在必须完成此程序中的其余步骤，才能在数据接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：数据接口 (Manager Access Interface: Data Interface)** 以及**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

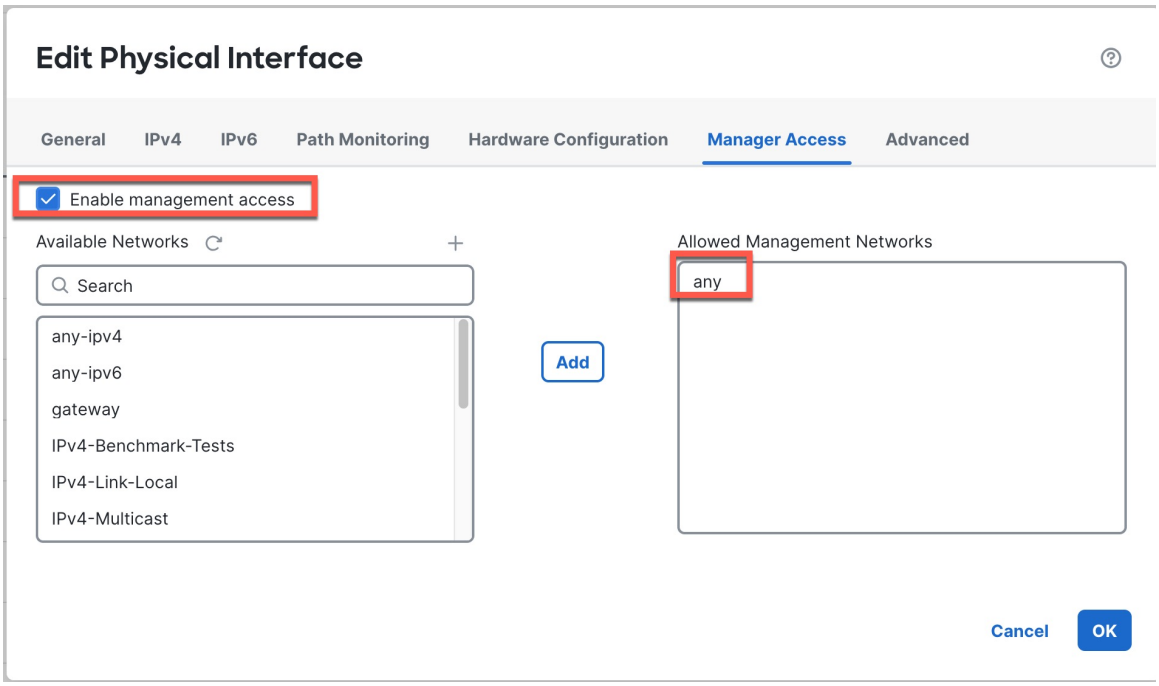
图 ***366:*** 管理器访问



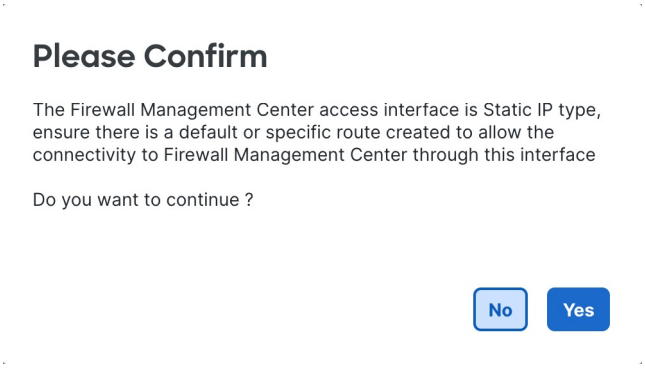
如果点击**配置 (Configuration)**，将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 将显示“等待部署” (Deploy pending) 状态。

步骤 2 在数据接口上启用管理器访问。点击**接口 (Interfaces)**，点击接口的**编辑** ()，然后点击**管理器访问 (Manager Access**。

选中**启用管理访问 (Enable management access)**，然后点击**确定**。默认情况下，系统允许所有网络，但您可以在允许 防火墙管理中心 地址的情况下限制访问。



如果管理器访问接口使用静态 IP 地址，系统会提醒您为其配置路由。



在**接口 (Interfaces)** 页面上点击**保存**。有关接口设置的详细信息，请参阅配置路由模式接口，第 792 页。您可在一个数据接口以及一个可选的辅助接口上启用管理器访问。确保这些接口使用名称和 IP 地址进行了充分配置，并且已启用。

如果使用辅助接口实现冗余，请参阅配置冗余管理器访问数据接口，第 874 页以了解其他所需的配置。

步骤 3 （可选） 如果对接口使用DHCP，请在 **设备** 设备管理DHCPDDNS 页面上启用 Web 类型 DDNS 方法。导航至 **设备** > **设备管理**，然后点击 **DHCP** 选项卡下的 **DDNS** 。

请参阅配置动态 DNS，第 965 页。如果 FTD 的 IP 地址发生变化，DDNS 可确保 防火墙管理中心 接通完全限定域名 (FQDN) 内的 Firewall Threat Defense。

步骤 4 确保 Firewall Threat Defense 可以通过数据接口路由到防火墙管理中心；如果需要，在 设备 (Devices) 设备管理 (Device Management)路由 (Routing)静态路由 (Routing)上添加静态路由。导航至 **设备** > **设备管理** ，然后点击 **“路由”(Routing)** 选项卡下的 **静态路由 (Static Route)** 。

请参阅添加静态路由，第 1090 页。

步骤 5 （可选） 在平台设置策略中配置 DNS：选择 **设备** > **平台设置**，然后点击 **DNS**。将此策略应用到此设备。

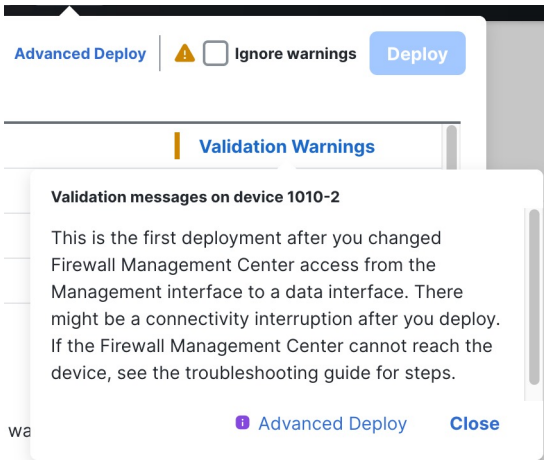
请参阅DNS，第 977 页。如果使用 DDNS，则需要 DNS。您也可以将 DNS 用于安全策略中的 FQDN。

步骤 6 （可选） 在平台设置策略中为数据接口启用 SSH，并通过**设备** > **设备管理**页面将其应用于此设备。点击设备的 **编辑** ()，然后点击 **SSH 访问 (SSH Access)**。

请参阅SSH 访问，第 991 页。默认情况下，数据接口上未启用 SSH，因此，如果要使用 SSH 管理 Firewall Threat Defense，则需要明确允许它。

步骤 7 部署配置更改；请参阅 部署配置更改，第 180 页。

您将看到一条验证错误，要求您确认更改是否更改了管理器访问接口。选中**忽略警告 (Ignore warnings)** 并再次部署。



防火墙管理中心 将通过当前管理接口部署配置更改。部署后，数据接口现在可供使用，但与管理的原始管理连接仍处于活动状态。

步骤 8 在 Firewall Threat Defense CLI（最好从控制台端口），将管理接口设置为使用静态 IP 地址，并将网关设置为使用数据接口。 对于高可用性，请在两台设备上执行此步骤。

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask* - 虽然您不打算使用管理接口，但必须设置静态IP地址，例如专用地址，以便将网关设置为 **数据接口**（请参阅下一个项目符号）。您无法使用 DHCP，因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。
- **data-interfaces** - 此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。

我们建议您使用控制台端口而不是 SSH 连接，因为当您更改管理接口网络设置时，您的 SSH 会话将断开。

步骤 9 如有必要，请重新连接 Firewall Threat Defense，使其能够到达数据接口上的 防火墙管理中心。 对于高可用性，请在两台设备上执行此步骤。

步骤 10 在 防火墙管理中心 中，禁用管理连接，在设备管理区域的 **设备 设备管理** 设备中更新 Firewall Threat Defense 的**远程主机地址**IP 地址和可选**辅助地址**，然后重新启用连接。**设备 > 设备管理**

请参阅更新防火墙管理中心中的主机名或 IP 地址，第 890 页。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 时使用了 Firewall Threat Defense 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

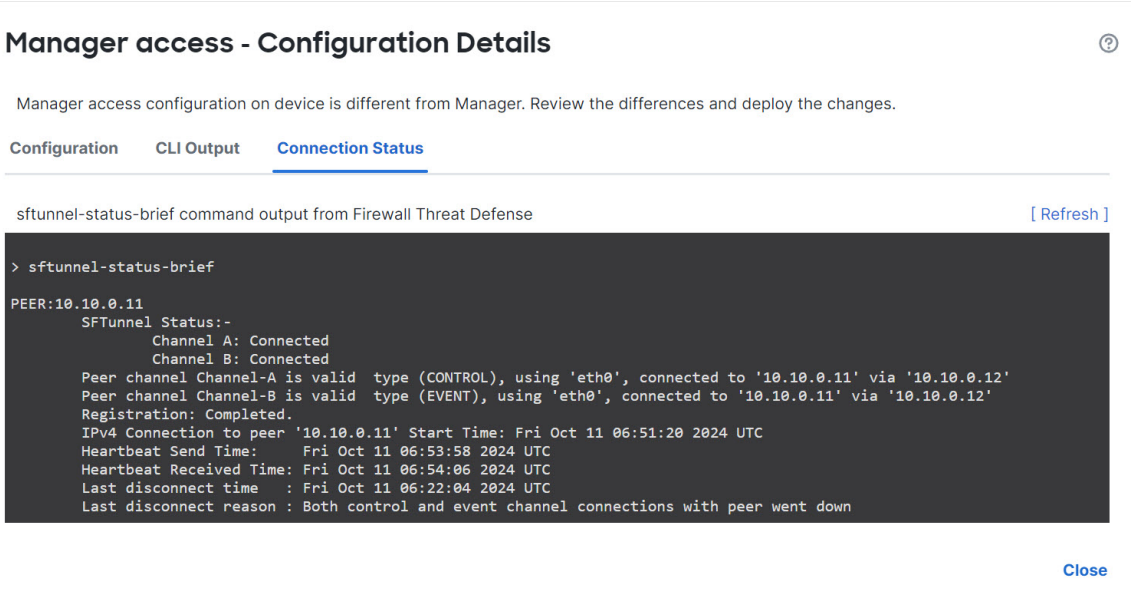
步骤 11 确保管理连接已重新建立。

在**设备 > 设备管理**页面，点击**管理器访问详细信息：配置 (Manager Access Details: Configuration)** 然后点击**连接状态 (Connection Status)**。

或者，您可以在 Firewall Threat Defense CLI 中进行检查。输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *367:* 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 910 页。

将管理器访问接口从数据更改为管理

你可以从专门的管理界面，或从数据界面管理 Firewall Threat Defense。如果要在添加设备到 防火墙管理中心 后更改管理器访问接口，请按照以下步骤从数据接口迁移到管理接口。要迁移另一个方向，请参阅将管理器访问接口从管理更改为数据，第 897 页。

启动从数据到管理的管理器访问迁移会导致 防火墙管理中心 在部署到 Firewall Threat Defense 时应用阻止。您必须在数据接口上禁用管理器访问权限才能删除数据块。

请参阅以下步骤以禁用数据接口上的管理器访问，并配置其他所需的设置。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

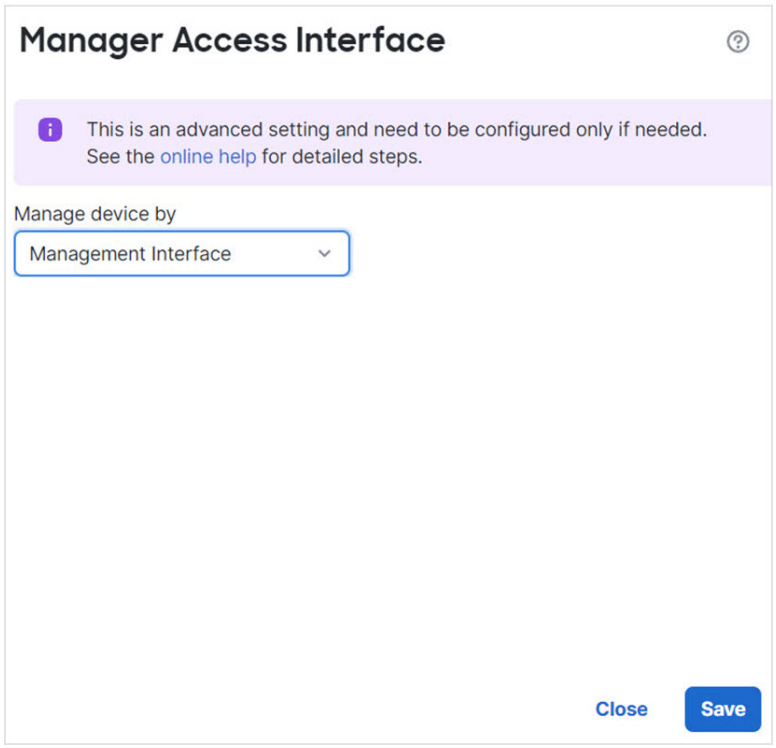
过程

步骤 1 初始化接口迁移。

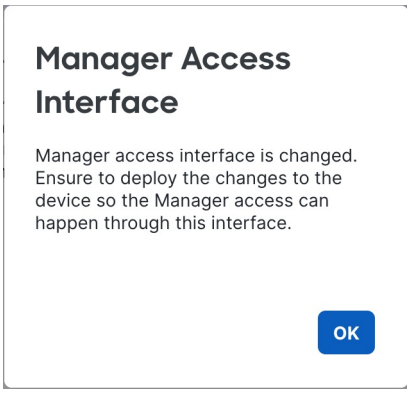
a) 在 设备设备管理 页面，然后点击设备的 **设备** > **设备管理** 。**编辑** (✎)**点击 设备**，然后在**管理**区域中点击FMC 访问接口的链接。

管理器访问接口 (Manager Access Interface) 字段会将当前管理接口显示为数据。点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型， **管理接口**。

图 ***368:*** 管理器访问接口



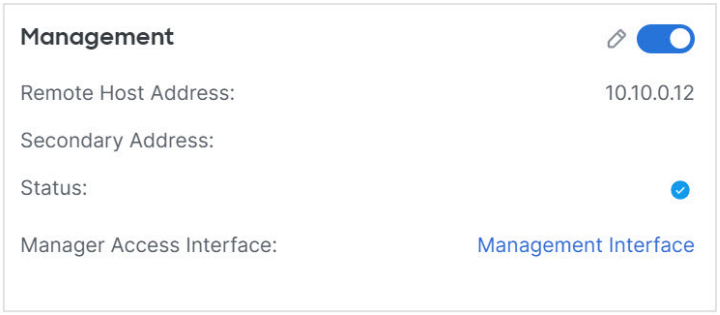
b) 点击**保存**。



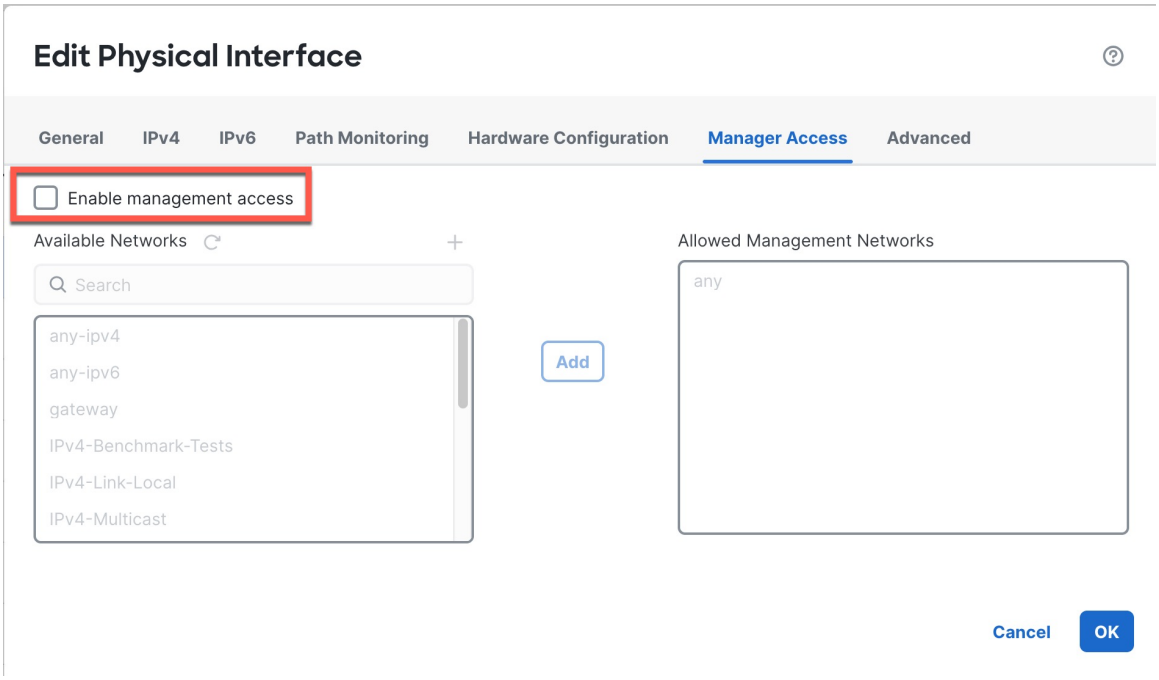
点击**确定**，然后点击**关闭 (Close)**。

您现在必须完成此程序中的其余步骤，才能在管理接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：管理接口 (Manager Access Interface: Management Interface)**。

图 ***369:*** 管理器访问



步骤 2 在数据接口上禁用管理器访问。点击 **接口 (Interfaces)**，点击接口所对应的 **编辑** (✎)，然后点击 **管理器访问 (Manager Access**。



取消选中**启用管理访问 (Enable management access)**，然后点击**确定**。在**接口 (Interfaces)** 页面上点击**保存**。此步骤将删除部署时的阻止。

步骤 3 如果尚未执行此操作，请在“平台设置”策略中为数据接口配置 DNS 设置，然后在 设备平台设置 DNS上将其应用至设备。**设备** > **设备管理**点击设备的 **编辑** (✎)，然后点击 **DNS**。

请参阅DNS，第 977 页。在数据接口上禁用管理器访问的防火墙管理中心 部署将删除任何本地 DNS 配置。如果该 DNS 服务器用于任何安全策略，例如访问规则中的 FQDN，则必须使用 防火墙管理中心 重新应用 DNS 配置。

步骤 4 部署配置更改；请参阅 部署配置更改，第 180 页。

将 防火墙管理中心 通过当前数据接口部署配置更改。

步骤 5 如有必要，请重新连接 Firewall Threat Defense，以便它可以到达管理接口上的 防火墙管理中心。 对于高可用性，请在两台设备上执行此步骤。

步骤 6 在 Firewall Threat Defense CLI 中，使用静态 IP 地址或 DHCP 配置管理接口 IP 地址和网关。 对于高可用性，请在两台设备上执行此步骤。

当您最初配置用于管理器访问的数据接口时，管理网关设置为 data-interfaces，它通过背板转发管理流量，以便可以通过管理器访问数据接口路由。您现在需要为管理网络上的网关设置 IP 地址。

静态 IP 地址：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **dhcp**

步骤 7 在 防火墙管理中心 中，禁用管理连接，在 **设备 (Devices) 设备管理 (Device Management)** 设备 (Device) 管理 (Management) 部分中更新 Firewall Threat Defense 的**远程主机地址 (Remote Host Address)**IP 地址 (IP address) 和可选**辅助地址 (Secondary Address)**，然后重新启用连接。**设备 > 设备管理**

请参阅更新防火墙管理中心中的主机名或 IP 地址，第 890 页。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 时使用了 Firewall Threat Defense 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

步骤 8 确保管理连接已重新建立。

在 防火墙管理中心 中，检查 **设备 (Devices) 设备管理 (Device Management) 设备 (Device)** 管理 (Management)状态 (Status)字段上的管理连接状态或查看 **设备 > 设备管理** 中的通知。防火墙管理中心

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 910 页。

查看数据接口管理的管理器访问详细信息

当使用数据接口进行 防火墙管理中心 管理而不是使用专用管理接口时，必须注意在 防火墙管理中心 中更改设备的接口和网络设置，以免中断连接。您也可以在设备上本地更改数据接口设置，这就要求您在 防火墙管理中心 中手动协调这些更改。**设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 设备管理 (Management) > 管理器访问 + 配置详细信息 (Manager Access - Configuration Details)** 对话框可帮助您解决 防火墙管理中心 和 Firewall Threat Defense 本地配置之间的任何差异。

通常，在将 Firewall Threat Defense 添加到 防火墙管理中心 之前，您可以作为初始 Firewall Threat Defense 设置的一部分来配置管理器访问数据接口。当您将 Firewall Threat Defense 添加到 防火墙管理中心时， 防火墙管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。对于 DNS 服务器，如果在注册期间发现了它，则在本地维护配置，但不会将其添加到 防火墙管理中心 中的平台设置策略。

将 Firewall Threat Defense 添加到 防火墙管理中心 后，如果使用 **configure network management-data-interface** 命令在 Firewall Threat Defense 上本地更改数据接口设置，则 防火墙管理中心 会检测到配置更改，并阻止部署到 Firewall Threat Defense。防火墙管理中心 会使用以下方法之一来检测配置更改：

- 部署到 Firewall Threat Defense。在部署 防火墙管理中心 之前，它将检测配置差异并停止部署。
- **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框上的**刷新 (Refresh)** 按钮

要删除阻止，您必须转到**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)**. 下次部署时，防火墙管理中心 配置将覆盖 Firewall Threat Defense 上任何剩余的冲突设置。在您重新部署之前，您有责任在 防火墙管理中心 中手动修复配置。

请参阅此对话框中的以下页面。

配置

查看 防火墙管理中心 和 Firewall Threat Defense 上的管理器访问数据接口的配置对比。

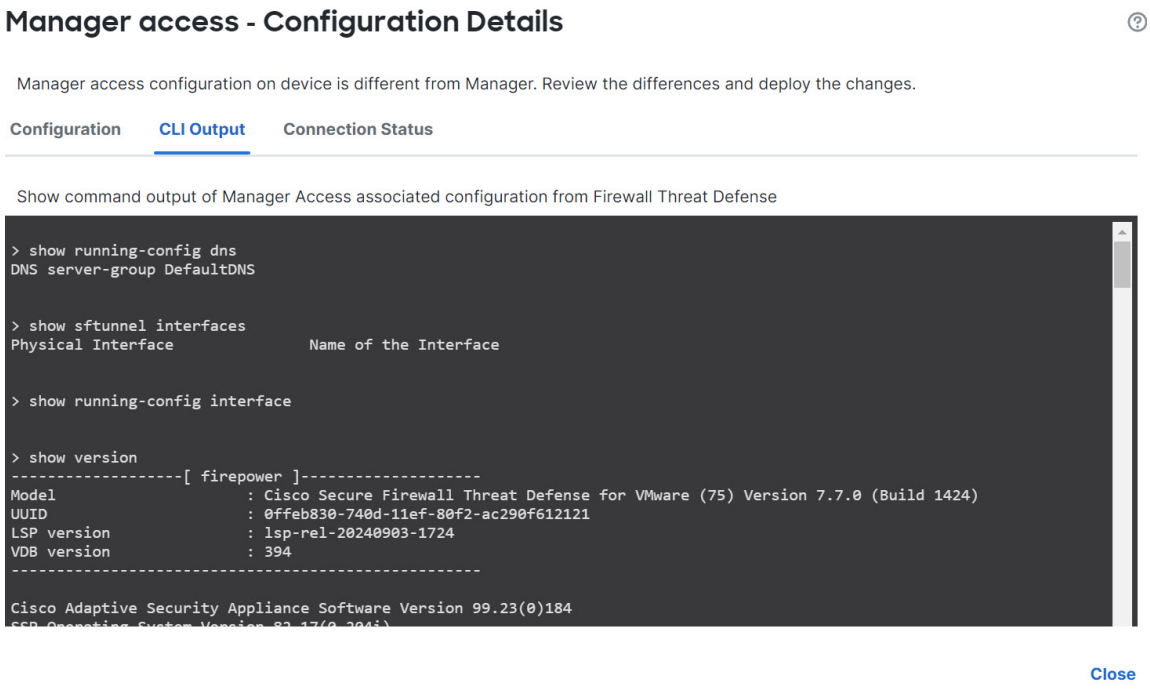
以下示例显示了在 Firewall Threat Defense 上输入 **configure network management-data-interface** 命令的位置的 Firewall Threat Defense 配置详细信息。以粉红色突出显示的内容显示了如果您**确认**差异但不匹配 防火墙管理中心 中的配置，则 Firewall Threat Defense 配置将被删除。以蓝色突出显示的内容显示了将在 Firewall Threat Defense 上修改的配置。以绿色突出显示的内容显示了将被添加到 Firewall Threat Defense 的配置。

以下示例显示在 防火墙管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。

CLI 输出

查看管理器访问数据接口的 CLI 配置，如果您熟悉底层 CLI，这将非常有用。

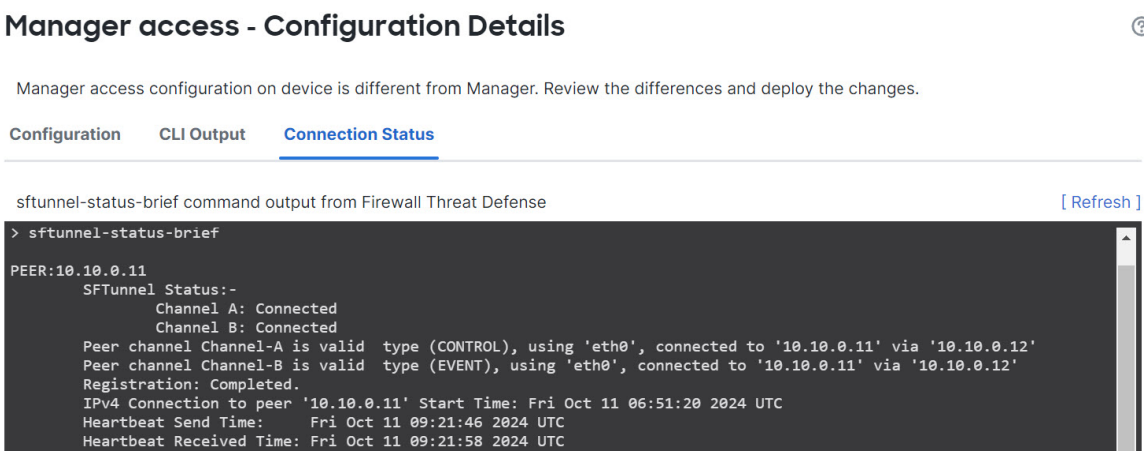
图 *370: CLI* 输出



连接状态

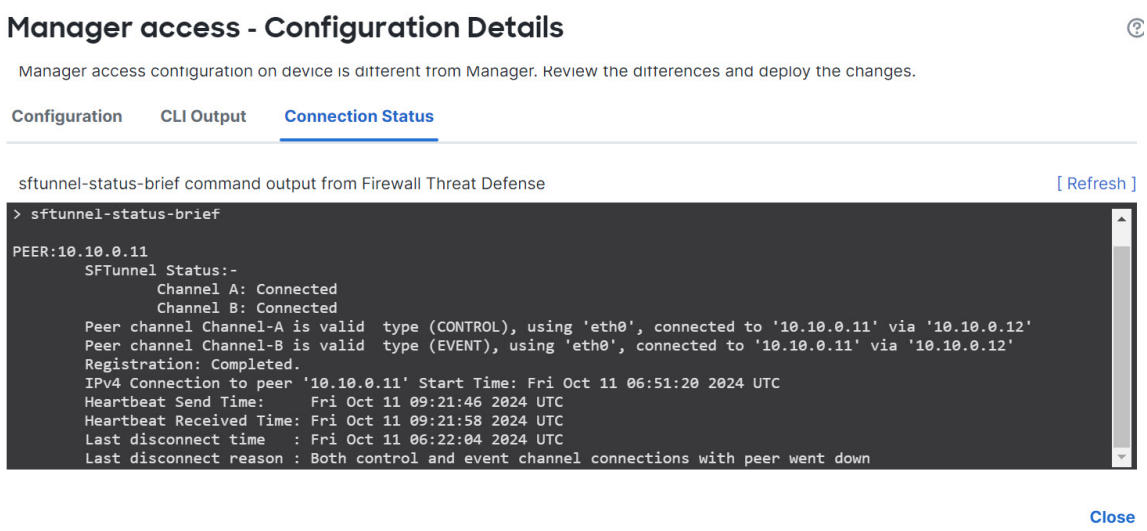
查看管理连接状态。以下示例显示了管理连接仍在使用管理“management0”接口。

图 *371:* 连接状态



以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *372:* 连接状态



请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
```

```
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

管理连接故障排除

如果防火墙管理中心断开连接，则手动回滚配置

如果将Firewall Threat Defense上的数据接口用于管理器访问，并从防火墙管理中心部署影响网络连接的配置更改，则可以将Firewall Threat Defense上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整防火墙管理中心中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

或者，如果在部署后失去连接，您可以启用配置的自动回滚；请参阅 编辑部署设置，第 921 页。

请参阅以下准则：

- 只有以前的部署可以在 Firewall Threat Defense 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 回滚只会影响您可以在防火墙管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 Firewall Threat Defense CLI 中进行配置。请注意，如果您在上次防火墙管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 防火墙管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在 Firewall Threat Defense CLI 中，回滚到之前的配置。

configure policy rollback

回滚后，Firewall Threat Defense 会通知 防火墙管理中心 已成功完成回滚。在 防火墙管理中心 中，部署屏幕将显示一条横幅，说明配置已回滚。

注释

如果回滚失败且 防火墙管理中心 管理已恢复，请参阅https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html以了解常见的部署问题。在某些情况下，恢复 防火墙管理中心 管理访问权限后回滚可能会失败；在这种情况下，您可以解决 防火墙管理中心 配置问题，并从 防火墙管理中心 重新部署。

示例：

对于使用数据接口进行管理器访问的 Firewall Threat Defense ：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

步骤 2 检查管理连接是否已重新建立。

在 防火墙管理中心中，在连接状态 (Connection Status) 页面上检查管理连接状态。导航到 **设备** > **设备管理** ，然后导航到 **设备** 选项卡下的 **管理 (Management)** 区域。在 **设备 (Device)** 区域中，点击管理器访问详细信息：配置 (Manager Access Details: Configuration)FMC 访问：配置 (FMC Access: Configuration)，然后点击连接状态 (Connection Status)。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 910 页。

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须注意在 防火墙管理中心 中更改 Firewall Threat Defense 的接口和网络设置，以免中断连接。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在防火墙管理中心中，在**设备** > **设备管理**页面上检查管理连接状态。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 Firewall Threat Defense 网络信息

在 Firewall Threat Defense CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
```

```
DNS Servers               : 72.163.47.11
Interfaces                : Ethernet1/1

==================[ Ethernet1/1 ]==================
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.6
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

检查向 防火墙管理中心注册 Firewall Threat Defense

在 Firewall Threat Defense CLI 中，检查 防火墙管理中心 注册是否已完成。请注意，此命令不会显示管理连接的 当前 状态。

show managers

```
> show managers
Type                      : Manager
Host                      : 16a3893c-caa7-11ee-8436-0925c06e7608DONTRESOLVE
Display name              : manager-1707852946.80444
Version                   : 7.6.0 (Build 1385)
Identifier                : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Registration              : Completed
Management type           : Configuration and analytics
```

Ping the 防火墙管理中心

在 Firewall Threat Defense CLI 上，使用以下命令从数据接口对 防火墙管理中心 执行 ping 操作：

ping *fmc_ip*

在 Firewall Threat Defense CLI 上，使用以下命令从管理接口对 防火墙管理中心 执行 ping 操作，该接口应通过背板路由到数据接口：

ping system *fmc_ip*

捕获 Firewall Threat Defense 内部接口上的数据包

在 Firewall Threat Defense CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

检查内部接口状态，统计信息和数据包计数

在 Firewall Threat Defense CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interface detail

```
> show interface detail
[...]
```

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

检查路由和 NAT

在 Firewall Threat Defense CLI 中，检查是否已添加默认路由 (S *)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在防火墙管理中心的**设备** > **设备管理**页面上看到许多这些命令。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

检查 DDNS 更新是否成功

在 Firewall Threat Defense CLI 中，检查 DDNS 更新是否成功：

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：

show crypto ca certificates *trustpoint_name*

要检查 DDNS 操作，请执行以下操作：

show ddns update interface *fmc_访问_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

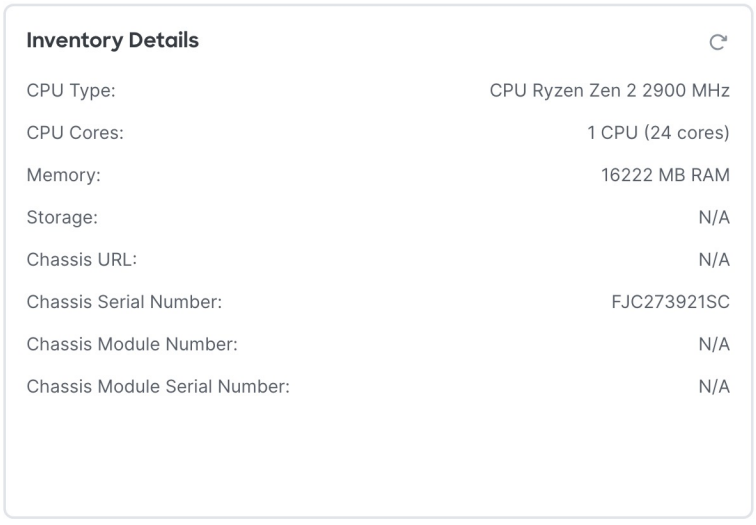
检查 防火墙管理中心 日志文件

请参阅 https://cisco.com/go/fmc-reg-error。

查看清单详细信息

设备 (Device) 页面上的**清单详细信息 (Inventory Details)** 部分会显示机箱详细信息，例如 CPU 和内存。

图 *373:* 设备清单详细信息



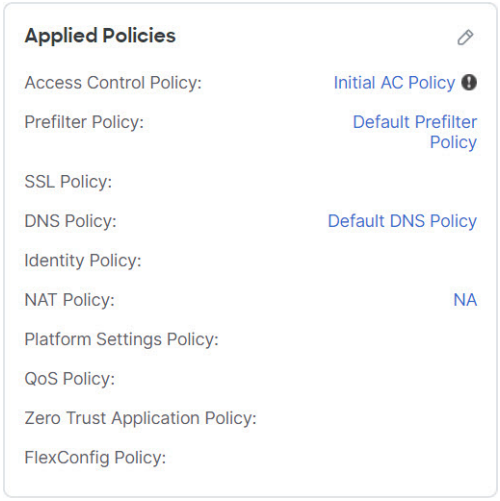
此部分显示机箱序列号。防火墙包含两个序列号：机箱序列号和 PCB（电路板）序列号。PCB 序列号显示在系统部分中。Firewall Threat Defense Virtual 没有机箱序列号。

要更新信息，请点击 **刷新** ()。

编辑应用的策略

设备 (Device) 页面的**应用的策略 (Applied Policies)** 部分显示了应用于防火墙的以下策略：

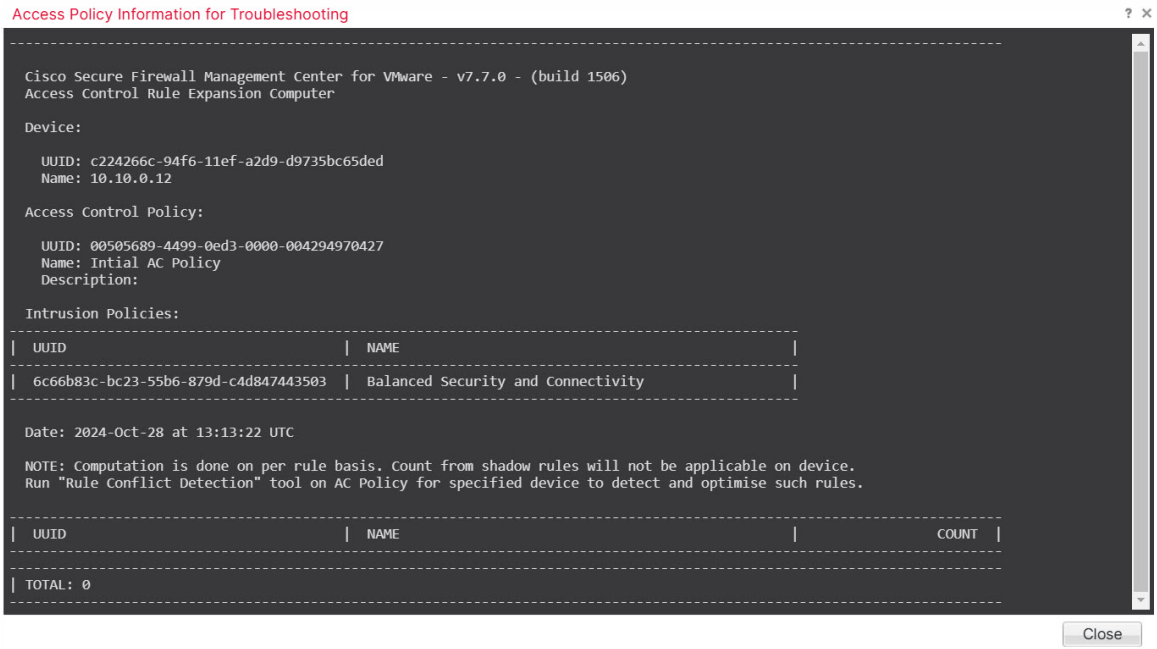
图 ***374:*** 应用的策略



对于包含链接的策略，您可以点击链接以查看策略。

对于访问控制策略，请点击 **感叹号 (!)** 图标以查看**用于故障排除的访问策略信息 (Access Policy Information for Troubleshooting)** 对话框。该对话框显示了如何将访问规则扩展为访问控制条目 (ACE)。

图 ***375:*** 用于故障排除的访问策略信息



您可以从**设备管理 (Device Management)** 页面将策略分配给单个设备。

过程

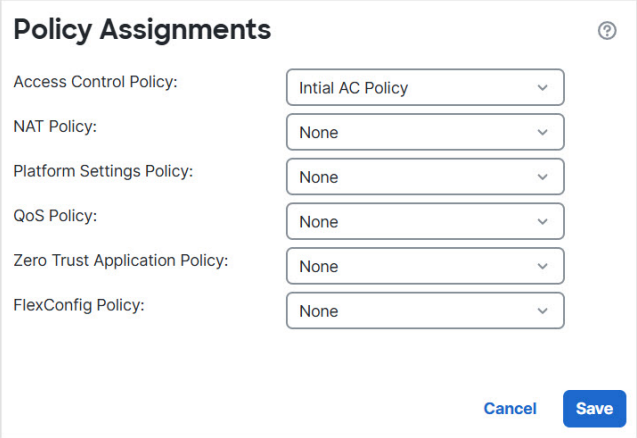
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 在 **应用的策略** 部分中，点击 **编辑** ()。

图 *376:* 策略分配



步骤 5 对于每种策略类型，请从下拉菜单选择一个策略。只有现有的策略会被列出。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

编辑高级设置

设备 (Device) 页面的**高级设置 (Advanced Settings)** 部分会显示高级配置设置表，如下所述。您可以编辑任何这些设置。

表 *61:* “高级” *(Advanced)* 部分表字段

字段	说明
应用绕行	设备上“自动应用绕行”的状态。

字段	说明
旁路阈值	“自动应用绕行”阈值（以毫秒为单位）。
对象组搜索	设备上对象组搜索的状态。运行时，FTD 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 Firepower 管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。 注释 默认情况下，当您首次在管理中心添加威胁防御时，将启用**对象组搜索 (Object Group Search)**。
接口对象优化	设备上的接口对象优化状态。部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

以下主题介绍如何编辑高级设备设置。

注释 有关“传输数据包”(Transfer Packets) 设置的信息，请参阅编辑常规设置，第 847 页。

配置自动应用旁路

自动应用绕行 (AAB) 允许数据包在 Snort 关闭或时绕过检测，或者对于经典设备，如果数据包处理时间过长，则 。AAB 会导致 Snort 在故障发生后的十分钟内重新启动，并生成可用于分析 Snort 故障原因的故障排除数据。

注意 部分激活 AAB 会重启 Snort 进程，这会暂时中断对几个数据包的检测。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

请参阅以下行为：

Firewall Threat Defense 行为：如果 Snort 关闭，则在指定的计时器持续时间后触发 AAB。如果 Snort 已启用，则即使数据包处理超过配置的计时器，也不会触发 AAB。

经典设备行为：AAB 限制通过接口处理数据包所允许的时间。通过网络的数据包延迟容限来平衡数据包处理时延。

该功能适用于任何部署；但在内联部署中最有价值。

通常，在超过延迟阈值后使用入侵策略中的“规则延迟阈值”通过快速路径传送数据包。“规则延迟阈值”不关闭引擎或生成故障排除数据。

如果绕过了检测，则设备会生成运行状况监控警报。

AAB 默认为禁用；要启用 AAB，请按照所述步骤进行操作。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑高级设备设置的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)**，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** (✎) 。

步骤 4 选中**自动应用旁路**。

步骤 5 输入介于 250 毫秒到 60,000 毫秒之间的**旁路阈值**。默认设置为 3000 毫秒 (ms)。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置对象组搜索

运行时，Firewall Threat Defense 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 防火墙管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

启用对象组搜索可以降低包含网络或接口对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

默认情况下会为在防火墙管理中心中首次添加的威胁防御设备启用对象组搜索。对于升级的设备，如果设备配置了禁用的对象组搜索，则需要手动将其启用。一次只能在一台设备上启用；您无法将其全局启用。我们建议您在部署使用网络或接口对象的访问规则的任何设备上将其启用。

注释 如果您启用对象组搜索，然后配置并操作设备一段时间，请注意，随后禁用该功能可能会导致不良结果。如果禁用对象组搜索，现有访问控制规则将按照设备的运行配置进行扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。如果设备运行正常，则在启用对象组搜索后不应将其禁用。

开始之前

- 型号支持—Firewall Threat Defense
- 我们建议您同时在每台设备上启用事务提交。在设备 CLI 中，输入 **asp rule-engine transactional-commit access-group** 命令。
- 更改此设置可能会在设备重新编译ACL时中断系统操作。我们建议您在维护窗口期间更改此设置。
- 可以使用 **object-group-search threshold** 命令启用阈值，以有助于防止性能下降。使用阈值运行时，对于每个连接，将根据网络对象匹配源和目标IP地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。配置规则以防止过多的匹配项。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 Firewall Threat Defense设备旁，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** (✎) 。

步骤 4 选中**对象组搜索 (Object Group Search)**。

步骤 5 要使对象组搜索除网络对象外还适用于接口对象，请选中**接口对象优化 (Interface Object Optimization)**。

如果不选择**接口对象优化 (Interface Object Optimization)**，则系统会为每个源/接口对部署单独的规则，而不是使用规则中使用的安全区域和接口组。这意味着接口组不可用于对象组搜索处理。

步骤 6 点击**保存**。

配置接口对象优化

部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

默认情况下，接口对象优化处于禁用状态。一次只能在一台设备上启用；您无法将其全局启用。

注释 如果禁用接口对象优化，则现有访问控制规则将在不使用接口对象的情况下进行部署，但这样可能会延长部署时间。此外，如果启用了对象组搜索，则其优势将不会应用于接口对象，并且您可能会在设备的运行配置中看到访问控制规则的扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。

开始之前

型号支持—Firewall Threat Defense

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 Firewall Threat Defense设备旁，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** (✎) 。

步骤 4 选中**接口对象优化 (Interface Object Optimization)**。

步骤 5 点击**保存**。

编辑部署设置

设备 (Device) 页面上的**运行状况 (Deployment Settings)** 部分显示下表所述信息。

图 *377:* 部署设置

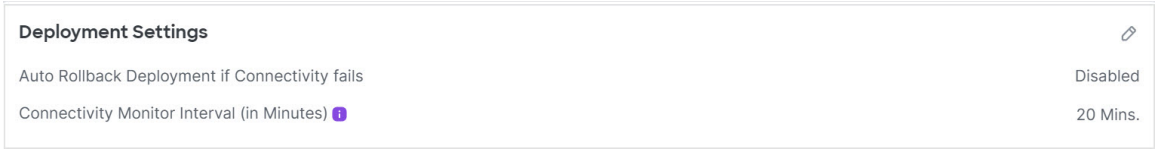


表 *62:* 部署设置

字段	说明
连接失败时自动回滚部署	“启用”(Enabled) 或“禁用”(Disabled)。 您可以在管理连接因部署而失败时启用自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。
连接监控间隔（分钟）	显示在回滚配置之前等待的时间。

您可以从**设备管理 (Device Management)** 页面设置部署设置。部署设置包括在管理连接因部署而失败时启用部署自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。您也可以使用 **configure policy rollback** 命令手动回滚配置（请参阅如果防火墙管理中心断开连接，则手动回滚配置，第 909 页）。

请参阅以下准则：

- 只有以前的部署可以在 Firewall Threat Defense 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。

- 回滚只会影响您可以在防火墙管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 Firewall Threat Defense CLI 中进行配置。请注意，如果您在上次防火墙管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 防火墙管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

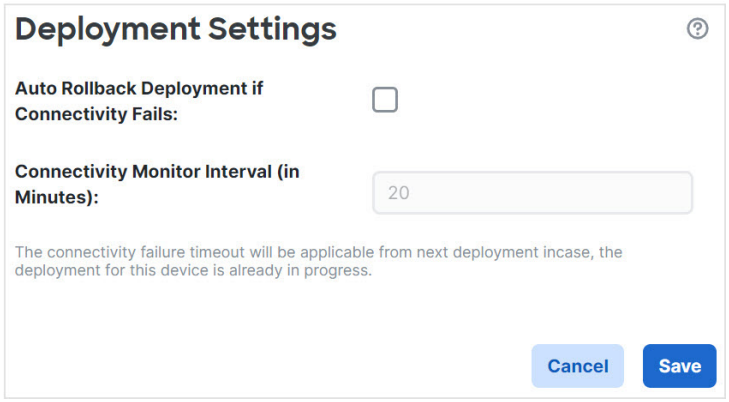
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)**。

步骤 4 在**部署设置 (Deployment Settings)** 部分中，点击 **编辑** (✎)。

图 *378:* 部署设置



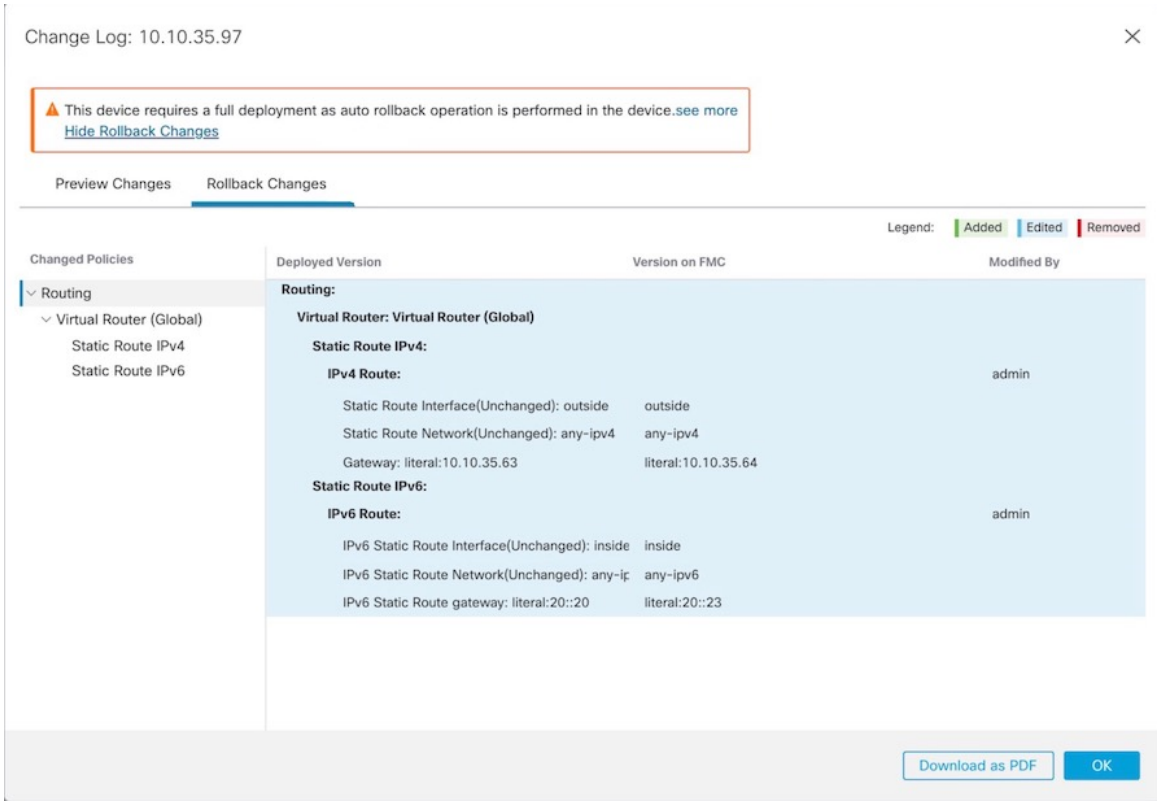
步骤 5 选中**连接失败时自动回滚部署 (Auto Rollback Deployment if Connectivity Fails)** 以启用自动回滚。

步骤 6 设置**连接监控间隔（分钟）(Connectivity Monitor Interval [in Minutes])** 以设置在回滚配置之前要等待的时间。默认值为 20 分钟。

步骤 7 如果发生回滚，请参阅以下内容以了解后续步骤。

- 如果自动回滚成功，您会看到一条成功消息，指示您执行完整部署。
- 您还可以转到 **部署 (Deployment)** **高级部署 (Advanced Deploy)** 屏幕，然后点击 **预览** (🔍) 图标以查看已回滚的配置部分（请参阅部署配置更改，第 180 页）。点击**显示回滚更改 (Show Rollback Changes)** 以查看更改，然后点击**隐藏回滚更改 (Hide Rollback Changes)** 以隐藏更改。

图 *379:* 回滚更改



- 在部署历史记录预览中，您可以查看回滚更改。请参阅查看部署历史记录，第 187 页。

步骤 8 检查管理连接是否已重新建立。

在防火墙管理中心中，检查连接状态页面上的管理连接状态。导航至**设备>设备管理**，然后在“**设备**”选项卡下的“**管理**”区域中，点击“**连接状态**”以查看“**连接状态**”页面。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 910 页。

编辑集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *380:* 集群运行状况监控设置

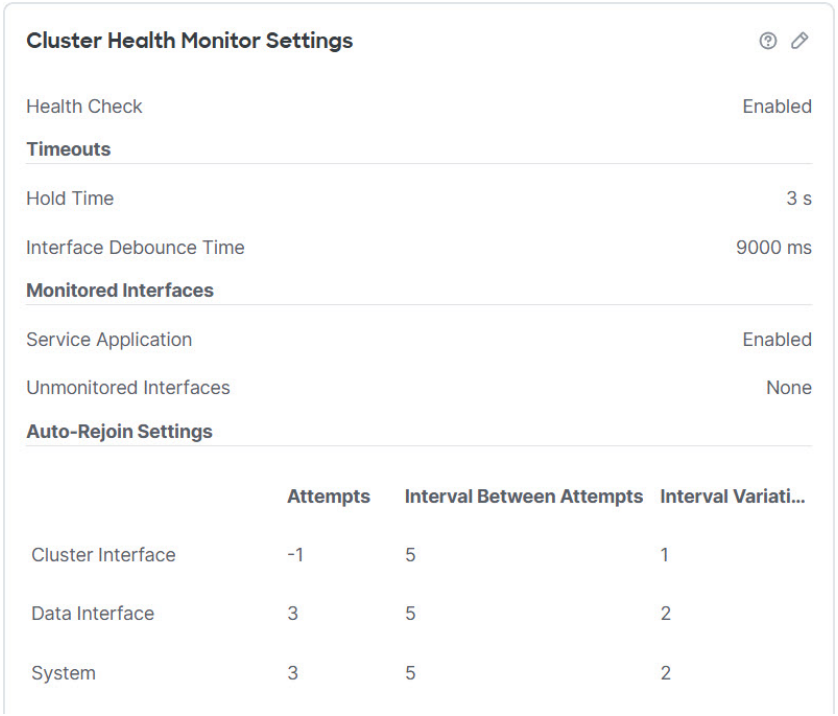


表 *63:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。

字段	说明
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。



注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

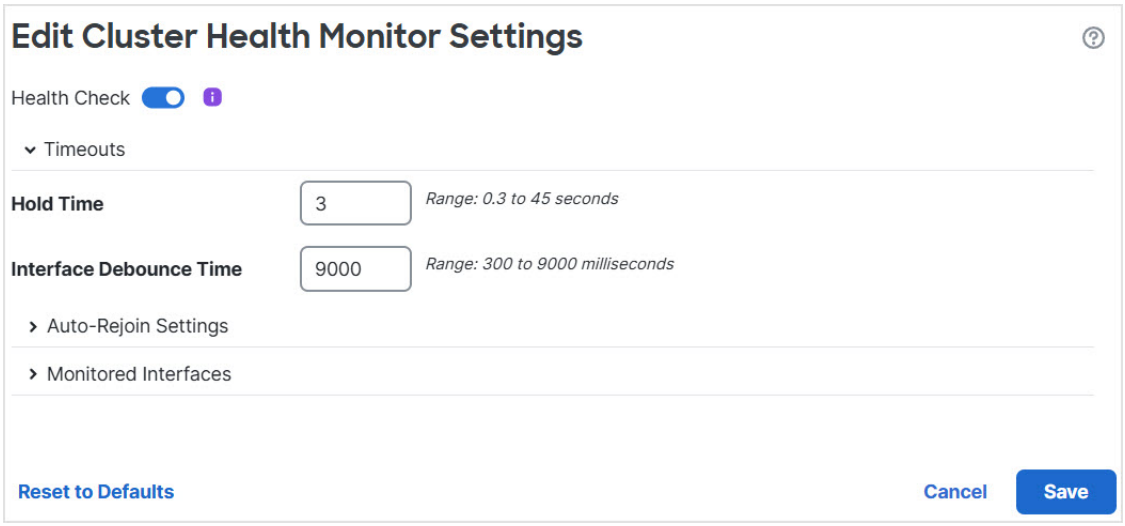
步骤 2 在要修改的集群旁边，点击 **编辑** (✎)。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 ***381:*** 禁用系统运行状况检查



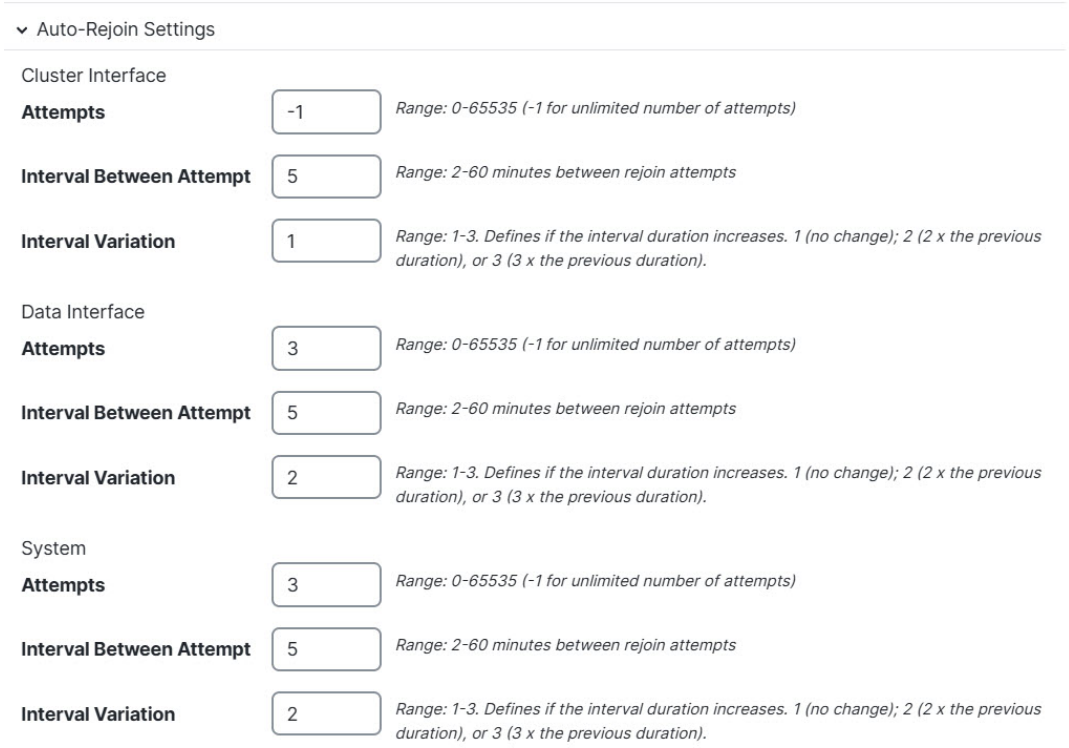
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *382:* 配置自动重新加入设置

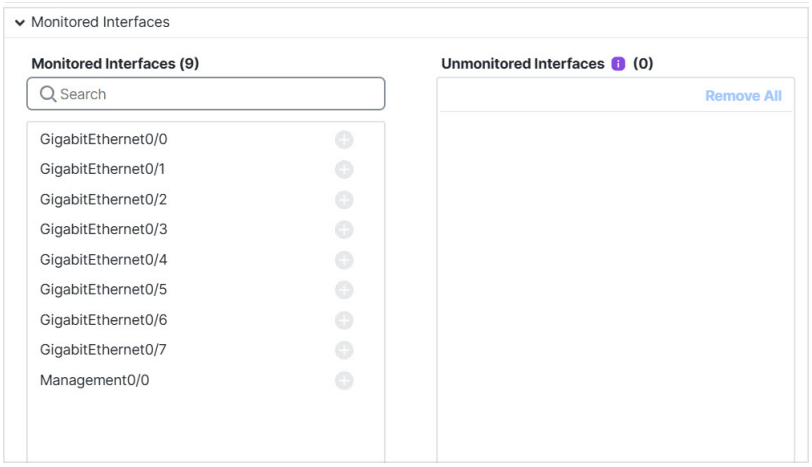


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *383:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改，第 180 页。

热插拔 SSD

如果您有两个 SSD，它们会在您启动时形成 RAID。防火墙启动时，您可以在 CLI 上执行以下任务：
Firewall Threat Defense

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

  当您在 Secure Firewall 设备中仅使用一块 SSD 时，**驱动器状态**将显示为**降级**。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
```

```
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

configure raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

禁用 USB 端口

默认情况下，type-A USB 端口已启用。出于安全考虑，您可能希望禁用 USB 端口访问。以下型号支持禁用 USB：

- Firepower 1000 系列
- Cisco Secure Firewall 200 系列
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100 系列

准则

- 启用或禁用 USB 端口需要 重新启动。
- 如果USB端口被禁用，并且您降级到不支持此功能的版本，则端口将保持禁用状态，并且在不清除 NVRAM 的情况下无法重新启用端口（FXOS local-mgmt **erase secure all** 命令）。
- 如果执行 ROMMON **factory-reset** 或 FXOS local-mgmt **erase secure**，USB 端口将重新启用。
- 对于高可用性 或集群，您必须在每台设备上单独禁用或重新启用端口。



注释 此功能不会影响 USB 控制台端口（如果有）。

禁用设备上的 USB 端口。

要禁用设备上的 USB 端口，您可以在 Firewall Threat Defense CLI 中执行此操作。

过程

步骤 1 禁用 USB 端口。

system support usb configure disable

reboot

要重新启用 USB 端口，请输入 **system support usb configure enable**。

示例：

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.

>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

步骤 2 查看端口状态。

system support usb show

管理状态显示 USB 端口配置。运行状态显示当前操作。例如，如果禁用 USB 端口但不重新加载，则管理状态将显示为禁用，而运行状态将显示为启用。

示例：

```
>system support usb show
USB Port Info
---------------
Admin State: disabled
Oper State: disabled
```

在多实例模式下禁用 USB 端口

要在多实例模式下禁用 USB 端口，可以在 FXOS CLI 中执行此操作。

过程

步骤 1 禁用 USB 端口并重新启动，以使更改生效。

a) 禁用 USB 端口。

scope fabric-interconnect

disable usb-port

commit buffer

b) 重新启动机箱。

connect local-mgmt

reboot

示例：

```
firepower-4245 /fabric-interconnect # disable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

步骤 2 启用 USB 端口并重新启动，以使更改生效。

a) 启用 USB 端口。

scope fabric-interconnect

enable usb-port

commit buffer

b) 重新启动机箱。

connect local-mgmt

reboot

示例：

```
firepower-4245 /fabric-interconnect # enable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

步骤 3 查看 USB 端口状态。

scope fabric-interconnect

show usb-port

管理状态显示 USB 端口配置。运行状态显示当前操作。例如，如果禁用 USB 端口但不重新加载，则管理状态将显示为“已禁用”，而“运行状态”将显示为“启用”。

示例：

```
firepower-4245# scope fabric-interconnect
firepower-4245 /fabric-interconnect # show usb-port
Usb Port:
Equipment         Admin State Oper State
----------------- ----------- ----------
A                 Disabled    Disabled
```

为 FXOS 配置 SNMP

您可以为控制底层机箱功能的底层 FXOS 操作系统配置简单网络管理协议 (SNMP)。有关 Firewall Threat Defense 的 SNMP 配置，请参阅SNMP，第 994 页。

SNMP 是一种应用层协议，提供 SNMP 管理器和代理之间的通信消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制和监控网络设备的活动的系统。

- SNMP 代理 - 机箱内的软件组件，用于维护机箱的数据并根据需要向 SNMP 管理器报告数据。机箱包含代理和 MIB 集合。要启用 SNMP 代理并创建管理器和代理之间的关系，请在 防火墙管理中心 中启用并配置 SNMP。
- 管理信息库 (MIB) - SNMP 代理上的托管对象集合。

机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 使用基于社区的安全形式；SNMPv3 使用用户名和密码作为安全形式。

为 FXOS 启用 SNMP

启用 SNMP 并配置设置。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击 **SNMP**。

步骤 3 填写以下字段：

名称	说明
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。

名称	说明
社区字段	Firepower机箱在它发送给SNMP主机的任何陷阱消息中包含的默认 SNMPv1 或 v2 社区名或 SNMP v3 用户名和密码。 请为 SNMPv1 和 SNMPv2 输入有效的社区字符串： • 字母数字字符串和特殊字符集，长度在 1 - 32 个字符之间。（感叹号）、-（连字符）、~（代字号）、&&（双与号）、[ ]（方括号）、^（克拉）、'（单引号）、 "（双引号）和 < >（尖括号） ）。 • 请勿使用 @（at 号）、\（反斜线）、?（问号）或空格。 • 字符串也可以是 0x21 到 0x7E 范围内的 ASCII 字符，不包括 HTML 插词向量，即单引号 (')、双引号 (") 和尖括号 (< >)。 输入 SNMPv3 的有效用户名和密码： • 用户名可以是字母数字字符串，并且可以包含@（at符号）、\（反斜线）。（句点）、_（下划线）和 -（连字符）。 • 密码限制与社区字符串限制相同。 请注意，如果**社区**字段已设置，空字段右侧会显示文本**已设置：是**。如果**社区**字段尚未填充值，空字段右侧会显示文本**已设置：否**。
系统管理员名称字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如邮件地址或姓名和电话号码。
位置字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 4 点击**保存**。

下一步做什么

创建 SNMP 陷阱和用户。

为 FXOS 创建 SNMP 陷阱

创建 SNMP 陷阱

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **SNMP**。

步骤 3 在 **SNMP 陷阱配置 (SNMP Traps Configuration)** 区域中，点击**添加 (Add)**。

步骤 4 在 **SNMP 陷阱配置**对话框中，填写以下字段：

名称	说明
主机名 (Host Name) 字段	Firepower 机箱应向其发送陷阱的 SNMP 主机的主机名或 IP 地址。
社区字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入一个介于 1 和 65535 之间的整数。
版本 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： • **V1** • **V2** • **V3**
类型字段	如果为版本选择 **V2** 或 **V3**，则是要发送的陷阱类型。这可以是以下其中一项： • **陷阱** • **告知 (Informs)**
权限字段	如果为版本选择 **V3**，与陷阱相关联的权限。这可以是以下其中一项： • **身份验证 (Auth)** - 有身份验证，但没有加密 • **无身份验证 (Noauth)** - 没有身份验证和加密 • **权限 (Priv)** - 有身份验证和加密

步骤 5 点击**确定 (OK)** 以关闭 **SNMP 陷阱配置 (SNMP Trap Configuration)** 对话框。

步骤 6 点击保存。

为 FXOS 创建 SNMP 用户

创建 SNMP 用户。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 点击 **SNMP**。

步骤 3 在 **SNMP 用户配置 (SNMP Users Configuration)** 区域中，点击添加 **(Add)**。

步骤 4 在 **SNMP 用户配置**对话框中，填写以下字段：

名称	说明
用户名字段	分配给 SNMP 用户的用户名。 最多输入 32 个字母或数字。名称必须以字母开始，也可以指定 _（下划线）、.（句点）、@（邮箱符号）和 -（连字符）。
授权语法类型字段	授权类型：**SHA**。
使用 **AES-128** 复选框	如果选中此复选框，则此用户使用 AES-128 加密。 注释 SNMPv3 不支持 DES。如果未选中 AES-128 框，则不会进行隐私加密，任何配置的隐私密码都不会生效。
身份验证密码字段	用户的密码。
确认字段	用于确认目的的再次输入的密码。
加密密码字段	用户的隐私密码。
确认字段	用于确认目的的再次输入的隐私密码。

步骤 5 点击确定 **(OK)** 以关闭 **SNMP 用户配置 (SNMP User Configuration)** 对话框。

步骤 6 点击保存。

配置 ISA 3000 的报警

您可以配置思科 ISA 3000 设备上的报警系统，以便在出现不正常情况时发出警告。

关于告警

您可以将 ISA 3000 配置为在多种条件下发出报警。如果有任何条件与配置的设置不匹配，系统会触发报警，报警的报告方式为 LED、系统日志消息、SNMP 陷阱以及连接到报警输出接口的外部设备。默认情况下，触发的报警仅会发出系统日志消息。

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

ISA 3000 具有内部传感器、2 个报警输入接口以及 1 个报警输出接口。您可以将外部传感器（如门禁传感器）连接到报警输入接口，将外部报警设备（如蜂鸣器或指示灯）连接到报警输出接口。

报警输出接口是一个中继装置。根据报警条件，中继处于连接或断开状态。当处于连接状态时，连接至该接口的任何设备都将被激活。当中继处于断开状态时，会导致连接的任何设备都处于非活动状态。只要触发了报警，中继就会保持连接状态。

有关连接外部传感器和告警继电器的信息，请参阅《Cisco ASA 系列通用操作 CLI 配置指南》中的“Cisco ISA 3000 警报”一章。请参阅《Cisco ISA 3000 工业安全设备硬件安装指南》。

报警输入接口

您可以将报警输入接口（或触点）连接到外部传感器，例如检测门是否打开的传感器。

每个报警输入接口都有一个对应的 LED。这些 LED 负责传达每个报警输入的报警状态。您可以为每个报警输入配置触发器和严重性。除了 LED，您还可以配置触点来触发输出中继（用于激活外部报警），以发送系统日志消息和 SNMP 陷阱。

下表介绍与报警输入的报警条件所对应的 LED 状态。表中还介绍了启用这些报警输入响应时输出中继、系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	次要报警 - 红色长亮 重大报警 - 红色闪烁	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

告警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

报警输出接口充当一个中继，并且还有一个对应的 LED，用于传达连接到输入接口的外部传感器以及内部传感器（例如双电源和温度传感器）的报警状态。请配置哪些报警应该激活输出中继（如果有）。

下表介绍与报警条件对应的LED和输出中继的状态。表中还介绍了启用这些报警响应时系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	红色常亮	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

系统日志报警

默认情况下，触发任何报警时，系统都会发送系统日志消息。如果您不希望收到这些消息，可以禁用系统日志消息传递。

要让系统日志报警正常工作，您还必须启用诊断日志记录。选择 **设备** > **平台设置**，添加或编辑分配给设备的FTD平台设置策略，并在**系统日志**页面上配置目标和设置。例如，您可以配置系统日志服务器、控制台日志记录或内部缓冲区日志记录。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 报警

您可以选择配置报警，将SNMP陷阱发送到SNMP服务器。要让SNMP陷阱报警正常使用，您还必须配置 SNMP 设置。

选择 **设备** > **平台设置**，添加或编辑分配给该设备的威胁防御平台设置策略，并在 **SNMP** 页面上启用 SNMP 并配置设置。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
报警触点 1	启用	关闭状态	次要	Disabled	Disabled	已启用
报警触点 2	启用	关闭状态	次要	Disabled	Disabled	已启用
冗余电源（在启用时）	启用	—	—	Disabled	Disabled	已启用

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
温度	为主温度报警启用（高阈值和低阈值的默认值分别为 92°C 和 -40°C） 为辅助报警禁用。	—	—	为主温度报警启用	为主温度报警启用	为主温度报警启用

报警先决条件

型号支持

ISA 3000 上的 Firewall Threat Defense。

配置 ISA 3000 的报警

请使用 FlexConfig 为 ISA 3000 配置报警。以下主题介绍如何配置不同类型的报警。

配置报警输入触点

如果您将报警输入触点（接口）连接到外部传感器，可以将触点配置为基于传感器的输入发出报警。事实上，如果触点关闭，即电流停止流经触点，系统会默认启用触点来发送系统日志消息。只有当默认设置不符合您的要求时，才需要配置触点。

报警触点的编号分别是 1 和 2，您需要了解如何连接物理引脚以配置正确的设置。单独配置每个触点。

过程

步骤 1 创建 FlexConfig 对象以配置警报输入联系人。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Configure_Alarm_Contacts。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。

- **对象正文 (Object body)** - 在对象正文中，键入配置警报联系人所需的命令。以下步骤介绍了这些命令。

c) 配置报警触点的说明。

alarm contact {**1** | **2**} **description** *string*

例如，要将触点 1 的说明设置为“Door Open”，请输入以下命令：

```
alarm contact 1 description Door Open
```

d) 配置报警触点的严重性。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

您可以指定 **any** 更改所有触点的严重性，而不是配置一个触点。严重性控制与触点关联的 LED 指示灯的行为。

- **major**- LED 指示灯红色闪烁。
- **minor**- LED 指示灯红色长亮。这是默认值。
- **none**- LED 指示灯熄灭。

例如，要将触点 1 的严重级别设置为“Major”，请输入以下命令：

```
alarm contact 1 severity major
```

e) 配置报警触点的触发器。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

您可以指定 **any** 更改所有触点的触发器，而不是配置一个触点。触发器决定发出报警信号的电气条件。

- **open**- 触点的正常状态为闭合，即电流流经触点。如果触点变成打开状态，即电流停止流动，会触发警报。
- **closed**- 触点的正常状态为打开，即电流不通过触点。如果触点变成闭合状态，即电流开始流经触点，会触发警报。这是默认值。

例如，将门禁传感器连接到报警输入触点1，该触点的正常状态为没有电流流经报警触点（即打开）。如果门被打开，触点会变成闭合状态，电流将流经报警触点。您应将报警触发器设为关闭，以便当电流开始流动时，警报响起。

```
alarm contact 1 trigger closed
```

f) 配置触发报警触点时采取的操作。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

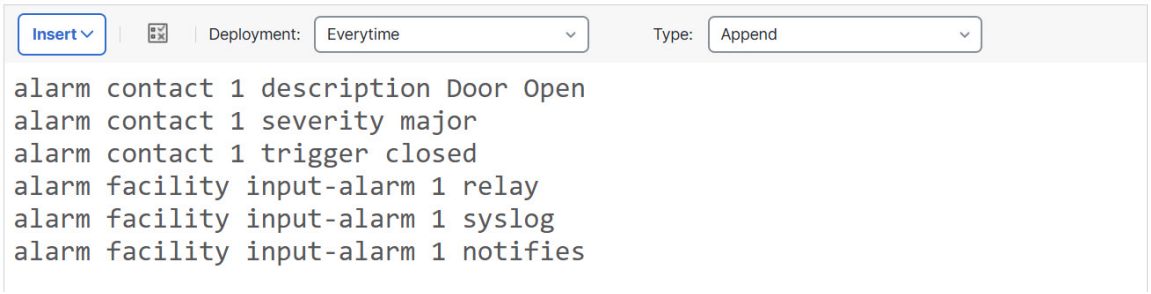
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

g) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

此对象正文应如下所示：



h) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

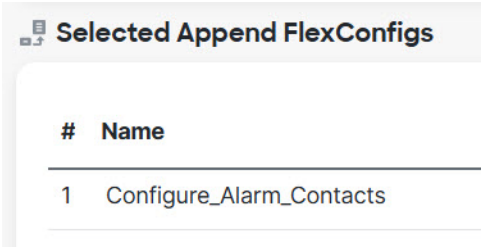
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择警报联系人 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于警报联系人命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 1071 页。

配置电源报警

ISA 3000 包含两个电源。默认情况下，系统在单电源模式下运行。但是，您可以配置系统在双电源模式下运行，其中第二个电源会在主电源发生故障时自动供电。启用双电源模式时，自动启用电源报警来发送系统日志警报，但您可以完全禁用警报，或同时启用 SNMP 陷阱或报警硬件中继。

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 创建 FlexConfig 对象以配置电源警报。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Power_Supply_Alarms。

- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置电源警报所需的命令。以下步骤介绍了这些命令。

c) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

d) 配置触发电源报警时要采取的操作。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。
- **禁用** - 禁用电源报警。为电源报警配置的任何其他操作都无法运行。

例如，要启用电源报警的所有操作，请输入以下命令：

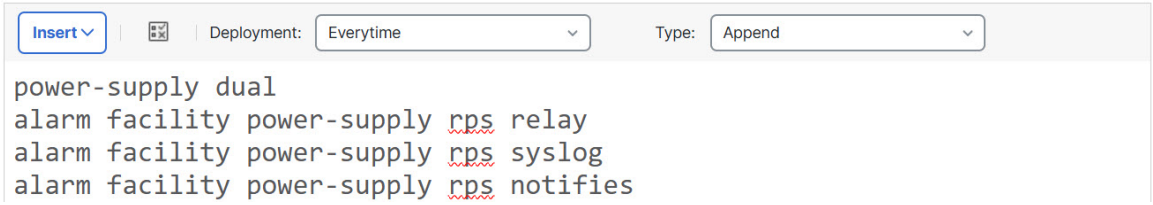
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

e) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

此对象正文应如下所示：



f) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

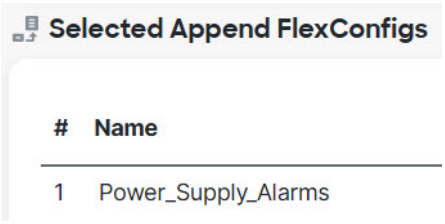
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择电源警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于电源警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 1071 页。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

您可以设置主要和辅助温度范围。如果温度低于低阈值，或超过高阈值，则触发报警。

默认对所有报警操作启用主温度报警：输出中继、系统日志和 SNMP。主要温度范围的默认设置为 -40°C 至 92°C。

默认情况下，禁用辅助温度报警。您可以将辅助温度范围设置为 -35°C 至 85°C。

由于辅助温度范围比主范围更严格，如果您设置辅助低温度或高温度，该设置将禁用对应的主要设置，即使您为主设置配置非默认值。您不能启用两个单独的高温度报警和两个单独的低温度报警。

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 创建 FlexConfig 对象以配置温度警报。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Configure_Temperature_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置温度警报所需的命令。以下步骤介绍了这些命令。

c) 配置可接受的温度范围。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度单位为摄氏度。主要报警的允许范围为 -40 至 92，这也是默认的范围。辅助报警的允许范围是 -35 到 85。低值必须小于高值。

例如，要设置更严格的 -20 至 80 温度范围（在辅助报警的允许范围内），请按如下所示配置辅助报警：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

d) 配置触发温度报警时要采取的操作。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。
- **通知** - 发送 SNMP 陷阱。

例如，要启用辅助温度报警的所有操作，请输入以下命令：

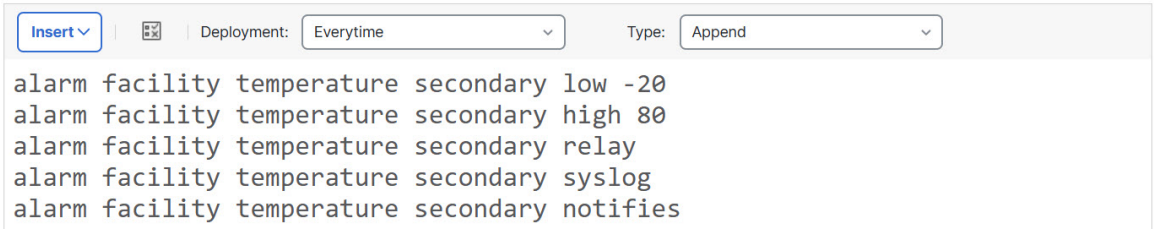
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

e) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

此对象正文应如下所示：



f) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

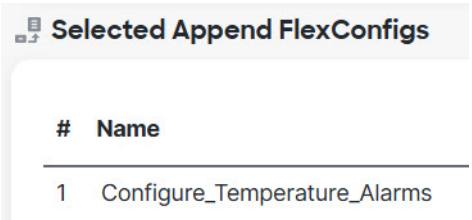
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择温度警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。
e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。
f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于温度警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 1071 页。

关闭外部告警

如果您使用连接到报警输出的外部报警，并触发了报警，可以使用 **clear facility-alarm output** 命令从设备 CLI 关闭外部报警。此命令会断开输出引脚，同时关闭输出 LED。

监控告警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

  显示每个可能的报警的当前配置。

- **show environment alarm-contact**

  显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

  显示有关已触发输出中继的报警信息。

- **show facility-alarm status** [**info** | **major** | **minor**]

显示所有已触发报警的信息。您可以通过过滤 **major** 或 **minor** 状态来限制视图。**info** 关键字提供与不使用关键字时相同的视图。

监控报警系统日志消息

根据您配置的报警类型，您可能会看到以下系统日志消息。

双电源报警

- %FTD-1-735005：电源设备冗余正常
- %FTD-1-735006：电源设备冗余丢失

温度报警

在这些报警中，*Celsius* 将替换为设备上检测到的温度，以摄氏为单位。

- %FTD-6-806001：主要报警 CPU 温度高 *Celsius*
- %FTD-6-806002：CPU 高温主要报警已清除
- %FTD-6-806003：主要报警 CPU 温度低 *Celsius*
- %FTD-6-806004：CPU 低温主要报警已清除
- %FTD-6-806005：辅助报警 CPU 温度高 *Celsius*
- %FTD-6-806006：CPU 高温辅助报警已清除
- %FTD-6-806007：辅助报警 CPU 温度低 *Celsius*
- %FTD-6-806008：CPU 低温辅助报警已清除

报警输入触点报警

在这些报警中，*description* 是您所配置触点的说明。

- %FTD-6-806009：与 ALARM_IN_1 *alarm_1_description* 对应的报警已确定
- %FTD-6-806010：与 ALARM_IN_1 *alarm_1_description* 对应的报警已清除
- %FTD-6-806011：与 ALARM_IN_2 *alarm_2_description* 对应的警报已确定
- %FTD-6-806012：与 ALARM_IN_2 *alarm_2_description* 对应的报警已清除

设备设置历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息

恢复配置模式现在支持NAT命令以及其他接口命令	10.0.0	10.0.0	恢复配置模式现在支持：
			• **nat** 以及相关的 **object** 和 **object-group** 命令。
			• 请参阅以下命令：**interface**
			  • **duplex**
			  • **fec**
			  • **negotiate-auto**
			  • **speed**
			这些 **interface** 命令以及 **shutdown**不支持在集群控制链路或故障转移链路的恢复配置模式下使用。
			新增/修改的诊断 CLI (**system support diagnostic-cli**) 命令： **configure recovery-config**

查看可现场更换内存模块的清单详细信息	10.0.0	10.0.0	此版本为受支持的设备引入了可现场更换的内存模块资产。现在可以在“设备管理”界面的**系统**部分查看可现场更换内存模块的详细信息。清单详细信息包括运行状态，以提高内存模块的现场可维护性。 新增/修改的命令：**show inventory** 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**编辑 (✎)

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
恢复配置模式用于在防火墙管理中心上进行紧急设备上配置和带外配置检测	7.7.0	7.7.0	如果断开了与设备的管理连接，您可以直接通过设备 CLI 选择配置更改： • 如果使用数据接口进行管理器访问，则恢复管理连接 • 选择无法等到连接恢复后再进行的策略更改 在恢复管理连接后，防火墙管理中心将检测设备上的配置更改。它不会自动更新 防火墙管理中心 中的设备配置；您必须查看配置差异，确认设备配置不同，然后在部署之前在 防火墙管理中心 中手动进行相同的更改。 新增/修改的诊断 CLI (**system support diagnostic-cli**) 命令： **configure recovery-config** 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** **运行状况 (Health)** > **带外状态 (Out of Band Status)** **编辑** (✎)
通过冗余管理器访问数据接口支持高可用性	7.7.0	7.7.0	现在，您可以使用具有高可用性的冗余管理器访问数据接口。
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** 注释 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
冗余管理器访问数据接口。	7.3.0	7.3.0	在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。设备会使用SLA监控来跟踪包含两个接口的静态路由和ECMP区域的可行性，以便管理流量可以使用这两个接口。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **管理器访问 (Manager Access)**
策略支持回滚以实现高可用性设备。	7.2.0	7.2.0	**configure policy rollback** 命令支持高可用性设备。
导致管理连接丢失的部署的自动回滚。	7.2.0	7.2.0	如果部署导致管理中心和威胁防御之间的管理连接断开，您现在就可以启用配置的自动回滚。以前，您只能使用 **configure policy rollback** 命令手动回滚配置。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **部署设置 (Deployment Settings)** • **部署 (Deploy)** > **高级部署 (Advanced Deploy)** > **预览 (Preview)** • **部署 (Deploy)** > **部署历史 (Deployment History)** > **预览 (Preview)**
默认情况下会为访问控制规则启用对象组搜索。	7.2.0	7.2.0	从版本 7.2.0 开始，托管设备默认启用**对象组搜索 (Object Group Search)** 设置。在“设备管理”页面上编辑设备设置时，此选项位于 **高级设置 (Advanced Settings)** 部分中。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
导入和导出设备配置。	7.1.0	7.1.0	您可以导出设备特定的配置，然后可以在以下使用案例中为同一设备导入已保存的配置： • 将设备移至其他 FMC。 • 恢复老旧配置。 • 重新注册设备。 新增/修改的屏幕： **设备** > **设备管理** > **设备** > **常规**
更新 FTD 上的 FMC IP 地址。	6.7.0	6.7.0	如果更改 FMC IP 地址，现在可以使用 FTD CLI 更新设备。 新增/经修改的命令： **configure manager edit**
思科 ISA 3000 系列的报警。	6.7	任意	已使用 FlexConfig 验证思科 ISA 3000 系列的警报配置。您应该能够在支持 FlexConfig 的旧版本中配置警报，但双电源警报除外。 支持的平台：ISA 3000 上的 Cisco Secure Firewall Threat Defense



第 18 章

DHCP 和 DDNS

以下主题介绍 DHCP 和 DDNS 服务以及如何在威胁防御设备上配置这些服务。

- 关于 DHCP 和 DDNS 服务， 第 955 页
- DHCP 和 DDNS 的要求和前提条件， 第 956 页
- DHCP 和 DDNS 服务准则， 第 957 页
- 配置 DHCPv4 服务器， 第 958 页
- 配置 DHCPv6 无状态服务器， 第 960 页
- 配置 DHCP 中继代理， 第 964 页
- 配置动态 DNS， 第 965 页
- DHCP 和 DDNS 的历史记录， 第 971 页

关于 DHCP 和 DDNS 服务

以下主题介绍 DHCP 服务器、DHCP 中继代理和 DDNS 更新。

关于 DHCPv4 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。Firewall 威胁防御设备 可以为连接到 Firewall 威胁防御设备 接口的 DHCP 客户端提供 DHCP 服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

DHCP 选项

DHCP 提供用于将配置信息传递至 TCP/IP 网络中主机的标准。配置参数在存储于 DHCP 消息的 Options 字段中的标记项目中携带，数据也称为选项。供应商信息也存储在 Options 中，并且所有供应商信息扩展均可用作 DHCP 选项。

例如，思科 IP 电话从 TFTP 服务器下载其配置。当思科 IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。
- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。
- DHCP 选项 3 设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 上已配置这两个选项，则 Firewall 威胁防御 DHCP 服务器将在响应中为两个选项提供值。

您可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数；DHCP 选项 15 用于 DNS 域名后缀。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器来发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

关于 DHCPv6 无状态服务器

对于结合前缀授权功能 (启用 IPv6 前缀授权客户端， 第 804 页) 使用无状态地址自动配置 (SLAAC) 的客户端，可以通过定义 DHCP IPv6 池并将其分配给 DHCPv6 服务器来配置 Firewall Threat Defense，以便在它们向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 Firewall Threat Defense 的前缀。

关于 DHCP 中继代理

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 Firewall 威胁防御设备 进行转发，因为它不转发广播流量。DHCP 中继代理可用于配置用来接收广播的 Firewall 威胁防御设备 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

DHCP 和 DDNS 的要求和前提条件

型号支持

Firewall Threat Defense

用户角色

- 管理员
- 访问管理员
- 网络管理员

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

防火墙模式

- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCP 中继。
- 在网桥组成员接口上的透明防火墙模式下，支持 DHCP 服务器。 在路由模式下，在 BVI 接口（而非网桥组成员接口）上支持 DHCP 服务器。BVI 必须具有名称，DHCP 服务器才能运行。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DDNS。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCPv6 无状态服务器。

集群

- 集群不支持 DHCPv6 无状态服务。

IPv6

支持 IPv6 用于 DHCP 无状态服务器和 DHCP 中继。

DHCPv4 服务器

- 最大可用 DHCP 池为 256 个地址。
- 您可以在具有名称和 IP 地址的任何接口（例如物理接口、子接口或路由模式下的 BVI）上配置 DHCP 服务器。
- 对于使用 DHCP 或 PPPoE 获取其地址的接口，请勿选择作为 DHCP 服务器接口。
- 只能在每个接口上配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置（如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 如果某个接口也启用了 DHCP 服务器，则不能将该接口配置为 DHCP 客户端；您必须使用静态 IP 地址。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。

- Firewall Threat Defense 不支持 DHCP 中继服务器背后的 DHCP 客户端；客户端必须直接连接到 Firewall Threat Defense。
- DHCP 服务器不支持 BOOTP 请求。

DHCPv6 服务器

- 在已配置 DHCPv6 地址、前缀委派客户端或 DHCPv6 中继的接口上，无法配置 DHCPv6 无状态服务器。

DHCP 中继

- 每个虚拟路由最多可以配置 10 台 DHCPv4 中继服务器，这些服务器为全局和接口专用服务器的组合，其中每个接口最多允许 4 台服务器。
- 每个虚拟路由 最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的接口专用服务器。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 对于使用 DHCP 或 PPPoE 获取其地址的接口，请勿选择作为 DHCP 中继接口。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下 DHCP 中继服务不可用。但是，可以通过使用访问规则允许 DHCP 流量通过。要允许 DHCP 请求和回复通过 Firewall Threat Defense，需要配置两条访问规则，一条允许从内部接口到外部接口（UDP 目标端口 67）的 DCHP 请求，另一条允许来自其他方向（UDP 目标端口 68）的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 Firewall Threat Defense 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，Firewall Threat Defense支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 Firewall Threat Defense 中继请求的 DHCP 服务器位于不同接口。
- 不能在流量区域内的接口上启用 DHCP 中继。

DDNS 服务

防火墙的 DDNS 仅支持 DynDNS 服务。因此，请确保使用以下语法中的更新 URL 配置 DDNS：

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

配置 DHCPv4 服务器

请参阅以下步骤来配置 DHCPv4 服务器。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **DHCP > DHCP 服务器**。

步骤 3 配置以下 DHCP 服务器选项：

- **Ping 超时** - Firewall Threat Defense设备等待 DHCP ping 尝试超时的时间量（以毫秒为单位）。值的范围为 10 到 10000 毫秒。默认值为 50 毫秒。

  为避免地址冲突，Firewall Threat Defense设备会向一个地址发动两个 ICMP ping 数据包，然后再将该地址分配给 DHCP 客户端。

- **租赁时长** - 客户端在租赁到期前可以使用其已分配的 IP 地址的时间量（以秒为单位）。值的范围为 300 到 1048575 秒。默认值为 3600 秒（1 小时）。

- （路由模式）**自动配置** - 在 Firewall Threat Defense设备上启用 DHCP 自动配置。自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。否则，可以禁用自动配置，并在第 4 步自行添加值。

- （路由模式）**接口** - 指定用于自动配置的接口。 对于具有虚拟路由功能的设备，此接口只能是全局虚拟路由器接口。

步骤 4 要覆盖自动配置的设置，请进行以下操作：

- 输入接口的域名：例如，您的设备可能位于 Your_Company 域中。
- 从下拉列表中，选择为该接口配置的 DNS 服务器（主服务器和辅助服务器）。要添加新的 DNS 服务器，请参阅创建网络对象，第 2660 页。
- 从下拉列表中，选择为该接口配置的 WINS 服务器（主服务器和辅助服务器）。要添加新的 WINS 服务器，请参阅创建网络对象，第 2660 页。

步骤 5 选择 **服务器**，点击 **添加**，然后配置以下选项：

- **接口** -- 从下拉列表中选择接口。在透明模式下，指定命名桥接组成员接口。 在路由模式下，请指定一个命名路由接口或命名 BVI；请勿指定桥接组成员接口。请注意，还必须指定 BVI 每个桥接组成员接口才能使 DHCP 服务器运行。
- **地址池** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **启用 DHCP 服务器** - 在所选接口上启用 DHCP 服务器。

步骤 6 点击**确定** 以保存 DHCP 服务器配置。

步骤 7 （可选）选择 **高级**，点击 **添加**，然后指定希望该选项返回到 DHCP 客户端的信息的类型：

- **选项代码** - Firewall Threat Defense设备支持 RFC 2132、RFC 2562 和 RFC 5510 中列出的 DHCP 选项，以发送信息。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50 – 54、58 – 59、61、67 和 82 除外。有关 DHCP 选项代码的更多信息，请参阅关于 DHCPv4 服务器，第 955 页。

  注释
  Firewall Threat Defense设备不会验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值匹配。有关选项代码及其关联的类型和期望值的详细信息，请参阅 RFC 2132。

- **类型** - DHCP 选项类型。可用选项包括 **IP**、**ASCII** 和 **十六进制**。如果选择了“IP”，则必须在“IP 地址”字段中添加 IP 地址。如果选择了“ASCII”，则必须在“ASCII”字段中添加 ASCII 值。如果选择了“十六进制”，则必须在“十六进制”字段中添加十六进制值。
- **IP 地址 1** 和 **IP 地址 2** - 要通过此选项代码返回的 IP 地址。要添加新的 IP 地址，请参阅创建网络对象，第 2660 页。
- **ASCII** - 将返回到 DHCP 客户端的 ASCII 值。字符串不能包含空格。
- **十六进制** - 将返回到 DHCP 客户端的十六进制值。该字符串的位数必须是偶数，并且不含空格。您无需使用 0x 前缀。

步骤 8 点击**确定** 以保存选项代码配置。

步骤 9 在“DHCP”页面上点击**保存**，以保存更改。

步骤 10 要查看 DHCP 绑定，请使用以下命令。

show dhcpd binding

示例：

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

配置 DHCPv6 无状态服务器

对于结合前缀授权功能使用无状态地址自动配置 (SLAAC) 的客户端，可以配置 Firewall Threat Defense 以在它们向 Firewall Threat Defense发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。

创建 DHCP IPv6 池

创建用于 DHCPv6 服务器的 DHCP IPv6 池。DHCPv6 服务器会在向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器和域名等信息。DHCP IPv6 池会定义要在 IR 消息中发送的参数。

此功能仅支持路由模式。此功能不支持集群或高可用性。

过程

步骤 1 选择**对象 (Objects)** > **DHCP IPv6 池 (DHCP IPv6 Pool)**。

步骤 2 请点击 添加 ()。

步骤 3 配置 **DNS 服务器 (DNS Server)** 和**域名 (Domain Name)**。

您可以手动定义值并点击**添加 (Add)**，或者您可以选中**导入 (Import)** 使用 Firewall Threat Defense 在前缀代理客户端接口上从 DHCPv6 服务器获取的一个或多个参数。您可以混合搭配手动配置的参数与导入的参数；但是，手动配置相同的参数与使用**导入 (Import)** 配置的参数不能相同。

图 *384:* 手动定义值

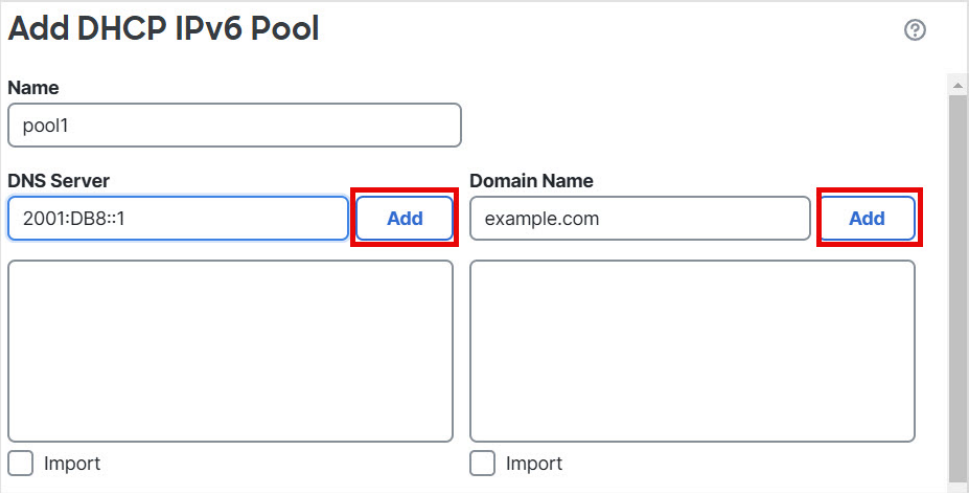
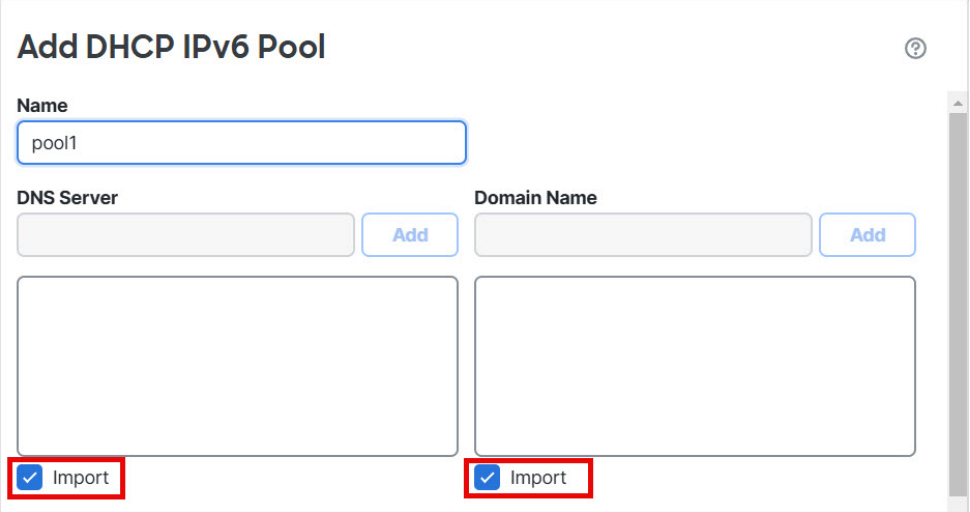


图 *385:* 导入值



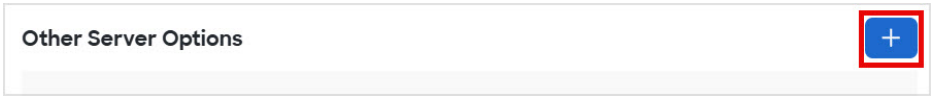
步骤 4 定义**其他服务器选项 (Other Server Options)**。

您可以为以下服务器定义域名和 IP 地址：

- NIS
- NISP
- SIP
- SNTP

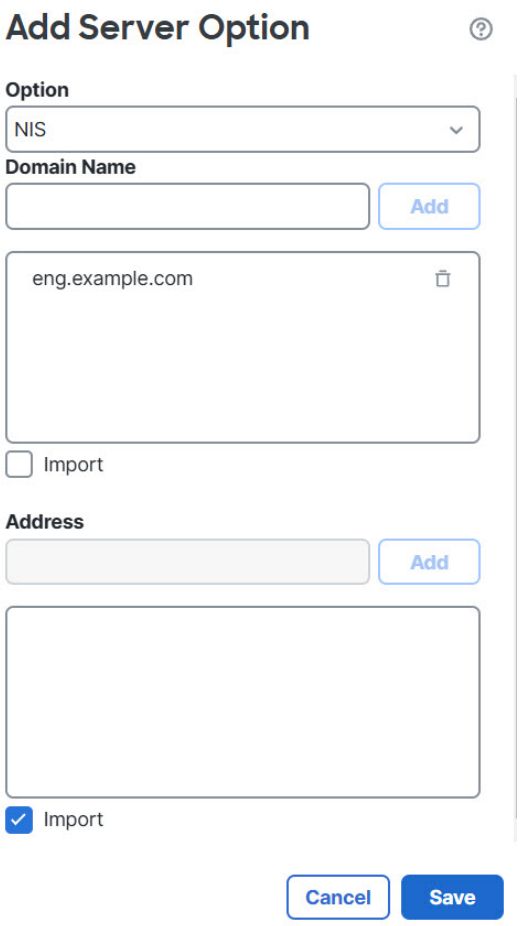
a) 请点击 添加 (+)。

图 *386:* 其他服务器选项



b) 在选项 **(Option)** 下选择服务器类型，然后手动定义域名 **(Domain Name)** 和地址 **(Address)**，或者选中导入 **(Import)**。

图 *387:* 定义服务器域名和地址



导入 **(Import)** 使用 Firewall Threat Defense 在前缀代理客户端接口上从 DHCPv6 服务器获取的一个或多个参数。您可以混合搭配手动配置的参数与导入的参数；但是，手动配置相同的参数与使用导入 **(Import)** 配置的参数不能相同。

c) 点击保存。

d) 对每个服务器类型重复上述步骤。

步骤 **5** 点击保存。

步骤 6 将此池与 DHCPv6 服务器配合使用。请参阅启用 DHCPv6 无状态服务器，第 963 页。

启用 DHCPv6 无状态服务器

对于结合前缀授权功能 (启用 IPv6 前缀授权客户端，第 804 页) 使用无状态地址自动配置 (SLAAC) 的客户端，可以配置 Firewall Threat Defense 以在它们向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 Firewall Threat Defense 的前缀。

此功能仅支持路由模式。此功能不支持集群或高可用性。

开始之前

添加 DHCP IPv6 池对象。请参阅创建 DHCP IPv6 池，第 960 页。此对象定义 IR 消息中包含的服务器参数。

过程

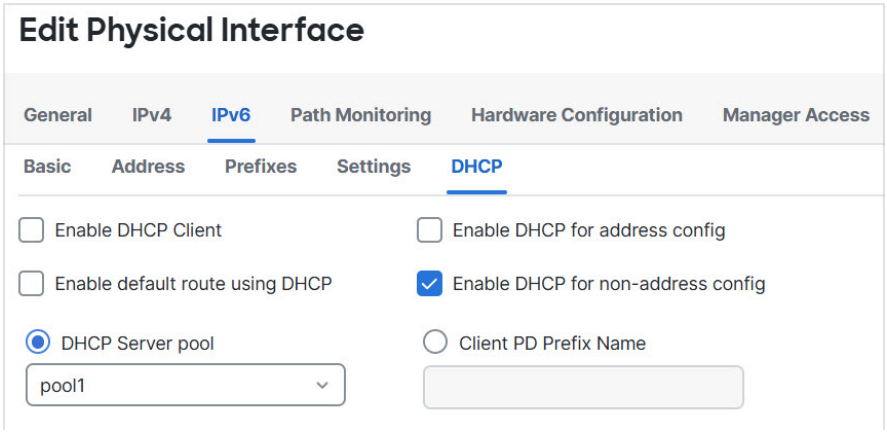
步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **IPv6** 页面，然后点击 **DHCP**。

步骤 4 点击 **DHCP 服务器池 (DHCP Server Pool)**，然后选择您之前创建的对象。

图 ***388:*** 启用 ***DHCPv6*** 服务器



步骤 5 选中**为非地址配置启用 DHCP (Enable DHCP for non-address config)** 以通知 SLAAC 客户端有关 DHCPv6 服务器的信息。

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 DHCP 中继代理

您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 Firewall Threat Defense 设备进行转发，因为它不转发广播流量。

您可以通过配置接收广播来将 DHCP 请求转发到另一个接口上 DHCP 服务器的 Firewall Threat Defense 设备接口来对此情况做出补救。

注释 在透明防火墙模式下不支持 DHCP 中继。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **DHCP** > **DHCP 中继**。

步骤 3 在 **IPv4 中继超时 IPv6 中继超时** 字段中，输入 Firewall Threat Defense 设备等待 DHCP 中继代理超时的时间（以秒为单位）。值的范围为 1 到 3600 秒。默认值为 60 秒。

超时用于通过本地 DHCP 中继代理进行的地址协商。

步骤 4 （可选） 选中 **信任所有信息** ，将所有客户端接口设置为受信任。

您可以将接口配置为受信任接口以保留 DHCP Option 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 Firewall Threat Defense DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段（在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 Firewall Threat Defense 默认丢弃该数据包。可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。

步骤 5 在 **DHCP 中继代理**上，点击**添加**，并配置以下选项：

- **接口** - 连接到 DHCP 客户端的接口。
- **启用 IPv4 中继** - 为该接口启用 IPv4 DHCP 中继。

- **设置路由** - （对于 IPv4）将来自服务器的 DHCP 消息中默认网关地址更改为最接近 DHCP 客户端的 Firewall Threat Defense设备接口的地址，该客户端中继原始 DHCP 请求。通过此操作，客户端可以将其默认路由设置为指向 Firewall Threat Defense设备，即使 DHCP 服务器指定了另一个路由器也如此。如果数据包内无默认路由器选项，则 Firewall Threat Defense设备将添加一个包含接口地址的选项。
- **启用 IPv6 中继** - 为该接口启用 IPv6 DHCP 中继。

步骤 6 点击**确定**，保存 DHCP 中继代理更改。

步骤 7 在 **DHCP 服务器 (DHCP Servers)** 上，点击**添加 (Add)**，并配置以下选项：

将 IPv4 和 IPv6 服务器地址添加为单独的条目，即使它们属于同一台服务器亦是如此。

- **服务器** - DHCP 服务器的 IP 地址。从该下拉列表中选择一个 IP 地址。要添加新的 IP 地址，请参阅 创建网络对象，第 2660 页
- **接口** - 指定的 DHCP 服务器连接到的接口。DHCP 中继代理和 DHCP 服务器不能配置在同一接口上。

步骤 8 点击**确定**，保存 DHCP 服务器更改。

步骤 9 在“DHCP”页面上点击**保存**，以保存更改。

配置动态 DNS

当接口使用 DHCP IP 寻址时，分配的 IP 地址可以在续约 DHCP 租用时更改。当需要使用完全限定域名 (FQDN) 访问接口时，更改 IP 地址可能导致 DNS 服务器资源记录 (RR) 失效。动态 DNS (DDNS) 提供一种机制，会在 IP 地址或主机名更改时更新 DNS RR。您还可以将 DDNS 用于静态或 PPPoE IP 寻址。

DDNS 在 DNS 服务器上更新以下 RR：A RR 包括名称到 IP 地址的映射，而 PTR RR 将地址映射到名称。

Firewall Threat Defense 支持以下 DDNS 更新方法：

- 标准 DDNS，即标准 DDNS 更新方法由 RFC 2136 定义。

  通过此方法，Firewall Threat Defense 和 DHCP 服务器使用 DNS 请求更新 DNS RR。Firewall Threat Defense 或 DHCP 服务器向其本地 DNS 服务器发送 DNS 请求以获取有关主机名的信息，并根据响应确定拥有 RR 的主 DNS 服务器。然后，Firewall Threat Defense 或 DHCP 服务器直接向主 DNS 服务器发送更新请求。请参阅以下典型场景。

  - Firewall Threat Defense 更新 A RR，而 DHCP 服务器更新 PTR RR。

    通常情况下，Firewall Threat Defense“拥有” A RR，而 DHCP 服务器“拥有” PTR RR，因此两个实体需要单独请求更新。当 IP 地址或主机名更改时，Firewall Threat Defense 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 PTR RR 更新。

  - DHCP 服务器既更新 A，也更新 PTR RR。

如果 Firewall Threat Defense 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，Firewall Threat Defense 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 A 和 PTR RR 更新。

您可以根据安全需求和主 DNS 服务器的要求配置不同的所有权。例如，对于静态地址，Firewall Threat Defense 应拥有两个记录的更新。

- Web - Web 更新方法使用使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。

  使用此方法，当 IP 地址或主机名更改时，Firewall Threat Defense 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。

注释 对于从外部接口使用 零接触调配 注册的设备，使用“fmcOnly”方法自动启用 DDNS，该方法类似于 Web 方法。此方法仅适用于 零接触调配 设备。您可以使用此屏幕编辑此方法的某些选项，或删除该方法并配置其他方法。有关 零接触调配 的详细信息，请参阅使用序列号添加设备（零接触调配） - 基本配置，第 39 页。

DDNS 页面还支持设置与 DDNS 相关的 DHCP 服务器设置。

注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 在 **对象** > **DNS 服务器组**上配置 DNS 服务器组，然后为 **设备** > **平台设置**上的接口启用该组，创建或编辑威胁防御策略并点击 **DNS**。请参阅DNS，第 977 页。
- 配置设备主机名。您可以在执行 Firewall Threat Defense 初始设置时配置主机名，也可以使用 **configure network hostname** 命令配置主机名。如果未指定每个接口的主机名，则使用设备主机名。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **DHCP** > **DDNS**.

步骤 3 标准 DDNS 方法： 配置 DDNS 更新方法以启用来自 Firewall Threat Defense 的 DNS 请求。

如果 DHCP 服务器将执行所有请求，则无需配置 DDNS 更新方法。

a) 在 **DDNS 更新方法**上，点击 **添加**。
b) 设置 **方法名称**。
c) 点击 **DDNS**。

d) （可选） 配置 DNS 请求之间的**更新间隔**。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置**天数**(0-364)、**小时**、**分钟**和**秒**。

e) 设置您希望 Firewall Threat Defense 更新的**更新记录**。

此设置仅影响您要直接从 Firewall Threat Defense 更新的记录；要确定您希望 DHCP 服务器更新的记录，请按接口或全局配置 DHCP 客户端设置。请参阅步骤 5，第 967 页。

- **未定义 (Not Defined)** - 未从 Firewall Threat Defense 禁用 DNS 更新。
- **A 和 PTR 两者记录 (Both A and PTR Records)** - 将 Firewall Threat Defense 设置为同时更新 A 和 PTR RR。使用此选项进行静态或 PPPoE IP 寻址。
- **A 记录 (A Records)** - 将 Firewall Threat Defense 设置为仅更新 A RR。如果您希望 DHCP 服务器更新 PTR RR，请使用此选项。

f) 点击**确定**。

g) 将此方法分配在 步骤 5，第 967 页 中的接口。

步骤 4 Web 方法：配置 DDNS 更新方法，启用来自 Firewall Threat Defense 的 HTTP 更新请求。

a) 在 **DDNS 更新方法**上，点击 **添加**。

b) 设置 **方法名称**。

c) 点击 **Web**。

d) 设置 **Web 更新类型** 以更新 IPv4 和/或 IPv6 地址类型。

e) 设置 **Web URL**。指定更新 URL。请咨询您的 DNS 提供商，获取所需的 URL。

使用以下语法：

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

示例：

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) （可选） 配置 DNS 请求之间的**更新间隔**。默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置**天数**(0-364)、**小时**、**分钟**和**秒**。

g) 点击**确定**。

h) 将此方法分配在 步骤 5，第 967 页 中的接口。

i) DDNS 的 Web 类型方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参阅步骤 9，第 969 页。

步骤 5 配置 DDNS 的接口设置，包括为此接口设置更新方法、DHCP 客户端设置和主机名。

a) 在 **DDNS 接口设置**上，点击 **添加**。

b) 从下拉列表中选择**接口**。

c) 选择在 **DDNS 更新方法** 页面中创建的 **方法名称** 。

（标准 DDNS 方法）如果您希望 DHCP 服务器执行所有更新，则无需分配方法。

d) 设置此接口的 **主机名** 。

如果未设置主机名，则会使用设备主机名。如果未指定 FQDN，则会附加 DNS 服务器组中的默认域（用于静态或 PPPoE IP 寻址），或附加来自 DHCP 服务器的域名（用于 DHCP IP 寻址）。

e) 标准 DDNS 方法： 配置 **DHCP 客户端请求 DHCP 服务器以更新请求**，以确定希望 DHCP 服务器更新哪些记录。

Firewall Threat Defense 将 DHCP 客户端请求发送到 DHCP 服务器。请注意，还必须将 DHCP 服务器配置为支持 DDNS。可以将该服务器配置为满足客户端请求，也可以覆盖客户端（在这种情况下，它将回复客户端，因此客户端也不会尝试执行服务器正在执行的更新）。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释
还可以在 **DDNS** 页面上为所有接口全局设置这些值。每个接口的设置优先于全局设置。

- **未选择**-禁用对 DHCP 服务器的 DDNS 请求。即使客户端不请求 DDNS 更新，也可以将 DHCP 服务器配置为始终发送更新。
- **无更新**-请求 DHCP 服务器不执行更新。此设置与**同时启用了 A 和 PTR 记录**的 DDNS 更新方法配合一起使用。
- **仅 PTR**-请求 DHCP 服务器执行 PTR RR 更新。此设置与启用 **A 记录**的 DDNS 更新方法配合使用。使用此设置启用 DHCP 选项 81。
- **A 和 PTR 两者记录**-请求 DHCP 服务器同时执行 A 和 PTR RR 更新。此设置不需要将 DDNS 更新方法与接口关联。

f) 点击**确定**。

注释
当您在 Firewall Threat Defense 上启用 DHCP 服务器时， **动态 DNS 更新 (Dynamic DNS Update)** 设置与 DHCP 服务器设置相关。有关详细信息，请参阅步骤 6，第 968 页。

步骤 6 如果在 Firewall Threat Defense 上启用 DHCP 服务器，则可以为 DDNS 配置 DHCP 服务器设置。

要启用 DHCP 服务器，请参阅配置 DHCPv4 服务器，第 958 页）。您可以配置 DHCP 客户端使用标准 DDNS 更新方法时的服务器行为。如果服务器执行任何更新，则如果客户端租约到期（且未续约），则服务器将请求 DNS 服务器删除其负责的 RR。

a) 您可以全局或按接口配置服务器设置。有关全局设置，请参阅 **DDNS** 主页。有关每个接口的设置，请参阅 **DDNS接口设置** 页面。接口的设置优先于全局设置。
b) 配置您希望 DHCP 服务器在 **动态 DNS 更新**下更新的 DNS RR。

- **未选定**-未禁用 DDNS 更新，即使客户端请求也是如此。
- **仅 PTR**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将仅更新 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN 选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。
- **A 和 PTR 两者记录**-启用 DDNS 更新。如果启用 **覆盖 DHCP 客户端请求** 设置，则服务器将同时更新 A 和 PTR RR。否则，服务器将更新客户端请求的 RR。如果客户端未使用 FQDN 选项发送更新请求，则服务器将使用 DHCP 选项 12 中发现的主机名请求 A 和 PTR RR 的更新。

c) 要覆盖 DHCP 客户端请求的更新操作，请选中 **覆盖 DHCP 客户端请求**。

服务器会回复客户端，表示请求被覆盖了，所以客户端不会同时尝试执行服务器正在执行的更新。

步骤 7 （可选）配置常规 DHCP 客户端设置。这些设置与 DDNS 不相关，但与 DHCP 客户端的行为相关。

a) 在 **DDNS** 页面上，选中 **启用 DHCP 客户端广播** 以请求 DHCP 服务器广播 DHCP 应答（DHCP 选项 1）。

b) 要强制将 MAC 地址存储在选项 61 的 DHCP 请求数据包中而不是默认内部生成的字符串中，请在 **DDNS** > **DHCP 客户端 ID 接口**，从 **可用接口** 列表中选择接口，然后点击 **添加** 将其移动到 **选定的接口** 列表。

某些 ISP 期望选项 61 成为接口 MAC 地址。如果 MAC 地址未包含在 DHCP 请求数据包中，则不会分配 IP 地址。此设置与 DDNS 不直接相关，而是常规 DHCP 客户端设置。

步骤 8 点击设备页面上的 **保存** 以保存更改。

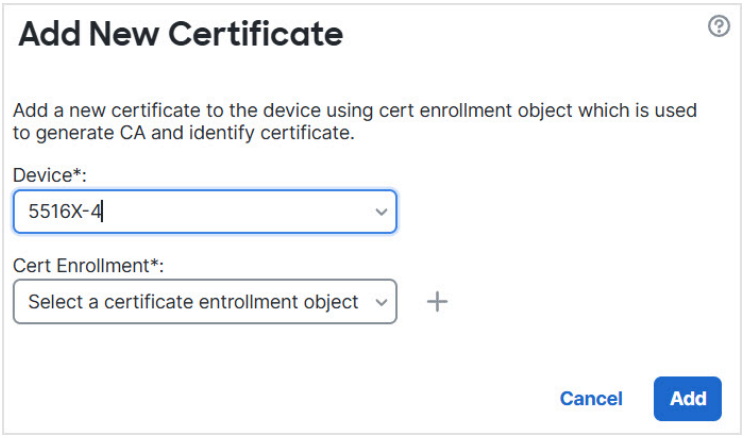
步骤 9 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。

以下示例显示如何将 DDNS 服务器的证书添加为信任点。

a) 获取 DDNS 服务器 CA 证书。此程序显示使用 PEM 格式的手动导入，但您也可以使用 PKCS12。

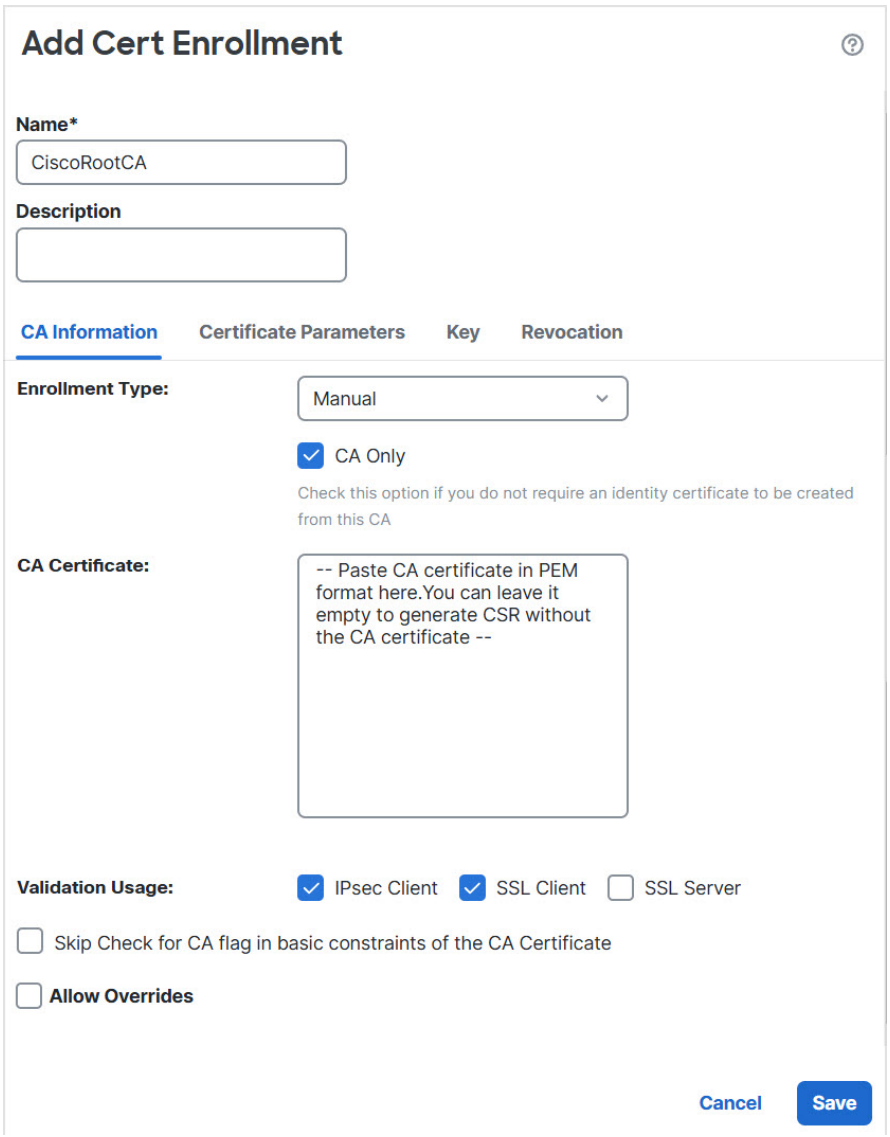
b) 在防火墙管理中心，选择**设备** > **证书**，然后点击**添加**。

c) 选择 **设备**，点击 **添加** (+)。



系统将显示**添加证书注册 (Add Cert Enrollment)** 对话框。

d) 输入以下字段值，然后点击 **保存**。



- 输入 **Name**。
- 选择 **注册类型** > **手动**。
- 点击 **仅 CA**。
- 从步骤 9.a，第 969 页粘贴 CA 文本。

e) 点击**保存**。

DHCP 和 DDNS 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
从防火墙管理中心 Web 界面配置 DHCP 中继受信任接口。	7.2.6/7.4.1	任意	**升级影响。升级后重新设置任何相关的 FlexConfig。** 现在，您可以使用防火墙管理中心 Web 界面将接口配置为受信任接口，以保留 DHCP 选项 82。如果执行此操作，这些设置将覆盖任何现有的 FlexConfig，但您应将其删除。 下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 Firewall Threat Defense DHCP 中继代理接收到一个已设置选项 82 的 DHCP 数据包，但是 giaddr 字段（在将数据包转发到服务器之前，指定由中继代理设置的 DHCP 中继代理地址）设置为 0，则 Firewall Threat Defense 默认丢弃该数据包。可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 新增/修改的菜单项：**设备 (Devices)** > **设备管理 (Device Management)** > **添加/编辑设备 (Add/Edit Device)** > **DHCP** > **DHCP 中继 (DHCP Relay)**
DHCPv6 无状态服务器	7.3.0	7.3.0	使用 DHCPv6 前缀委派客户端时，Firewall Threat Defense 现在支持轻型 DHCPv6 无状态服务器。当 SLAAC 客户端向 Firewall Threat Defense 发送信息请求 (IR) 数据包时，Firewall Threat Defense 会向它们提供域名等其他信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加/编辑接口 (Add/Edit Interfaces)** > **IPv6** > **DHCP** • **对象 (Objects)** > **对象管理 (Object Management)** > **DHCP IPv6 池 (DHCP IPv6 Pool)** 新增/修改的命令：**show ipv6 dhcp**



第 19 章

平台设置

Firewall Threat Defense 设备的平台设置用于配置您可能希望在多台设备之间共享其值的一系列无关功能。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

注释 在 7.4 及更高版本，管理和诊断接口已被合并。如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略（7.3 和更早版本，和某些升级后的 7.4 设备）。

- 平台设置简介， 第 974 页
- 平台设置策略的要求和前提条件， 第 974 页
- 管理平台设置策略， 第 974 页
- 机箱平台设置， 第 975 页
- ARP 检测， 第 975 页
- 横幅， 第 977 页
- DNS， 第 977 页
- 外部身份验证， 第 980 页
- 为平台的外部身份验证启用虚拟路由器感知接口， 第 985 页
- 片段设置， 第 986 页
- **HTTP 访问**， 第 987 页
- **ICMP 访问**， 第 988 页
- NetFlow， 第 990 页
- **SSH 访问**， 第 991 页
- SMTP 服务器， 第 993 页
- SNMP， 第 994 页
- SSL ， 第 1007 页
- 系统日志， 第 1011 页
- 超时， 第 1028 页
- 时间同步， 第 1030 页
- 时区， 第 1031 页
- UCAPL/CC 合规性， 第 1032 页

• 性能配置文件，第 1033 页
• 平台设置的历史记录，第 1034 页

平台设置简介

平台设置策略是用于定义托管设备的可能类似于您的部署中其他托管设备的方面（例如时间设置和外部身份验证）的共享功能集或参数集。

通过共享策略，可以同时配置多个托管设备，从而在部署中提供一致性并精简管理工作。对平台设置策略的任何更改都会影响已应用该策略的所有托管设备。即使您希望每台设备的设置不同，也必须创建共享策略并将其应用到所需设备。

例如，您的组织的安全策略可能会要求您的设备在用户登录时显示“无授权使用”(No Unauthorized Use) 消息。通过平台设置，您可以在平台设置策略中设置一次登录横幅。

在单一 防火墙管理中心上具有多个平台设置策略也有好处。例如，如果您具有在不同情况下使用的不同邮件中继主机，或者如果要测试不同的访问列表，则可以创建多个平台设置策略并在其之间切换，而非编辑单个策略。

平台设置策略的要求和前提条件

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

管理平台设置策略

使用 **平台设置** 页面（**设备** > **平台设置**）管理平台设置策略。此页面指示每个策略的设备类型。 **状态** 列显示策略的设备目标。

过程

步骤 1 选择**设备** > **平台设置**。

步骤 2 对于现有策略，您可以**复制** ()、**编辑** ()或**删除** ()策略。

注意

不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

步骤 3 要创建新策略，请点击**新建策略 (New Policy)**。

a) 从下拉列表中选择设备类型。

- **威胁防御设置** 以创建 Firewall Threat Defense 托管设备的共享策略。
- **机箱平台设置** 用于在多实例模式下为托管 Firewall Threat Defense 机箱创建共享策略。

b) 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。

c) 或者，选择要应用策略的 **可用设备** 或 **可用机箱**，然后点击 **添加** 到策略（或拖放）以添加所选设备。可以在**搜索 (Search)** 字段中输入搜索字符串以缩小设备列表。

d) 点击**保存**。

系统创建策略，并打开以进行编辑。

步骤 4 要更改策略的目标设备，请点击要编辑的平台设置策略旁边的 **编辑** (✎) 图标。

a) 点击**策略分配 (Policy Assignment)**。

b) 要将设备、高可用性对或设备组分配给策略，请在 **可用设备** 或 **可用机箱** 列表中将其选中，然后点击 **添加**。还可以进行拖放。

c) 要删除设备分配，请点击 **所选设备** 或 **所选机箱** 列表中的设备、高可用性对或设备组旁边的 **删除** (🗑)。

d) 点击**确定**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

机箱平台设置

机箱平台设置适用于多实例模式机箱。有关这些设置的详细信息，请参阅 配置机箱平台设置，第 245 页。

ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP 检测可防止恶意用户模拟其他主机或路由器（称为 ARP 欺骗）。ARP 欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。

但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，Firewall 威胁防御设备 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 Firewall 威胁防御设备 会丢弃数据包。
- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 Firewall 威胁防御设备 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。



注释 即使此参数设置为 flood，专用管理接口也绝不会以泛洪方式传输数据包。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**ARP 检测**。

步骤 3 将条目添加到 ARP 检查表。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 选择所需的选项。

- **已启用检查** - 对选定接口和区域执行 ARP 检查。
- **已启用洪流** - 是否将不匹配静态 ARP 条目的 ARP 请求以洪流形式自除原始接口或专用管理接口以外的所有接口发出。此为默认行为。

  如果您不选择以洪流形式发出 ARP 请求，则只允许与静态 ARP 条目完全匹配的请求。
- **安全区域** - 添加包含要在其上执行所选操作的接口的区域。区域必须为交换区域。对于不在区域中的接口，您可以在“所选安全区域”列表下方的字段中键入接口名称，然后点击**添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定**。

步骤 4 根据添加静态 ARP 条目，第 821 页中所述添加静态 ARP 条目。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

横幅

您可以将消息配置为在用户连接到设备命令行界面 (CLI) 时显示这些用户。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**横幅**。

步骤 3 配置横幅。

下面是关于横幅的几点提示和要求。

- 只允许使用 ASCII 字符。您可以使用换行符（按 Enter），但不能使用制表符。
- 通过包含变量 **$(hostname)** 或 **$(domain)**，可以动态添加设备的主机名或域名。
- 虽然横幅上没有绝对长度限制，但如果没有足够的系统内存来处理横幅消息，则 Telnet 或 SSH 会话将关闭。
- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。有两种适用于不同类型流量的 DNS 服务器设置：数据流量和特殊管理流量。数据流量包括使用需要进行 DNS 查找的 FQDN 的任何服务，例如访问控制规则和远程访问 VPN。特殊管理流量包括管理接口上发出的流量，例如配置和数据库更新。此程序仅适用于 数据 DNS 服务器。有关 管理 DNS 设置，请参阅 CLI **configure network dns servers** 和 **configure network dns searchdomains** 命令。

为了确定 DNS 服务器通信的正确接口，托管设备使用路由查找，但使用哪种路由表取决于您启用 DNS 的接口。有关详细信息，请参阅下面的接口设置。

您可以选择配置多个 DNS 服务器组，并使用它们来解析不同的 DNS 域。例如，您可能有一个使用公共DNS服务器的可捕获默认组，用于与互联网的连接。然后，您可以配置一个单独的组，以将内

部 DNS 服务器用于内部流量，例如，与 example.com 域中的计算机的任何连接。因此，使用您的组织的域名与FQDN的连接将使用内部DNS服务器进行解析，而与公共服务器的连接则使用外部DNS服务器。这些解析由使用数据 DNS 解析的任何功能使用，例如 NAT 和访问控制规则。

您可以使用受信任 DNS 服务器选项卡为 DNS 监听配置受信任 DNS 服务。DNS 监听用于将应用域映射到IP，以便检测第一个数据包上的应用。除了配置受信任的DNS服务器之外，您还可以将DNS组，DHCP 池，DHCP 中继和 DHCP 客户端中已配置的服务器作为受信任的 DNS 服务器。

注释 对于基于应用的 PBR，必须配置受信任的 DNS 服务器。您还必须确保 DNS 流量以明文格式通过 Firewall Threat Defense （不支持加密 DNS），以便解析域以检测应用。

开始之前

- 确保已创建一个或多个DNS服务器组。有关详细信息，请参阅创建DNS服务器组对象，第2640页。
- 确保您已创建用于连接到 DNS 服务器的接口对象。
- 确保托管设备具有适当的静态路由或动态路由来访问 DNS 服务器。

过程

步骤 1 选择 **设备** > **平台设置**并创建或编辑威胁防御策略。

步骤 2 点击 **DNS**。

步骤 3 点击 **DNS 设置** 选项卡。

步骤 4 选中 **启用按设备 DNS 域名解析**。

步骤 5 配置 DNS 服务器组。

a) 在 DNS 服务器组列表中执行以下任一操作：

- 要将值添加到列表，请点击 **添加**。如果在现有服务器组列表中配置了 30 个过滤器域，则无法添加其他组。
- 要编辑组的设置，请点击组旁边的 **编辑** (✎) 。
- 要删除组，请点击该组旁边的 **删除** (🗑) 。删除组不会删除 DNS 服务器组对象，只是将其从此列表中删除。

b) 在添加或编辑组时，请配置以下设置，然后点击 **确定**：

- **选择 DNS 组**-选择现有 DNS 服务器组对象，或点击 + 创建新的 DNS 服务器组对象。
- **作为默认**-选择此选项可使此组成为默认组。任何与其他组的过滤器不匹配的DNS解析请求都将使用此组中的服务器进行解析。

- **过滤域**-仅对于非默认组，是逗号分隔的域名列表，例如example.com，example2.com。不能包含空格。

  该组将仅用于这些域的DNS解析。您可以在添加到此DNS平台设置策略的所有组中最多输入30个单独的域。每个名称最多可包含127个字符。

  请注意，这些过滤器域与该组的默认域名无关。过滤器列表可以与默认域不同。

步骤 6 （可选）输入 **过期条目计时器** 和 **轮询计时器** 值，以分钟计。

这些选项仅适用于在网络对象中指定的FQDN。这些不适用于其他功能中使用的FQDN。

- **到期条目计时器** 指定DNS条目的最短生存时间（TTL），以分钟为单位。如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。到期后，该条目将从DNS查找表中删除。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些DNS条目可以有非常短的TTL（短至3秒），所以您能够使用此设置实际上延长TTL。默认值为1分钟（即，所有分辨率的最小TTL为1分钟）。范围为 1 至 65535 分钟。

  请注意，对于运行7.0或更早版本的系统，到期时间实际上会添加到TTL中：它不指定最小值。

- **轮询计时器** 指定设备查询 DNS 服务器以解析网络对象中定义的 FQDN 的时间限制。在轮询 DNS 计时器到期时或解析的 IP 条目的 TTL 到期时（以先到者为准），定期解析 FQDN。

步骤 7 在所有接口或特定接口上启用 DNS 查找。这些选择还会影响所使用的路由表。

请注意，在接口上启用DNS查找与指定用于查找的源接口不同。Firewall Threat Defense始终使用路由查询来确定源接口。不能使用除专用管理接口之外的管理专用接口。

- 未选择任何接口 - 在所有接口上启用 DNS 查找。Firewall Threat Defense 仅检查数据路由表。
- 选择了特定接口而不是**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic/management interface also)** 选项 - 在指定接口上启用 DNS 查找。Firewall Threat Defense仅检查数据路由表。
- 选择了特定接口并且选择了**同时通过诊断/管理接口启用 DNS 查找 (Enable DNS Lookup via diagnostic/management interface also)** 选项 - 在指定接口和 管理 接口上启用 DNS 查找。Firewall Threat Defense 检查数据路由表，如果未找到路由，则回退到管理专用路由表。
- 仅限 **通过诊断启用 DNS 查找/管理 接口及** 选项-在 管理上启用 DNS 查找。Firewall Threat Defense仅检查管理专用路由表。

步骤 8 要配置受信任的 DNS 服务器，请点击 **受信任的 DNS 服务器** 选项卡。

步骤 9 默认情况下，在 DHCP 池，DHCP 中继，DHCP 客户端或 DNS 服务器组中配置的现有DNS服务器作为受信任DNS服务器。如果要排除其中任何一个，请取消选中相应的复选框。

步骤 10 要添加受信任的 DNS 服务器，请在 **指定 DNS 服务器**下，点击 **编辑**。

步骤 11 在 **选择 DNS 服务器** 对话框中，选择主机对象作为受信任 DNS 服务器或直接指定受信任 DNS 服务器的 IP 地址：

a) 要选择现有主机对象，请在 **可用主机对象**下，选择所需的主机对象，然后点击 **添加** 以将其包含到 **所选DNS服务器**中。有关添加主机对象的信息，请参阅 创建网络对象， 第 2660 页。

b) 要直接提供受信任 DNS 服务器的 IP 地址（IPv4 或 IPv6），请在给定文本字段中输入地址，然后点击 **添加** 以将其包含到 **所选 DNS 服务器**中。

c) 点击**保存**。添加的DNS服务器显示在 **受信任的 DNS 服务器** 页面中。

注释
每个策略最多可以配置 12 个 DNS 服务器。

步骤 12 （可选）要使用主机名或 IP 地址搜索已添加的 DNS 服务器，请使用 **指定 DNS 服务器** 下的搜索字段。

步骤 13 点击**保存**。

下一步做什么

要将 FQDN 对象用于访问控制规则，请创建一个 FQDN 网络对象，然后将其分配给访问控制规则。有关说明，请参阅创建网络对象， 第 2660 页。

外部身份验证

注释 您必须具有管理员权限才能执行此任务。

在为管理用户启用外部身份验证时，Firewall Threat Defense会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

共享外部身份验证对象

防火墙管理中心 和 Firewall Threat Defense 设备可使用外部身份验证对象。防火墙管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意， Firewall Threat Defense 支持在 RADIUS 服务器上定义用户，而防火墙管理中心要求您在外部身份验证对象中预定义用户列表。您可以选择针对 Firewall Threat Defense使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 Firewall Threat Defense 和 防火墙管理中心创建单独的对象。

注释 Firewall Threat Defense 和 防火墙管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense 外部身份验证配置将不起作用。

为设备分配外部身份验证对象

对于 防火墙管理中心，请直接在 系统用户外部身份验证启用外部身份验证对象；此设置仅会影响 **管理** > **用户** > **外部身份验证** 的使用情况，无需为了托管设备的使用而启用此设置。防火墙管理中心

对于 Firewall Threat Defense 设备，必须在部署到设备的平台设置中启用外部身份验证对象，并且每个策略只能激活一个外部认证对象。已启用 CAC 身份验证的 LDAP 对象也不能用于 CLI 访问。确保即使您未共享对象，Firewall Threat Defense 和 防火墙管理中心 也都可以访问 LDAP 服务器。防火墙管理中心 对于检索用户列表并将其下载到设备至关重要。

Firewall Threat Defense 支持的字段

只有外部身份验证对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 防火墙管理中心，则将使用这些字段。此程序仅涵盖 Firewall Threat Defense 支持的字段。 有关其他字段，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 《配置 防火墙管理中心 外部身份验证》 。

用户名

用户名必须为使用字母数字字符加句点 (.) 或连字符 (-) 的 Linux 有效用户名，且仅可使用小写字母。不支持其他特殊字符，例如 at 符号 (@) 和斜线 (/)。您无法添加以下默认内部用户以进行外部身份验证： **root**、**daemon**、**bin**、**sys**、**sync**、**游戏**、**man**、**lp**、**mail**、**news**、**uucp**、**proxy**、**www-data**、**backup**、**list**、**irc**、 **nats**、 **ntp** 、 **lldpd**、**bind**、**dhcp**、**qemu**、**rpcuser**、**rpc**、**sshd**、**radiusd**、**messagebus**、**admin**、 **MySQL**、**www**、**sfrna**、**snorty**、**sfsnort**、**sfreemediation**、**nobody**、**samdme**、**extuser**、**p2puser**、**rloginUser**。只能在防火墙管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在防火墙管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 Firewall Threat Defense 首先对照此内部用户检查密码，如果失败，再检查 AAA 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。 对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

特权等级

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

开始之前

- 管理接口上的 SSH 访问默认处于启用状态。要在数据接口上启用 SSH 访问，请参阅SSH 访问，第 991 页。
- 请告知 RADIUS 用户以下操作，使他们合理设定预期：
  - 外部用户首次登录时，Firewall Threat Defense 会创建所需的结构，但不能同时创建用户会话。用户只需再次进行身份验证，即可启动会话。用户将看到与以下消息类似的消息：“已识别新的外部用户名。请重新登录以启动会话。”
  - 如果用户的 Service-Type 属性未在 RADIUS 服务器中定义或配置不正确，并且在使用 RADIUS 定义的用户进行身份验证时，用户将看到类似于以下内容的消息：“您的用户名未定义服务类型。您无权访问系统？。

    在某些情况下，SSH 客户端会在 SSH 连接不成功时关闭 CLI 窗口，甚至在显示失败消息之前也是如此。因此，请确保在 RADIUS 服务器中正确定义用户的 Service-Type 属性。

- 同样地，如果自上次登录以来，用户的 Service-Type 授权发生了更改，则用户将需要重新进行身份验证。用户将看到与以下消息类似的消息：“您的授权权限已更改。请重新登录以启动会话。”

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击**管理外部身份验证服务器 (Manage External Authentication Server)** 链接。

您还可以通过点击 **系统 (System)** > **用户 (Users)** > **外部身份验证 (External Authentication)**打开外部身份验证屏幕。

步骤 4 配置 LDAP 身份验证对象。

a) 点击**添加外部身份验证对象 (Add External Authentication Object)**。

b) 将**身份验证方法**设置为 **LDAP**

c) 输入**名称**和可选**说明**。

d) 从下拉列表中选择**服务器类型**。

e) 对于**主服务器**，输入**主机名/IP 地址**。

注释
如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

f) （可选） 更改**端口**使用的默认值。

g) （可选） 输入**备份服务器**参数。

h) 输入 **LDAP 特定参数**。

- **基础 DN** - 为要访问的 LDAP 目录输入基本可分辨名称。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN (Fetch DNs)**，然后从下拉列表中选择相应的基本可分辨名称。
- **基本过滤器** - 例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且纽约办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索纽约办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。
- **用户名** - 为有足够凭证浏览 LDAP 服务器的用户输入可分辨的名称。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。
- **密码**和**确认密码** - 输入并确认用户的密码。
- （可选）**显示高级选项** - 配置以下高级选项。
  - **加密 (Encryption)** - 点击**无 (None)**、**TLS** 或 **SSL**。

注释
如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或**TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径 (SSL Certificate Upload Path)** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件 (Choose File)** 选择一个证书。
- （未使用）**用户名模板** - Firewall Threat Defense 未使用。
- **超超时 (Timeout)** - 输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

注释
Firewall Threat Defense 和 防火墙管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense 外部身份验证配置将不起作用。

i) （可选） 如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性** 。例如，在 Microsoft Active Directory Server 上，通过在 **CLI 访问属性** 字段中键入 `sAMAccountName` 来使用 `sAMAccountName` 外壳访问属性检索外壳访问用户。

j) 设置 **CLI 访问过滤器**。

选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

LDAP 服务器上的名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

k) 点击**保存**。

步骤 5 对于LDAP，如果以后在LDAP服务器上添加或删除用户，必须刷新用户列表并重新部署平台设置。

a) 选择**管理** > **用户** > **外部身份验证**。

b) 点击 LDAP 服务器旁边的 **刷新** ( ) 。

如果用户列表发生变化，您将看到一条消息，建议您为设备部署配置更改。Firepower Threat Defense 平台设置还会显示它在“*x* 个目标设备上过时。"

c) 部署配置更改；请参阅部署配置更改 ，第 180 页。

步骤 6 配置 RADIUS 身份验证对象。

a) 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤6.k，第 984 页）。要在为 Firewall Threat Defense使用 Service-Type 属性的同时对 Firewall Threat Defense 和 防火墙管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 防火墙管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 Firewall Threat Defense）。

b) 在 防火墙管理中心 中，点击**添加外部身份验证对象 (Add External Authentication Object)**。

c) 将**身份验证方法**设置为 **RADIUS**。

d) 选中**启用 RADIUS 服务器的消息身份验证器 (RADIUS Server-Enabled Message Authenticator)** 复选框，要求在所有 RADIUS 响应中使用消息验证器属性，确保 RADIUS 服务器的每个响应都经过 Firewall Threat Defense 的安全验证。

新 RADIUS 服务器默认启用此功能。建议您在升级后为现有服务器启用此功能。禁用消息验证器可能会使防火墙暴露于潜在的攻击。确保 RADIUS 服务器具有消息验证器配置。

e) 输入**名称**和可选**说明**。

f) 对于**主服务器**，输入**主机名/IP 地址**。

注释
如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

g) （可选） 更改**端口**使用的默认值。

h) 输入 **RADIUS 服务器密钥**。

i) （可选） 输入**备份服务器**参数。

j) 输入 **RADIUS 特定参数**。

- **超时（秒）** - 输入滚动到备份连接之前等待的秒数。默认值为 30。
- **重试次数** - 输入在滚动到备份连接之前应当尝试主服务器连接的次数。默认值为 3。

k) （可选）不使用 RADIUS 定义的用户，在 **CLI 访问过滤器**下，在 **管理员 CLI 访问用户列表** 字段中输入一个逗号分隔的用户名列表。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

您可能想要使用 Firewall Threat Defense 的 **CLI 访问过滤器** 方法以便对 Firewall Threat Defense 和其他平台类型使用相同的外部身份验证对象。请注意，如果想要使用RADIUS定义的用户，则必须将 **CLI 访问过滤器** 留空。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

注释
如果要在 RADIUS 服务器上仅定义用户，则必须将此部分留空。

l) 点击**保存**。

步骤 7 返回至 **管理** > **用户** > **外部身份验证**。

步骤 8 点击 **刷新** ( ) 可查看新添加的任何对象。

为 LDAP 指定 SSL 或 TLS 加密时，必须上传证书才能进行连接；否则，此窗口中将不会列出该服务器。

步骤 9 点击要使用的外部身份验证对象旁边的 **滑块已启用** ( ) 。只能启用一个对象。

步骤 10 点击**保存**。

步骤 11 部署配置更改；请参阅部署配置更改，第 180 页。

为平台的外部身份验证启用虚拟路由器感知接口

Firewall Threat Defense 设备的认证、授权和记账 (AAA) 通过设备的管理接口进行管理。您还可以启用虚拟路由器感知数据接口、数据子接口、端口通道或子端口通道，以管理 Firewall Threat Defense 设备的 AAA。启用后，AAA 路由查找位于虚拟路由和转发 (VRF) 路由域中，并且 AAA 管理流量将转发到数据接口。将虚拟路由器感知数据接口用于 AAA 时，支持以下服务器配置：

- 用于外部身份验证的 RADIUS 或 LDAP 服务器
- FQDN、IPv4 或 IPv6 服务器地址

要将虚拟路由器感知接口用于 Firewall Threat Defense 设备的外部身份验证，请通过将身份验证服务器与设备的虚拟路由器感知接口关联来修改其外部身份验证策略。

开始之前

- 确保已为设备配置所需的虚拟路由和转发 (VRF) 接口。有关配置 VRF 接口的信息，请参阅配置虚拟路由器，第 1114 页；有关添加静态路由的信息，请参阅添加静态路由，第 1090 页。
- 确保存在具有单个虚拟路由器感知接口的安全区域或接口组。有关创建安全区域和接口组的信息，请参阅创建安全区域和接口组对象，第 715 页。

- 确保已配置并启用外部身份验证服务器对象。有关配置外部身份验证的信息，请参阅配置 FTD 的外部身份验证，第 139 页。
- 如果主身份验证服务器配置了服务器的 FQDN，请确保备份身份验证服务器（如果已配置）也使用其 FQDN。此外，在威胁防御设备的管理接口中配置 DNS 服务器。有关 DNS 服务器配置的信息，请参阅配置 DNS。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 点击**外部身份验证 (External Authentication)** 并编辑外部身份验证策略。

步骤 3 在**外部身份验证 (External Authentication)** 对话框中，列出了可用的安全区域和接口组。要将虚拟路由器感知接口与外部身份验证服务器关联，请选择具有单个虚拟路由器感知接口的安全区域或接口组，然后执行以下操作：

a) 要将接口对象与主身份验证服务器关联，请点击**添加到主服务器 (Add to Primary Server)**。

b) （可选）要将接口对象与备份身份验证服务器关联，请点击**添加到备份服务器 (Add to Backup Server)**。如果**添加到备份服务器 (Add to Backup Server)** 按钮处于非活动状态，则表示设备中未配置用于外部身份验证的备份服务器。从**系统** > **用户** > **外部身份验证**配置备份服务器。有关配置备份身份验证服务器的信息，请参阅配置 FTD 的外部身份验证，第 139 页。

步骤 4 点击**确定**。

步骤 5 保存并部署更改。

片段设置

默认情况下，Firewall Threat Defense设备允许每个 IP 数据包最多包含 24 个分段，以及最多 200 个等待重组的分段。如果您有定期对数据包进行分段的应用（如 NFS over UDP），可能需要让分段位于您的网络上。但如果您没有对流量进行分段的应用，则我们建议您通过将**链**设置为 1 来禁止分段。分段数据包通常用作拒绝服务 (DoS) 攻击。

注释 这些设置将为已分配此策略的设备建立默认值。可以通过选择接口配置中的**覆盖默认分段设置**，为设备上的特定接口覆盖这些设置。在编辑接口时，可以找到**高级 (Advanced)** > **安全配置 (Security Configuration)** 上的选项。选择 **设备** > **设备管理**，编辑 Firewall Threat Defense 设备，然后选择**接口**以编辑接口属性。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**碎片设置 (Fragment Settings)**。

步骤 3 配置以下选项。如果希望使用默认设置，请点击**重置为默认值**。

- **大小（块）** - 来自所有连接的可能正在等待重组的总体数据包分段的最大数量。默认值为 200 个分段。
- **链（分段）** - 可将一个完整 IP 数据包分段为数据包的最大数量。默认为 24 个数据包。将此选项设置为 1 将禁止分段。
- **超时（秒）** - 等待整个分段数据包到达所需的最大秒数。默认值为 5 秒。如果在此时间内未收到所有分段，则将放弃所有分段。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

HTTP 访问

您可以启用HTTPS服务器，以便为云负载均衡器提供运行状况检查机制，例如，使用应用负载均衡器为 AWS 上的 Firewall Threat Defense Virtual 提供运行状况检查机制。

不支持在 Firewall Threat Defense 上使用HTTPs的其他用途；例如，Firewall Threat Defense 没有用于在此管理模式下进行配置的 Web 接口。

此配置仅适用于数据接口，包括您配置为仅管理的任何接口。它主题不适用于专用管理接口。管理接口与设备上的其他接口分离。它用于设置设备并将其注册到防火墙管理中心。它具有独立IP地址和静态路由。

要使用 HTTPS，无需允许主机 IP 地址的访问规则。只需按照本部分配置 HTTPS。

只能将 HTTPS 用于可访问的接口；如果 HTTPS 主机位于外部接口上，则只能向该外部接口直接发起管理连接。

开始之前

- 不能在同一接口上为同一 TCP 端口同时配置 HTTPS 和 Cisco Secure Client AnyConnect VPN 模块 。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果必须在同一接口上同时配置这两项功能，则请使用不同的端口。例如，在端口 4443 上打开 HTTPS。
- 需要网络对象，用于定义将要允许建立到设备的HTTPS连接的主机或网络。您可以在此过程中添加对象，但如果要使用对象组标识一组IP地址，请确保规则中所需的组已经存在。选择**对象**以配置对象。

注释 不能使用系统提供的**任意**网络对象组。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **HTTP 访问**。

步骤 3 选中 **启用 HTTP 服务器** 复选框以启用 HTTP 服务器。

步骤 4 （可选） 更改 HTTP 端口。默认值为 443。

步骤 5 标识允许 HTTP 连接的接口和 IP 地址。

使用此表来限制哪些接口将接受 HTTP 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**- 用于标识允许建立 HTTP 连接的主机或网络的网络对象 或组 。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **可用区域/接口**- 添加包含将允许进行 HTTP 连接的接口的区域。对于不在区域中的接口，可以在**所选区域/接口**列表下方的字段中键入接口名称，然后点击**添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定**。

步骤 6 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

ICMP 访问

默认情况下，您可以使用 IPv4 或 IPv6 将 ICMP 数据包发送到任何接口，以下情况例外：

- Firewall 威胁防御 不响应定向至广播地址的 ICMP 回显请求。
- Firewall 威胁防御 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

为了保护设备免受攻击，您可以使用 ICMP 规则将接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为ICMP不可到达消息类型（类型3）授予权限。拒绝ICMP不可达消息会禁用ICMP路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。

开始之前

确保规则中所需的对象已经存在。选择**对象**以配置对象。您需要网络对象或组来定义所需的主机或网络，并且需要端口对象来定义要控制的 ICMP 消息类型。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **ICMP 访问**。

步骤 3 配置 ICMP 规则。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **操作** - 许可（允许）还是拒绝（丢弃）匹配的流量。
- **ICMP 服务** - 标识 ICMP 消息类型的端口对象。
- **网络 (Network)** - 标识您要控制其访问权限的主机或网络的网络对象或组。
- **可用区域/接口**-添加包含您所保护的接口的区域。对于不在区域中的接口，可以在**所选区域/接口** 列表下方的字段中键入接口名称，然后点击 **添加**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定**。

步骤 4 （可选。）设置对 ICMPv4 无法访问的消息的速率限制。

- **速率限制** - 设置不可达消息的速率限制，该限制介于每秒 1 至 100 条消息之间。默认值为每秒 1 条消息。
- **突发大小** - 设置突发速率，其值介于 1 至 10 之间。系统会发送此数量的回复，但在达到速率限制之前不会发送后续回复。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

NetFlow

NetFlow 功能使您能够收集进入或退出接口的 IP 网络流量信息。收集的流量信息将作为收集的记录发送到 NetFlow 收集器服务器或 NetFlow 分析器。您可以分析来自 NetFlow 的数据并确定信息，例如流量的源和目的地、服务类别、流量模式、带宽使用情况、流量类型、流量和拥塞原因。

使用本机 NetFlow 配置支持时，必须禁用通过系统日志流导出启用的流量信息收集。

NetFlow 提供配置流导出器和收集器以及必须监控的流事件类型的选项。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **NetFlow**。

步骤 3 启用启用流导出开关以 **启用 NetFlow** 数据导出。

步骤 4 配置用于控制事件推送到收集器的频率的常规 NetFlow 参数。

a) **活动刷新间隔**- 对于活动连接，指定流更新事件之间的时间间隔（以分钟为单位）。

b) **延迟流创建** - 指定发送流创建事件之前的延迟（以秒为单位）。如果没有输入任何值，则不会延迟，并会在创建流后立即导出流创建事件。

c) **模板超时速率** - 指定将模板记录发送到收集器的间隔（以分钟为单位）。

步骤 5 点击 **添加收集器** 以配置收集器。请参阅在 NetFlow 中添加收集器，第 990 页。

步骤 6 点击 **添加流量类** 以配置流量类。请参阅将流量类添加到 NetFlow，第 991 页。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

在 NetFlow 中添加收集器

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **NetFlow**。

步骤 3 启用启用流导出开关以 **启用 NetFlow** 数据导出。

步骤 4 点击 **添加收集器** 以配置收集器。您最多可以配置五个收集器。

步骤 5 从 **主机** 下拉列表中，选择必须将 NetFlow 数据包发送到的 NetFlow 事件收集器或服务器的收集器主机 IP 地址（仅限 IPv4）。或者，您可以点击 (+) 图标创建新的网络主机。

步骤 6 在 **端口** 字段中，输入收集器上必须将 NetFlow 数据包发送到的 UDP 端口。

步骤 7 从 **可用接口或接口组**中，选择必须通过其访问收集器的接口或接口组。您可以选择多个接口或接口组。接口组对象只能包含给定设备的一个接口。只能通过一个接口访问收集器。该对象可以包括虚拟路由器感知接口。NetFlow 上不支持环回接口。

点击 (+) 图标以创建新接口组。

步骤 8 点击 **添加** 以添加所选接口。

步骤 9 您还可以输入接口名称，然后点击 **添加** 以添加接口。

步骤 10 点击**确定**。

将流量类添加到 NetFlow

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **NetFlow**。

步骤 3 启用启用流导出开关以 **启用 NetFlow** 数据导出。

步骤 4 点击 **添加流量类** 以配置流量类。

步骤 5 在 **名称** 字段中，输入必须与 NetFlow 事件匹配的流量类的名称。

步骤 6 在 **类型** 字段中，选择流量类以过滤要捕获的流量类型：

- **默认**- 如果没有任何流量类与该流量匹配，则匹配的流量类。
- **访问列表**- 必须与为 NetFlow 事件捕获的流量匹配的特定流量类。

步骤 7 如果您选择 **访问列表** 作为 **类型**，则必须从 **访问列表对象** 下拉列表中选择访问列表对象。

注释

您还可以点击 (+) 图标创建新的扩展访问列表对象。请参阅配置扩展 ACL 对象 ， 第 2625 页。

步骤 8 在 **事件类型**中，选中要捕获并发送到收集器的不同 NetFlow 事件的复选框。

步骤 9 点击**确定**。

SSH 访问

如果在数据接口（例如外部）上启用了防火墙管理中心访问，则应使用此程序在该接口上启用SSH。本节介绍如何启用 Firewall Threat Defense上一个或多个 数据 接口的 SSH 连接。

注释 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

要使用 SSH，您也不需要允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。

数据与管理 SSH

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到防火墙管理中心。数据接口的SSH与管理接口的SSH共用内部和外部用户列表。其他设置单独进行配置：对于数据接口，使用此屏幕启用SSH和访问列表；数据接口的SSH流量使用常规路由配置，并不是所有静态路由均在设置时或CLI中配置。不使用在设置时或CLI中配置的管理接口路由。

对于管理接口，要配置 SSH 访问列表，请参阅 *Cisco Secure Firewall Threat Defense* 命令参考中的 **configure ssh-access-list** 命令。要配置静态路由，请参阅 **configure network static-routes** 命令。默认情况下，在初始设置时通过管理接口配置默认路由。

接口访问

您只能SSH到可访问接口（包括用户定义的虚拟路由器界面）；如果SSH主机位于外部接口上，则只能直接向外部接口发起管理连接。在用户定义的虚拟路由器中启用SSH并希望VPN用户访问SSH时，请确保终止同一虚拟路由器上的VPN。但如果VPN在另一个虚拟路由器上终止，则必须在虚拟路由器之间配置路由泄漏。

密码和密钥交换

SSH 支持以下密码和密钥交换：

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256

SSH 堆栈

Firewall Threat Defense 使用基于 OpenSSH 的 CiscoSSH 堆栈。CiscoSSH 支持 FIPS 合规性和定期更新，包括来自思科和开源社区的更新。

最大尝试次数

在您连续三次尝试使用 SSH 登录 CLI 失败后，设备会终止 SSH 连接。

开始之前

- 可以使用 **configure user add** 命令在 CLI 中配置 SSH 内部用户，请参阅 在 CLI 中添加内部用户，第 137 页。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。还可以通过在平台设置中配置**外部身份验证**，在 LDAP 或 RADIUS 上配置外部用户。请参阅外部身份验证，第 980 页。
- 您需要定义允许与设备建立SSH连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组IP地址，请确保规则中所需的组已经存在。选择**对象**以配置对象。

注释 不能使用系统提供的 **any** 网络对象。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**SSH 访问 (SSH Access)**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

使用此表可以限制哪些接口将接受 SSH 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的网络对象 或组 。从下拉列表中选择一个对象，或者点击 + 以添加新的网络对象。
- **可用区域/接口 (Available Zones/Interfaces)** - 添加包含将允许进行 SSH 连接的接口的区域。对于不在区域中的接口，可以在**所选区域/接口 (Selected Zones/Interfaces)** 列表下方的字段中键入接口名称，然后点击**添加 (Add)**。 您还可以添加环回接口和虚拟路由器感知接口。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定**。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

SMTP 服务器

如果在“系统日志”设置中配置了邮件警报，则必须标识 SMTP 服务器。为“系统日志”配置的源邮件地址必须是 SMTP 服务器上的有效帐户。

开始之前

确保存在用于定义主 SMTP 服务器和辅助 SMTP 服务器的主机地址的网络对象。选择 **对象** 以定义对象。或者，也可以在编辑策略时创建对象。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 点击 **SMTP 服务器**。

步骤 3 选择标识**主服务器 IP 地址**的网络对象，以及可选的**辅助服务器 IP 地址**。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

SNMP

简单网络管理协议 (SNMP) 为在 PC 或工作站上运行的网络管理工作站定义了一种监控许多类型的设备（包括交换机、路由器和安全设备）的运行状况和状态的标准方法。您可以使用 SNMP 页面来配置防火墙设备，以便通过 SNMP 管理工作站进行监控。

简单网络管理协议 (SNMP) 支持从中心位置监控网络设备。思科安全设备支持使用 SNMP 版本 1、2c 和 3 进行网络监控，也支持陷阱和 SNMP 读取访问，但不支持 SNMP 写入访问。

SNMPv3 支持使用 DES（已弃用）、3DES、AES256、AES192 和 AES128 的只读用户和加密。

注释 DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于 Firewall Threat Defense运行 6.6 及更低版本的 。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 防火墙管理中心 管理任何运行版本 7.0+ 的 Firewall Threat Defense，则将使用 DES 加密的平台设置策略部署到这些 Firewall Threat Defense将会失败。

注释 SNMP 配置仅支持路由和诊断接口。

注释 要向外部 SNMP 服务器创建警报，请访问**管理** > **警报**

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择 **SNMP**。

步骤 3 启用 SNMP 并配置基本选项。

- **启用 SNMP 服务器** - 是否向配置的 SNMP 主机提供 SNMP 信息。您可以取消选择此选项，以便在保留配置信息的同时禁用 SNMP 监控。
- **读取社区字符串、确认** - 输入在向 Firewall Threat Defense设备发送请求时，SNMP 管理工作站使用的密码。SNMP 社区字符串是 SNMP 管理工作站与托管网络节点之间的共享密钥。安全设备使用此密码确定传入的 SNMP 请求是否有效。密码是区分大小写的字母数字字符串，最多可包含 32 个字符；不允许使用空格和特殊字符。
- **系统管理员名称** - 输入设备管理员或其他联系人的名称。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **位置** - 输入此安全设备的位置（例如，54 区 42 号楼）。该字符串区分大小写，最多可以包含 127 个字符。接受空格，但多个空间缩为一个空格。
- **端口** - 输入将在其上接受传入请求的 UDP 端口。默认值为 161。

步骤 4 （仅限 SNMPv3）。添加 SNMPv3 用户，第 1000 页。

步骤 5 添加 SNMP 主机，第 1003 页。

步骤 6 配置 SNMP 陷阱，第 1005 页。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

关于 SNMP

SNMP 是一种应用层协议，可促进网络设备之间的管理信息交换，是 TCP/IP 协议簇的一部分。Firewall Threat Defense 为使用 SNMP 版本 1、2c 和 3 的网络监控提供支持，并支持同时使用所有三个版本。利用在 Firewall Threat Defense 接口上运行的 SNMP 代理，您可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控网络设备。Firewall Threat Defense 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 Firewall Threat Defense 配置为向 NMS 发送陷阱，即针对特定事件从托管设备发送到管理站的未经请求的消息（事件通知），也可以使用 NMS 浏览安全设备上的管理信息库 (MIB)。MIB 是定义的集合，而 Firewall Threat Defense 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

SNMP 代理可在发生预定义为需要通知（例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。代理还会在管理站请求信息时进行回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 *64: SNMP* 术语

术语	说明
代理	在 Cisco Secure Firewall Threat Defense 上运行的 SNMP 服务器。SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障转移等的信息的标准化数据结构。MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	设置 PC 或工作站是为了监控 SNMP 事件和管理设备。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。 **coldStart** - 配置 SNMP 后，SNMP 代理启动时发生的 coldStart 陷阱。当代理在系统重启后启动时，也会出现此陷阱。 注释 对于集群和 HA 节点，重载后，如果接口重启时间超过 5 分钟（预设阈值），陷阱就会被丢弃。当集群和 HA 节点重启成功后，所有其他陷阱都会按预期发送。 **snmp-server enable traps snmp coldstart** 命令用于启用和禁用这些陷阱的传输。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 ASA 软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

浏览 SNMP 对象导航器，从以下位置查找思科 MIB、陷阱和 OID：

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB 中支持的表格和对象

以下部分列出了对指定 MIB 支持的表和对象。

远程接入 VPN 轮询

表 *65: CISCO-REMOTE-ACCESS-MONITOR-MIB*

计数器	OID	说明
活动会话	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	当前活动会话的数量。
用户	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	具有活动会话的用户数。
峰值会话	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	自系统启动以来的峰值 RA 会话数。

站点间 VPN 隧道轮询

表 *66: CISCO-REMOTE-ACCESS-MONITOR-MIB*

计数器	OID	说明
LAN 到 LAN 会话	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	当前活动的 LAN 到 LAN 会话数。
峰值 LAN 到 LAN 会话数	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	自系统启动以来的峰值并发 LAN 会话数。

连接轮询

表 *67: CISCO-FIREWALL-MIB*

计数器	OID	说明
活动连接数	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	整个防火墙当前使用的连接数。
峰值连接	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	自系统启动以来在任何时间使用的最高连接数。

计数器	OID	说明
每秒连接数	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	防火墙上的当前每秒连接数。
每秒峰值连接数	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	自系统启动以来防火墙上的每秒最高连接数。

NAT 转换轮询

表 68: CISCO-NAT-EXT-MIB

计数器	OID	说明
活动转换	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	NAT 设备中当前可用的地址转换条目总数。这表示从静态和动态地址转换机制创建的转换条目的汇总。
峰值活动转换	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	自系统启动以来任何时候处于活动状态的最大地址转换条目数。这表示自系统启动以来任何时候处于活动状态的地址转换条目的高水印。 该对象包括从静态和动态地址转换机制创建的转换条目。

路由表条目轮询

表 69: IP-FORWARD-MIB

计数器	OID	说明
活动转换	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	当前有效的 inetCidrRouteTable 条目总数。

接口双工状态轮询

表 70: CISCO-IF-EXTENSION-MIB

计数器	OID	说明
双工状态	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	此对象会指定给定接口上配置的双工状态。
检测到的双工状态	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	此对象指定给定接口上检测到的双工状态。

Snort 3 入侵事件速率轮询

表 71: CISCO-UNIFIED-FIREWALL-MIB

计数器	OID	说明
Snort 3 入侵事件速率	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	在过去 300 秒内，Snort 在此防火墙上记录入侵事件的平均速率。

BGP 对等翻板陷阱通知

表 72: BGP4-MIB

计数器	OID	说明
BGP 对等翻板	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	当BGP FSM从较高编号状态移动到较低编号状态时，就会生成BGPBackwardTransition事件。

CPU 利用率轮询

表 73: CISCO-PROCESS-MIB

计数器	OID	说明
CPU 总利用率	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	最近一分钟总系统 CPU 利用率。

计数器	OID	说明
单个 CPU 核心利用率	cpmCPUTotal1minRev 的关联参数和值 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 至 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	最近一分钟的各个 CPU 核心利用率值，其中“n”表示核心数。 示例： • 3.6.1.4.1.99.109.1.1.1.1.7(n+2) - 聚合系统 CPU 使用率百分比（此值与单情景模式下 3.6.1.4.1.9.9.109.1.1.1.1.7.1 中的系统 CPU 使用率相同）。 • 3.6.1.4.1.99.109.1.1.1.1.7(n+3) - Snort 平均 CPU 使用率百分比（所有 snort 实例的总值） • 3.6.1.4.1.99.109.1.1.1.1.7(n+4) - 系统进程平均百分比（“Sysproc”核心的平均值）

注释 在 ASA FirePOWER 上删除了与 CPU 监控（hrProcessorTable 和 hrNetworkTable）相关的 SNMP OID 1.3.6.1.2.1.25.3.3 和 1.3.6.1.2.1.25.3.4。您只能通过设备管理器查看和监控设备的 CPU 运行状况详细信息。

在 ENTITY-MIB 中，为插槽 2 和插槽 3 的 Cisco Secure Firewall 4200 的双 EPM 2X100G 和 4X200G 卡添加了两个新的供应商 OID - cevFPRNM4X200Gng 和 cevFPRNM2X100Gng。

添加 SNMPv3 用户

注释 您只为 SNMPv3 创建用户。这些步骤不适用于 SNMPv1 或 SNMPv2c。

请注意，SNMPv3 只支持只读用户。

SNMP 用户具有指定的用户名、身份验证密码、加密密码以及要使用的身份验证和加密算法。

注释 将 SNMPv3 用于群集或高可用性时，如果在初始群集形成后添加新的群集设备或更换高可用性设备，则 SNMPv3 用户不会复制到新设备。您必须删除用户、重新添加，然后重新部署配置，以强制用户复制到新单元。

身份验证算法选项

要成功进行 SNMPv3 用户身份验证，身份验证密钥大小应等于或大于加密密钥大小。例如，使用 SHA-1 和 AES256 进行的用户身份验证失败，而使用 SHA256 和 AES256 进行的身份验证成功。

版本	支持的算法		弃用的算法	
	身份验证	加密	身份验证	加密
< 6.4	MD5 和 SHA	DES、3DES、AES256、AES192 和 AES128	-	-
6.5	SHA	3DES、AES256、AES192 和 AES128	MD5*	DES**
6.6 和 6.7	SHA 和 SHA256	3DES、AES256、AES192 和 AES128	-	-
7.0+	SHA、SHA224、SHA256 和 SHA384	3DES、AES256、AES192 和 AES128	-	-

* 如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 Firewall Threat Defense 设备。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 防火墙管理中心 管理任何运行 7.0 以上版本的 Firewall Threat Defense 设备，则将使用 MD5 身份验证算法的平台设置策略部署到这些设备将失败。

** 如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 Firewall Threat Defense 设备。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 防火墙管理中心 管理任何运行版本 7.0+ 的 Firewall Threat Defense 设备，则将使用 DES 加密的平台设置策略部署到这些设备将会失败。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 请点击 **SNMP** > **用户 (Users)**。

步骤 3 点击**添加 (Add)**。

步骤 4 从**安全级别**下拉列表中选择用户的安全级别。

- **Auth** - 有身份验证但无隐私，意味着消息会进行身份验证。
- **No Auth** - 无身份验证且无隐私，意味着未对消息应用安全设置。
- **Priv** - 有身份验证且有隐私，意味着对消息进行身份验证和加密。

步骤 5 在**用户名**字段中输入 SNMP 用户的名字。用户名长度不得超过 32 个字符

步骤 6 在**加密密码类型**下拉列表中选择要使用的密码类型。

- **明文** - Firewall Threat Defense设备在部署到设备时仍将对密码进行加密。
- **加密** - Firewall Threat Defense设备将直接部署加密的密码。

步骤 7 在 **授权算法类型** 下拉列表中选择要使用的身份验证类型： SHA、 SHA224、 SHA256或 SHA384。

注释
MD5 选项已被弃用。如果您的部署包括使用 6.5 之前版本创建的使用 MD5 身份验证算法的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 FTD。但是，您无法编辑这些用户并保留 MD5 身份验证算法，或使用 MD5 身份验证算法创建新用户。如果您的 防火墙管理中心 管理任何运行 7.0 以上版本的 Firewall Threat Defense，则将使用 MD5 身份验证算法的平台设置策略部署到这些 Firewall Threat Defense将失败。

步骤 8 在**身份验证密码**字段中，输入用于身份验证的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。

注释
密码的长度将取决于所选的身份验证算法。对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 9 在**加密类型 (Encryption Type)** 下拉列表中，选择要使用的加密类型：AES128、AES192、AES256、3DES。

注释
要使用 AES 或 3DES 加密，必须在设备上安装相应的许可证。

注释
DES 选项已被弃用。如果您的部署包括使用 6.5 之前的版本创建的使用 DES 加密的 SNMP v3 用户，则可以继续将这些用户用于运行 6.7 及更低版本的 Firewall Threat Defense。但是，您不能编辑这些用户并保留 DES 加密，也不能使用 DES 加密创建新用户。如果您的 防火墙管理中心 管理任何运行版本 7.0+ 的 Firewall Threat Defense，则将使用 DES 加密的平台设置策略部署到这些 Firewall Threat Defense将会失败。

步骤 10 在**加密密码 (Encryption Password)** 字段中输入用于加密的密码。如果选择“加密为加密密码类型”，则密码必须格式化为 xx:xx:xx...，其中 xx 为十六进制值。对于加密的密码，密码的长度取决于所选的加密类型。密码大小如下（每个 xx 是一个八进制值）：

- AES 128 需要 16 个八进制值
- AES 192 需要 24 个八进制值

- AES 256 需要 32 个八进制值
- 3DES 需要 32 个八进制值
- DES 可以是任意大小

注释
对于所有密码，长度必须不能超过 256个字符。

如果选择“明文”作为“加密密码”类型，请在**确认**字段中重复该密码。

步骤 11 点击**确定**。

步骤 12 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

添加 SNMP 主机

使用“主机”(Host) 以在 SNMP 页面上的“SNMP 主机”(SNMP Hosts) 表中添加或编辑条目。这些条目表示允许访问 Firewall Threat Defense设备的 SNMP 管理站。

最多可以添加 8192 台主机。但是，其中仅 128 台可用于陷阱。

注释 在 7.4 及更高版本，管理和诊断接口已被合并。如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略（7.3 和更早版本，和某些升级后的 7.4 FTD）。

开始之前

确保存在定义 SNMP 管理站的网络对象。选择**设备** > **对象管理**以配置网络对象。

注释 支持的网络对象包括 IPv6 主机、IPv4 主机、IPv4 范围和 IPv4 子网地址。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 点击 **SNMP** > **主机 (Hosts)**。

步骤 3 点击**添加 (Add)**。

步骤 4 在 **IP 地址**字段中，输入有效的 IPv6 或 IPv4 主机或选择定义 SNMP 管理站主机地址的网络对象。

IP 地址可以是 IPv6 主机、IPv4 主机、IPv4 范围或 IPv4 子网。

步骤 5 从 **SNMP 版本**下拉列表中选择适当的 SNMP 版本。

步骤 6 （仅限 SNMPv3。）从**用户名**下拉列表中选择您配置的 SNMP 用户的用户名。

注释
每个 SNMP 主机最多可以关联 23 个 SNMP 用户。

步骤 7 （仅限 SNMPv1、2c。）在**读取社区字符串**字段中，输入已配置的社区字符串，以便对设备进行读取访问。重新输入该字符串以进行确认。

注释
仅当与此 SNMP 工作站一起使用的字符串与**启用 SNMP 服务器**部分中定义的字符串不同时，才需要此字符串。

步骤 8 选择设备与 SNMP 管理站之间的通信类型。您可以选择以下两种类型。

- **轮询** - 管理站会定期从设备请求信息。
- **陷阱** - 在发生陷阱事件时，设备将陷阱事件发送到管理站。

注释
当 SNMP 主机 IP 地址是 IPv4 范围或 IPv4 子网时，您可以配置**轮询**或**陷阱**，而不是同时配置两者。

步骤 9 在**端口**字段中，输入 SNMP 主机的 UDP 端口号。默认值为 162。有效范围为 1 至 65535。

步骤 10 在**访问方式 (Reachable By)** 选项下，选择设备与 SNMP 管理站之间通信的接口类型。您可以选择设备的管理接口或可用的安全区域/命名接口。

- **设备管理接口 (Device Management Interface)** - 设备和 SNMP 管理站之间通过管理接口进行通信。
  - 当您选择此接口进行 SNMPv3 轮询时，系统将允许所有已配置的 SNMPv3 用户进行轮询，而不限于 步骤 6，第 1004 页中选择的用户。此处，SNMPv3 主机不允许 SNMPv1 和 SNMPv2c。
  - 当您为 SNMPv1 和 SNMPv2c 轮询选择此接口时，轮询完全不受 步骤 5，第 1004 页中所选版本的限制。
- **安全区域或命名接口 (Security Zones or Named Interface)** - 设备和 SNMP 管理站之间通过安全区域或接口进行通信。
  - 在**可用区域 (Available Zones)** 字段中搜索区域。
  - 添加包含设备可通过其与管理站通信的接口的区域至 **选择的区域/接口 (Selected Zone/Interface)** 字段中。对于不在区域中的接口，您可以在**所选区域/接口 (Selected Zone/Interface)** 列表下方的字段中键入接口名称，然后点击**添加 (Add)**。您还可以添加环回接口 和虚拟路由器感知接口。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 11 点击**确定**。

步骤 12 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置 SNMP 陷阱

使用“SNMP 陷阱”为 Firewall Threat Defense 设备配置 SNMP 陷阱（事件通知）。 陷阱不同于浏览；它们是特定事件（例如上行链路、下行链路和系统日志事件）的从 Firewall Threat Defense设备到管理站的未经请求的“注释"。该设备的 SNMP 对象 ID (OID) 显示在从设备发送的 SNMP 事件陷阱中。

某些陷阱不适用于某些硬件型号。如果将策略应用于其中某个型号，则这些陷阱将被忽略。例如，并非所有型号都有可现场更换的设备，因此不会在这些型号上配置**现场可更换的设备插入/删除**陷阱。

SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 Firewall Threat Defense软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

从以下位置浏览思科 MIB、陷阱和 OID 的完整列表：

SNMP 对象导航器

此外，从以下位置通过 FTP 下载思科 OID：

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 使用 **SNMP** > **SNMP 陷阱** 为 Firewall Threat Defense 设备配置 SNMP 陷阱（事件通知）。

步骤 3 选择适当的“启用陷阱”选项。您可以选择其中任一或两个选项。

a) 选中**启用所有 SNMP 陷阱**可在随后的四个部分中快速选择所有陷阱。

b) 选中**启用所有系统日志陷阱**以启用与陷阱相关的系统日志消息的传输。

注释
SNMP 陷阱预计近乎是实时的，因此优先级高于 Firewall Threat Defense发出的其他通知消息。启用所有 SNMP 或系统日志陷阱时，SNMP 进程可能会消耗代理和网络中的过多资源，导致系统挂起。如果您发现系统延迟、未完成的请求或超，可以选择性地启用 SNMP 和系统日志陷阱。您也可以限制按严重性级别或消息 ID 生成系统日志消息的速率。例如，所有以数字 212 开头的系统日志消息 ID 都与 SNMP 类相关联。请参阅限制系统日志消息生成速率，第 1024 页。

步骤 4 默认情况下，为现有策略启用**标准**部分中的事件通知陷阱：

- **身份验证** - 未经授权的 SNMP 访问。对于具有不正确的社区字符串的数据包，将会出现此身份验证失败。

- **上行链路 (Link Up)** - 设备的一个通信链路已变为可用（已“出现"），如通知中所示。
- **下行链路 (Link Down)** - 设备的一个通信链路已出现故障，如通知中所示。
- **冷启动 (Cold Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现可能被更改。
- **热启动 (Warm Start)** - 设备正在重新初始化自身，以使其配置或协议实体实现不更改。

步骤 5 在**实体 MIB** 部分中选择所需的事件通知陷阱：

- **现场可更换设备插入** - 已插入现场可更换单元 (FRU)，如通知中所示。（FRU 包括电源、风扇、处理器模块、接口模块等组件）
- **现场可更换设备删除** - 已删除现场可更换单元 (FRU)，如通知中所示。
- **配置更改** - 已发生硬件更改，如通知中所示

步骤 6 在**资源**部分中选择所需的事件通知陷阱：

- **已达到连接限制** - 此陷阱指示连接尝试被拒绝，因为已达到配置的连接限制。

步骤 7 在**其他**部分中选择所需的事件通知陷阱：

- **NAT 数据包丢弃** - 此通知在 NAT 功能丢弃 IP 数据包时生成。可用的网络地址转换地址或端口已低于所配置的阈值。
- **CPU 上升阈值 (CPU Rising Threshold)** - 在配置的时间段内，当 CPU 使用率上升超过预定义阈值时，生成此通知。选中此选项可启用 CPU 上升阈值通知：
  - **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 10% 和 94% 之间。临界阈值硬编码为 95%。
  - **期间 (Period)** - 默认监控周期为 1 分钟；范围介于 1 到 60 分钟之间。
- **内存上升阈值 (Memory Rising Threshold)** - 当内存利用率上升超过预定义阈值时，会生成此通知，从而减少可用内存。选中此选项可启用内存上升阈值通知：
  - **百分比 (Percentage)** - 对于高阈值通知，默认值为 70%；范围介于 50% 和 95% 之间。
- **故障转移 (Failover)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告的故障转移状态发生变化时，生成此通知。
- **集群 (Cluster)** - 当 CISCO-UNIFIED-FIREWALL-MIB 报告集群运行状况发生变化时，生成此通知。
- **对等体摆动** - 当存在 BGP 路由摆动（即 BGP 系统发送过多的更新消息来通告网络可访问性信息）时，生成此通知。

步骤 8 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

SSL



注释 您必须具有管理员权限并在分叶域中才能执行此任务。

必须确保您运行的是 Secure Firewall Management Center的完全许可版本。如果是在评估模式下运行 Secure Firewall Management Center 时，“SSL 设置”将被禁用。此外，当许可的 Secure Firewall Management Center 版本不符合导出条件时，“SSL 设置”将被禁用。如果您使用的是带有 SSL 的远程访问 VPN，则您的智能帐户必须启用强加密功能。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的许可证类型和限制。

过程

步骤 1 选择 **设备** > **平台设置**，并创建或编辑身份策略。Firewall Threat Defense

步骤 2 选择 **SSL**。

步骤 3 将条目添加到**添加 SSL 配置**表中。

a) 点击**添加**以创建新条目，如果该条目已存在，则点击**编辑**。

b) 从下拉列表中选择所需的安全配置。

- **协议版本** - 指定在建立远程访问 VPN 会话时要使用的 TLS 协议。
- **安全级别** - 指示希望为 SSL 设置的安全定位类型。

步骤 4 根据您选择的协议版本选择**可用算法**，然后点击**添加**以针对所选协议包括这些算法。有关详细信息，请参阅关于 SSL 设置，第 1007 页。

这些算法根据您选择的协议版本列出。每个安全协议标识用于设置安全级别的唯一算法。

步骤 5 点击**确定** 以保存更改。

下一步做什么

选择 **部署** > **部署** 然后点击 **部署** 以将策略部署到所分配的设备。

关于 SSL 设置

Firewall Threat Defense设备使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 对来自远程客户端的远程访问 VPN 连接支持安全消息传输。通过 SSL 设置窗口，您可以配置在通过 SSL 远程 VPN 访问传输邮件过程中协商和使用的 SSL 版本和加密算法。

注释 虽然配置 防火墙管理中心 和 Firewall Threat Defense 以便在安全认证（UCAPL、CC 或 FIPS）合规性模式下运行，但 防火墙管理中心 允许配置不受支持的密码。例如，在启用 FIPS 的模式下，管理中心允许配置不符合 FIPS 的 DH 组 5。但是，由于使用了不合规的密码，VPN 隧道不会进行协商。

在以下位置配置 SSL 设置：

设备 > **平台设置**，然后点击 **SSL**。

字段

充当服务器时的最低 SSL 版本- 指定在充当服务器时， Firewall Threat Defense 设备使用的最低 SSL/TLS 协议版本。例如，用作远程访问 VPN 网关时。

TLS 版本—从下拉列表中选择以下 TLS 版本之一：

TLS V1	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。
TLSV1.1	接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。
TLSV1.2	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。
TLSv1.3	接受 SSLv2 客户端问候并协商 TLSv1.3（或更高版本）。

注释 远程访问 VPN 中的 TLS 1.3 需要 Cisco Secure Client 版本 5.0 及更高版本。

DTLS 版本—根据所选的 TLS 版本，从下拉列表中选择 DTLS 版本。默认情况下，DTLSv1 在 Firewall Threat Defense 设备上配置，您可以根据需要选择 DTLS 版本。

注释 确保 TLS 协议版本高于或等于所选的 DTLS 协议版本。TLS 协议版本支持以下 DTLS 版本：

TLS V1	DTLSv1
TLSV1.1	DTLSv1
TLSV1.2	DTLSv1、DTLSv1.2
TLSv1.3	DTLSv1、DTLSv1.2

Diffie-Hellman 组—从下拉列表中选择一个组。可用选项为 Group1 - 768 位模数、Group2 - 1024 位模数、Group5 - 1536 位模数、Group14 - 2048 位模数、224 位素数阶和 Group24 - 2048 位模数、256 位素数阶。默认值为 Group1。

椭圆曲线 Diffie-Hellman 组 - 从下拉列表中选择一个组。可用选项为 Group19 - 256 位 EC、Group20 - 384 位 EC 和 Group21 - 521 位 EC。默认值为 Group19。

TLSv1.2 增加了对以下密码的支持：

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256



注释 ECDSA 和 DHE 密码具有最高优先级。

TLSv1.3 增加了对以下密码的支持：

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

SSL 配置表可用于指定要在 Cisco Secure Firewall Threat Defense设备上支持的协议版本、安全级别和密码算法。

协议版本 - 列出 Cisco Secure Firewall Threat Defense设备支持和用于 SSL 连接的协议版本。可用的协议版本有：

- 默认
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSv1.3
- DTLSv1

- DTLSv1.2

安全级别—列出 Firewall Threat Defense设备支持和用于 SSL 连接的加密安全级别。

如果您的 Firewall Threat Defense 设备具有评估许可证，默认情况下安全级别为“低”。使用 Firewall Threat Defense 智能许可证时，默认安全级别为“高”。您可以选择以下选项之一来配置所需的安全级别：

- **All** 包括 NULL-SHA 等所有密码。
- **Low** 包括除 NULL-SHA 之外的所有密码。
- **Medium** 包括所有密码，但 NULL-SHA、DES-CBC-SHA、RC4-SHA 和 RC4-MD5（这是默认密码）除外。
- **Fips** 包括所有符合 FIPS 的密码，但 NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA、TLS_CHACHA20_POLY1305_SHA256 除外。
- **High** 只包含带有 SHA-2 加密的 AES-256，并适用于 TLS 版本 1.2 和默认版本。
- **Custom** 包括您在 Cipher algorithms/custom string 框中指定的一个或多个密码。此选项使您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。

密码算法/自定义字符串- 列出 Firewall Threat Defense 设备支持和用于 SSL 连接的加密算法。有关使用 OpenSSL 的密码的详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html

仅受 TLSv1.2 支持的密码

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256

DHE-RSA-AES128-SHA256
AES128-SHA256

注释 ECDSA 和 DHE 密码具有最高优先级。

TLSv1.1 或 TLSv1.2 不支持的密码

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

系统日志

您可以为 Firewall Threat Defense设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。您还可以将一些安全事件发送到系统日志服务器。以下主题介绍日志记录以及如何配置日志记录。

关于系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

表 *74: ...*的系统日志 *Cisco Secure Firewall Threat Defense*

与以下各项相关的日志	详细信息	配置位置
设备和系统运行状况、网络配置	此系统日志配置可为在数据平面上运行的功能（即在 CLI 配置中定义的功能，可以使用 **show running-config** 命令查看这些功能）生成消息。这包括诸如路由、VPN、数据接口、DHCP 服务器、NAT 等功能。数据平面系统日志消息将被编号，并且这些消息与运行 ASA 软件的设备所生成的那些消息相同。但是，Cisco Secure Firewall Threat Defense不一定会生成每种可用于 ASA 软件的消息类型。有关这些消息的信息，请参阅思科 *Cisco Secure Firewall Threat Defense*系统日志消息，网址为：https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html。此配置将在以下主题中加以说明。	平台设置

与以下各项相关的日志	详细信息	配置位置
安全事件	此系统日志配置会生成文件和恶意软件、连接、安全智能和入侵事件的警报。有关详细信息，请参阅关于发送安全事件的系统日志消息和*Cisco Secure Firewall Management Center* 管理指南中的子主题。	访问控制策略中的**平台设置**和**日志记录**
（所有设备） 策略、规则和事件	此系统日志配置将为访问控制规则、入侵规则和中所述的其他高级服务生成警报，如*Cisco Secure Firewall Management Center* 管理指南中的配置支持警报响应所述。这些消息不会被编号。有关配置这种类型的系统日志的信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的创建系统日志警报响应。	访问控制策略中的**警报响应**和**日志记录**

可以配置多个系统日志服务器，并可控制发送到每个服务器的消息和事件。还可配置不同目标，如控制台、邮件、内部缓冲区等。

严重性级别

下表列出系统日志消息严重性级别。

表 *75:* 系统日志消息严重级别

级别号	严重性级别	说明
0	**应急**	系统不可用。
1	**警报**	需要立即采取措施。
2	**严重**	严重情况。
3	**错误**	错误情况。
4	**警告**	警告情况。
5	**通知**	正常但重大的情况。
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 Firewall Threat Defense不会生成严重性级别为零（紧急）的系统日志消息。

要优化设备存储空间，您可以选择最小日志记录，即仅记录通知及以上级别的消息。这会减少各种系统日志文件中的日志记录数量。最小日志记录设置不影响事件日志记录；访问控制策略的日志记录不受影响。可以使用 CLI 命令管理日志记录级别。有关详细信息，请参阅 系统支持日志记录 命令，详见 *Cisco Secure Firewall Threat Defense 命令参考* 指南。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，您可以将 Firewall 威胁防御设备 配置为将所有系统日志消息发送至一个输出目标，而将这些系统日志消息中的一部分发送至其他输出目标。

具体而言，您可以根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

- 系统日志消息严重性级别
- 系统日志消息类（相当于一个功能区）

  （这不适用于连接和入侵事件等安全事件的系统日志消息。）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，可以将 Firewall 威胁防御设备 配置为将一个特定的消息类发送至每种类型的输出目标，而不管消息列表是什么。

（消息列表不适用于连接和入侵事件等安全事件的系统日志消息。）

系统日志消息类

注释 此主题不适用于安全事件（连接、入侵等）的消息。

可以通过两种方法使用系统日志消息类：

- 指定整个类别的系统日志消息的输出位置。
- 创建指定消息类的消息列表。

系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，RIP 类表示 RIP 路由。

特定类中的所有系统日志消息共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成系统日志消息时对象未知，则不显示特定的 heading = value 组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

下表列出消息类以及每个类中的消息 ID 范围。

表 *76:* 系统日志消息类和关联的消息 *ID* 号

类别	定义	系统日志消息 ID 号
access-list*	访问列表	106
application-firewall*	应用防火墙	415
auth	用户身份验证	109、113
botnet-traffic-filtering*	僵尸网络流量筛选	338
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
card-management*	卡管理	323
citrix	Citrix Client	723
clustering*	集群	747
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
environment-monitoring*	环境监控	735
ha	故障转移	101、102、103、104、105、210、311、709
identity-based-firewall*	基于身份认证的防火墙	746
ids	入侵检测系统	400、733

类别	定义	系统日志消息 ID 号
ikev2-toolkit*	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	400、401、420
ipv6*	IPv6	325
licensing*	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
nat-and-pat*	NAT 与 PAT	305
network-access-point*	网络无线接入点	713
np	网络处理器	319
np-ssl*	NP SSL	725
ospf	OSPF 路由	318、409、503、613
password-encryption*	密码加密	742
phone-proxy*	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
scansafe*	ScanSafe	775
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
smart-call-home*	Smart Call Home	120
snmp	SNMP	212
ssl	SSL 堆栈	725

类别	定义	系统日志消息 ID 号
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
tag-switching	服务标记交换	779
threat-detection*	威胁检测	733
transactional-rule-engine-tre*	事务规则引擎	780
uc-ims*	UC-IMS	339
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障转移	720
vpnlb	VPN 负载均衡	718
vxlan*	VXLAN	778
webfo	WebVPN 故障转移	721
webvpn	WebVPN 和 Secure Client	716

*这些类在管理中心 Web 界面中进行调配，以便于创建事件列表。这些类不会显示在设备控制台上。

日志记录准则

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 准则

- 支持 IPv6。可以使用 TCP 或 UDP 发送系统日志。
- 确保配置用于发送系统日志的接口已经启用，支持 IPv6，并且可以通过指定接口到达系统日志服务器。
- 不支持通过 IPv6 进行安全登录。

其他准则

- 请勿配置 防火墙管理中心 为主系统日志服务器。 防火墙管理中心 可以记录一些系统日志。但是，它没有足够的存储调配来容纳来自每个传感器的连接事件的大量信息，尤其是在使用多个传感器并且都发送系统日志时。
- Firewall Threat Defense 系统日志支持单向 TLS 以确保日志安全。它不支持客户端证书身份验证、系统日志信任点配置或双向 TLS（X.509 证书）。
- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows 提供了一个系统日志服务器，作为其操作系统的组成部分。
- 系统日志服务器基于防火墙系统的 syslog-ng 进程运行。请勿使用外部配置文件，例如 SecureWorks 的 *scwx.conf* 文件。此类文件与设备不兼容。使用它们将导致解析错误，最终 syslog-ng 进程将失败。
- 系统日志确定出口接口
  - 如果指定的仅管理接口已启用管理访问，则管理中心将执行路由表查找，并根据最佳路由逻辑确定出口接口（可以是数据接口，也可以是管理接口）。
  - 如果将未启用管理访问的管理专用接口配置为日志记录主机，则管理中心将使用该接口，而不考虑路由表条目。

    因此，要使管理中心始终对系统日志流量使用专用管理路径，请配置没有 management-access 的管理接口，然后在日志记录主机中指定接口：

    ```
    interface <management-interface>
    management-only ----->Do not include management-access

    logging host <management-interface> <syslog-server-ip>
    ```

- 当系统日志速率超过每秒 50,000 条消息时，请确保将数据接口而不是管理接口用作出口接口。
- 要查看由 Firewall 威胁防御设备 生成的日志，必须指定日志记录输出目标。如果启用日志记录而未指定日志记录输出目标，则 Firewall 威胁防御设备 会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。
- 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。
- 不能将两个不同的列表或类分配给不同的系统日志服务器或相同位置。
- 您最多可以配置 16 个系统日志服务器。
- 应该可以通过 Firewall 威胁防御设备 到达系统日志服务器。应将该设备配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制系统日志 313001、313004 和 313005 的生成。
- 用于系统日志的 UDP 连接数与硬件平台上的 CPU 数量和您配置的系统日志服务器数量直接相关。在任何时刻，UDP 系统日志连接的数量都等于 CPU 数量乘以已配置的系统日志服务器数量

的积。这是预期行为。请注意，全局 UDP 连接空闲超时适用于这些会话，默认值为 2 分钟。如果您想更快关闭这些会话，可以调整该设置，但超时适用于所有 UDP 连接，而不仅是系统日志。

- 当 Firewall 威胁防御设备 通过 TCP 发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。
- 当 TCP 日志记录主机关闭时，其连接状态从“已 连接”*(Connected)* 更改为 “未连接”*(Not connected)*需要大约 6 分钟。日志记录依赖 TCP 检测通道状态；在此之前，日志记录通过通道发送日志。在此期间，当您执行 **show log**时，输出会将 TCP 日志记录主机显示为已连接。TCP 通道关闭后，TCP 日志记录主机状态将更新为 未连接。
- 将数据接口配置为生产监控和审计用的系统日志源接口。仅将管理接口用于临时测试。此方法可确保最佳系统日志可靠性，并避免管理接口受速率限制影响。

配置 Firewall Threat Defense 设备的系统日志日志记录

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 Firewall Threat Defense 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

要配置系统日志设置，请执行以下步骤：

开始之前

请参阅日志记录准则，第 1016 页中的要求。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 从目录中选择**系统日志**。

步骤 3 点击**日志记录设置 (Logging Setup)** 以启用日志记录，指定 FTP 服务器设置，并指定闪存用法。有关详细信息，请参阅启用日志记录并配置基本设置，第 1019 页

步骤 4 点击**日志记录目标 (Logging Destinations)** 可以启用对特定目标的日志记录，并指定对邮件严重性级别、事件类或自定义事件列表的过滤。有关详细信息，请参阅启用日志记录目标，第 1021 页

必须启用日志记录目标才能查看该目标的消息。

步骤 5 点击**邮件设置 (E-mail Setup)** 以指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。有关详细信息，请参阅将系统日志消息发送给邮件消息，第 1022 页

步骤 6 点击**事件列表 (Events List)** 可定义包括事件类、严重性级别和事件 ID 的自定义事件列表。有关详细信息，请参阅创建自定义事件列表，第 1023 页

步骤 7 点击**速率限制 (Rate Limit)** 可指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。有关详细信息，请参阅限制系统日志消息生成速率，第 1024 页

步骤 8 点击**系统日志设置 (Syslog Settings)** 以指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。有关详细信息，请参阅配置系统日志设置，第 1025 页

步骤 9 点击**系统日志服务器 (Syslog Servers)** 以便为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。有关详细信息，请参阅配置系统日志服务器，第 1026 页。

适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置

“安全事件”包括连接、安全智能、入侵以及文件和恶意软件事件。

在**系统日志**页面（**设备** > **平台设置**，编辑威胁防御策略，然后点击**系统日志**）及其选项卡上配置的某些系统日志设置适用于安全事件的系统日志消息，但大多数只适用于与系统运行状况和网络有关的事件的信息。

以下设置适用于安全事件的系统日志消息：

- **日志记录设置**选项卡：
  - **发送 EMBLEM 格式的系统日志**
- **系统日志设置**选项卡：
  - **在系统日志消息中启用时间戳**
  - **时间戳格式**
  - **启用系统日志设备 ID**
- **系统日志服务器**选项卡：
  - **添加系统日志服务器**表单 （以及已配置的服务器列表） 上的所有选项。

启用日志记录并配置基本设置

启用日志记录并配置基本设置，以便系统为数据平面事件生成系统日志消息。您还可以将闪存或FTP服务器上的存档设置为本地缓冲区已满时使用的存储位置。您可以在保存日志记录数据后对其进行操作。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

下面的过程介绍了一些基本系统日志设置。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 Firewall Threat Defense 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**系统日志** > **日志记录设置**。

步骤 3 启用日志记录并配置基本日志记录设置。

- **启用日志记录 (Enable Logging)** - 为 Firewall Threat Defense设备启用数据平面系统日志记录。
- **在故障转移备用设备上启用日志记录** - 为 Firewall Threat Defense设备的备用设备（如果有）启用日志记录。
- **以 EMBLEM 格式发送系统日志** - 为每个日志记录目标启用 EMBLEM 格式日志记录。如果启用 EMBLEM，必须使用 UDP 协议来发布系统日志消息，EMBLEM 与 TCP 不兼容。

  EMBLEM 系统日志格式是基于 RFC 3164 和 RFC 5424 标准构建的思科特定约定。因此，当启用 EMBLEM 时，系统日志消息会在 <PRI> 字段后打印冒号 (:)，这与 RFC 5424 格式不同。

  注释
  RFC5424 格式的系统日志消息通常显示优先级值（PRI）。但是，在 防火墙管理中心中，只有当您启用 Cisco EMBLEM 格式的日志记录时，才会显示托管 Firewall Threat Defense 的系统日志消息中的 PRI 值。此外，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。

- **发送调试消息作为系统日志** - 将所有调试跟踪输出重定向到系统日志。如果启用了此选项，则控制台中不会显示系统日志消息。因此，要查看调试消息，必须在控制台上启用日志记录并将其配置为调试系统日志消息编号和日志记录级别的目标。使用的系统日志消息编号是 711001。此系统日志的默认日志记录级别为调试。
- **内部缓冲区的内存大小** - 指定在启用了日志记录缓冲区的情况下，将系统日志消息保存到的内部缓冲区的大小。当缓冲区填满时，它将被覆盖。默认值为 4096 字节。范围为 4096 到 52428800。

步骤 4 (可选）配置将系统日志消息记录到 防火墙管理中心。

a) 点击**所有日志 (All Logs)** 单选按钮启用记录所有与所选严重性级别对应的故障诊断系统日志信息，或点击 **VPN 日志 (VPN Logs)** 单选按钮仅启用记录与所选严重性级别对应的 VPN 故障诊断信息。

b) 从**日志记录级别 (Logging Level)** 下拉列表中选择日志记录消息的系统日志严重性级别。

- **所有日志 (All Logs)** 的日志记录级别默认设置为**严重**。您可以选择将严重性级别为**严重**、**警报**或**紧急情况**的系统日志消息发送到 防火墙管理中心。
- VPN 消息的日志记录级别默认设置为**错误**。

  VPN 故障排除系统日志可能会在 防火墙管理中心上增加过多的负载。因此，请谨慎使用此选项。此外，只要您配置了具有站点间或远程访问 VPN 的设备，它就会默认自动启用将 VPN 系统日志发送至管理中心。我们建议您将日志记录级别限制为 **错误** 及以上，以限制系统日志过多地流向 防火墙管理中心，尤其是在涉及多个设备的 RAVPN 的情况下。

有关级别的信息，请参阅严重性级别 ，第 1012 页。

步骤 5 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到 FTP 服务器，请配置该服务器。指定 FTP 服务器信息。

- **FTP 服务器缓冲区回绕 (FTP Server Buffer Wrap)** - 要在缓冲区内容被覆盖之前将其保存到 FTP 服务器，请选中此框并在以下字段中输入必要的目标信息。要删除 FTP 配置，请取消选择此选项。
- **IP 地址** - 选择包含 FTP 服务器 IP 地址的主机网络对象。
- **用户名 (User Name)** - 输入连接到 FTP 服务器时要使用的用户名。
- **路径** - 输入相对于 FTP 根目录的路径，缓冲区内容应保存在此处。
- **密码/确认 (Password/ Confirm)** - 输入并确认用于对访问 FTP 服务器的用户名进行身份验证的密码。

步骤 6 （可选）如果要在覆盖缓冲区之前将日志缓冲区内容保存到闪存，请指定闪存大小。

- **闪存** - 要在缓冲区内容被覆盖之前将其保存到闪存，请选中此框。
- **日志记录所使用的最大闪存大小 (KB) (Maximum flash to be used by logging [KB])** - 指定用于日志记录的闪存所使用的最大空间（以 KB 为单位）。范围为 4 至 8044176 千字节。
- **要保留的最小可用空间 (KB)** - 指定要在闪存中保留的最小可用空间（以 KB 为单位）。范围为 0 至 8044176 千字节。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

启用日志记录目标

必须启用日志记录目标才能查看该目标的消息。启用目标时，还必须为该目标指定消息过滤器。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**系统日志** > **日志记录目标**。

步骤 3 点击**添加**以启用目标并应用日志记录过滤器，或编辑现有目标。

步骤 4 在**日志记录目标**对话框中，选择目标并配置用于目标的过滤器：

a) 在**日志记录目标**下拉列表中，选择要启用的目标。您可以为每个目标创建一个过滤器：控制台、邮件、内部缓冲区、SNMP 陷阱、SSH 会话和系统日志服务器。

注释

控制台和 SSH 会话日志记录只有在诊断 CLI 中工作。输入 **system support diagnostic-cli**。

b) 在**事件类**中，选择将应用于表中未列出的所有类的过滤器。

您可以配置这些过滤器：

- **基于严重性过滤** - 选择严重性级别。此级别或更高级别的消息将会发送到目标
- **使用事件列表** - 选择定义过滤器的事件列表。在**事件列表 (Event Lists)** 页面上创建这些列表。
- **禁用日志记录** - 阻止消息发送到此目标。

c) 如果要为每个事件类创建过滤器，请点击**添加**以创建新过滤器，或编辑现有过滤器，然后选择事件类和严重性级别以限制该类中的消息。点击**确定 (OK)** 以保存过滤器。

有关事件类的说明，请参阅系统日志消息类，第 1013 页。

d) 点击**确定 (OK)**。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

将系统日志消息发送给邮件消息

您可以设置以邮件形式发送的系统日志消息收件人列表。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

开始之前

- 在 SMTP 服务器平台设置页面上配置 SMTP 服务器
- 启用日志记录并配置基本设置，第 1019 页
- 将邮件设置为日志记录目标

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**系统日志** > **邮件设置**。

步骤 3 指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。

步骤 4 点击 **Add** 以输入指定的系统日志消息的新邮件地址收件人。

步骤 5 从下拉列表中选择发送给收件人的系统日志消息的严重性级别。

用于目标邮件地址的系统日志消息严重性过滤器会导致发送指定严重性级别和更高严重性级别的消息。有关级别的信息，请参阅严重性级别，第 1012 页。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

创建自定义事件列表

事件列表是一个自定义筛选器，您可以将其应用于日志记录目标，以控制将哪些消息发送到目标。通常，只根据严重性来筛选目标消息，但可以使用事件列表根据事件类、严重性和消息标识符 (ID) 组合进一步控制要发送的消息。

创建自定义事件列表分为两步。在**事件列表 (Event Lists)** 中创建自定义列表，然后使用事件列表在**日志记录目标 (Logging Destinations)** 中为各种类型的目标定义日志记录筛选。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数 FTD 平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**系统日志** > **事件列表**。

步骤 3 配置事件列表。

a) 点击**添加**以添加新列表或编辑现有列表。

b) 在**名称**字段中输入事件列表的名称。不允许使用空格。

c) 要根据严重性或事件类来标识消息，请选择**严重性/事件类**选项卡，并添加或编辑条目。

有关可用类的信息，请参阅系统日志消息类，第 1013 页。

有关级别的信息，请参阅严重性级别，第 1012 页。

某些事件类在透明模式下不适用于该设备。如果配置了此类选项，将绕过这些选项，不予以部署。

d) 若要通过消息 ID 明确标识消息，请选择**消息 ID (Message ID)**，并添加或编辑 ID。

您可以使用连字符输入 ID 范围，例如 100000-200000。ID 是六位数字。有关初始三位数字如何映射到功能的信息，请参阅系统日志消息类，第 1013 页。

有关特定的消息编号，请参阅 Cisco ASA 系列日志消息。

e) 点击**确定**保存事件列表。

步骤 4 点击**日志记录目标 (Logging Destinations)**，然后添加或编辑应使用过滤器的目标。

请参阅启用日志记录目标，第 1021 页。

步骤 5 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

限制系统日志消息生成速率

您可以限制按严重性级别或消息ID生成系统日志消息的速率。您可以为每个日志记录级别和每个系统日志消息 ID 指定单独的限制。如果设置冲突，则会优先考虑系统日志消息 ID 限制。

提示 如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则大多数FTD平台设置不适用于这些消息。请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**系统日志** > **速率限制**。

步骤 3 要按严重性级别限制邮件生成，请点击**日志记录级别 (Logging Level)** > **添加 (Add)**，然后配置以下选项：

- **日志记录级别** - 您要限制速率的严重性级别。有关级别的信息，请参阅严重性级别，第 1012 页。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 4 点击**确定 (OK)**。

步骤 5 要按系统日志消息 ID 限制邮件生成，请点击**系统日志级别 (Syslog Level)** > **添加 (Add)**，然后配置以下选项：

- **系统日志 ID** - 您要限制速率的系统日志消息 ID。有关特定消息编号，请参阅思科 ASA 系列系统日志消息。
- **消息数** - 在指定时间段内允许的指定类型的最大消息数。
- **间隔** - 在速率限制计数器重置之前的秒数。

步骤 6 点击**确定**。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

配置系统日志设置

可以配置一般系统日志设置，以设置要包括在将被发送到系统日志服务器的系统日志消息中的设备代码；指定是否在每条消息中包括时间戳；指定是否将设备ID包括在消息中；查看和修改消息的严重性级别；以及禁用特定消息的生成。

如果要配置设备以发送有关安全事件（例如连接和入侵事件）的系统日志消息，则此页面上的某些设置不适用于这些消息。也请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 适用于安全事件系统日志消息的威胁防御平台设置 。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 依次选择**系统日志** > **系统日志设置**。

步骤 3 在**设备**下拉列表中为系统日志服务器选择要用作文件消息基础的系统日志设备。

默认值为大多数 UNIX 系统期望的 LOCAL4(20)。但是，由于网络设备共享可用设施，因此可能需要为系统日志更改此值。

设施值通常与安全事件无关。如果需要在消息中包含设施值，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 安全事件系统日志消息中的设施。

步骤 4 选中**在每个系统日志消息上启用时间戳**复选框, 以包括在系统日志消息中生成消息的日期和时间。

步骤 5 选择系统日志消息的**时间戳格式**：

- 传统 (MMM dd yyyy HH:mm:ss) 格式为系统日志消息的默认格式。

  选择此时间戳格式时，消息不会指示时区，该时区始终为 UTC。

- RFC 5424 (yyyy-MM-ddTHH:mm:ssZ) 使用 RFC 5424 系统日志格式中指定的 ISO 8601 时间戳格式。

  如果选择RFC 5424格式，则会在每个时间戳的末尾附加“Z”，以指示时间戳使用UTC时区。

步骤 6 如果希望向系统日志消息添加设备标识符（它将被放置在消息的开头），则请选中**启用系统日志设备 ID** 复选框，然后选择 ID 的类型。

- **接口** - 使用所选接口的 IP 地址，无论设备通过哪个接口发送消息。选择标识接口的安全区。该区域必须映射到某一接口。
- **用户定义的 ID** - 使用所选的文本字符串（最多 16 个字符）。
- **主机名** - 使用设备的主机名。

步骤 7 使用“系统日志消息”表来更改特定系统日志消息的默认设置。仅当希望更改默认设置时，才需要此表中的配置规则。可以更改分配给消息的严重性，或者可以禁用消息的生成。

默认情况下，将启用 Netflow，并在表中显示条目。

a) 要抑制因 Netflow 而冗余的系统日志消息，请选择 **Netflow 等效系统日志**。

这会将消息作为受抑制的消息添加到该表中。

注释
如果其中任何等效系统日志已经位于该表中，则不会覆盖现有规则。

b) 要添加新规则，请点击**添加 (Add)**。

c) 如果希望更改所选消息编号的配置，则请进入**系统日志 ID** 下拉列表，然后从**日志记录级别**下拉列表中选择新的严重性级别，或者选择**已抑制**以禁用消息的生成。通常不会更改严重性级别并禁用消息，但如果需要，可以对这两个字段进行更改。

d) 点击**确定 (OK)** 以将规则添加到该表中。

步骤 8 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置系统日志服务器

要配置系统日志服务器，以处理您的系统生成的消息，请执行以下步骤。

如果您希望此系统日志服务器接收连接和入侵事件等安全事件，另请参阅适用于安全事件系统日志消息的 Firewall Threat Defense 平台设置，第 1019 页。

注释 在 7.4 及更高版本，管理和诊断接口已被合并。如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略（7.3 和更早版本，和某些升级后的 7.4 Firewall Threat Defense）。

开始之前

- 请参阅日志记录准则，第 1016 页中的要求。
- 请确保您的设备可以通过网络访问您的系统日志收集器。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 依次选择**系统日志** > **系统日志服务器**。

步骤 3 如果任何使用TCP协议的系统日志服务器关闭，则请选中**在系统日志服务器关闭时允许用户流量传递（推荐）** 复选框，以允许流量。

注释

- 默认情况下，此选项已启用。除非需要，否则当设备无法访问外部 TCP 系统日志服务器时，我们建议您允许通过 威胁防御设备 设备进行连接。
- 在 防火墙管理中心 版本 6.2.x 或更低版本中禁用 **TCP 系统日志服务器关闭时，允许用户流量通过** 选项时，即使在升级到版本 6.3 或更高版本后，它仍将处于禁用状态。确保手动启用它。
- 在禁用此选项的情况下，当设备中配置了多个TCP系统日志服务器时，如果 威胁防御设备可访问至少一个服务器，则允许用户流量通过。因此，仅当设备中配置的 TCP 系统日志服务器都不可达时，才会应用禁用选项。设备会生成以下系统日志，描述通过设备的流量被拒绝的根本原因：

```
%FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New connections
are denied based on logging permit-hostdown policy
```

步骤 4 在**消息队列大小（消息）(Message queue size [messages])** 字段中输入当系统日志服务器繁忙时安全应用上用于存储系统日志消息的队列的大小。最小值为 1 条消息。默认值为 512。指定 0 可允许不限数量的消息排队（受可用块内存约束）。

当消息超过配置的队列大小时，它们会被丢弃并导致系统日志丢失。要确定理想的队列大小，您需要确定可用的块内存。使用**show blocks**命令了解当前内存使用率。有关命令及其属性的详细信息，请参阅《*Cisco Secure Firewall ASA* 系列命令参考指南》。如需进一步帮助，请与思科 TAC 联系。

步骤 5 点击**添加 (Add)** 以添加新系统日志服务器。

a) 在 **IP 地址**下拉列表中，选择包含系统日志服务器 IP 地址的网络主机对象。

b) 选择协议（TCP 或 UDP），然后输入用于 Firewall Threat Defense设备与系统日志服务器之间通信的端口号。

UDP 比 TCP 更快，并且在设备上使用的资源更少。

默认 UDP 端口为 514。您必须为 TCP 手动配置端口 1470。任一协议的有效非默认端口值为 1025 至 65535。

c) 选中 **Log messages in Cisco EMBLEM format (UDP only)** 复选框以指定是否记录思科 EMBLEM 格式的消息（仅在选择 UDP 作为协议的情况下才可用）。

EMBLEM 系统日志格式是基于 RFC 3164 和 RFC 5424 标准构建的思科特定约定。因此，在启用 EMBLEM 时，系统日志消息会在<PRI>字段中输入密码。

注释

RFC5424格式的系统日志消息通常显示优先级值（PRI）。但是，在防火墙管理中心中，只有当您启用 Cisco EMBLEM 格式的日志记录时，才会显示托管 Firewall Threat Defense 的系统日志消息中的 PRI 值。此外，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。

d) 选中**启用安全系统日志**复选框，以使用SSL/TLS over TCP对设备与服务器之间的连接进行加密。

注释

要使用此选项，必须选择 TCP 及其端口值（介于 1025 和 65535 之间）。还必须在 **设备** > **证书** 页面上上传与系统日志服务器通信所需的证书。最后，将该证书从 Firewall Threat Defense设备上传到系统日志服务器，以完成安全关系，并允许其对流量进行解密。设备管理界面不支持 **启用安全系统日志** 选项。

e) 选择**设备管理接口**或**安全区域或指定接口**，以与系统日志服务器通信。

- **设备管理接口**：从管理接口发送系统日志。 我们建议您在配置 Snort 事件的系统日志时使用此选项。

  注释
  设备管理界面 选项不支持 **启用安全系统日志** 选项。

- **安全区域或指定接口 (Security Zones or Named Interfaces)**：从**可用区域 (Available Zones)** 列表中选择接口，然后点击**添加 (Add)**。您还可以添加虚拟路由器感知接口。

  重要事项
  Firewall Threat Defense 数据平面 (Lina) 系统日志消息无法通过诊断接口发出。配置其他接口或管理接口 (Br1/Management0)，以发出数据平面系统日志消息。

f) 点击**确定**。

步骤 6 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

超时

可以设置各种协议的连接和转换插槽的全局空闲超时持续时间。如果插槽在指定的空闲时间内未使用，资源将返回到空闲池。

还可以为设备的控制台会话设置超时。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**超时**。

步骤 3 配置要更改的超时。

对于任何给定的设置，请选择**自定义**来定义您自己的值，选择**默认**将恢复系统默认值。在大多数情况下，最大超时为 1193 小时。

您可以通过选择**禁用**来禁用某些超时。

- **控制台超时** - 关闭到控制台的连接之前的空闲时间，范围为0 或 5 到 1440 分钟。默认超时时间为 0，表示会话不会超时。如果更改该值，现有的控制台会话将使用原来的超时值。新值仅适用于新连接。
- **转换插槽** - NAT 转换插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **连接** - 连接插槽释放前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 1 小时。
- **半封闭** - TCP 半闭合连接关闭前的空闲时间。如果同时收到 FIN 和 FIN-ACK，则连接会被认为是半关闭的。如果只看到了 FIN，则常规连接超时适用。最小值为 30 秒。默认值为 10 分钟。
- **UDP** - UDP 连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **ICMP** - 通用 ICMP 状态关闭前的空闲时间。默认值（及最小值）是 2 秒。
- **RPC/Sun RPC** - SunRPC 插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。

  在基于 Sun RPC 的连接中，当父连接被删除或出现超时时，新的子连接可能不会被视为父-子连接的一部分，因此可以根据策略或系统中设置的规则来评估新的连接。父连接超时后，现有的子连接仅在达到超时值集之前有效。
- **H.225** - H.225 信令连接关闭前的空闲时间。默认值为 1 小时。若要在清除所有调用后立即关闭连接，建议使用超时值 1 秒 (0:0:1)。
- **H.323** - TH.245 (TCP) 和 H.323 (UDP) 媒体连接关闭前的空闲时间。默认值（和最小值）为 5 分钟。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323（RTP 和 RTCP）媒体连接共享空闲超时。
- **SIP** - SIP 信令端口连接关闭前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 30 分钟。
- **SIP 媒体** - SIP 媒体端口连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
- **SIP 断开连接** - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，SIP 会话删除之前的空闲时间，该值介于 0:0:1 至 00:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **SIP 邀请** - PROVISIONAL 响应和媒体转换的针孔关闭前的空闲时间，该值介于 0:1:0 至 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **SIP 临时媒体** - SIP 临时媒体连接的超时值，该值介于 1 至 30 分钟之间。默认值为 2 分钟。
- **Floating Connection** - 当某个网络存在具有不同指标的多个路由时，系统会使用连接创建时指标最佳的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。此计时器不适用于通过虚拟隧道接口 (VTI) 的连接。如果通过 VTI 的连接卡住，您必须手动将其清除。

- **Xlate PAT** - PAT 转换插槽释放前的空闲时间，该值介于 0:0:30 至 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。
- **TCP 代理重组** - 等待重组的缓冲数据包丢弃前的空闲时间，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
- **ARP 超时**-ARP 表重建之间的秒数，从 60 到 4294967。默认值为 14,400 秒（4 小时）。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

时间同步

使用网络时间协议 (NTP) 服务器同步设备上的时钟设置。建议您将 防火墙管理中心 托管的所有 Firewall Threat Defense 配置为使用同一台 NTP 服务器作为 防火墙管理中心。Firewall Threat Defense 直接从配置的NTP服务器获取时间。如果 Firewall Threat Defense 配置的NTP服务器由于任何原因无法访问，则会与 防火墙管理中心 同步时间。

设备支持 NTPv4。



注释 如果要在 Firepower 4100/9300 机箱上部署 Firewall Threat Defense，则必须在 Firepower 4100/9300 机箱上配置NTP，以便智能许可正常运行，并确保设备注册采用正确的时间戳。对于Firepower 4100/9300 机箱和 防火墙管理中心，应使用相同的 NTP 服务器。

开始之前

- 如果您的组织有一个或多个 Firewall Threat Defense 可访问的 NTP 服务器，请为您的设备使用与您在 防火墙管理中心 上的 **管理** > **配置** 页面的“时间同步”中配置的相同 NTP 服务器。
- 如果您选择了**仅当为配置 NTP 服务器**防火墙管理中心时使用仅通过身份验证的 NTP 服务器防火墙管理中心，则对于您的设备，仅使用配置为通过进行身份验证的NTP服务器。（托管设备将使用与 防火墙管理中心 相同的 NTP 服务器，但其 NTP 连接将不使用身份验证。）
- 如果您的设备无法访问 NTP 服务器或您的组织没有 NTP 服务器，则必须使用以下程序中讨论的**通过管理中心通过 NTP** 选项。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**时间同步 (Time Synchronization)**。

步骤 3 配置以下时钟选项之一：

- **通过 NTP从管理中心：**（默认）。托管设备从为 防火墙管理中心 配置的 NTP 服务器（经过身份验证的NTP 服务器除外）获取时间，并直接与这些服务器同步时间。但是，如果满足以下任一条件，则托管设备将从 防火墙管理中心 同步时间：
  - 设备无法访问 防火墙管理中心 的 NTP 服务器。
  - 防火墙管理中心 没有未经身份验证的服务器。
- **通过来自网络的 NTP** - 如果您的 防火墙管理中心 正在使用网络上的 NTP 服务器，请选择此选项并输入您在 **管理** > **配置** > **时间同步** 中指定的相同 NTP 服务器的完全限定 DNS 名称（如 ntp.example.com）或 IPv4 或 IPv6 地址。如果无法访问 NTP 服务器，则 防火墙管理中心将充当 NTP 服务器。

当配置了多个 NTP 服务器时，设备将使用根据 RFC 中定义的条件认为适当的 NTP 服务器。因此，特定 NTP 服务器的“正在使用”状态表示该服务器当前由设备使用。

步骤 4 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

时区

默认情况下，系统使用 UTC 时区。要为设备指定不同的时区，请使用此程序。

您指定的时区将仅用于支持此功能的策略中基于时间的策略应用。

过程

步骤 1 选择 **设备** > **平台设置**，并创建或编辑身份策略。Firewall Threat Defense

您还可以从 对象 >对象管理 > 时区 页面创建时区对象。**对象** > **时区**

步骤 2 通过点击 +创建新的时区对象。

步骤 3 选择时区。

步骤 4 点击**保存**。

下一步做什么

- 创建时间范围对象，在访问控制和预过滤器规则中选择适用的时间范围，并将父策略分配给与正确时区关联的设备。
- 部署配置更改；请参阅 部署配置更改 ， 第 180 页。

UCAPL/CC 合规性

有关此设置以及如何为 防火墙管理中心启用此设置的详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南。

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

开始之前

- Cisco Secure Firewall Threat Defense 设备不能使用评估许可证；您的 智能软件管理器 账户必须启用出口管制功能。
- Cisco Secure Firewall Threat Defense 设备必须在路由模式下部署。
- 您必须是管理员用户才能执行此任务。
- 如果 Firewall Threat Defense 设备处于高可用性状态，则无法更改安全认证合规性模式。在形成高可用性配对之前，修改安全认证合规模式。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 点击 **UCAPL/CC 合规性 (UCAPL/CC Compliance)**。

步骤 3 要在设备上永久启用安全认证合规性，您有两种选择：

- 要在通用条件模式中启用安全认证合规性，请从下拉列表中选择 **CC**。
- 要在统一功能获批产品列表模式中启用安全认证合规性，请从下拉列表中选择 **UCAPL**。

步骤 4 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

性能配置文件

性能配置文件确定如何将设备上的 CPU 核心分配给两个主系统进程：数据平面 (Lina) 和 Snort。数据平面可处理 VPN 连接、路由和其他基本的第 3/4 层处理。Snort 可提供高级检测，包括入侵和恶意软件防御、URL 过滤、应用过滤以及需要深度数据包检测的其他功能。

如果您使用平衡的基本功能和高级功能，请不要更改性能配置文件。系统旨在为这些进程提供均衡的核心分配。分配会因硬件型号而异。

但是，如果您将设备主要用于VPN或入侵和其他高级检测，则可以调整性能配置文件，以便将更多核心分配给使用更频繁的功能。这样可能会提高系统性能。

开始之前

- 这些设置仅适用于运行 7.3+ 版本的系统。
- 以下设备类型支持性能配置文件：
  - Firepower 4100/9300
  - Cisco Secure Firewall 3100/4200 (7.4+)
  - Cisco Secure Firewall 6100(10.0+)
  - Secure Firewall Threat Defense Virtual
- 集群或高可用性组中的设备或为多实例配置的设备不支持对性能配置文件进行更改。如果将配置文件分配给除独立设备以外的任何设备，则部署会被阻止。
- 核心分配的最小数量为 2。根据所选性能配置文件以偶数分配核心。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑 Firewall Threat Defense 策略。

步骤 2 选择**性能配置文件 (Performance Profile)**。

步骤 3 选择一个配置文件：

- **默认 (Default)** - 这是建议的设置，如果同时配置 VPN 和入侵检测，则是最佳选项。
- **包含预过滤器快速路径的 VPN 密集型** - 如果您主要将设备用作 VPN 终端或头端，并在预过滤器策略中配置规则以快速路径 VPN 流量，则可以选择此选项将大多数 CPU 核心分配给数据平面。分配比例为数据平面 90%，Snort 10%。
- **包含检测的 VPN 密集型** - 如果您主要将设备用作 VPN 终端或头端，但不使用预过滤器策略对VPN流量进行快速路径，则可以选择此选项将大多数CPU核心分配给数据平面。此选项假定您将入侵检测、URL 过滤和其他使用 Snort 的高级功能保留给网络中的不同设备。分配比例为数据平面 60%，Snort 40%。

- **IPS 密集型 (IPS Heavy)** - 如果不配置 VPN，但使用设备进行入侵防御，则可以选择此选项，以便将大部分 CPU 核心分配给 Snort 进程。分配比例为数据平面 30%，Snort 70%。

步骤 4 点击**保存**。

步骤 5 部署策略。

步骤 6 部署完成后，您必须重新启动每个受影响的设备，这样才能进行新的核心分配。

平台设置的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
用户定义的 VRF 接口上支持设备管理服务。	7.6.0	7.6.0	用户定义的虚拟路由和转发 (VRF) 接口现在支持设备访问管理。 请参阅：平台设置
查看“统一事件”(Unified Events) 表中的诊断系统日志消息。	7.6.0	任意	现在，您可以配置 Firewall Threat Defense 设备以便将所有设备系统日志发送到 防火墙管理中心。转到分配给托管设备的 Firewall Threat Defense 平台设置策略，并在**记录到 Cisco Secure Firewall Management Center (Logging to Secure Firewall Management Center)** 设置下选择**所有日志 (All Logs)**。启用日志记录设置后，就可以在**统一事件 (Unified Events)** 表中以名为**故障排除事件 (Troubleshoot Events)** 的新事件类型查看设备系统日志。
删除了对 Firepower 平台设置策略的支持。	7.6.0	7.6.0	删除了用于管理 Firepower 平台设置策略的调配。
用户定义的 VRF 接口上支持设备管理服务。	7.4.1	7.4.1	Firewall Threat Defense平台设置中配置的设备管理服务（NetFlow、SSH 访问、SNMP 主机、系统日志服务器）现在支持用户定义的虚拟路由和转发 (VRF) 接口。 平台限制：不支持容器实例或集群设备。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Cisco Secure Firewall 3100的机箱平台设置：	7.4.1	7.4.1	Cisco Secure Firewall 3100 上多实例机箱的新平台设置。 新增/修改的菜单项： • **设备** > **平台设置** > **添加** > **机箱平台设置** • **设备** > **平台设置** > **添加** > **机箱平台设置** > **DNS** • **设备** > **平台设置** > **添加** > **机箱平台设置** > **SSH** • **设备** > **平台设置** > **添加** > **机箱平台设置** > **时间同步** • **设备** > **平台设置** > **添加** > **机箱平台设置** > **时区** • **设备** > **平台设置** > **添加** > **机箱平台设置** > **SSH** 支持的平台：Cisco Secure Firewall 3100
Cisco Secure Firewall 3100/4200的性能配置文件支持。	7.4.0	7.4.0	平台设置策略中可用的性能配置文件设置现在适用于 Cisco Secure Firewall 3100/4200 设备。
环回接口支持 DNS、HTTP、ICMP、NetFlow、SNMP 和 SSH。	7.4.0	7.4.0	您可以创建环回接口并将其用于： • DNS • HTTP • ICMP • NetFlow • SNMP • SSH 新增/修改的菜单项： • **设备** > **平台设置** > **DNS** > **DNS 设置** **设备** > **平台设置** > **HTTP 访问** > **添加** **设备** > **平台设置** > **ICMP 访问** > **添加** • **设备** > **平台设置** > **网络流** > **添加收集器** • **设备** > **平台设置** > **SNMP** > **主机** > **添加** • **设备** > **平台设置** > **SSH 访问** > **添加**

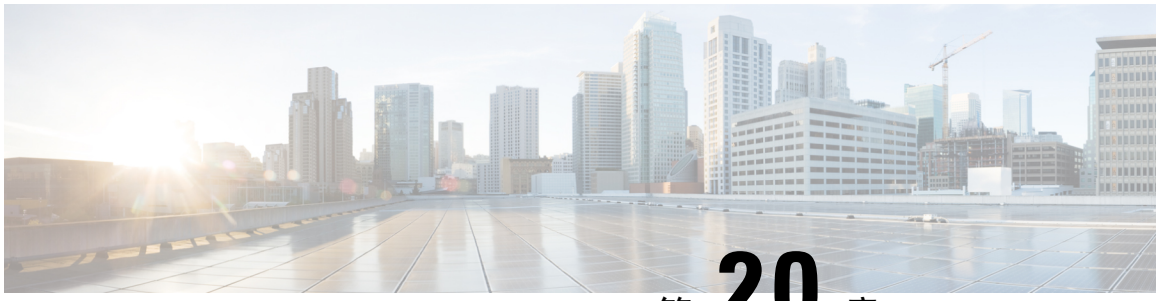
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
合并的管理接口和诊断接口。	7.4.0	7.4.0	对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。 如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 对于平台设置，这意味着： • 您无法再启用 HTTP、ICMP 或 SMTP 进行诊断。 • 对于 SNMP，可以允许“管理”而不是“诊断”上的主机。 • 对于系统日志服务器，您可以通过“管理”而不是“诊断”来访问它们。 • 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 • 如果不指定接口，DNS 查找不会再回退到管理专用路由表。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** 新增/经修改的命令： **show management-interface convergence**
CPU核心分配的性能配置文件。	7.3.0	7.3.0	您可以调整分配给数据平面和 Snort 的系统核心百分比，以便对系统性能进行调整。调整基于 VPN 和入侵策略的相对使用。如果要同时使用两者，请将核心分配保留为默认值。如果系统将主要用于VPN（不应用入侵策略）或用作 IPS（无 VPN 配置），则可以将核心分配倾斜到数据平面（用于 VPN）或 Snort（用于入侵检测）。 我们在平台设置策略中添加了**性能配置文件 (Performance Profile)** 页面。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
远程访问 VPN 中的 TLS 1.3。	7.3.0	7.3.0	您现在可以使用 TLS 1.3 加密远程接入 VPN 连接。 使用威胁防御平台设置指定设备在充当远程接入 VPN 服务器时必须使用 TLS 1.3 协议。 TLS 1.3 增加了对以下密码的支持： • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 此功能需要思科安全客户端版本 5.0 及更高版本。 新增/修改的屏幕：**设备** > **平台设置** > **新策略** > **添加/编辑威胁防御设置** > **SSL** > **TLS 版本**
用于解析 DNS 请求的多个 DNS 服务器组。	7.2.0	7.2.0	您可以配置多个 DNS 组来解析来自客户端系统的 DNS 请求。您可以使用这些 DNS 服务器组来解析对不同 DNS 域的请求。例如，您可能有一个使用公共DNS服务器的可捕获默认组，用于与互联网的连接。然后，您可以配置一个单独的组，以将内部DNS服务器用于内部流量，例如，与 example.com 域中的计算机的任何连接。因此，使用您的组织的域名与 FQDN 的连接将使用内部 DNS 服务器进行解析，而与公共服务器的连接则使用外部 DNS 服务器。 我们更改了**平台设置 (Platform Settings)** > **DNS** 页面。
网络对象支持 HTTP、ICMP 和 SSH 平台设置。	7.1.0	7.1.0	现在，在威胁防御平台设置策略中配置IP地址时，可以使用包含主机或网络的网络对象的网络对象组。 支持的平台： Firewall Threat Defense
支持指定受信任的DNS服务器。	7.1.0	7.1.0	引入了用于指定在使用直接互联网访问时可以用于地址解析的可信DNS服务器的选项。 我们为在配置直接互联网访问时配置受信任 DNS 服务器添加了一个选项卡：**设备 (Devices)** > **平台设置 (Platform Settings)** > **DNS** > **受信任 DNS 服务器 (Trusted DNS Servers)**。 支持的平台： Firewall Threat Defense

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
对 SNMPv3 用户使用 MD5 身份验证算法或 DES 加密的平台设置无法部署到运行 7.0+ 版本的 Firewall Threat Defense 设备。	7.0.0	7.0.0	Firewall Threat Defense 上 SNMPv3 用户的 MD5 身份验证算法和 DES 加密在版本 6.5 中已被弃用。如果您的部署包括使用 MD5 认证算法或 DES 加密的 SNMPv3 用户，而这些用户是用 6.4 版或更早的版本创建的，则可以继续对运行版本 6.7 或更早版本的 Firewall Threat Defense 设备使用这些用户。但是，您无法编辑这些用户并保留 MD5 或 DES 设置，也无法使用 MD5 或 DES 设置来创建新用户。如果您的 防火墙管理中心 管理任何运行版本 7.0+ 的 Firewall Threat Defense，则使用 MD5 身份验证算法或 DES 加密为 SNMP v3 用户向这些 Firewall Threat Defense 部署平台设置策略将失败。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SNMP** > **主机 (Hosts)** 支持的平台： Firewall Threat Defense
为 SNMPv3 用户的授权算法指定 SHA224 或 SHA384。	7.0.0	7.0.0	现在，您可以为 SNMPv3 用户的授权算法选择 SHA224 或 SHA384。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SNMP** > **用户 (Users)** 支持的平台： Firewall Threat Defense
指定设备的时区。	6.6.0	6.6.0	为托管设备指定本地时区，以用于基于时间的策略应用。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **时区 (Time Zone)** 支持的平台： Firewall Threat Defense
指定用于 SNMP 通信的管理接口。	6.6.0	6.6.0	您现在可以选择用于在设备和 SNMP 管理站之间进行通信的管理接口。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SNMP** > **主机 (Hosts)** 支持的平台： Firewall Threat Defense
为 SNMPv3 用户的授权算法指定 SHA256。	6.6.0	6.6.0	您现在可以为 SNMPv3 用户的授权算法选择 SHA256。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SNMP** > **用户 (Users)** 支持的平台： Firewall Threat Defense

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firewall Threat Defense上SNMPv3用户的DES加密和MD5身份验证算法已被弃用。	6.5.0	任意	我们建议您不要在 Firewall Threat Defense 设备上对 SNMPv3 用户使用 MD5 身份验证算法或 DES 加密，因为这些选项已被弃用。如果您的部署包括使用 6.4 之前的版本创建的使用 MD5 身份验证算法或 DES 加密的SNMPv3用户，则可以继续使用这些用户。但是，您无法编辑这些用户并保留 MD5 或 DES 设置，也无法使用 MD5 或 DES 设置来创建新用户。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SNMP** > **用户 (Users)** 支持的平台： Firewall Threat Defense
TCP 系统日志服务器关闭时，允许用户流量通过。	6.3.0	6.3.0	当设备无法访问外部 TCP 系统日志服务器时，我们建议您允许通过 威胁防御设备 进行连接。默认情况下，平台设置中的 **允许用户流量在TCP系统日志服务器关闭时通过（建议启用）** 选项已启用。
限制 SSH 登录失败次数。	6.3.0	6.3.0	当用户通过SSH访问任何设备并连续三次尝试登录失败时，设备会终止 SSH 会话。
为SSH添加的外部身份验证。	6.2.3	6.2.3	现在，您可以配置外部身份验证以便对使用LDAP或RADIUS的Firewall Threat Defense进行 SSH 访问。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **外部身份验证 (External Authentication)** 支持的平台： Firewall Threat Defense
支持 UC/APPL 合规性模式。	6.2.1	6.2.1	可以在 CC 模式或 UCAPL 模式下启用安全认证合规性。启用安全认证合规性不保证严格符合所选安全模式的所有要求。有关强化操作步骤的详细信息，请参阅由认证实体提供的此产品的相关准则。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **UC/APPL 合规性 (UC/APPL Compliance)** 支持的平台：任何设备
用于远程接入 VPN 的 SSL 设置。	6.2.1	6.2.1	Firewall Threat Defense设备使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 对来自远程客户端的远程接入VPN连接支持安全消息传输。您可以配置在通过 SSL 远程 VPN 接入传输邮件过程中协商和使用的 SSL 版本和加密算法。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **SSL** 支持的平台： Firewall Threat Defense

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
已删除适用于 SSH 和 HTML 的外部身份验证。	6.1.0	6.1.0	由于更改以支持融合的管理访问，因此仅支持本地用户使用 SSH 和 HTML 访问数据接口。此外，您还可以不再使用SSH访问诊断接口；而是能够使用SSH访问逻辑管理接口（这将共享同一物理端口）。以前，仅支持外部身份验证使用 SSH 和 HTML 访问诊断和数据接口，同时仅支持本地用户访问管理接口。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **外部身份验证 (External Authentication)** 支持的平台： Firewall Threat Defense
Firepower Threat Defense 支持。	6.0.1	6.0.1	引入了此功能。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** 支持的平台： Firewall Threat Defense



第 20 章

FlexConfig 策略

以下主题介绍如何配置和部署 FlexConfig 策略。

- FlexConfig 策略概述， 第 1041 页
- FlexConfig 策略的要求和先决条件， 第 1060 页
- FlexConfig 的准则与限制， 第 1060 页
- 使用 FlexConfig 策略自定义设备配置， 第 1061 页
- FlexConfig 示例， 第 1074 页
- 迁移 FlexConfig 策略， 第 1080 页
- FlexConfig 的历史记录， 第 1082 页

FlexConfig 策略概述

FlexConfig 策略是 FlexConfig 对象的有序列表的容器。每个对象都包含一系列 Apache Velocity 脚本语言命令（即 ASA 配置命令）和您定义的变量。每个 FlexConfig 对象的内容实质上是一个程序，它生成一系列 ASA 命令，然后将其部署到指定的设备。然后，此命令序列会在 Firewall Threat Defense 设备上配置相关功能。

Firewall Threat Defense使用 ASA 配置命令实现一些功能，但不是所有功能。没有唯一的一组 Firewall Threat Defense配置命令。相反，FlexConfig 的要点是允许您配置尚未通过 防火墙管理中心策略和设置直接支持的功能。

⚠

注意 思科强烈建议仅具有较强 ASA 背景且自承风险的高级用户使用 FlexConfig 策略。您可以配置不受禁止的任何命令。通过 FlexConfig 启用功能可能会导致配置的其他功能出现意想不到的结果。

您可以联系思科技术支持中心获取有关您已配置的 FlexConfig 策略的支持。思科技术支持中心不代表任何客户设计或编写自定义配置。思科不保证正确的操作或与其他功能的互通性。FlexConfig 功能可能随时被摒弃。为获得充分保证的功能支持，您必须等待防火墙管理中心支持。当有疑问时，请勿使用 FlexConfig 策略。

FlexConfig 策略的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 转换为 Firewall Threat Defense，并且存在您正在使用（且需要继续使用）的 防火墙管理中心 不直接支持的兼容功能。在这种情况下，请在 ASA 上使用 **show running-config** 命令来查看功能配置，并创建 FlexConfig 对象以实施此功能。尝试使用对象的部署设置（一次/每次和追加/预置）以获得正确的设置。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 Firewall Threat Defense，但有一个设置或功能需要配置，例如思科技术援助中心告诉您特定的设置应解决您遇到的特定问题。对于复杂功能，请使用实验室设备测试FlexConfig，并验证您是否将得到预期行为。

系统包含一组预定义的 FlexConfig 对象，它们代表已测试的配置。如果所需的功能没有由这些对象表示，请首先确定是否可以在标准策略中配置等效功能。例如，访问控制策略包括ASA使用单独功能实现的入侵检测和预防、HTTP 和其他类型的协议检查、URL 过滤、应用过滤和访问控制。由于许多功能并未使用 CLI 命令予以配置，因此，您不会看到各策略均显示在 **show running-config** 输出内。

注释 在任何时候，请记住 ASA 和 Firewall Threat Defense之间不存在一对一重叠关系。请勿尝试在 Firewall Threat Defense设备上完全重新创建 ASA 配置。您必须仔细测试使用 FlexConfig 配置的各项功能。

FlexConfig 对象中的 CLI 命令

Firewall Threat Defense 设备使用 ASA 配置命令配置某些功能。虽然并非所有 ASA 功能都与 Firewall Threat Defense 兼容，但有一些功能可以在 Firewall Threat Defense 设备上使用，但不能在 防火墙管理中心 策略中进行配置。可以使用 FlexConfig 对象指定配置这些功能所需的 CLI。

如果您决定使用 FlexConfig 手动配置功能，则应根据正确的语法了解和执行这些命令。FlexConfig 策略不验证 CLI 命令语法。有关正确语法和配置 CLI 命令的更多信息，请使用以下 ASA 文档作为参考：

- ASA CLI 配置指南介绍了如何配置功能。指南位于：https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- ASA 命令参考提供按命令名称排序的附加信息。参考位于：https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

以下主题介绍了有关配置命令的更多信息。

确定 ASA 软件版本和当前 CLI 配置

由于系统使用 ASA 软件命令配置某些功能，因此需要确定在 Firewall Threat Defense设备上运行的软件中使用的当前 ASA 版本。此版本号指示用于指导配置功能的 ASA CLI 配置指南。此外，您还应检查当前基于 CLI 的配置，并将其与要实施的 ASA 配置进行比较。

注意，任何 ASA 配置都与 Firewall Threat Defense 配置有着显著的差异。许多 Firewall Threat Defense 策略都是在 CLI 之外配置的，因此查看这些命令看不到配置。请勿尝试在 ASA 和 Firewall Threat Defense 配置之间创建一对一的对应关系。

要查看此信息，请与设备的管理界面建立 SSH 连接，并发出以下命令：

- **show version system** 并查找思科自适应安全装置软件版本号。（如果您通过 Secure Firewall Management Center CLI 工具发出命令，请忽略 **system** 关键字。）
- **show running-config** 查看当前的 CLI 配置。
- **show running-config all** 包括当前 CLI 配置中的所有默认命令。

也可以使用以下过程在 防火墙管理中心中发出这些命令。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

步骤 2 点击 FlexConfig 策略适用的设备的名称。

您可能需要点击“状态”表中**计数**列中的打开/关闭箭头来查看任何设备。

步骤 3 点击 **查看系统和故障排除详细信息**。

步骤 4 点击**高级故障排除 (Advanced Troubleshooting)**。

步骤 5 点击**威胁防御 CLI (Threat Defense CLI)**。

步骤 6 选择 **设备**，然后选择 **显示** 作为命令，然后键入 **版本** 或其他命令之一作为参数。

步骤 7 点击**执行 (Execute)**

对于版本，请搜索思科自适应安全设备软件版本号的输出。

您可以选择输出并按 Ctrl+C 组合键，然后将其粘贴到文本文件中以供日后分析之用。

禁止的 CLI 命令

FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 防火墙管理中心在 Firewall Threat Defense设备上配置的功能。

因此，您无法配置在 防火墙管理中心中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。

此外，一些 **clear** 命令已被禁止，因为它们与多项托管策略重叠，并且可以删除托管策略的部分配置。

FlexConfig 对象编辑器可防止将被禁止的命令纳入对象中。

禁止的 CLI 命令	说明
AAA	阻止配置。

禁止的 CLI 命令	说明
AAA-Server	阻止配置。
Access-list	阻止高级 ACL、扩展 ACL 和标准 ACL。允许 Ethertype ACL。 可以使用在模板内的对象管理器中定义的标准和扩展ACL对象作为变量。
ARP 检测	阻止配置。
As-path Object	阻止配置。
Banner	阻止配置。
BGP	阻止配置。
Clock	阻止配置。
Community-list Object	阻止配置。
Copy	阻止配置。
Delete	阻止配置。
DHCP	阻止配置。
Enable Password	阻止配置。
Erase	阻止配置。
Fragment Setting	被阻止，**fragment reassembly**除外。
Fsck	阻止配置。
HTTP	阻止配置。
ICMP	阻止配置。
Interface	仅阻止 **nameif**、**mode**、**shutdown**、**ip address** 和 **mac-address** 命令。
组播路由	阻止配置。
NAT	阻止配置。
Network Object/Object-group	将阻止在 FlexConfig 对象中创建网络对象，但可使用在模板内的对象管理器中定义的网络对象和组作为变量。
NTP	阻止配置。
OSPF/OSPFv3	阻止配置。

禁止的 **CLI** 命令	说明
pager	阻止配置。
Password Encryption	阻止配置。
Policy-list Object	阻止配置。
Prefix-list Object	阻止配置。
重新加载	不能安排重新加载。系统不使用 **reload** 命令重启系统，它使用的是 **reboot** 命令。
RIP	阻止配置。
Route-Map Object	将阻止 FlexConfig 对象中创建路由映射对象，但可使用在模板内的对象管理器中定义的路由映射对象作为变量。
Service Object/Object-group	将阻止 FlexConfig 对象中创建服务对象，但可使用在模板内的对象管理器中定义的端口对象作为变量。
SNMP	阻止配置。
SSH	阻止配置。
Static Route	阻止配置。
Syslog	阻止配置。
Time Synchronization	阻止配置。
Timeout	阻止配置。
VPN	阻止配置。

模板脚本

您可以使用脚本语言来控制 FlexConfig 对象内的处理。脚本语言指令是 Apache Velocity 1.3.1 模板引擎中支持的命令子集，它是一种支持循环、if/else 语句和变量的基于 Java 的脚本语言。

要了解如何使用该脚本语言，请参阅 http://velocity.apache.org/engine/devel/developer-guide.html 的 *Velocity* 开发人员指南。

FlexConfig 变量

在命令或处理指令的一部分依赖于运行时信息而不是静态信息的情况下，可以在 FlexConfig 对象中使用变量。在部署过程中，变量将替换为基于变量类型从设备的其他配置所获得的字符串：

- 策略对象变量被替换为从 防火墙管理中心中定义的对象获取的字符串。

- 系统变量会被替换为从设备本身或为其配置的策略中获取的信息。
- 处理脚本命令时，处理变量随策略对象或系统变量的内容一起加载。例如，在循环中将策略对象或系统变量中的一个值通过迭代方式加载到处理变量中，然后使用处理变量组成命令字符串或执行其他操作。这些处理变量在 FlexConfig 对象中的变量列表中不显示。此外，也不要使用 FlexConfig 对象编辑器中的**插入**菜单添加这些变量。
- 密钥变量被替换为 FlexConfig 对象中为该变量定义的单个字符串。

以 $ 字符开头的变量，除以 @ 字符开头的密钥变量变量之外。例如，在下面的命令中 $ifname 是一个策略对象变量，而 @keyname 是一个密钥。

```
interface $ifname
key @keyname
```



注释 第一次插入策略对象或系统变量时，必须通过 FlexConfig 对象编辑器中的**插入**菜单执行操作。此操作可将变量添加到 FlexConfig 对象编辑器底部的**变量**列表中。但您必须在随后的使用中键入变量字符串，即使在使用系统变量时也是如此。如果添加的处理变量没有对象或系统变量赋值，请不要使用**插入**菜单。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

变量是否被解析为单个字符串、字符串列表或值表取决于分配给变量的策略对象或系统变量的类型。（密钥始终解析为单个字符串）。您必须了解返回的内容，以便正确处理变量。

以下主题解释各种类型的变量以及如何处理这些变量。

如何处理变量

在运行时，变量可以解析为单个字符串、相同类型的字符串列表、不同类型的字符串列表或命名值表。此外，解析为多个值的变量的长度可以是确定的，也可以是不定的。您必须了解要返回的内容才能正确处理这些值。

以下是可能出现的主要情况：

单值变量

如果变量始终解析为单个字符串，则在 FlexConfig 脚本中直接使用该变量而不进行修改。

例如，预定义的文本变量 tcpMssBytes 始终解析为单个值（必须为数字）。然后，**Sysopt_basic** FlexConfig 使用 if/then/else 结构根据另一个单值文本变量 tcpMssMinimum 的值设置最大段大小：

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $tcpMssBytes 的第一个用例，但您可以直接在 #else 行中键入变量。

密钥变量是一种特殊类型的单值变量。对于密钥，始终使用**插入**菜单添加变量，即使是用于第二次和后续的使用。这些变量在 FlexConfig 对象中的变量列表中不显示。



注释 网络对象的策略对象变量也等同于单个 IP 地址规范，即主机地址、网络地址或地址范围。但在这种情况下，您必须清楚需要什么类型的地址，因为 ASA 命令需要特定的地址类型。例如，如果命令需要主机地址，使用指向包含网络地址的对象的网络对象变量将导致部署过程中出错。

多值变量，所有值都具有相同类型

多个策略对象和系统变量解析为同一类型的多个值。例如，指向网络对象组的对象变量解析为组中 IP 地址的列表。同样，系统变量 $SYS_FW_INTERFACE_NAME_LIST 解析为接口名称的列表。

还可以为同一类型的多个值创建文本对象。例如，预定义的文本对象 enableInspectProtocolList 可以包含多个协议名称。

解析为同一类型项目列表的多值变量通常具有不定长度。例如，您无法预先知道命名了设备上的多少个接口，因为用户可以随时配置或取消配置接口。

因此，您通常使用循环来处理同一类型的多值变量。例如，预定义的 FlexConfig **Default_Inspection_Protocol_Enable** 使用 #foreach 循环来遍历 enableInspectProtocolList 对象并处理每个值。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

在此示例中，该脚本依次将每个值分配给 $protocol 变量，然后在 ASA **inspect** 命令中使用该变量为该协议启用检测引擎。在这种情况下，您只需键入 $protocol 作为变量名称。您不使用**插入**菜单来添加它，因为您没有将对象或系统值分配给该变量。但是，必须使用**插入**菜单添加 $enableInspectProtocolList。

系统在 #foreach 和 #end 之间循环遍历代码，直到 $enableInspectProtocolList 中没有剩余的值。

多个值变量，值具有不同的类型

可以创建多个值文本对象，但每个值都有不同的用途。例如，预定义的 **netflow_Destination** 文本对象应具有 3 个值，分别表示接口名称、目标 IP 地址和 UDP 端口号。

以这种方式定义的对象应具有确定的值数。否则，它们将很难处理。

使用 get 方法处理这些对象。在对象名称的末尾键入 **.get(*n*)**，并将 *n* 替换为对象中的索引。从 0 开始计数，即使文本对象从 1 开始列出其值亦是如此。

例如，Netflow_Add_Destination 对象使用以下行将 netflow_Destination 中的 3 个值添加到 ASA **flow-export** 命令。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
```

```
$netflow_Destination.get(2)
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $netflow_Destination 的第一次使用，然后添加 **get(0)**。但您可以直接为 **$netflow_Destination.get(1)** 和 **$netflow_Destination.get(2)** 规范键入该变量。

解析为值表的多个值变量

有些系统变量会返回一个值表。这些变量包括其名称中的 MAP，例如 $SYS_FTD_ROUTED_INTF_MAP_LIST。路由接口映射返回的数据如下所示（为了清楚起见，添加了换行）：

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]
```

在上面的示例中，将为 4 个接口返回信息。每个 接口都包括一个指定值表。例如，intf_hardwarare_id 是 接口硬件名称属性的名称，并将返回诸如 GigabitEthernet0/0 的字符串。

这种类型的变量通常长度不确定，因此您需要 使用环路来处理值。但您还需要将属性 名称添加到变量名称中，以指示要检索哪个值。

例如，IS-IS 配置需要在接口配置模式下将 ASA **isis** 命令添加到某一具有逻辑名称的接口。但您可以使用该接口的 硬件名称进入该模式。因此，您需要确定哪些接口具有 逻辑名称，然后仅配置使用其硬件名称的那些接口。预定义了 ISIS_Interface_Configuration 的 FlexConfig 使用 嵌套在环路中的 if/then 结构来进行此操作。在下面的代码中，可以看到 #foreach 脚本命令会将每个接口映射加载到 $intf 变量中， 然后 #if 语句将切断映射 ($intf.intf_logical_name) 中的 intf_logical_name 值，并且如果该值位于 isisIntfList 预定义文本变量中定义的列表中，则请使用 intf_hardwarare_id 值 ($intf.intf_hardwarare_id) 输入接口命令。您需要编辑 isisIntfList 变量以添加要在其上配置 IS-IS 的接口的 名称。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

如何查看将为设备返回什么变量

评估将会返回什么变量的一种简单方式是创建一个简单的 FlexConfig 对象，该对象除了处理带有注释的变量列表以外，不进行任何其他操作。随后可将该对象分配给某一 FlexConfig 策略，再将该策略分配给某一设备，保存该策略，然后预览该设备的配置。该预览将显示解析出来的值。可以选择预览文本，按 Ctrl+C 键，然后将输出粘贴到文本文件中用于分析。



注释 但不要将此 FlexConfig 部署到设备，因为它不会包含任何有效的配制命令。您将收到部署错误。在获得预览后，请从 FlexConfig 策略中删除该 FlexConfig 对象，然后保存该策略。

例如，可以构建以下 FlexConfig 对象：

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

此对象的 预览可能如下所示（为了清楚起见，添加了换行）：

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:
```

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, management]
```

FlexConfig 策略对象变量

策略对象变量与在对象管理器中配置的特定策略对象关联。在 FlexConfig 对象中插入策略对象变量时，将为该变量提供一个名称，并选择与其关联的对象。

尽管可以为变量提供与关联对象完全相同的名称，但变量本身与关联对象不同。必须使用FlexConfig对象编辑器中的**插入** > **插入策略对象** > **对象类型**菜单首次将该变量添加到 FlexConfig 中的脚本，以建立与该对象的关联。仅键入前面带有 $ 符号的对象的名称不会创建策略对象变量。

您可以创建变量以指向以下类型的对象。确保为每个变量创建正确的对象类型。要创建对象，请转到**对象**页面。

- **文本对象** - 适用于文本字符串，可以包括 IP 地址、数字和其他自由格式文本，如接口或区域名称。从目录中选择 **FlexConfig** > **文本对象**，然后点击**添加文本对象**。可以将这些对象配置为包含单个值或多个值。这些对象具有高度的灵活性，专用于 FlexConfig 对象。有关详细信息，请参阅配置 FlexConfig 文本对象，第 1067 页。
- **网络** - 适用于 IP 地址。可以使用网络对象或组。从目录中选择**网络**，然后选择**添加网络** > **添加对象**或**添加组**。如果使用组对象，该变量将返回组中每个 IP 地址规范的列表。地址可以是主机、网络或地址范围，具体取决于对象内容。请参阅网络，第 2658 页。
- **安全区域** - 适用于安全区域或接口组中的接口。从目录中选择**接口**，然后选择**添加** > **安全区域**或**接口组**。安全区域变量将为正配置的设备返回该区域或组内的接口列表。请参阅接口，第2655页。
- **标准的 ACL 对象** - 适用于标准访问控制列表。标准 ACL 变量返回标准 ACL 对象的名称。从目录中选择**访问列表** > **标准**，然后点击**添加标准访问列表对象**。请参阅访问列表，第 2625 页。
- **扩展 ACL 对象** - 适用于扩展访问控制列表。扩展 ACL 变量将返回扩展 ACL 对象的名称。从目录中选择**访问列表** > **扩展**，然后点击**添加扩展访问列表对象**。请参阅访问列表，第 2625 页。

- **路由映射** - 适用于路由映射对象。路由映射变量将返回路由映射对象的名称。从目录中选择**路由映射**，然后点击**添加路由映射**。请参阅路由映射，第 2685 页。

FlexConfig 系统变量

系统变量会被替换为从设备本身或为其配置的策略中获取的信息。

必须使用 FlexConfig 对象编辑器中的**插入** > **插入系统变量** > **变量名**菜单，第一次就开始将变量添加到 FlexConfig 中的脚本以建立与系统变量的关联。只键入系统变量的名称并前跟 $ 符号不会在 FlexConfig 对象的上下文中创建系统变量。

下表介绍了可用的系统变量。在使用变量之前，检查通常为变量返回的内容；请参阅如何查看将为设备返回什么变量，第 1049 页。

名称	说明
SYS_FW_OS_MODE	设备的操作系统模式。可能的值包括 ROUTED 或 TRANSPARENT。
SYS_FW_OS_MULTIPLICITY	设备在单情景模式还是多情景模式下运行。可能的值包括 SINGLE、MULTI 或 NOT_APPLICABLE。
SYS_FW_MANAGEMENT_IP	设备的管理 IP 地址
SYS_FW_HOST_NAME	设备主机名
SYS_FTD_INTF_POLICY_MAP	以接口名称作为键并将策略映射为值的映射。如果设备上没有定义基于接口的服务策略，则此变量将不返回任何值。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	启用了检查的协议的列表。
SYS_FTD_ROUTED_INTF_MAP_LIST	设备上路由接口映射的列表。每个映射都包含一组与路由接口配置相关的命名值。
SYS_FTD_SWITCHED_INTF_MAP_LIST	设备上交换接口映射的列表。每个映射都包含一组与交换接口配置相关的命名值。
SYS_FTD_INLINE_INTF_MAP_LIST	设备上内联接口映射的列表。每个映射都包含一组与内联集接口配置相关的命名值。
SYS_FTD_PASSIVE_INTF_MAP_LIST	设备上被动接口映射的列表。每个映射都包含一组与被动接口配置相关的命名值。
SYS_FTD_INTF_BVI_MAP_LIST	设备上网桥虚拟接口映射的列表。每个映射都包含一组与 BVI 配置相关的命名值。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	设备上接口硬件名称（如 GigabitEthernet0/0）的列表。
SYS_FW_INTERFACE_NAME_LIST	设备上接口逻辑名称（如内部）的列表。
SYS_FW_INLINE_INTERFACE_NAME_LIST	配置为被动或 ERSPAN 被动的接口的逻辑名称列表。

名称	说明
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	不属于内联集的接口（如所有路由接口）的逻辑名称列表。

预定义的 FlexConfig 对象

预定义的 FlexConfig 对象为选定功能提供经过测试的配置。如果需要配置这些功能，请使用这些对象，否则无法使用 防火墙管理中心配置这些功能。

下表列出了可用的对象。记下关联的文本对象。您必须编辑这些文本对象，才能自定义预定义 FlexConfig 对象的行为。文本对象使您可以使用网络和设备所需的 IP 地址和其他属性来自定义配置。

如果需要修改预定义 FlexConfig 对象，请复制该对象，对副本进行更改，然后使用新名称进行保存。不能直接编辑预定义 FlexConfig 对象。

尽管您可以使用 FlexConfig 配置其他基于 ASA 的功能，但这些功能的配置尚未经过测试。如果某个 ASA 功能与您可以在 防火墙管理中心策略中配置的内容重叠，请勿尝试通过 FlexConfig 对该功能进行配置。

例如，Snort 检查包括 HTTP 协议，因此不可启用 ASA 式 HTTP 检查。（实际上，您无法将 **http** 添加到 enableInspectProtocolList 对象。在这种情况下，您将被阻止以免错误配置您的设备。）相反，应根据需要配置访问控制策略以执行应用或 URL 过滤，以实施 HTTP 检查要求。

表 *77:* 预定义的 *FlexConfig* 对象

FlexConfig 对象名称	**Description**	关联的文本对象
Default_Inspection_Protocol_Disable	在 global_policy 默认策略映射中禁用协议。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	在 global_policy 默认策略映射中启用协议。	enableInspectProtocolList
Inspect_IPv6_Configure	在 global_policy 策略映射中配置 IPv6 检查，从而根据 IPv6 报头内容记录和丢弃流量。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。
Inspect_IPv6_UnConfigure	清除并禁用 IPv6 检查。	—
ISIS_Configure	为 IS-IS 路由配置全局参数。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	接口级别 IS-IS 配置。	isIsAddressFamily、IsIsIntfList 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	清除设备上的 IS-IS 路由器配置。	—
ISIS_Unconfigure_All	从设备中清除 IS-IS 路由器配置，包括来自设备接口的路由器分配。	—

FlexConfig 对象名称	Description	关联的文本对象
NGFW_TCP_NORMALIZATION	修改默认 TCP 规范化配置。	—
Policy_Based_Routing	要使用此示例配置，请复制它，修改接口名称，然后使用 r-map-object 文本对象标识对象管理器中的路由映射对象。	—
Policy_Based_Routing_Clear	从设备中清除策略型路由配置。	—
Sysopt_AAA_radius	忽略 RADIUS 记帐响应中的身份验证密钥。	—
Sysopt_AAA_radius_negate	使 Sysopt_AAA_radius 配置失效。	—
Sysopt_basic	配置 sysopt 等待时间、TCP 数据包的最大报文段长度以及详细流量统计信息。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	清除 sysopt_basic 详细流量统计信息、等待时间和 TCP 最大报文段长度。	—
Sysopt_clear_all	从设备中清除所有 sysopt 配置。	—
Sysopt_noproxyarp	配置 noproxy-arp CLI。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	清除 Sysopt_noproxyarp 配置。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	配置 syopt 保留 VPN 流。	—
Sysopt_Preserve_Vpn_Flow_negate	清除 Sysopt_Preserve_Vpn_Flow 配置。	—
Sysopt_Reclassify_Vpn	配置 sysopt 重新分类 VPN。	—
Sysopt_Reclassify_Vpn_Negate	否定 sysopt 重新分类 VPN。	—
Threat_Detection_Clear	清除威胁检测 TCP 拦截配置。	—
Threat_Detection_Configure	配置 TCP 拦截所拦截攻击的威胁检测统计信息。	threat_detection_statistics
Wccp_Configure	此模板提供了一个配置 WCCP 的示例。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	清除 WCCP 配置。	—

弃用的 FlexConfig 对象

下表列出了用于配置您现在可以在 GUI 中本地配置的功能的对象。尽早停止使用这些对象。

表 *78:* 弃用的预定义 *FlexConfig* 对象

弃用的版本	FlexConfig 对象	Description	现在配置在
7.3	DHCPv6_Prefix_Delegation_Configure	为 IPv6 前缀委派配置一个外部接口（前缀委派客户端）和一个内部接口（委派前缀的接收者）。要使用此模板，请对其进行复制并修改变量。 关联的文本对象：pdoutside、pdinside 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST	接口 IPv6 设置。
7.3	DHCPv6_Prefix_Delegation_UnConfigure	删除 DHCPv6 前缀委派配置。	接口 IPv6 设置。
6.3	Default_DNS_Configure	配置默认 DNS 组，该组定义在数据接口上解析完全限定域名时可以使用的 DNS 服务器。 关联的文本对象：defaultDNSNameServerList、defaultDNSParameters	平台设置。
6.3	DNS_Configure	在非默认 DNS 服务器组中配置 DNS 服务器。复制对象以更改组的名称。	对象管理器中的**DNS 服务器组** 。
6.3	DNS_UnConfigure	删除由 Default_DNS_Configure 和 DNS_Configure 执行的 DNS 服务器配置。如果您更改了 DNS_Configure，则复制该对象以更改 DNS 服务器组名称。	对象管理器中的**DNS 服务器组** 。
7.2	Eigrp_Configure	配置 EIGRP 路由 next-hop、auto-summary、router-id、eigrp-stub。 关联的文本对象：eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary	有关所有 EIGRP 对象，请参阅 EIGRP，第 1203 页。 系统允许您部署升级后，但也会警告您重新执行 EIGRP 配置。为了帮助您完成此过程，我们提供了一个命令行迁移工具。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	Eigrp_Interface_Configure	配置 EIGRP 接口身份验证模式、身份验证密钥、呼叫间隔、保持时间、水平分割。 关联的文本对象：eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	从设备中清除自治系统的 EIGRP 配置。	
7.2	Eigrp_Unconfigure_all	清除所有 EIGRP 配置。	
7.4	Netflow_Add_Destination	创建和配置 Netflow 导出目标。 关联的文本对象：Netflow_Destinations、netflow_Event_Types	平台设置。
7.4	Netflow_Clear_Parameters	恢复 Netflow 导出全局默认设置。	平台设置。
7.4	Netflow_Delete_Destination	删除 Netflow 导出目标。 关联的文本对象：Netflow_Destinations、netflow_Event_Types	平台设置。
7.4	Netflow_Set_Parameters	为 Netflow 导出设置全局参数。 关联的文本对象：netflow_Parameters	平台设置。
6.3	TCP_Embryonic_Conn_Limit	配置初始连接限制以防止 SYN 泛洪拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_limit	服务政策。
6.3	TCP_Embryonic_Conn_Timeout	配置初始连接超时以防止 SYN 洪流拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_timeout	服务政策。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	VxLAN_Clear_Nve	从设备中删除使用 VxLAN_Configure_Port_And_Nve 时配置的 NVE 1。	有关所有 VxLAN 对象，请参阅配置 VXLAN 接口，第 774 页。 如果在以前的版本中使用 FlexConfig 配置了 VXLAN 接口，它们将继续工作。实际上，在这种情况下，FlexConfig 优先 - 如果您在 Web 接口中重做 VXLAN 配置，请删除 FlexConfig 设置。
7.2	VxLAN_Clear_Nve_Only	在部署时，清除在接口上配置的 NVE。	
7.2	VxLAN_Configure_Port_And_Nve	配置 VLAN 端口和 NVE 1。 关联的文本对象：vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	仅为 NVE 设置接口。 关联的文本对象：vxlan_Nve_Only 还使用系统变量 SYS_FTD_ROUTED_MAP_LIST 和 SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	创建 VNI 接口。部署此项后，您必须先注销设备，然后再重新注册设备，才能正确发现 VNI 接口。 关联的文本对象：vxlan_Vni	

预定义文本对象

有多种预定义的文本对象。这些对象与预定义的 FlexConfig 对象中使用的变量关联。在大多数情况下，如果您使用关联的 FlexConfig 对象，则必须编辑这些对象才能添加值，否则将在部署过程中出错。尽管其中一些对象包含默认值，但其他一些则为空。

有关编辑文本对象的信息，请参阅配置 FlexConfig 文本对象，第 1067 页。

名称	说明	关联的 **FlexConfig** 对象
defaultDNSNameServerList （已弃用。）	要在默认 DNS 组中配置的 DNS 服务器 IP 地址。 从版本 6.3 开始，在威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
defaultDNSParameters （已弃用。）	用于控制默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、过期条目计时器、轮询计时器、域名条目。 从版本 6.3 开始，在威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
disableInspectProtocolList	在默认策略映射 (global_policy) 中禁用协议。	Disable_Default_Inspection_Protocol
dnsNameServerList	要在用户定义的 DNS 组中配置的 DNS 服务器 IP 地址。	DNS_Configure
dnsParameters	用于控制非默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、域名、域名服务器条目。	DNS_Configure
enableInspectProtocolList	在默认策略映射 (global_policy) 中启用协议。您将不允许添加其检查与 Snort 检查冲突的协议。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	要禁止的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，而不记录此丢弃。	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	要禁止和记录的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，并发送有关此丢弃的系统日志消息。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	要允许但会记录的 IPv6 路由报头类型的列表。IPv6 检查会允许包含这些报头的数据包，并发送有关存在报头的系统日志消息。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 或 IPv6 地址系列。	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	逻辑接口名称的列表。	ISIS_Interface_Configuration

名称	说明	关联的 **FlexConfig** 对象
isIsISType	IS 类型（级别 1、级别 2 或级别 1-2）。	ISIS_Configure
isIsNet	网络实体。	ISIS_Configure
isServiceIdentifier	如果为 false，则使用标准的 **web-cache** 服务标识符。	Wccp_Configure
netflow_Destination	定义单个 NetFlow 导出目标的接口、目标和 UDP 端口号。	Netflow_Add_Destination
netflow_Event_Types	将要为目标导出的事件类型定义为以下任意项的子集：**all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update**。	Netflow_Add_Destination
netflow_Parameters	提供 NetFlow 导出全局设置：活动刷新间隔（流更新事件之间的分钟数）、延迟（以秒为单位的流创建延迟；默认值 0 = 命令不会出现）和以分钟为单位的模板超时速率。	Netflow_Set_Parameters
PrefixDelegationInside	为 DHCPv6 前缀委派配置内部接口。该对象包含多个条目，依次为接口名称、包含前缀长度的 IPv6 后缀以及前缀池名称。	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
PrefixDelegationOutside	配置外部 DHCPv6 前缀委派客户端。该对象包括多个条目，依次为接口名称和 IPv6 前缀长度条目	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
serviceIdentifier	动态 WCCP 服务标识符编号。	Wccp_Configure
tcp_conn_limit （已弃用。）	用于配置 TCP 初始连接限制的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit
tcp_conn_misc （已弃用。）	用于配置 TCP 初始连接设置的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit、TCP_Embryonic_Conn_Timeout

名称	说明	关联的 **FlexConfig** 对象
tcp_conn_timeout （已弃用。）	用于配置 TCP 初始连接超时的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Timeout
tcpMssBytes	最大段大小（以字节为单位）。	Sysopt_basic
tcpMssMinimum	检查是否设置最大段大小 (MSS)，只有此标志为 true 时才设置该值。	Sysopt_basic
threat_detection_statistics	用于TCP拦截的威胁检测统计信息的参数。	Threat_Detection_Configure
vxlan_Nve_Only	用于在接口上配置仅 NVE 的参数： • 接口的逻辑名称 • IPv4 地址（对于路由接口而言可选） • Ipv4 网络掩码（对于路由接口而言可选）	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	用于为 VXLAN 配置端口和 NVE 的参数： • Vxlan 端口 • 源接口（逻辑名称） • 类型（对等体或组播） • 对等体 IP 地址或 default-mcast-grooup	VxLAN_Configure_Port_And_Nve

名称	说明	关联的 FlexConfig 对象
vxlan_Vni	用于创建 VNI 的参数： • 接口编号 (1-10000) • segment-id (1-16777215) • nameif（接口的逻辑名称） • 类型（路由或透明） • IP 地址（如果是路由模式设备时使用）或网桥组编号（如果是透明模式设备时使用） • 网络掩码（如果设备处于路由模式）或未使用	VxLAN_Make_Vni
wccpPassword	WCCP 密码。	Wccp_Configure

FlexConfig 策略的要求和先决条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

FlexConfig 的准则与限制

- 如果您在 FlexConfig 策略中犯错，系统将回滚包含失败的 FlexConfig 的部署尝试中包含的所有更改。由于部署失败导致的回滚包括了清除配置，因此这可能会中断您的网络。考虑将FlexConfig 更改纳入非营业时间的计时部署中。此外，请考虑隔离部署，使其仅包括 FlexConfig 更改而不包括其他策略更新。
- 使用 VxLAN_Make_VNI 对象时，必须在形成集群或高可用性对之前，将相同的 FlexConfig 部署到该集群或高可用性对中的所有设备。在形成集群或高可用性对之前，管理中心要求VXLAN 接口在所有设备上都匹配。

- 必须仅在全局 webvpn 配置模式下配置 **webvpn keepout** 命令。webvpn group-policy 属性或用户名属性配置模式不支持 **keepout** 命令。请勿在策略组 FlexConfig 对象中包含 **keepout** 命令。
- 如果配置适用于连接的任何服务（例如 SIP 检测），请转至设备 CLI 并输入 **clear conn** 命令以清除连接。重建连接时，新配置将应用于会话。
- QoS 规则和服务策略规则（在访问控制策略中）将转换为防火墙上的命令。这包括创建策略映射。每个接口只能有一个策略映射。系统会自动将 QoS 和服务策略配置合并到每个接口的单个策略映射中。

  但是，您也可以使用 FlexConfig 手动创建策略映射。对于低端防火墙（例如 Cisco Secure Firewall 3100），您可以在配置中创建多达 64 个策略映射。对于功能更强大的防火墙（例如 Firepower 4100），您最多可以创建 128 个策略映射。请注意不要超过此限制，否则部署将失败。您可以从 CLI 查看设备配置，也可以使用部署脚本查看如何将规则转换为命令。

使用 FlexConfig 策略自定义设备配置

使用 FlexConfig 策略自定义 Firewall Threat Defense设备的配置。

在使用 FlexConfig 之前，请尝试使用 防火墙管理中心中的其他功能配置所需的所有策略和设置。FlexConfig 是一种配置基于 ASA 的与 Firewall Threat Defense兼容但在 防火墙管理中心中不可配置的功能的必备方法。

以下是配置和部署 FlexConfig 策略的端到端过程。

过程

步骤 1 确定要配置的 CLI 命令序列。

如果在 ASA 设备上具有有效的配置，请使用 **show running-config** 获取所需命令的序列。根据需要对接口名称和 IP 地址等项目进行调整。

如果此步骤是面向新功能，最好尝试在实验室设置中的ASA 设备上实现，以验证您具有正确的命令序列。

有关详细信息，请参阅以下主题：

- FlexConfig 策略的建议用法，第 1042 页
- FlexConfig 对象中的 CLI 命令，第 1042 页

步骤 2 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

检查预定义的 FlexConfig 对象，以确定是否能够生成所需的命令。点击 **视图**（） 以查看对象内容。如果现有对象接近您所需的内容，请首先复制该对象，然后编辑副本。请参阅预定义的FlexConfig 对象，第 1052 页。

检查这些对象还可以让您了解 FlexConfig 对象的结构、命令语法和预期顺序。

注释
如果找到要使用的任何对象（直接对象或或是副本），请检查对象底部的“变量”列表。记下变量名称，但全部采用以 SYS 开头的大写字母的变量除外，这些是系统变量。这些变量是您编辑和定义覆盖可能需要的文本对象，尤其是在默认值列显示对象没有值的情况下更是如此。

步骤 3 如果需要创建自己的 FlexConfig 对象，请确定需要哪些变量并创建关联对象。

您需要部署的 CLI 可能包含 IP 地址、接口名称、端口号以及以后可能需要调整的其他参数。这些变量已经与指向包含所需值的变量实现了最好的分隔。对于属于配置一部分，但以后可能会更改的字符串，您可能也需要变量。

此外，还要确定是否要为您将为其分配策略的每个设备使用不同的值。例如，您可能希望在三个设备上配置该功能，但可能需要为其中每个设备在给定命令上指定不同的接口名称或 IP 地址。如果需要为每个设备自定义对象，请确保在创建对象时启用覆盖，然后按设备定义覆盖值。

有关各种类型的变量的解释以及如何在需要时配置相关对象，请参阅下列主题。

- FlexConfig 变量， 第 1045 页
- FlexConfig 策略对象变量， 第 1050 页
- FlexConfig 系统变量， 第 1051 页
- 配置 FlexConfig 文本对象， 第 1067 页

步骤 4 如果使用预定义的 FlexConfig 对象，请编辑用作变量的文本对象。

请参阅配置 FlexConfig 文本对象， 第 1067 页。

步骤 5 （如有必要。）配置 FlexConfig 对象， 第 1063 页。

只有在预定义的对象无法创建对象时，您才需要执行此操作。

步骤 6 配置 FlexConfig 策略， 第 1068 页。

步骤 7 为 FlexConfig 策略设置目标设备， 第 1069 页。

还可以在创建策略时将策略分配给设备。策略必须至少有一个已分配的设备，您才能预览它。

步骤 8 预览 FlexConfig 策略， 第 1070 页。

必须先保存更改，才能预览策略。

验证所生成的命令是否是所预期的，以及所有变量是否都在正确解析。

步骤 9 在菜单栏中选择**部署 (Deploy)** > **部署 (Deployment)**。

步骤 10 选择分配给该策略的设备，然后点击**部署 (Deploy)**。

等待部署完成。

步骤 11 验证部署的配置， 第 1071 页。

步骤 12 （如有必要。）删除使用 FlexConfig 配置的功能， 第 1072 页。

与其他类型的策略不同，仅仅从一台设备取消分配 FlexConfig 可能不会删除相关的配置。如果要删除 FlexConfig 生成的配置，需要遵循上述程序。

如果您要删除某项功能，因为产品目前已支持该功能，另请参阅从 FlexConfig 转换为管理功能，第 1074 页。

配置 FlexConfig 对象

使用 FlexConfig 对象定义要部署到设备的配置。每个 FlexConfig 策略由一个 FlexConfig 对象列表组成，因此这些对象实质上是由 Apache 速度脚本命令、ASA 软件配置命令和变量组成的代码模块。

有几个可以直接使用的预定义 FlexConfig 对象，或者如果需要编辑这些对象，可以制作对象副本。还可以从头创建自定义对象。FlexConfig 对象的内容可以是从一个简单的命令字符串到复杂 CLI 命令结构的任何内容，复杂CLI命令结构使用变量和脚本命令来部署其内容因设备或部署而异的命令。

还可以在定义 FlexConfig 策略时创建 FlexConfig 策略对象。

开始之前

记住以下几点：

- FlexConfig 对象转换为随后部署到设备的命令。这些命令已在全局配置模式下发出。因此，请不要将 **enable** 和 **configure terminal** 命令作为 FlexConfig 对象的一部分。
- 确定所需的变量类型，并创建所需的任何策略对象。编辑 FlexConfig 对象时，不能为变量创建对象。
- 确保您的命令与设备上的 VPN 或访问控制配置没有任何冲突。
- 如果接口有多组命令，只部署最后一组命令。因此，我们建议您不要使用开始和结束命令来配置接口。有关配置接口的示例，请参阅 ISIS_Interface_Configuration 预定义的 FlexConfig 对象。

过程

步骤 1 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

步骤 2 执行以下操作之一：

- 点击**添加 FlexConfig 对象**以创建新对象。
- 点击 **编辑** (✎) 以编辑现有对象。
- 点击 **视图**（🔍） 可查看预定义对象的内容。
- 如果要编辑预定义对象，请点击 **克隆** （⧉） 以创建具有相同内容的新对象。

步骤 3 为对象输入**名称**和（可选）说明

步骤 4 在对象正文区域中，输入生成所需配置的命令和说明。

对象内容是生成有效的 ASA 软件命令序列的脚本命令和配置命令序列。Firewall Threat Defense设备使用 ASA 软件命令来配置某些功能。有关脚本和配置命令的详细信息，请参阅：

- 模板脚本，第 1045 页
- FlexConfig 对象中的 CLI 命令，第 1042 页

您可以使用变量来提供只有在运行时才知道的信息，或者每个设备都不同的信息。您只需键入处理变量，但必须使用**插入**菜单添加与策略对象或系统变量相关联的变量，或者是密钥的变量。有关变量的完整讨论，请参阅FlexConfig 变量，第 1045 页。

- 要插入系统变量，请选择**插入** > **插入系统变量** > **变量名称**。有关这些变量的详细说明，请参阅FlexConfig 系统变量，第 1051 页。
- 要插入策略对象变量，请选择**插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。然后，为变量命名（可以与关联的策略对象同名），选择要与该变量关联的对象，然后点击**保存**。有关这些类型的详细说明，请参阅FlexConfig 策略对象变量，第 1050 页。有关过程的详细信息，请参阅将策略对象变量添加到 FlexConfig 对象，第 1065 页。
- 要插入密钥变量，请选择**插入** > **密钥**并定义变量名称和值。有关过程的详细信息，请参阅配置密钥，第 1066 页。

注释
必须使用**插入**菜单来创建新的策略对象或系统变量。但是，对于该变量的后续使用，您必须键入该变量，包括 $。系统变量也是如此：第一次使用变量时，请从**插入**菜单中添加这些变量。然后，键入该变量以供后续使用。如果对系统变量多次使用**插入**菜单，系统变量将多次添加到变量列表中，FlexConfig 将无法验证，这意味着您无法保存更改。对于处理变量（与策略对象或系统变量不关联的变量），只需输入变量即可。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

步骤 5 选择部署频率和类型。

- **部署** - 将对象中的命令部署为**一次**还是**每次**。选择正确选项的唯一方法是测试部署结果。

  通过选择**每次**来开始操作。然后，在将对象附加到FlexConfig 策略后，部署配置。成功部署后，返回 FlexConfig 策略并预览其中一个已分配设备的配置，如预览 FlexConfig 策略，第 1070 页中所述。如果标记为 `###CLI generated from managed features ###` 的部分包含清除或否定对象中命令的命令，且 `###Flex-config Appended CLI ###` 部分包含重新配置此功能的命令，您便可以知道**每次**是正确的选项。

  即使没有看到否定命令，也需对设备配置进行一些细微更改，然后再运行另一个部署。如果成功完成部署，则可以检查部署脚本（请参阅验证部署的配置，第 1071 页）。如果您看到命令再次发出（即使它们已经配置）且没有出错，则可以保留**每次**选项。

  仅当系统在再次发出对象中的命令之前没有首先否定命令，或者部署导致出现特定于命令的错误时，才更改为**一次**。在某些情况下，系统不允许您发出已配置的命令，但这是例外情况。

  一些额外提示：

- 如果 FlexConfig 对象指向系统托管对象，例如网络或 ACL 对象，请选择**每次**。否则，可能无法部署对象的更新。
- 如果您在对象中执行的唯一操作是清除配置，请选择**一次**。然后，在下一次部署后从 FlexConfig 策略中删除此对象。

- **类型** - 选择以下一个选项：
  - **追加** -（默认值）。对象中的命令将放在从 防火墙管理中心 策略生成的配置的末尾。如果使用策略对象变量（指向从托管对象生成的对象），则必须使用追加。如果为其他策略生成的命令与对象中指定的指令重叠，则应选择此选项，以使您的命令不会被覆盖。这是最安全的选项。
  - **预置** - 对象中的命令放在从 防火墙管理中心 策略生成的配置的开始处。通常对清除或否定配置的命令使用预置。

步骤 6 （可选。）点击对象正文上方的 **验证** （）以检查脚本的完整性。

点击**保存**时始终验证该对象。无法保存无效对象。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

将策略对象变量添加到 FlexConfig 对象

可以向与其他类型的策略对象相关联的 FlexConfig 策略对象中插入变量。在将 FlexConfig 部署到某一设备后，这些变量将解析到相关联对象的名称或内容。

对于首次在 FlexConfig 对象中使用策略对象变量，可以使用以下程序。如果需要再次引用该对象，则请键入该变量（包括 $ 符号）。要了解如何使用这些变量，请参阅如何处理变量，第 1046 页。

开始之前

有关编辑 FlexConfig 对象的更多信息，请参阅 配置 FlexConfig 对象，第 1063 页。

过程

步骤 1 在编辑 FlexConfig 策略对象时，依次选择 **插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。

步骤 2 输入变量的名称和说明（后者为可选项）。

该名称在 FlexConfig 对象的上下文中必须是唯一的。其中不能包含空格。允许使用跟与变量相关联的对象完全相同的名称。

步骤 3 选择要与变量相关联的对象，然后点击**添加**，以将其移至**选定对象**列表中。

只能使一个变量与一个对象相关联。

注释
对于文本对象，可以根据需要选择任何预定义对象。不过，很多此类对象没有默认值。必须更新这些对象，以直接或以覆盖方式，为将要向其部署 FlexConfig 对象的设备添加所需的值。尝试在不更新这些对象的情况下部署 FlexConfig，通常会导致部署错误。

步骤 4 点击**保存**。

该变量将显示在位于 FlexConfig 对象编辑器底部的“变量”列表中。

配置密钥

密钥是要屏蔽其内容的任何单字符串变量，如密码。系统为这些变量提供特殊处理，以帮助您防止敏感信息的散播。

密钥变量不会显示在 FlexConfig 对象中的“变量”列表中。

使用以下过程在 FlexConfig 对象中创建、插入以及以其他方式管理密钥变量。与其他类型的变量不同，您可以在每次需要插入给定的密钥变量时使用**插入**命令。在处理方面，这些变量的行为类似于单值文本对象变量；请参阅单值变量，第 1046 页。



注释 在密钥变量中定义的任何数据都将对用户屏蔽，预览 FlexConfig 策略时除外。此外，如果导出 FlexConfig 策略，则会删除任何密钥变量的内容。导入策略时，需要手动编辑每个密钥变量以输入数据。

开始之前

有关编辑 FlexConfig 对象的更多信息，请参阅配置 FlexConfig 对象，第 1063 页。

过程

步骤 1 编辑 FlexConfig 策略对象时，请选择**插入** > **密钥**。

步骤 2 在 **插入密钥** 对话框中，执行以下任意操作：

- 要创建新密钥，请点击**添加密钥 (Add Secret Key)**，然后填写以下信息并点击**添加 (Add)**。
  - **密钥名称** - 变量的名称。此名称显示在 FlexConfig 对象中，以 @ 为前缀。
  - **密码**、**确认密码** - 密钥字符串，在键入时用星号进行隐蔽。
- 要在 FlexConfig 对象中插入一个密钥变量，请选中该变量对应的复选框。

- 要编辑密钥变量的值，请点击该变量的 **编辑** (✎) 。进行更改并点击**添加 (Add)**。
- 要删除密钥变量，请点击该变量的 **删除** (🗑) 。

步骤 3 点击**保存**。

配置 FlexConfig 文本对象

将 FlexConfig 对象中的文本对象用作策略对象变量的目标。您可以使用变量来提供只有在运行时才知道的信息，或者每个设备都不同的信息。在部署过程中，指向文本对象的变量将替换为文本对象的内容。

文本对象可以包含自由格式的字符串，可以是关键字、接口名称、数字、IP 地址等等。内容取决于您在 FlexConfig 脚本中使用这些信息的方式。

在创建或编辑文本对象之前，请准确确定需要的内容。这包括您打算如何处理对象，这将有助于您在创建单字符串或多字符串对象之间做出决定。阅读以下主题：

- FlexConfig 变量，第 1045 页
- 如何处理变量，第 1046 页

过程

步骤 1 选择**对象** > **FlexConfig** > **文本对象**。

步骤 2 执行以下操作之一：

- 点击**添加文本对象**以创建一个新对象。
- 点击 **编辑** (✎) 以编辑现有对象。您可以编辑预定义的文本对象，如果您打算使用预定义的 FlexConfig 对象，则需要这样做。

步骤 3 为对象输入**名称**和（可选）说明。

步骤 4 （仅新对象。）从下拉列表中选择**变量类型**：

- **单个** - 如果对象应包含单个文本字符串。
- **多个** - 如果对象应包含文本字符串列表。

保存对象后，则无法更改变量类型。

步骤 5 如果变量类型为**多个**，则使用向上和向下箭头指定**计数**。

在更改数字时，会在对象中添加或删除行。

步骤 6 向对象添加内容。

您可以在变量号旁边的文本框中点击并键入一个值，也可以为每个将被分配使用此文本对象的 FlexConfig 对象的设备设置设备覆盖。您也可以同时执行这两种方法，在这种情况下，在基本对象中配置的值在给定设备的覆盖不存在的情况下充当默认值。

在编辑预定义对象时，最好使用设备覆盖，这样，对于可能需要在不同 FlexConfig 策略中使用该对象的其他用户来说，系统默认值仍然存在。您所采取的方法取决于组织的要求。

提示
某些预定义对象需要多个值，其中每个值都有特定的用途。仔细阅读说明文本以确定对象中的预期值。在某些情况下，这些说明指定您必须使用覆盖而不是更改基本值。如果是 enableInspectProtocolList，您将无法进入其检测与 Snort 检查不兼容的协议。

如果决定使用覆盖，请执行以下操作。

a) 选中 **允许覆盖** 复选框。
b) 展开“覆盖”区域（如果需要），然后点击**添加 (Add)**。

   如果设备已存在覆盖，请点击该覆盖的编辑以更改它。

c) 在“添加对象覆盖”对话框的 **目标** 卡上，选择要为其定义值的设备，然后点击 **添加** 将其移动到“选定设备”列表中。
d) 点击 **覆盖**，根据需要调整 **计数** ，然后在变量字段中点击并键入设备的值。
e) 点击**添加 (Add)**。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改 ， 第 180 页。

配置 FlexConfig 策略

FlexConfig 策略包含 FlexConfig 对象的两个有序列表，一个预置列表和一个附加列表。有关对预置/附加的解释，请参阅配置 FlexConfig 对象 ， 第 1063 页。

FlexConfig 策略是可以分配给多个设备的共享策略。

过程

步骤 1 选择**设备** > **+ 显示更多** > **FlexConfig**。

步骤 2 执行以下操作之一：

- 点击**新建策略**创建新的 FlexConfig 策略。系统将提示您输入名称。（可选）选择“可用设备”列表中的设备，然后点击**添加到策略**以分配设备。点击**保存**。
- 点击 **编辑** (✎) 以编辑现有策略。可以通过在编辑模式下点击名称或说明来对其进行更改。

- 点击 **复制** () 以创建具有相同内容的新策略。系统将提示您输入名称。系统不会为副本保留设备分配。
- 点击删除可删除不再需要的策略。

步骤 3 从**可用 FlexConfig** 列表中选择策略所需的 FlexConfig 对象，然后点击 > 将它们添加到策略中。

对象将根据 FlexConfig 对象中指定的部署类型自动添加到预置或附加列表中。

要删除所选对象，请点击对象旁边的 **删除** () 。

步骤 4 对于每个所选对象，点击该对象旁边 **视图**（） 可以标识该对象中使用的变量。

除了系统变量（从 SYS 开始），您需要确保与变量关联的对象不为空。在它们之间没有任何内容的空白或方括号 [] 表示空对象。在部署策略之前，您需要编辑这些对象。

注释
如果使用对象覆盖，则这些值不会显示在此视图中。因此，空的默认值不一定表示您没有使用所需的值更新对象。预览配置将显示变量是否对给定设备正确解析。请参阅预览FlexConfig策略，第1070页。

步骤 5 点击**保存**。

下一步做什么

- 设置策略的目标设备；请参阅为 FlexConfig 策略设置目标设备，第 1069 页。
- 部署配置更改；请参阅 部署配置更改，第 180 页。

为 FlexConfig 策略设置目标设备

创建FlexConfig策略时，可以选择使用该策略的设备。您可以随后更改策略的设备分配，如下所述。

注释 通常，当您从设备取消分配策略时，系统会在下次部署时自动删除关联的配置。但是，由于FlexConfig对象是用于部署自定义命令的脚本，因此只从设备取消分配 FlexConfig 策略不会删除由 FlexConfig 对象配置的命令。如果您打算从设备配置中删除FlexConfig生成的命令，请参阅删除使用FlexConfig配置的功能，第 1072 页。

过程

步骤 1 选择**设备** > **+ 显示更多** > **FlexConfig**并编辑 FlexConfig 策略。

步骤 2 点击**策略分配**。

步骤 3 在 **目标设备** 上，建立目标列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。可以将策略分配给设备、高可用性对和集群设备。
- 删除 - 点击单个设备旁边的 **删除** ( )，或选择多个设备，点击右键，然后选择 **删除选择**。

步骤 4 点击**确定**，保存选择。

步骤 5 点击**保存**以保存 FlexConfig 策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

预览 FlexConfig 策略

预览 FlexConfig 策略可以查看 FlexConfig 对象如何转换为 CLI 命令。预览将显示从 FlexConfig 对象中使用的脚本和变量为选定设备生成的命令。这些变量基于设备的配置进行解析，因此您可以清楚地了解将部署什么。

使用预览可以查找 FlexConfig 对象中存在的潜在问题。更正对象，直到预览显示预期结果为止。

您必须单独预览每个设备的配置，因为这些变量可以基于设备配置进行不同的解析。

过程

步骤 1 选择**设备** > **+ 显示更多** > **FlexConfig**并编辑 FlexConfig 策略。

步骤 2 如果有任何待保存的更改，请点击**保存**。

预览仅显示最近保存的策略版本中的那些 FlexConfig 对象的结果。必须保存策略才能查看新添加对象的预览。

步骤 3 点击**预览配置**。

步骤 4 从**选择设备**下拉列表中选择设备。

系统从设备和配置的策略中检索信息，并确定将在下次部署到设备时生成哪些 CLI 命令。您可以选择输出并使用 Ctrl+C 将其复制到剪贴板，您可以再次将其粘贴到文本文件中以进行进一步分析。

预览包括以下部分：

- Flex-config 预置 CLI - 这些是由 FlexConfigs 生成、的命令，这些命令。
- 从托管功能生成的 CLI - 这些是为在 防火墙管理中心中配置的策略生成的命令。自上次成功部署到设备后，系统将为新的或更改的策略生成命令。这些命令并不代表实现分配的策略所需的所有命令。本部分中的任何命令都不是从 FlexConfig 对象中生成。
- Flex-config 附加 CLI - 这些是由 FlexConfigs 生成、将被附加到配置的命令。

步骤 5 点击**关闭**以关闭预览对话框。

验证部署的配置

在将 FlexConfig 策略部署到设备后，请验证部署是否成功，以及得到的配置是否是您所预期的。此外，请验证设备是否按预期工作。

过程

步骤 1 要验证部署是否成功，请执行以下操作：

a) 点击菜单栏中的 **通知** ，即 **部署** 和 **系统**之间的未命名。

该图标看起来像以下图标中的一个，如果有错误，它可能会包括数字：

- **指示无警告** - 指示系统上不存在任何警告或错误。
- 指示 **一个或多个警告** - 指示系统上存在一个或多个警告而没有错误。
- **指示一个或多个错误** - 指示系统上存在一个或多个错误和任意数量的警告。

b) 在 **部署**上，验证部署是否成功。

c) 要查看更多详细信息，特别是对于失败的部署，请点击**显示历史记录**。

d) 在左侧列的作业列表中选择部署作业。

作业以倒序顺序列出，最近的作业位于列表顶部。

e) 在右侧列中点击设备的 **脚本** 列中的下载。

部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示您通过 FlexConfig 发送的命令错误的消息。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释
为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示 防火墙管理中心 发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为 0。Firewall Threat Defense 不会将安全级别用于任何操作。与 FlexConfig 相关的消息在该脚本的“CLI 应用”部分中。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

步骤 2 验证部署的配置是否包含预期的命令。

您可以通过与设备的管理 IP 地址建立 SSH 连接来完成此项工作。使用 **show running-config** 命令查看配置。

或者，在 Secure Firewall Management Center中使用 CLI 工具。

a) 选择 > **运行状况** > **监控器故障排除** 并点击设备名称。

   您可能需要点击状态表中**计数**列中的打开/关闭箭头来查看任何设备。

b) 点击**高级故障排除 (Advanced Troubleshooting)**。
c) 点击**威胁防御 CLI (Threat Defense CLI)**。
d) 选择 **show** 作为命令，然后键入 **running-config** 作为参数。
e) 点击**执行 (Execute)**

   正在运行的配置显示在文本框中。您可以选择配置并按Ctrl+C，然后将其粘贴到文本文件中以供以后分析。

步骤 3 验证设备是否按预期工作。

使用与此功能相关的**show**命令可查看详细信息和统计信息。例如，如果您启用了其他协议检查，则**show service-policy** 命令会提供此信息。要使用的确切命令与功能相关，并且应在您用来了解如何配置此功能的 ASA 配置指南和命令参考中提及。

如果显示统计信息的命令指示数字未发生更改（例如，命中次数、连接计数等），则配置可能有效，但没有意义。如果您知道流量正在通过应在统计中显示的设备，则查找配置中缺少的内容。例如，NAT 或访问规则可能需要丢弃或更改流量，才能对其应用此功能。

您可以从 SSH 会话或通过 防火墙管理中心 CLI 工具使用 **show** 命令。

但是，如果您需要使用的 **show** 命令无法直接从 Firewall Threat Defense CLI 中获得，则需要与设备建立 SSH 连接才能使用这些命令。在 CLI 中，输入以下命令序列以在诊断 CLI 中进入特权 EXEC 模式。您可以在此处输入这些不受支持的 **show** 命令。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

删除使用 FlexConfig 配置的功能

如果您决定需要删除使用 FlexConfig 配置的一组配置命令，则可能需要手动删除该配置。从设备取消分配 FlexConfig 策略可能不会删除所有配置。

要手动删除该配置，请创建新的 FlexConfig 对象以清除或取消配置命令。

开始之前

要确定是否需要手动删除对象生成的部分或全部配置，请执行以下操作：

1. 检查配置预览，如预览 FlexConfig 策略，第 1070 页中所述。如果 `###CLI generated from managed features ###` 部分包含清除或否定命令以删除 FlexConfig 对象中的所有命令，您只需从 FlexConfig 策略中删除此对象，保存并重新部署。
2. 从 FlexConfig 策略中删除对象，保存更改，然后再次预览配置。如果 `###CLI generated from managed features ###` 部分仍不包含所需的清除或否定命令，则必须按照此程序手动删除配置。

过程

步骤 1 选择 **对象** 并创建用于清除或否定配置命令的 FlexConfig 对象。

如果某个功能具有可以删除所有配置设置的 **clear** 命令，则使用此命令。例如，预定义的 ISIS_Unconfigure_All 对象就包含一个可以删除所有与 ISIS 相关的配置命令的命令：

```
clear configure router isis
```

如果此功能没有 **clear** 命令，则需要使用每个要删除的命令的 **no** 形式。例如，预定义的 Sysopt_basic_negate 对象将删除通过预定义的 Sysopt_basic 对象配置的命令。

```
no sysopt traffic detailed-statistics
```

```
no sysopt connection timewait
```

通常，您将配置一个 FlexConfig 对象，以预置的一次性部署对象形式删除配置。

步骤 2 选择 **设备** > **+ 显示更多** > **FlexConfig** 并创建新的 FlexConfig 策略或编辑现有策略。

如果要保留部署配置命令的 FlexConfig 策略，请创建一个专门用于取消命令的新策略，并将设备分配给该策略。然后，将新的 FlexConfig 对象添加到该策略。

如果要从所有设备中完全删除 FlexConfig 配置对象，只需从现有 FlexConfig 策略中删除这些命令，并将它们替换为取消该配置的对象。

步骤 3 点击**保存**以保存 FlexConfig 策略。

步骤 4 点击**预览配置**并确认清除和取消命令会正确生成。

步骤 5 选择菜单栏中的 **部署** > **部署** ，选择该设备，然后点击 **部署**。

等待部署完成。

步骤 6 验证是否已删除命令。

查看设备上正在运行的配置，以确认这些命令已被删除。有关详细信息，请参阅验证部署的配置，第 1071 页。

步骤 7 编辑 FlexConfig 策略时，点击**策略分配**并删除该设备。（可选）从策略中删除 FlexConfig 对象。

假定 FlexConfig 策略仅删除不需要的配置命令，则在删除完成后无需保留分配给该设备的策略。

但是，如果 FlexConfig 策略保留了您仍希望在设备上配置的选项，请从策略中删除取消对象。不再需要保留它们。

从 FlexConfig 转换为管理功能

每个软件版本都会向产品添加托管功能，也就是您通过在 FlexConfig 外部控制的策略直接配置的功能。这可能会弃用您当前使用的 FlexConfig 命令；您的配置不会自动转换。在升级后，您无法使用新近弃用的命令来分配或创建 FlexConfig 对象。在升级软件后，检查 FlexConfig 策略和对象。

在使用 FlexConfig 配置的功能开始受支持作为托管功能时，您必须从使用 FlexConfig 转换为使用托管功能。在大多数情况下，您现有的 FlexConfig 配置会在升级后继续工作，您仍然可以进行部署。但在某些情况下，使用已弃用的命令可能会导致部署问题。不支持同时在 GUI 和 FlexConfig 中配置功能。

注释 如果迁移工具支持您要迁移的功能配置，请使用迁移工具来代替此程序。

过程

步骤 1 删除 FlexConfig，如删除使用 FlexConfig 配置的功能，第 1072 页中所述。

步骤 2 配置最新支持的托管功能中的设置。

版本说明包含了该版本的新功能列表。

FlexConfig 示例

以下是使用 FlexConfig 的一些示例。

如何配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 Firewall Threat Defense 设备配置为透明时钟。 Firewall Threat Defense 设备不会将其时钟与 PTP 时钟同步。 Firewall Threat Defense 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，可以配置多个 PTP 域，然后将每个非 PTP 设备配置为特定域使用 PTP 时钟。

开始之前

确定设备应使用的 PTP 时钟上配置的域编号。此示例假定 PTP 域编号为 10。另外，确定系统可通过哪些接口到达域中的 PTP 时钟。

以下是 PTP 配置准则：

- 此功能在思科 ISA 3000 设备上不可用。
- 思科 PTP 仅支持组播 PTP 消息。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网数据接口支持 PTP 配置，无论是独立式还是网桥组成员。管理接口、子接口、Etherchannel 接口、桥接虚拟接口 (BVI) 或任何其他虚拟接口均不支持此版本。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。PTP 流量由 UDP 目标端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此允许此流量的任何访问控制规则均应有效。
- 在路由防火墙模式下，必须为 PTP 组播组启用组播路由：此外，如果启用 PTP 的接口**不**在网桥组中，则必须将该接口配置为加入 IGMP 组播组 224.0.1.129。如果物理接口是网桥组成员，则不要将其配置为加入 IGMP 组播组。

过程

步骤 1 （仅路由模式。）启用组播路由，并为接口配置 IGMP 组。

在路由模式下，必须启用组播路由。此外，对于独立物理接口（即非网桥组成员），还必须配置接口以加入 224.0.1.129 IGMP 组。您无法将网桥组成员配置为加入 IGMP 组，但网桥组成员上的 PTP 配置将在没有 IGMP 加入的情况下起效。

对要配置 PTP 的每台设备执行此程序。

注释
记下每个设备上每个面向 PTP 时钟的接口的硬件名称，例如，GigabitEthernet1/1。

a) 选择 **设备** > **设备管理**，然后编辑设备。
b) 点击**路由 (Routing)**。
c) 选择 **组播路由** > **IGMP**。
d) 选中**启用组播路由**复选框。
e) 点击**加入组 (Join Group)**。
f) 点击 **添加**，，然后在 **添加 IGMP 加入组参数** 对话框中，配置以下选项，然后点击 **确定**。
   - **接口 (Interface)** - 选择面向 PTP 时钟的独立接口。

- **加入组 (Join Group)** - 点击 + 以添加新的网络对象。使用地址 224.0.1.129 来创建主机对象。在配置其他接口时，可直接选择此对象。（请参阅创建网络对象，第 2660 页。）

对设备上每个面向 PTP 时钟的独立接口重复此步骤。

g) 点击“路由”页面上的**保存**。

步骤 2 创建 FlexConfig 对象，以便全局启用 PTP 以及在接口上启用 PTP。

以下程序假定您正在配置的每台设备上的面向 PTP 时钟的接口均相同。如果在不同的设备上使用了不同的接口，则您需要为每个不同的组合创建单独的对象。例如，如果您在设备 A 和 B 上使用 GigabitEthernet1/1，在设备 C 和 D 上使用 GigabitEthernet1/2，在设备 E 和 F 上同时使用 GigabitEthernet1/1 和 1/2，则您需要 3 个单独的 FlexConfig 对象，随后还需要 3 个单独的 FlexConfig 策略（将在下一步中进行说明）。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Enable_PTP。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。这样可确保在这些命令之前配置对接口配置所做的任何其他更改。
- **对象正文 (Object body)** - 在对象正文中，键入在每个面向 PTP 时钟的接口上全局配置 PTP 所需的命令。例如，PTP 域 10 的全局配置和 GigabitEthernet1/1 上的接口配置所需的命令如下：

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

此对象正文应如下所示：



步骤 3 创建 FlexConfig 策略并将其分配给设备。

如果为面向 PTP 时钟的接口的不同组合创建了多个 FlexConfig 对象，则需要为每个对象创建单独的 FlexConfig 策略，并根据需要配置的接口将这些策略分配给正确的设备。对每组设备重复以下程序。

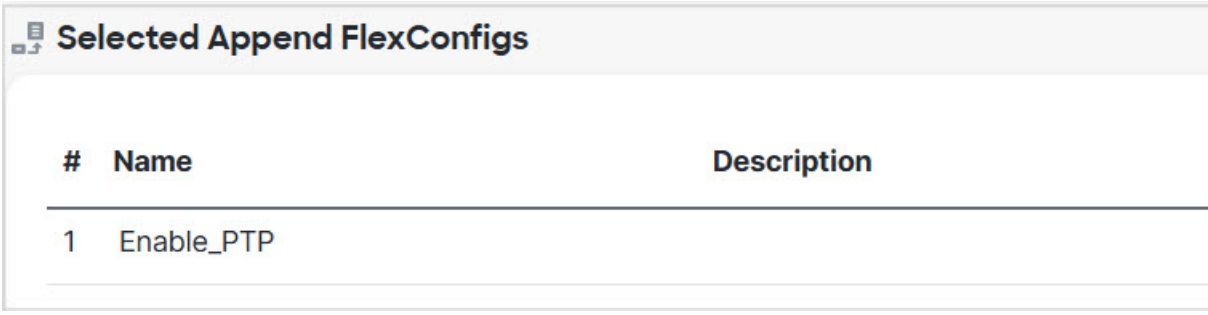
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择 PTP FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 PTP FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于 PTP 命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

步骤 4 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 1071 页。

步骤 5 在每台设备上验证 PTP 配置。

从 SSH 或控制台会话到每台设备，验证 PTP 设置：

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
```

```
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 1
 PTP version: 2
 Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 2
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 3
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

如何对电源故障配置自动硬件旁路 (ISA 3000)

您可以启用硬件旁路，使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件旁路。

启用硬件旁路时，流量将在这些接口对之间的第 1 层传递。Firewall Threat Defense CLI 将显示接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

在 CLI 控制台或 SSH 会话中，使用 **show hardware-bypass** 命令以监控运行状态。

开始之前

要使用硬件旁路：

- 必须将接口对放置在同一网桥组内。
- 必须将接口连接到交换机的接入端口。不能将它们连接到中继端口。

我们建议您通过使用附加到分配给设备的访问控制策略的威胁防御服务策略，来全局禁用 TCP 序列号随机化。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。硬件旁路激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时关闭。

过程

步骤 1 创建 FlexConfig 对象以启用自动旁路。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。
b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Enable_HW-Bypass。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入启用自动硬件旁路所需的命令。例如，两个可能的接口对所需的命令：

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

此对象正文应如下所示：



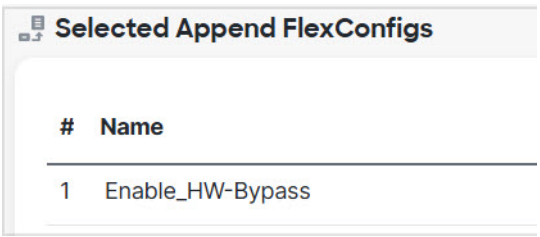
步骤 2 创建 FlexConfig 策略并将其分配给设备。

a) 选择**设备** > **+ 显示更多** > **FlexConfig**。
b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择硬件旁路 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。
e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。
f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从硬件旁路 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于硬件旁路命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 1071 页。

下一步做什么

如果您要手动调用硬件旁路或手动将其关闭，则需要创建两个 FlexConfig 对象：

- 一个是手动启动绕行，其中包含以下一个或两个命令，具体取决于您是否要为两个对调用绕行：

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- 另一个是手动关闭旁路，其中包含以下一个或两个命令：

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

然后，您需要将一个或另一个对象添加到 FlexConfig 策略中并部署更改，以打开或关闭绕行。您还需要在部署后立即从 FlexConfig 策略中删除该对象。如果您手动调用绕行，则需要重复该过程以再次将其关闭。因此，使用此手动方法需要经常仔细编辑 FlexConfig 策略和其他部署。

迁移 FlexConfig 策略

注意 有关迁移 FlexConfig 策略的本节仅适用于迁移 ECMP、VXLAN 和 EIGRP 策略。

使用 FlexConfig 对象和早期版本 防火墙管理中心中的策略配置了 ECMP、VXLAN 和 EIGRP 策略。您现在可以直接在管理中心UI中配置这些策略。从早期版本升级管理中心时，系统会保留FlexConfig配置。但是，要从 UI 管理策略，您必须在相应的**设备（编辑）(Device [Edit])** > **路由 (Routing)** 页面重新执行配置，并从 FlexConfig 中删除配置。要在 UI 中自动创建策略，防火墙管理中心 提供了将策略从FlexConfig迁移到UI的选项。但是，它不会从FlexConfig中删除已迁移的策略。有关迁移后的程序，请参阅步骤 7，第 1081 页。

开始之前

- 确保部署的FlexConfig策略是最新的，而不是过时的。只有当策略在至少1台设备上为最新时，迁移选项才可用。对于具有过期策略的设备不会进行迁移。
- 如果在 FlexConfig 和管理中心中配置了策略：
  - 如果已在**设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** 中配置了策略，则不会发起迁移。
  - 在部署期间，管理中心会显示错误消息。示例 EIGRP 迁移错误消息 - *EIGRP* 通过 *FlexConfig* 对象进行配置，也可在设备的“设备列表”*(Device Listing)* -> “路由 *EIGRP*”*(Routing EIGRP)* 下进行配置。在路由 *EIGRP* 或 *FlexConfig* 中维护 *EIGRP* 配置。
- 如果策略中使用的网络对象存在于管理中心，则在迁移期间，它们会被重用。在迁移过程中，当与 IP 配置匹配的网络对象不可用时，会创建一个新的网络对象，即 *bb* 附加时间戳和整数，例如 ***bb_<timestamp>_<integer>*** 。对于多个此类网络对象，名称中的整数变量将递增一。

过程

步骤 1 选择 **设备** > **+ 显示更多** > **FlexConfig**，点击要迁移的 FlexConfig 策略旁边的 **编辑** (✎)。

步骤 2 点击**迁移配置 (Migrate Config)**。

注释
迁移开始后，**迁移配置 (Migrate Config)** 和 FlexConfig **编辑 (Edit)** 选项都将不可用。

在以下情况下，**迁移配置 (Migrate Config)** 选项不可用：

- 没有要迁移的适用 FlexConfig CLI。
- FlexConfig 策略没有与任何 FlexConfig 对象关联。
- 没有设备与 FlexConfig 策略关联。

步骤 3 在**迁移 Flex 配置**对话框中，选择要向其迁移配置的设备，然后点击**确定**。

迁移进度会显示为任务通知。迁移完成后，点击查看详细信息 *(View Details)* 链接并下载迁移报告（PDF 格式）。

步骤 4 要查看策略更改，请选择 **事件和日志** > **分析** > **审核日志** 并点击 *FlexConfig* 迁移消息。

步骤 5 要查看 FlexConfig 迁移报告，请选择 **事件和日志** > **分析** > **审核日志** 并点击 *FlexConfig* 迁移消息。要查看完整的迁移报告，请点击**报告 (Report)** 图标。

步骤 6 在对应的**设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** 页面中验证已迁移的配置设置。

步骤 7 要从 FlexConfig 中删除设备的特定策略配置，请在管理中心执行以下操作：

a) 确定设备的已迁移 FlexConfig 策略。
b) 使用复制选项并创建 FlexConfig 策略的副本。
c) 从复制的 FlexConfig 策略中删除对应的 CLI 对象。
d) 将设备关联到复制的 FlexConfig 策略。

步骤 8 保存并部署配置。

FlexConfig 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 1000/2100 和 Firepower 4100/9300 的数据平面故障后恢复速度更快。	7.4.1	7.4.1	如果数据平面进程崩溃，系统现在仅重新加载数据平面进程，而不是重新启动设备。随着数据平面进程重新加载，Snort 和其他几个进程也会重新加载。 但是，如果数据平面进程在启动期间崩溃，设备将遵循正常的重新加载/重新启动顺序，这有助于避免发生重新加载过程循环。 默认情况下，新设备和升级设备均启用此功能。 新增/修改的CLI 命令： **data-plane quick-reload**、 **no data-plane quick-reload**、 **show data-plane quick-reload status** 支持的平台：Firepower 1000/2100、Firepower 4100/9300 平台限制：不支持多实例模式。 请参阅： *Cisco Secure Firewall Threat Defense 命令参考* 和 Cisco Secure Firewall ASA 系列命令参考。
迁移工具支持。	7.3.0	任意	引入了对将 Flex 配置的 ECMP、VXLAN 和 EIGRP 策略迁移到管理中心的支持。 新增/修改的屏幕： **设备 (Devices)** > **FlexConfig** > **迁移 FlexConfig (Migrate FlexConfig)**
删除 FlexConfig 中的 BFD 配置。	7.3.0	任意	引入了对直接在管理中心用户界面中配置 BFD 策略的支持。因此，用于配置 EIGRP 策略的 FlexConfig 支持已被删除。
删除优先级队列。	7.2.5	7.2.5	删除了在威胁防御中配置优先级队列的支持。
删除 FlexConfig 中的 EIGRP 配置。	7.2.0	任意	引入了对直接在管理中心用户界面中配置 EIGRP 的支持。因此，用于配置 EIGRP 策略的 FlexConfig 支持已被删除。
删除 PBR 配置。	7.1.0	7.1.0	支持直接在 FMC 用户界面上配置 PBR。因此，为 FTD 7.1 及更高版本配置 PBR 的 FlexConfig 支持已被删除。 新增/修改的命令： **policy-route route-map***routemap-object-name*。
在 FlexConfig 中删除 ECMP 区域创建支持。	7.1.0	任意	引入了对直接在 FMC 用户界面中配置 ECMP 区域的支持。因此，用于配置 ECMP 区域的 FlexConfig 支持已被删除。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。	6.5.0	任意	可以使用 FlexConfig 在 ISA 3000设备上配置精确时间协议 (PTP)。PTP 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。该协议专为工业、网络测量和控制系统而设计。 现在，我们允许在 FlexConfig 对象中包含 **ptp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 和 **ptp domain** 新增/修改的命令：**show ptp**。
弃用的 FlexConfig 对象。	6.3.0	任意	在以前的版本中使用 FlexConfig 配置的几个功能如今已在 FMC 中直接支持。如果正在使用这些 FlexConfig 对象，您需要将其删除，然后将配置转换为使用新对象。以下是已弃用的 FlexConfig 对象和文本对象。 • **Default_DNS_Configure**，包括 defaultDNSNameServerList 和 defaultDNSParameters 文本对象。现在，请使用平台设置策略为数据接口配置 DNS。 • **TCP_Embryonic_Conn_Limit**，以及 tcp_conn_misc 和 tcp_conn_limit 文本对象。在FTD 服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”(Advanced) 选项卡上找到该策略。 • **TCP_Embryonic_Conn_Timeout**，以及 tcp_conn_misc 和 tcp_conn_timeout 文本对象。在 FTD 服务策略中配置这些功能。
FlexConfig 更新。	6.2.1	任意	根据政府认证要求，密码、系统提供的共享密钥或用户定义的FlexConfig 对象中的所有敏感信息都应使用密钥变量来加以屏蔽。将FTD 更新为版本 6.2.1+ 后，FlexConfig 对象中的所有敏感信息都会被转换为密钥变量格式。 此外，还添加了以下新的 FlexConfig 模板： • **Default_DNS_Configure** 模板让您能够使用默认 DNS 组，以便用于解析通过数据接口解析名称的命令或功能的主机名。 • **TCP 初期连接限制和超时配置**模板让您能够配置初期连接限制/超时 CLI，以防止 SYN 泛洪 DoSA攻击。 • **启用威胁检测配置和清除**模板让您能为 TCP 拦截拦截的攻击配置威胁检测统计信息。 • **IPV6 路由器报头检测**模板让您能配置 IPV6 检测报头，以便选择性地允许/阻止某些不同类型的报头（例如，允许 RH 类型 2、移动）。 • **DHCPv6 前缀授权**模板让您能为 IPv6 前缀授权配置一个外部（PD 客户端）和一个内部接口（被授权前缀的接收者）。

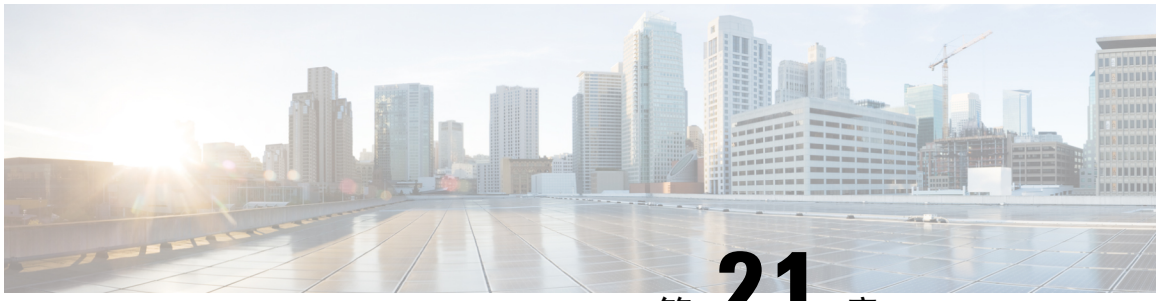
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
FlexConfig。	6.2.0	任意	FlexConfig 功能让您能使用 FMC 将基于 ASA CLI 的功能部署到 FTD 设备。此功能允许您启用 FTD 设备上当前不可用的一些最具价值的 ASA 功能。此功能被结构化为在策略中协同工作的模板和对象。思科 TAC 正式支持默认模板。 新增/修改的屏幕： • 设备 > **FlexConfig** • 对象 **(Objects)** > 对象管理 **(Object Management)** > **FlexConfig** > **FlexConfig** 对象 **(FlexConfig Objects)** • 对象 **(Objects)** > 对象管理 **(Object Management)** > **FlexConfig** > 文本对象 **(Text Object)**



第 IV 部分

路由

- 静态和默认路由， 第 1087 页
- 虚拟路由器， 第 1103 页
- ECMP， 第 1159 页
- 双向转发检测路由， 第 1169 页
- OSPF， 第 1175 页
- EIGRP， 第 1203 页
- BGP， 第 1213 页
- RIP， 第 1233 页
- 组播， 第 1239 页
- 策略型路由， 第 1259 页



第 21 章

静态和默认路由

本章介绍如何在 Firewall Threat Defense上配置静态路由和默认路由。

- 关于静态路由和默认路由，第 1087 页
- 静态路由的要求和前提条件，第 1089 页
- 静态和默认路由准则，第 1090 页
- 添加静态路由，第 1090 页
- 路由参考，第 1091 页

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，Firewall Threat Defense将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

Firewall Threat Defense 为数据接口和管理专用接口（包括特殊的 Linux 管理接口）提供单独的路由表。只能为数据路由表添加默认路由。 Firewall Threat Defense 会自动在管理专用路由表中添加一个将流量发送到 Linux 管理接口的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 Firewall Threat Defense CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 Firewall Threat Defense连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。
- 虚拟路由器使用静态路由来创建路由泄漏。路由泄漏使流量从虚拟路由器的接口流向另一个虚拟路由器中的另一个接口。有关详细信息，请参阅互联虚拟路由器，第 1106 页。

使用到 null0 接口的路由丢弃不必要的流量

通过访问规则，您可以根据其报头中包含的信息过滤数据包。到null0接口的静态路由是访问规则的补充性解决方案。您可以使用 null0 路由转发不必要或不需要的流量，从而丢弃该流量。

静态 null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。BGP 可以利用静态 null0 路由进行远程触发黑洞路由。

路由优先级

- 标识具体目标的路由优先于默认路由。
- 当存在通向同一目标的多个路由（静态或动态）时，路由的管理距离即可确定优先级。静态路由设置为 1，因此其通常是优先级最高的路由。
- 当您具有多个管理距离相同的通向同一目标的静态路由时，请参阅等价多路径 (ECMP) 路由，第 1099 页。
- 对于来自具有 Tunneled 选项的隧道的新流量，此路由覆盖任何其他已配置或已知悉的默认路由。

透明防火墙模式和网桥组路由

对于源自 Firewall 威胁防御设备并且通过网桥组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 Firewall 威胁防御设备了解通过哪个网桥组成员接口发出流量。源自 Firewall 威胁防御设备 的流量可能包括与系统日志服务器或 SNMP 服务器的通信。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。对于透明模式，不能将 BVI 指定为网关接口；只能使用成员接口。 对于路由模式下的网桥组，必须在静态路由中指定 BVI；不能指定成员接口。有关详细信息，请参阅MAC 地址与路由查找，第 128 页。

静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有 Firewall 威胁防御设备 上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP 的备用默认路由，以防主 ISP 不可用。

Firewall 威胁防御设备 通过将静态路由与 Firewall 威胁防御设备 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址
- 下一跳网关地址（如果您关注网关的可用性）
- 目标网络上的服务器，例如 Firewall 威胁防御设备 需要与之进行通信的系统日志服务器
- 目标网络上的持久网络对象

注释 可能会在夜间关闭的 PC 不是一个理想选择。

您可以为静态定义的路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

静态路由的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

网络管理员

静态和默认路由准则

防火墙模式和网桥组

- 在透明模式下，静态路由必须使用桥接组成员接口作为网关；不能指定 BVI。
- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

支持的网络地址

- IPv6 不支持静态路由跟踪。
- Firewall Threat Defense 不支持 E 类路由，因此 E 类网络不能在静态路由中路由。

集群

- 在集群中，仅控制节点上支持静态路由跟踪。

网络对象组

不能在静态路由中使用一系列网络对象或具有一系列 IP 地址的网络对象组。

ASP 和 RIB 路由条目

在 ASP 路由表中捕获设备上安装的所有路由及其距离。这对于所有静态和动态路由协议都是通用的。在 RIB 表中仅捕获最佳距离路由。

添加静态路由

静态路由用于定义为特定目标网络发送流量的位置。至少应定义一个默认路由。默认路由是以0.0.0.0/0作为目标 IP 地址的静态路由。

要为冗余管理器访问数据接口配置路由，请参阅配置冗余管理器访问数据接口。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 （可能需要）在虚拟路由器下拉列表中，选择要为其配置静态路由的虚拟路由器。

步骤 4 选择 **静态路由**。

步骤 5 点击**添加路由**。

步骤 6 点击 **IPv4** 或 **IPv6**，具体取决于要添加的静态路由的类型。

步骤 7 选择此静态路由应用至的**接口**。

对于透明模式，选择网桥组成员接口名称。对于具有网桥组的路由模式，您可以为 BVI 名称选择网桥组成员接口。要将不必要的流量转发到“黑洞”，请选择 **Null0** 接口。

对于使用虚拟路由的设备，您可以选择属于其他虚拟路由器的接口。如果要将流量从此虚拟路由器泄漏到另一个虚拟路由器，可以创建此类静态路由。有关详细信息，请参阅互联虚拟路由器，第 1106 页。

步骤 8 在**可用网络**列表中，选择目标网络。

要定义默认路由，请创建一个具有地址 0.0. 0.0/0 的对象，然后在此处选择它。

注释
虽然可以创建和选择一个包含 IP 地址范围的网络对象组，但 防火墙管理中心 不支持在静态路由中使用范围。

步骤 9 在**网关 (Gateway)**或 **IPv6 网关 (IPv6 Gateway)** 字段中，输入或选择是次路由下一跳的网关路由器。您可以提供 IP 地址或网络/主机对象。

当您为虚拟路由器使用静态路由配置泄漏路由时，请勿指定下一跳网关。

步骤 10 在**指标**字段中，输入到目标网络的跳数。有效值范围为 1 到 255；默认值为 1。

指标是基于到特定主机所在的网络的跳数对路由的“开销”的一种衡量。跳计数是网络数据包在到达最终目标之前必须遍历的网络数，包括目标网络。指标用于比较不同路由协议之间的路由。静态路由的默认管理距离为 1，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

步骤 11 （可选） 对于默认路由，选中**隧道**复选框可为 VPN 流量定义单独的默认路由。

如果希望 VPN 流量使用与非 VPN 流量不同的默认路由，可以为 VPN 流量定义单独的默认路由。例如，从VPN连接传入的流量可以轻松定向到内部网络，而来自内部网络的流量可以定向到外部。使用“隧道”选项创建默认路由时，来自终止于无法使用已获悉或静态路由进行路由的设备的隧道的所有流量都会发送到该路由。对于每台设备，您只能配置一条默认的隧道网关。不支持隧道流量的 ECMP。

步骤 12 （仅 IPv4 静态路由）要监控路由可用性，请在**路由跟踪**字段中输入或选择定义监控策略的 SLA（服务级别协议）监控对象的名称。

请参阅SLA 监控器，第 2700 页。

步骤 13 点击**确定 (OK)**。

路由参考

此部分介绍有关路由如何在 Firewall Threat Defense 内部运行的基本概念。

确定路径

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

支持的路由类型

路由器可以使用多种路由类型。Firewall 威胁防御设备 使用以下路由类型：

- 静态与动态
- 单路径与多路径
- 平面与分层
- 链路状态与距离矢量

静态与动态

静态路由算法实际上是网络管理员建立的表映射。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改，则路由软件会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器（所有无法路由的数据包都发送到的路由器的默认路由）指定为所有无法路由的数据包的存储库，从而确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器从最后一个主干路由器传播到最终目标。

路由系统通常会指定一些逻辑节点组，称为域、自治系统或区域。在分层系统中，一个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组（域）中。由于域内路由器只需知道其域中的其他路由器即可，因此可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离矢量

链路状态算法（也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与OSPF路由协议结合使用。

支持的互联网路由协议

Firewall 威胁防御设备 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP（反之亦然），从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网服务提供商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自

治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

路由表

Firewall威胁防御对数据流量（通过设备）和管理流量（来自设备）使用单独的路由表。本部分介绍路由表 的工作原理。有关管理路由表的信息，另请参阅 管理流量的路由表，第 1098 页。

路由表的填充方式

Firewall Threat Defense 路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于 Firewall Threat Defense 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 Firewall Threat Defense 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果 Firewall Threat Defense 设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 Firewall Threat Defense在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 Firewall Threat Defense支持的路由协议的默认管理距离值。

表 *79:* 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
VPN 路由	1
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 Firewall Threat Defense从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 Firewall Threat Defense 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 Firewall Threat Defense会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 Firewall Threat Defense的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 Firewall Threat Defense上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

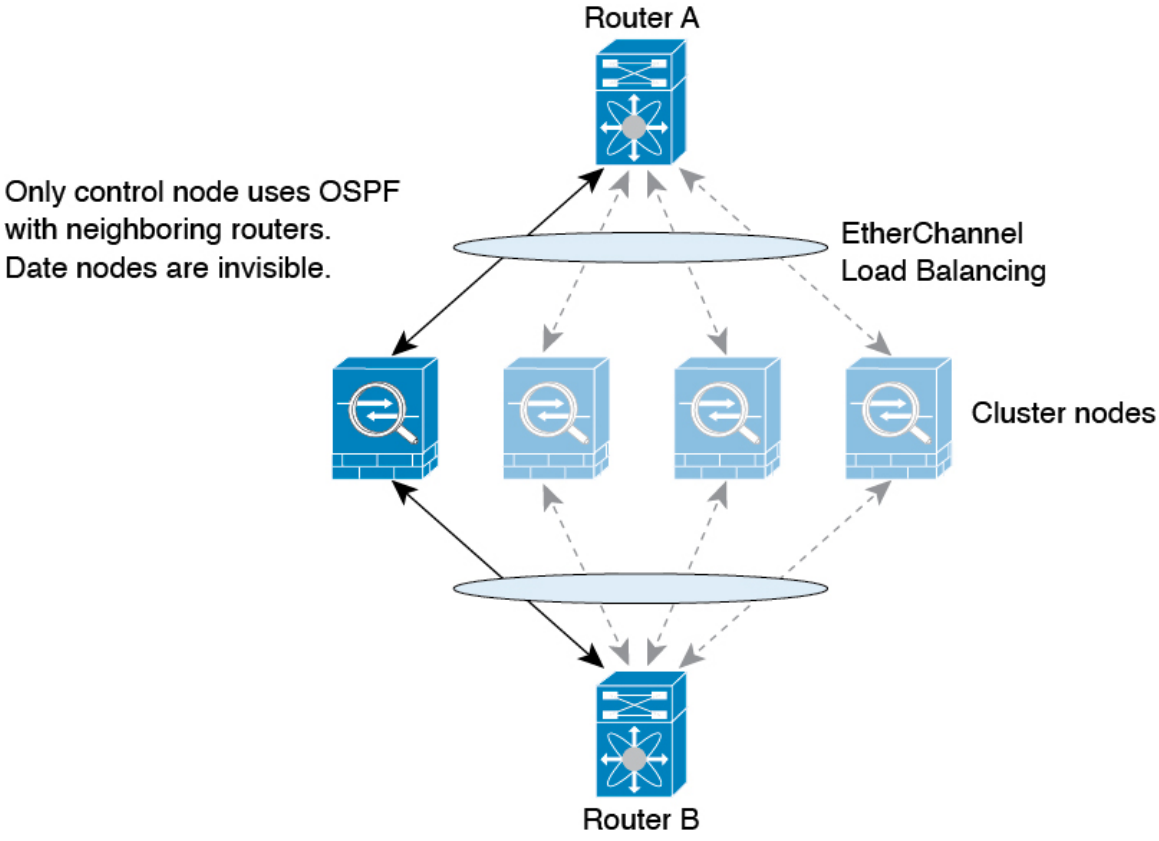
动态路由和

当主用设备上的路由表发生更改时，在备用设备上同步动态路由。这意味着主用设备上的所有添加、删除或更改都将立即传播到备用设备。如果备用设备在主用/备用就绪 对中处于活动状态，则它会有与前一个主用设备相同的路由表，因为路由作为 批量同步和连续复制过程的一部分进行同步。

集群下的动态路由

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *389:* 跨区以太网通道模式下的动态路由



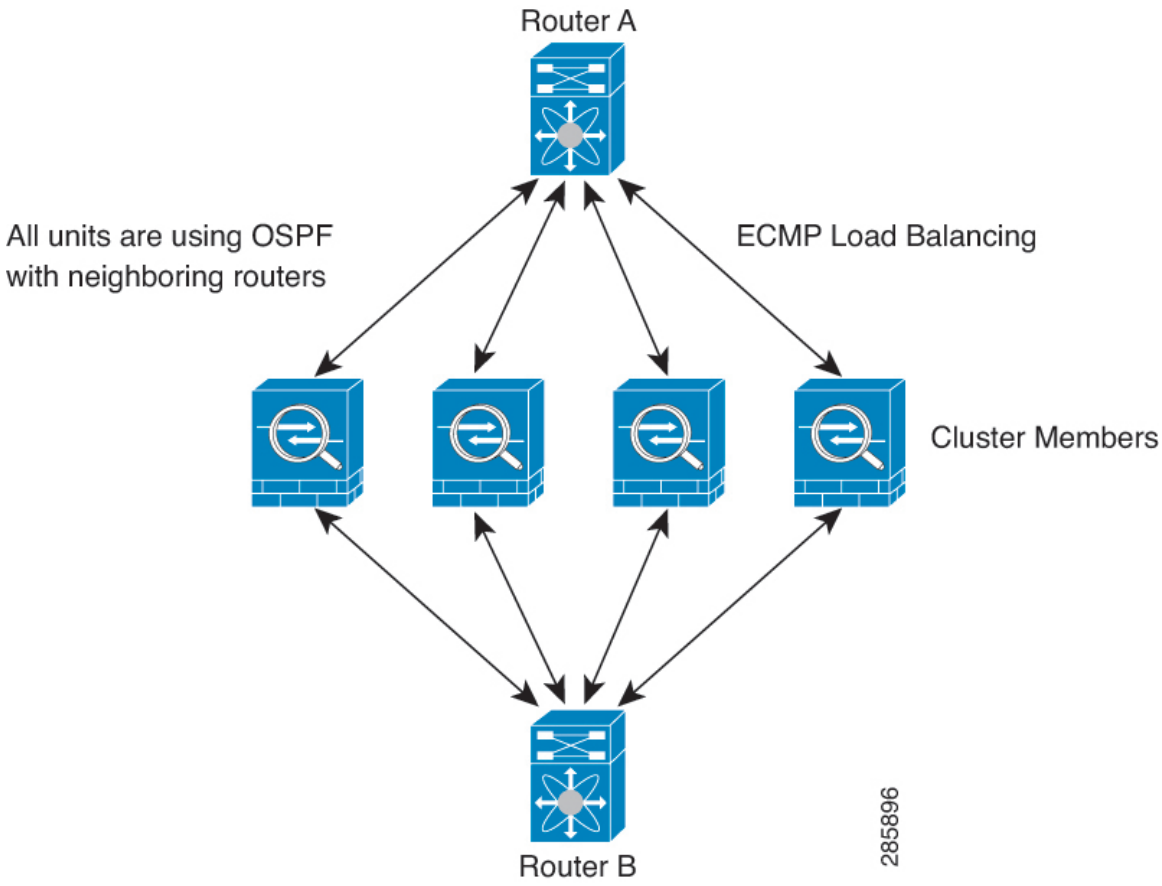
在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *390:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅创建 ECMP 区域，第 1161 页。

管理流量的路由表

Firewall Threat Defense 设备包括用于关联设备管理流量的以下路由表：

- Linux 管理路由表 — 来自管理接口的特殊管理流量（例如 防火墙管理中心 通信、 许可通信和数据库更新）始终使用 Linux 管理路由表。

- 数据路由表 - 默认情况下，所有关联设备流量（以及所有通过流量）使用数据路由表。所有常规数据接口都属于此路由表。大多数服务允许您选择特定接口，因此仅使用与该接口关联的路由。
- 管理专用路由表 - 管理接口和您设置为管理专用的所有数据接口都属于此路由表。要从这些接口中的任一接口发送关联设备流量，必须在配置服务时选择特定的管理专用接口。DNS 查找 和 ICMP （PING 和跟踪路由）存在一种例外情况：在某些情况下， Firewall Threat Defense 将使用数据路由表，然后在未找到路由时自动回退到管理路由表。您可以为管理专用接口添加静态路由，但不能为特殊管理接口添加静态路由。Firewall Threat Defense 设备会自动为管理接口添加一个将流量转发到 Linux 的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 Firewall Threat Defense CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

注释 对于尚未合并管理接口和旧诊断接口的设备，请参阅本指南 7.3 版之前的版本。

等价多路径 (ECMP) 路由

Firewall Threat Defense支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。Firewall Threat Defense使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

路由 GRE 流量

在 Firewall 威胁防御 中，使用双向流管理通用路由封装 (GRE) 流量。这意味着每个 GRE 会话都由处理终端之间入站和出站流量的单个流条目表示。对于双向流，仅执行一次路由查找，并将两个方向映射到同一接口。因此，系统无法为每个方向做出独立的路由决策，这在某些情况下可能导致次优路由。

关于路由映射

在将路由重新分发到 OSPF、RIP、EIGRP 或 BGP 路由进程时会使用路由映射。在为 OSPF 路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。

路由映射与广为人知的 ACL 具有许多相同功能。以下是两者共有的一些特征：

- 它们都是单独语句的有序序列，各自具有允许或拒绝结果。ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配相关联的操作。
- 它们是通用机制。条件匹配和匹配解释由它们的应用方式和使用它们的功能决定。应用于不同功能的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部路由。
- 每个 ACL 按照设计约定以隐式拒绝语句结尾。如果在匹配尝试期间到达路由映射的结尾，则结果取决于路由映射的特定应用。应用于重新分发的路由映射与 ACL 的行为方式相同：如果路由与路由映射中的任何子句不匹配，则会拒绝路由重新分发，就如同路由映射的结尾包含拒绝语句一样。

Permit 和 Deny 子句

路由映射可以具有 permit 和 deny 子句。deny 子句可拒绝来自重新分发的路由匹配。您可以使用 ACL 作为路由映射中的匹配标准。由于 ACL 还有 permit 和 deny 子句，因此数据包与 ACL 匹配时会应用以下规则：

- ACL permit + route map permit：重新分发路由。
- ACL permit + route map deny：重新分发路由。
- ACL deny + route map permit or deny：不匹配 route map 子句，并且对下一个 route-map 子句进行评估。

Match 和 Set 子句值

每个路由映射子句均具有两种类型的值：

- match 值用于选择应将此子句应用于的路由。
- set 值用于修改将重新分发到目标协议的信息。

对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则按照 permit 或 deny 子句的指示重新分发或拒绝路由，其某些属性可能会通过 set 命令设置的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射扫描将继续，直到发现匹配路由的子句或达到路由映射的结尾。

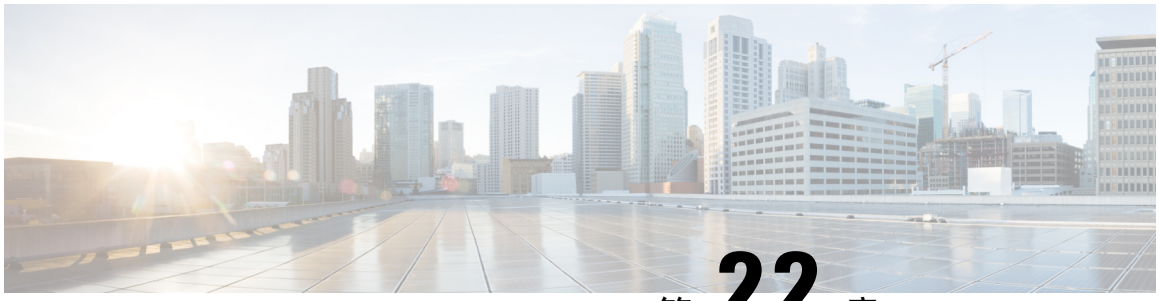
如果存在下列条件中的一个，则每个子句中的 match 值或 set 值可能会缺失或多次重复：

- 如果一个子句中存在多个匹配条目，则对于给定路由而言，所有这些条目必须都符合，该路由才与该子句匹配（也即，为多个 match 命令应用逻辑 AND 算法）。
- 如果一个 match 条目引用了一个条目中的多个对象，那么其中任何一个对象都应匹配（应用逻辑 OR 算法）。
- 如果匹配条目不存在，则所有路由都匹配子句。
- 如果一个 set 条目在 route map permit 子句中不存在，则该路由将被重新分发，而不修改其当前属性。



注释 请勿在 route map deny 子句中配置 set 条目，因为 deny 子句会禁止路由重新分发 - 没有要修改的信息。

没有 match 或 set 条目的 route map 子句需要执行操作。空 permit 子句允许重新分发剩余路由而不进行修改。空 deny 子句不允许重新分发其他路由（如果路由映射在经过完整扫描后，未发现明确的匹配项，此为默认操作）。



第 22 章

虚拟路由器

本章介绍了关于虚拟路由器的基本概念以及虚拟路由在 Cisco Secure Firewall Threat Defense 中的表现。

- 关于虚拟路由器和虚拟路由与转发 (VRF)，第 1103 页
- 按设备型号划分的最大虚拟路由器数量，第 1109 页
- 虚拟路由器的要求和前提条件，第 1111 页
- 虚拟路由器的准则和限制，第 1111 页
- 防火墙管理中心 Web 界面 - 路由页面修改，第 1113 页
- 管理虚拟路由器，第 1114 页
- 创建虚拟路由器，第 1114 页
- 监控虚拟路由器，第 1117 页
- 虚拟路由器的配置示例，第 1118 页
- 虚拟路由器的历史记录，第 1156 页

关于虚拟路由器和虚拟路由与转发 (VRF)

可以创建多个虚拟路由器来为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。

因此，您可以通过一组通用的网络设备为两个或多个不同的客户提供支持。您还可以使用虚拟路由器为自身网络的元素提供更多隔离，例如，将开发网络与一般用途的企业网络隔离。

虚拟路由器将实施虚拟路由和转发功能的“轻型”版本（或 VRF Lite），它不支持 BGP 的多协议扩展 (MBGP)。

创建虚拟路由器时，您需要为路由器分配接口。您可以将给定接口分配给一个且仅有一个虚拟路由器。然后即可定义静态路由，并为每个虚拟路由器配置路由协议（例如 OSPF 或 BGP）。还可在整个网络中配置单独的路由进程，以便所有参与设备的路由表都使用每个虚拟路由器相同的路由进程和表。使用虚拟路由器，可在同一物理网络上创建逻辑分隔的网络，以确保流经每个虚拟路由器的流量的隐私。

由于路由表独立存在，因此可以在虚拟路由器上使用相同或重叠的地址空间。例如，可以将 192.168.1.0/24 地址空间用于两个独立的虚拟路由器，分别由两个独立物理接口提供支持。

请注意，每个虚拟路由器有单独的管理和数据路由表。例如，如果将管理专用接口分配给虚拟路由器，则该接口的路由表会与分配给虚拟路由器的数据接口分离开来。

关于虚拟路由器和动态 VTI

虚拟路由器和动态 VTI

您可以创建虚拟路由器，将动态 VTI 与这些虚拟路由器关联，并在网络中扩展动态 VTI 的功能。可以将动态 VTI 与全局或用户定义的虚拟路由器关联。您可以只能将一个动态 VTI 分配给一个虚拟路由器。

与以下项关联的虚拟路由器：

- 动态 VTI 称为室内 VRF (IVRF)。
- 隧道源接口称为 Front Door VRF (FVRF)。

动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。隧道源接口可以是多个虚拟路由器的一部分。

要使用动态 VTI 为基于路由的站点间 VPN 配置虚拟路由器，请参阅 如何使用动态 VTI 配置虚拟路由器，第 1104 页。

有关配置示例的详细信息，请参阅 如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量，第 1136 页

如何使用动态 VTI 配置虚拟路由器

要在管理中心为路由型站点间 VPN 配置具有动态 VTI 的虚拟路由器，请执行以下操作：

步骤	相应操作	更多信息
1	使用中枢上的动态VTI接口和分支上的静态VTI创建基于路由的站点间VPN。	创建基于路由的站点间 VPN，第 1471 页
2	创建虚拟路由器。	创建虚拟路由器，第 1114 页
3	将接口分配给虚拟路由器。	配置虚拟路由器，第 1114 页
4	为中心辐射点配置路由策略。	为中心辐射型拓扑配置终端，第 1475 页
5	为中心辐射型配置访问控制策略。	为中心辐射型拓扑配置终端，第 1475 页

虚拟路由器的应用

您可以使用虚拟路由器来隔离共享资源上的网络，以及/或者隔离具有通用安全策略的网络。因此，虚拟路由器可以帮助您实现：

- 通过为每个客户或不同部门提供专用路由表来为客户分离流量。

- 不同部门或网络的通用安全策略管理。
- 不同部门或网络的共享互联网接入。

全局和用户定义的虚拟路由器

全局虚拟路由器

对于具有虚拟路由功能的设备，系统会默认创建一个全局虚拟路由器。系统会将网络中的所有接口分配给全局虚拟路由器。路由接口可以属于用户定义的虚拟路由器或全局虚拟路由器。在将Firewall Threat Defense升级到具有虚拟路由器功能的版本时，其所有现有路由配置将成为全局虚拟路由器的一部分。

用户定义的虚拟路由器

用户定义的虚拟路由器就是您定义的虚拟路由器。您可以在一台设备上创建多个虚拟路由器。但在任何时候，一个接口都只能分配给一个用户定义的虚拟路由器。虽然用户定义的虚拟路由器支持某些设备功能，但只有少数功能仅在全局虚拟路由器上受支持。用户定义的虚拟路由器支持基于路由的站点间 VPN（静态 VTI）（静态和动态 VTI）。

支持的功能和监控策略

您只能在全局虚拟路由器上配置以下功能：

- OSPFv3
- RIP
- EIGRP
- IS-IS
- 组播路由
- 策略型路由 (PBR)

通过防火墙管理中心中的 Flex Config 支持 ISIS（请参阅预定义的 FlexConfig 对象，第 1052 页）。只为这些功能配置全局虚拟路由器接口。

DHCP 服务器自动配置会使用从接口获知的 WINS/DNS 服务器。此接口只能是全局虚拟路由器接口。

您可以为每个用户定义的虚拟路由器单独配置以下功能：

- 静态路由及其 SLA 监控器
- OSPFv2
- BGPv4/v6
- 集成的路由与桥接 (IRB)

- SNMP

当查询或与远程系统通信时，系统会使用以下功能（传出流量）。这些功能仅使用全局虚拟路由器中的接口。这意味着，如果为该功能配置了接口，则接口必须属于全局虚拟路由器。作为一条规则，系统无论何时出于管理目的必须查找连接外部服务器的路由，它会在全局虚拟路由器中执行路由查找。

- DNS服务器用于解析访问控制规则中使用的完全限定名称，或解析**ping**命令的名称。如果指定**any** 作为 DNS 服务器的接口，则系统仅考虑全局虚拟路由器中的接口。
- 用于 VPN 的 AAA 服务器或身份领域。只能在全局虚拟路由器中的接口上配置 VPN。因此，用于 VPN 的外部 AAA 服务器（如 Active Directory）必须可通过全局虚拟路由器中的接口访问。

配置策略以感知虚拟路由器

创建虚拟路由器时，该虚拟路由器的路由表会自动与全局虚拟路由器或任何其他虚拟路由器分离开来。但是，安全策略不会自动识别虚拟路由器。

例如，如果编写适用于“任何”源或目标安全区的访问控制规则，则该规则将应用于所有虚拟路由器上的所有接口。这实际上可能正是您所希望得到的结果。例如，可能所有客户都想阻止访问相同系列的令人反感的 URL 类别。

但是，如果需要仅向其中一个虚拟路由器应用策略，则需要创建仅包含来自该单一虚拟路由器的接口的安全区。然后，在安全策略的源和目标条件中使用虚拟路由器限制的安全区。

通过使用其成员身份限制为分配给单个虚拟路由器的接口的安全区，您可以在以下策略中编写虚拟路由器感知规则：

- 访问控制策略。
- 入侵和文件策略。
- SSL 解密策略。
- 身份策略和用户到IP地址映射。如果在虚拟路由器中使用重叠地址空间，请确保为每个虚拟路由器创建单独的领域，并在身份策略规则中正确应用。

如果在虚拟路由器中使用重叠地址空间，则应使用安全区确保应用适当的策略。例如，如果在两个单独的虚拟路由器中使用 192.168.1.0/24 地址空间，则指定 192.168.1.0/24 网络的访问控制规则将应用于两个虚拟路由器中的流量。如果这不是期望的结果，您可以通过只为其中一个虚拟路由器指定源/目标安全区来限制该规则的应用。

互联虚拟路由器

静态和动态路由泄漏

您可以配置设备来路由虚拟路由器之间的流量。路由泄漏过程可以通过设置静态路由手动完成，也可以通过 BGP 设置动态完成。

静态路由泄漏

您可以配置静态路由来路由虚拟路由器之间的流量。

例如，如果您在全局虚拟路由器中设有外部接口，则可以在每个其他虚拟路由器中设置静态默认路由，以将流量发送到该外部接口。然后，无法在给定虚拟路由器内路由的任何流量将被发送到全局路由器，以进行后续路由。

虚拟路由器之间的静态路由被称为路由泄漏，这是因为您会将流量泄漏到其他虚拟路由器。泄漏路由（例如，VR1 路由到 VR2）时，可以仅发起从 VR2 到 VR1 的连接。要使流量从 VR1 流向 VR2，必须配置反向路由。当您为另一个虚拟路由器中的接口创建静态路由时，不需要指定网关地址，而只需选择目标接口。

对于虚拟路由器间路由，系统会在源虚拟路由器中查找目标接口。然后，系统会查找目标虚拟路由器中下一跳的MAC地址。因此，目标虚拟路由器必须具有用于目标地址的所选接口的动态（获知）或静态路由。

通过配置将在不同虚拟路由器中使用源接口和目标接口的NAT规则，还允许在虚拟路由器之间路由流量。如果未选择NAT进行路由查找的选项，则每当发生目标转换时，规则就会将流量从目标接口发送到 NATed 地址。但是，目标虚拟路由器应具有一个已转换目标 IP 地址的路由，以便下一跳查找可以取得成功。

虽然NAT规则将流量从一个虚拟路由器泄漏到另一个虚拟路由器，但为了确保正确的路由，建议在这些虚拟路由器之间为转换后的流量配置静态路由泄漏。如果没有路由泄漏，有时该规则可能无法匹配您预期其匹配的流量，并且可能不会应用转换。

虚拟路由不支持级联或路由泄漏链。例如，假设 Firewall Threat Defense 具有 VR1、VR2 和 VR3 虚拟路由器；VR3 直接连接到网络 10.1.1.0/24。现在，假设您在 VR1 中通过 VR2 中的接口为网络 10.1.1.0/24 配置了路由泄漏，在 VR2 中通过 VR3 为 10.1.1.0/24 定义了路由泄漏。此路由泄漏链不允许流量从 VR1 跳到 VR2，然后从 VR3 退出。如果存在路由泄漏，路由查找将首先从输入虚拟路由器的路由表确定出口接口，然后查看虚拟路由器的路由表输出，以进行下一跳查找。在上述两次查找中，出口接口应匹配。在本示例中，出口接口不是同一接口，因此流量不会通过。

当目的网络不是上游（传出）VR 的直连子网时，请谨慎使用静态 VRF 间路由。例如，假设有两个 VR - VR1 和 VR2。VR1 处理通过 BGP 或任何动态路由协议从其外部对等体获取默认路由的传出流量，而 VR2 则处理配置了静态 VRF 间默认路由的传入流量，并将 VR1 作为下一跳。当 VR1 丢失来自其对等体的默认路由时，VR2将无法检测到其上游（传出）VR丢失了默认路由，并且仍会向VR1发送流量，该流量最终将被丢弃，而不会发出通知。在这种情况下，我们建议您通过 BGP 为 VR2 配置动态路由泄漏。

使用 BGP 完成的动态路由泄漏

您可以通过使用路由目标扩展社区将路由从源虚拟路由器（比如VR1）导出到源BGP表，然后将相同的路由目标扩展社区从源 BGP 表导入到目的 BGP 表来实现虚拟路由器间路由泄漏，导入的路由目标扩展社区将由目的虚拟路由器（比如 VR2）使用。您可以使用路由映射来过滤路由。全局虚拟路由器的路由也可以泄漏到用户定义的虚拟路由器，反之亦然。BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

有关配置 BGP 路由泄漏的详细信息，请参阅配置 BGP 路由导入/导出设置，第 1229 页。

BGP 路由泄漏准则

- 确保递归所需的所有路由均已导入并出现在入口虚拟路由器的路由表中。
- 每个虚拟路由器都支持 ECMP。因此，请不要在不同的虚拟路由器之间配置 ECMP。从不同虚拟路由器导入的重叠前缀无法形成 ECMP。也就是说，当您尝试将具有重叠地址的路由从两个不同的虚拟路由器导入到其他虚拟路由器（全局虚拟路由器或用户定义的虚拟路由器）时，只有一条路由（根据 BGP 最佳路径算法，是通告的第一个路由）会导入到相应的虚拟路由表中。例如，如果连接到 VR1 的网络 10.10.0.0/24 先通过 BGP 通告到全局虚拟路由器，之后连接到 VR2 的另一个具有相同地址 10.10.0.0/24 的网络也通过 BGP 通告到全局虚拟路由器，则只有 VR1 网络路由会导入到全局虚拟路由表中。
- 用户定义的虚拟路由器不支持 OSPFv3。因此，请不要将 BGPv6 配置为将 OSPFv3 用户定义的虚拟路由器泄漏到全局虚拟路由器。但是，您可以将 BGPv6 配置为通过重新分发将 OSPFv3 全局虚拟路由器路由泄漏到用户定义的虚拟路由器。
- 建议将 VTI 接口、受保护的内部接口（如果 VTI 支持，则为环回接口）保留为同一虚拟路由器的一部分，以防止需要路由泄漏。

重叠 IP 地址

虚拟路由器会创建多个独立的路由表实例，因此可以使用相同或重叠的 IP 地址，而且不会发生冲突。Firewall Threat Defense 允许同一网络成为两个或多个虚拟路由器的一部分。这涉及到要在接口或虚拟路由器级别应用的多个策略。

除了少数例外，路由功能以及大多数 NGFW 和 IPS 功能都不会受重叠 IP 地址的影响。以下部分介绍具有重叠 IP 地址限制的功能以及摆脱这些限制的建议。

重叠 IP 地址的限制

在多个虚拟路由器中使用重叠 IP 地址时，为确保正确应用策略，您必须修改某些功能的策略或规则。此类功能要求您拆分现有安全区域或根据需要使用新接口组，以便使用更具体的接口。

在使用重叠 IP 地址时，您需要修改以下功能才能正常运行：

- “网络映射”(Network Map) - 修改网络发现策略以排除一些重叠的 IP 网段，以确保没有映射的重叠 IP 地址。
- “身份策略”(Identity Policy) - 身份源来源无法区分虚拟路由器；要摆脱此限制，请在不同领域映射重叠地址空间或虚拟路由器。

对于以下功能，您需要在特定接口上应用规则，才能确保在重叠的 IP 网段上应用不同的策略：

- 访问策略
- 预过滤器策略
- QoS/速率限制
- SSL 策略

重叠 IP 地址的不支持的功能

- AC 策略中基于 ISE SGT 的规则 - 从思科身份服务引擎 (ISE) 下载的静态安全组标记 (SGT) 到 IP 地址的映射不会感知虚拟路由器。如果需要为每个虚拟路由器创建不同的 SGT 映射，请为每个虚拟路由器设置单独的 ISE 系统。如果打算将相同的 IP 地址映射到各个虚拟路由器中的相同 SGT 编号，则无需执行此操作。
- 不支持跨虚拟路由器使用重叠 DHCP 服务器池。
- 事件和分析 - 很多 防火墙管理中心 分析依赖于网络映射和身份映射，如果同一 IP 地址属于两个不同的终端主机，则无法区分。因此，当同一设备中存在重叠的 IP 网段但虚拟路由器不同时，这些分析并不准确。

在用户定义的虚拟路由器上配置 SNMP

除了在管理接口和全局虚拟路由器数据接口上支持 SNMP，Cisco Secure Firewall Threat Defense 现在还允许您在用户定义的虚拟路由器上配置 SNMP 主机。

在用户定义的虚拟路由器上配置 SNMP 主机包括以下过程：

1. 配置设备接口。
2. 在接口上配置虚拟路由器。
3. 在虚拟路由器接口上配置 SNMP 主机。



注释 SNMP 无法被虚拟路由器感知。因此，在用户定义的虚拟路由器上配置 SNMP 服务器时，请确保网络地址不是重叠的 IP 地址。

4. 将配置部署到 Cisco Secure Firewall Threat Defense。在成功部署后，SNMP 轮询和陷阱将通过虚拟路由器接口发送到网络管理站。

按设备型号划分的最大虚拟路由器数量

可以创建的最大虚拟路由器数量取决于设备型号。下表列出了最大限制。您可以通过输入 **show vrf counters** 命令对系统进行复核，该命令显示该平台的用户定义最大虚拟路由器数量（不包括全局虚拟路由器）。下表中的数字包括用户和全局路由器。对于 Firepower 4100/9300，这些数字适用于原生模式。

对于支持多实例功能的平台（例如 Firepower 4100/9300），通过以下方式确定每个容器实例的最大虚拟路由器数：将最大虚拟路由器数除以设备上的核心数，然后乘以分配给该实例的核心数，并四舍五入到最接近的整数。例如，如果平台最多支持 100 个虚拟路由器，并且它有 70 个核心，则每个核心最多支持 1.43 个虚拟路由器（四舍五入为一个）。因此，分配有 6 个核心的实例将支持 8.58 个虚拟路由器（四舍五入为 8 个），分配有 10 个核心的实例将支持 14.3 个虚拟路由器（四舍五入为 14 个）。

设备型号	最大虚拟路由器数量
Cisco Secure Firewall 220	5
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Cisco Secure Firewall 1210CE	5
Cisco Secure Firewall 1210CP	5
Cisco Secure Firewall 1220CX	10
Cisco Secure Firewall 1230	10
Cisco Secure Firewall 1240	10
Cisco Secure Firewall 1250	15
Cisco Secure Firewall 3105	10
Cisco Secure Firewall 3110	15
Cisco Secure Firewall 3120	25
Cisco Secure Firewall 3130	50
Cisco Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Cisco Secure Firewall 4215	100
Cisco Secure Firewall 4225	100
Cisco Secure Firewall 4245	100
Cisco Secure Firewall 6160	100
Cisco Secure Firewall 6170	100
Firepower 9300 设备，所有型号	100
Firewall Threat Defense Virtual，所有平台	30

设备型号	最大虚拟路由器数量
ISA 3000	10

相关主题

容器实例的要求和前提条件，第 302 页

虚拟路由器的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

网络管理员

安全审批人

虚拟路由器的准则和限制

防火墙模式指导原则

虚拟路由器仅在路由防火墙模式下支持。

接口指导原则

- 您可以只能将一个接口分配给一个虚拟路由器。
- 可以为虚拟路由器分配任意数量的接口。
- 只有具有逻辑名称 和 VTI 的路由接口才能被分配给用户定义的虚拟路由器。
- 如果要将虚拟路由器接口更改为非路由模式，请从虚拟路由器中删除该接口，然后再更改其模式。
- 您可以从全局虚拟路由器或其他用户定义的虚拟路由器将接口分配给虚拟路由器。
- 不能将以下接口分配给用户定义的虚拟路由器：
  - EtherChannel 的成员。
  - 冗余接口的成员。

- BVI 成员。

- VTI 是基于路由的 VPN。因此，在建立隧道后，必须通过路由控制使用 VTI 进行加密的流量。支持静态路由，以及使用 BGP、OSPFv2/v3, or EIGRP 的动态路由。
- 属于用户定义的虚拟路由器的接口无法用于站点间或 RA VPN。
- 动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。
- 必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。
- 用户定义的虚拟路由器仅支持 BGPv4/v6 和 OSPFv2 路由协议。
- 隧道源接口可以位于与动态 VTI 关联的虚拟路由器之外的用户定义的虚拟路由器中。
- 如果使用正在移动的接口或其虚拟路由器被删除的路由存在于源或目的虚拟路由器表中，请在移动接口或删除虚拟路由器之前删除这些路由。
- 由于为每个虚拟路由器维护了单独的路由表，因此当接口从一个虚拟路由器移至另一个虚拟路由器（无论是全局路由器还是用户定义的路由器）时，系统都会临时删除接口上配置的 IP 地址。接口上的所有现有连接都会被终止。因此，在虚拟路由器之间移动接口会对网络流量产生显著影响。因此，请不要在移动接口之前采取预防措施。

全局虚拟路由器准则

- 已命名但不属于其他虚拟路由器的接口是全局虚拟路由器的一部分。
- 您不能从全局虚拟路由器中删除路由接口。
- 您不能修改全局虚拟路由器。
- 通常，在配置接口后，如果取消注册并重新注册到同一或其他 防火墙管理中心，则接口配置会从设备导回。使用虚拟路由器支持时存在一个限制 - 只保留全局虚拟路由器接口的 IP 地址。

集群准则

- 当控制设备链路由于其接口故障而发生故障时，该设备会从全局路由表中删除其接口的所有泄漏路由，然后将非活动连接的静态路由传播到集群的其他设备。这样会导致从其他设备的路由表中删除这些泄漏的路由。这些删除发生在另一台设备成为新的控制设备之前，大约需要 500 毫秒。当另一台设备成为新的控制设备时，这些路由将通过 BGP 融合获知并添加回路由表中。因此，直到融合时间（约一分钟），泄漏的路由才可用于发生路由事件。
- 当集群中发生控制角色更改时，通过 BGP 获知的泄漏路由将通过最佳 ECMP 路径进行更新。但是，仅在 BGP 重新融合计时器过去后（即 210 秒），才会从集群路由表中删除非最佳 ECMP 路径。因此，在 BGP 重新融合计时器到期之前，旧的非最佳 ECMP 路径将继续作为路由事件的首选路由。

其他准则

- 在为虚拟路由器配置 BGP 时，您可以在同一虚拟路由器内重新分发属于不同协议的路由。例如，无法将 OSPF VR2 路由导入到 BGP VR1 中。您只能将 OSPF VR2 重新分发到 BGP VR2，然后在 BGP VR2 和 BGP VR1 之间配置路由泄漏。
- 您不能使用 IPv6 ACL 来过滤路由地图中的路由。只支持前缀列表。
- 安全智能策略 - 安全智能策略不会感知虚拟路由器。如果将 IP 地址、URL 或 DNS 名称添加到阻止列表，则会被所有虚拟路由器阻止。这一限制适用于具有安全区域的接口。
- NAT 规则 - 不要在 NAT 规则中混用接口。在虚拟路由中，如果指定的源和目的接口对象（接口组或安全区）有属于不同虚拟路由器的接口，那么 NAT 规则会将流量从一个虚拟路由器分流到另一个虚拟路由器。NAT 只会在虚拟路由器表中为入站接口执行路由查找。如有必要，请在源虚拟路由器中为目标接口定义静态路由。如果将接口保留为 **any**，则该规则适用于所有接口，而不考虑虚拟路由器成员关系。
- DHCP 中继 - 不支持为 DHCP 中继互连虚拟路由器。例如，如果在 VR1 接口上启用了 DHCP 中继客户端，而在 VR2 接口上启用了 DHCP 中继服务器，则 DHCP 请求将不会被转发到 VR2 接口之外。
- 重新创建已被删除的虚拟路由器 - 如果您重新创建一个在 10 秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续重新创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

防火墙管理中心 Web 界面 - 路由页面修改

虚拟路由功能不支持用于 Firewall Threat Defense 6.6 之前的设备和少数设备型号。对于此类不受支持的设备，防火墙管理中心 Web 界面显示的是 防火墙管理中心 6.5 或更早版本的“路由”(Routing) 页面。要了解支持使用虚拟路由功能的设备和平台，请参阅支持的设备型号。

您可以在支持设备的路由页面中配置虚拟路由器：

1. 导航至**设备** > **设备管理**，然后编辑虚拟路由器感知设备。
2. 点击**路由 (Routing)** 以进入虚拟路由器页面。

对于使用虚拟路由功能的设备，“路由”(Routing) 页面的左窗格显示以下选项：

- **管理虚拟路由器** - 允许您创建和管理虚拟路由器。
- 虚拟路由协议列表 - 列出可为虚拟路由器配置的路由协议。
- **常规设置** - 允许您配置适用于所有虚拟路由器的 BGP 常规设置。选中**启用 BGP** 复选框可定义其他 BGP 设置。要为虚拟路由器配置其他 BGP 设置，请导航至虚拟路由协议中的 **BGP**。

管理虚拟路由器

当您点击“虚拟路由器”(Virtual Routers) 窗格上的**管理虚拟路由器 (Manage Virtual Routers)** 时，将出现“管理虚拟路由器”(Manage Virtual Routers) 页面。此页面会显示设备和关联接口上的现有虚拟路由器。在此页面中，您可以**添加虚拟路由器** （+）到设备。您还可以**编辑** (✎)和**删除** (🗑)用户定义的虚拟路由器。您无法编辑或删除全局虚拟路由器。您只能**视图**（🔍）全局虚拟路由器的详细信息。

创建虚拟路由器

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击**管理虚拟路由器 (Manage Virtual Routers)**。

步骤 4 请点击 **添加虚拟路由器** （+）。

步骤 5 在“添加虚拟路由器”框中，输入虚拟路由器的名称和说明。

注释
如果您创建一个在10秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

步骤 6 点击**确定 (OK)**。

系统将显示“路由”(Routing) 页面，其中显示新创建的虚拟路由器页面。

下一步做什么

- 配置虚拟路由器。

配置虚拟路由器

您可以为用户定义的虚拟路由器分配接口，并为设备配置路由策略。虽然不能手动为全局虚拟路由器添加或删除接口，但可以为设备接口配置路由策略。

开始之前

- 要为用户定义的虚拟路由器配置路由策略，请添加路由器。请参阅创建虚拟路由器，第1114页。

- 非虚拟路由设备的所有路由配置设置也可用于全局虚拟路由器。有关设置的信息，请参阅路由设置。
- 用户定义的虚拟路由器只支持有限的路由协议。

过程

步骤 1 在**设备** > **设备管理**页面中，编辑虚拟路由器支持的设备。导航至**路由**。有关对路由页面的修改的信息，请参阅 防火墙管理中心 Web 界面 - 路由页面修改，第 1113 页。

步骤 2 从下拉列表中，选择所需的虚拟路由器。

步骤 3 在**虚拟路由器属性 (Virtual Router Properties)** 页面中，您可以修改说明。

步骤 4 要添加接口，请在**可用接口 (Available Interfaces)** 框下选择接口，然后点击**添加 (Add)**。

请记住以下几点：

- **可用接口**框下仅列出具有逻辑名称的接口。您可以编辑接口并在**接口**中提供逻辑名称。请记住保存更改，以使设置生效。
- 仅全域虚拟路由器可用于分配，**可用接口**框仅列出未分配给任何其他用户定义的虚拟路由器的接口。你可以给虚拟路由器分配物理接口、子接口、冗余接口、网桥组、VTI 和EtherChannels，但不能分配其成员接口。由于成员接口无法命名，因此无法在虚拟路由中使用。

  您只能将诊断接口 分配给全局虚拟路由器。

步骤 5 要保存设置，点击**保存 (Save)**。

步骤 6 要为虚拟路由器配置路由策略，请点击各自的名称，打开对应的设置页面：

- **OSPF** - 用户定义的虚拟路由器仅支持 OSPFv2。OSPFv2 的所有其他设置与非虚拟路由器感知接口一样适用，只是**接口**允许您仅选择您正在配置的虚拟路由器的接口。您可以为全局虚拟路由器定义 OSPFv3 和 OSPFv2 路由策略。有关 OSPF 设置的信息，请参阅OSPF，第 1175 页。
- **RIP** - 只能为全局虚拟路由器配置 RIP 路由策略。有关 RIP 设置的信息，请参阅RIP，第 1233 页。
- **BGP** - 此页面显示您在**设置 (Settings)** 中配置的 BGP 常规设置：
  - 除了路由器 ID 设置外，您无法修改此页面上的任何常规设置。您可以在此页面上进行编辑来覆盖在**设置 (Settings)** 页面中定义的路由器 ID 设置。
  - 要配置其他 BGP IPv4 或 IPv6 设置，必须在**常规设置 (General Settings)** 下的 **BGP** 页面中启用 BGP 选项。
  - 全局路由器和用户定义的虚拟路由器均支持 IPv4 和 IPv6 地址系列的 BGP 配置。

  有关配置 BGP 设置的信息，请参阅BGP，第 1213 页。
- **静态路由** - 使用此设置来定义为特定目标网络发送流量的位置。您还可以使用此设置来创建虚拟路由器间静态路由。您可以使用用户定义或全局虚拟路由器的接口创建连接或静态路由的泄

漏。**FMC 为接口添加** 前缀，以指示它属于另一个虚拟路由器并可用于路由泄漏。为使路由泄漏成功，请不要指定下一跳网关。

静态路由表在**已从虚拟路由器泄漏**列中显示其接口用于路由泄漏的虚拟路由器。如果不是路径泄漏，则该列显示 N/A。

无论静态路由属于哪个虚拟路由器，都会列出 Null0 接口以及与静态路由所属的同一虚拟路由器的接口。

有关静态路由设置的信息，请参阅静态和默认路由，第 1087 页。

- **组播** - 只能为全局虚拟路由器配置组播路由策略。有关组播设置的信息，请参阅组播，第 1239 页。

步骤 7 要保存设置，点击**保存 (Save)**。

下一步做什么

- 修改虚拟路由器。
- 删除虚拟路由器。

修改虚拟路由器

您可以修改虚拟路由器的说明和其他路由策略。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击**管理虚拟路由器 (Manage Virtual Routers)**。

所有虚拟路由器以及分配的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要修改虚拟路由器，请点击所需虚拟路由器旁边的 **编辑** ()。

注释
无法修改全局虚拟路由器的常规设置。因此，不能对全局路由器进行编辑； 而是提供 **视图**（）来查看设置。

步骤 5 要保存更改，请点击**保存 (Save)**。

下一步做什么

- 删除虚拟路由器。

删除虚拟路由器

开始之前

- 不能删除全局虚拟路由器。因此，删除选项不可用于全局虚拟路由器。
- 您可以一次删除多个虚拟路由器。
- 被删除的虚拟路由器的所有路由策略也被删除。
- 被删除的虚拟路由器的所有接口都移动到全局虚拟路由器。
- 如果接口的移动存在任何限制（例如重叠 IP、路由冲突等），则只有在解决冲突后才能删除路由器。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击**管理虚拟路由器 (Manage Virtual Routers)**。

所有虚拟路由器以及映射的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要删除虚拟路由器，请点击所需虚拟路由器旁边的 **删除** ()。

步骤 5 要删除多个路由器，请按住 CTRL 键，点击要删除的虚拟路由器。右键点击，然后点击**删除**。

步骤 6 要保存更改，请点击**保存 (Save)**。

监控虚拟路由器

要对虚拟路由器进行监控和故障排除，请登录设备 CLI 并使用以下命令。

- **show vrf**：显示虚拟路由器及其关联接口的详细信息。
- **show route vrf** <*vrf_name*>：显示虚拟路由器的路由详细信息。
- **show run router bgp all**：显示所有虚拟路由器的 BGP 路由详细信息。
- **show run router bgp vrf** <*vrf_name*>：显示虚拟路由器的 BGP 路由详细信息。
- **show crypto ipsec sa/show crypto ikev2 sa**：显示隧道和关联虚拟路由器的详细信息。
- 您可以在站点间监控控制面板中监控隧道（**概述** > **站点间 VPN**）。

  在 **隧道状态** 构件中，将鼠标悬停在拓扑上，点击查看 ，然后点击 **数据包跟踪器** 以查看威胁防御 VPN 隧道并进行故障排除。

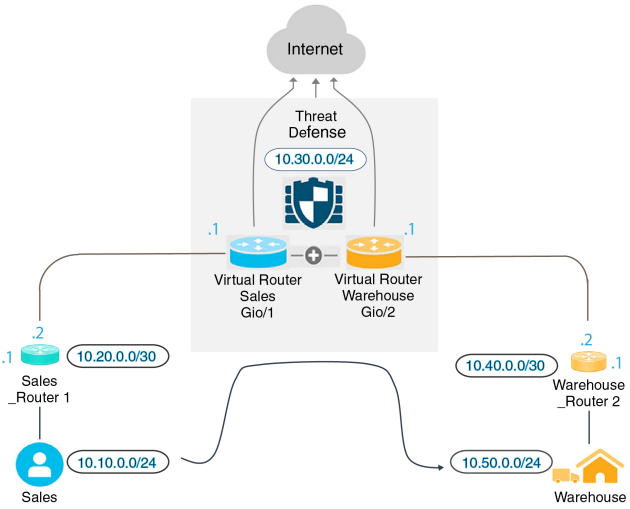
虚拟路由器的配置示例

如何通过虚拟路由器路由到远程服务器

在虚拟路由中，您可以创建多个虚拟路由器来为接口组维护单独的路由表，从而实现网络分离。在某些情况下，您可能需要访问只能通过单独的虚拟路由器访问的服务器。此示例提供了将虚拟路由器互联以访问相距多跳的主机的程序。

例如，假设一家服装公司的销售部成员想要在其工厂单位仓库部门维护的库存中进行查找。在虚拟路由环境中，您需要在目标（仓库部门）与销售部门相距多跳的虚拟路由器之间泄漏路由。路由泄漏是通过添加多跳路由泄漏来完成的，在此过程中，您需要在“销售”虚拟路由器（源）中配置一条通往“仓库”虚拟路由器（目标）中的接口的静态路由。当目标网络相距多跳时，您还需要为“仓库”虚拟路由器配置通往目标网络（即 10.50.0.0/24）的路由。

图 *391:* 互联两个虚拟路由器 - 示例



开始之前

此示例假设您已配置 Sales_Router1，从而将流量从 10.20.0.1/30 接口路由到 10.50.0.5/24。

过程

步骤 1 配置要分给“销售”虚拟路由器的设备的内部接口 (Gi0/1)：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击 **接口 (Interfaces)**。

b) 编辑 Gi0/1 接口：

- **名称** - 本例中为“VR-Sales”。
- 选中**启用**复选框。

- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 输入 10.30.0.1/24。

c) 点击**确定 (OK)**。
d) 点击**保存 (Save)**。

步骤 2 配置要分配给“仓库”虚拟路由器的设备的内部接口 (Gi0/2)：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击 **接口 (Interfaces)**。
b) 编辑 Gi0/2 接口：
   - **名称** - 本例中为“VR-Warehouse”。
   - 选中**启用**复选框。
   - 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
   - **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址 (10.30.0.1/24) 配置接口，因为您尚未创建用户定义的虚拟路由器。
c) 点击**确定 (OK)**。
d) 点击**保存 (Save)**。

步骤 3 创建“销售”和“仓库”虚拟路由器并分配其接口：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
b) 依次选择**路由** > **管理虚拟路由器**。
c) 点击**添加虚拟路由器**并创建“销售”虚拟路由器。
d) 点击**添加虚拟路由器**并创建“仓库”虚拟路由器。
e) 从虚拟路由器下拉列表中选择“销售”，然后在**虚拟路由器属性**中，添加“VR-Sales”作为**选定接口**并保存。
f) 从虚拟路由器下拉列表中选择“仓库”，然后在**虚拟路由器属性**中，添加“VR-Warehouse”作为**选定接口**并保存。

步骤 4 重新访问“VR-Warehouse”接口配置：

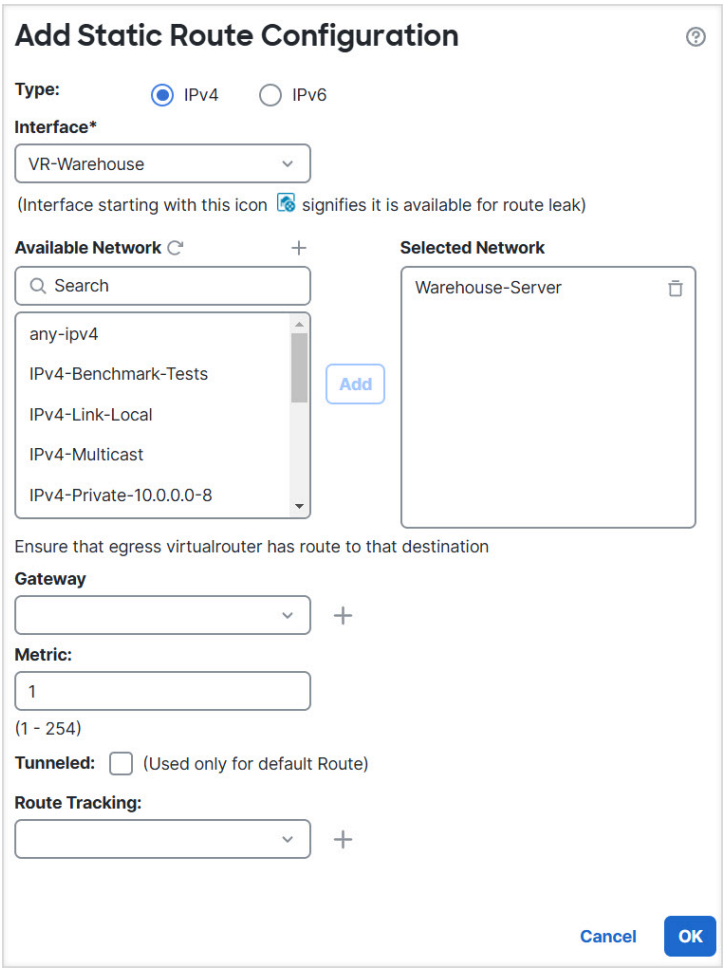
a) 选择 **设备** > **设备管理**，点击设备名称，然后点击 **接口 (Interfaces)**。
b) 针对“VR-Warehouse”接口点击**编辑**。将 IP 地址指定为 10.30.0.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用“VR-Sales”的同一 IP 地址进行配置。
c) 点击**确定 (OK)**。
d) 点击**保存 (Save)**。

步骤 5 为仓库服务器 (10.50.0.0/24) 和仓库网关 (10.40.0.2/30) 创建网络对象：

a) 选择**对象**。
b) 依次选择**添加网络** > **添加对象**：
   - **名称** - 本例中为“Warehouse-Server”。
   - **网络** - 点击“网络”并输入 10.50.0.0/24。

c) 点击**保存 (Save)**。
d) 依次选择**添加网络** > **添加对象**：
   - **名称** - 本例中为“Warehouse-Gateway”。
   - **网络** - 点击“主机”并输入 10.40.0.2。
e) 点击**保存 (Save)**。

步骤 6 定义指向“VR-Warehouse”接口的“销售”虚拟路由器中的路由泄漏：
a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
b) 选择**路由**。
c) 从下拉列表中选择“销售”虚拟路由器，然后点击**静态路由**。
d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：
   - **接口** - 选择“VR-Warehouse”。
   - **网络** - 选择 Warehouse-Server 对象。
   - **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



e) 点击**确定 (OK)**。

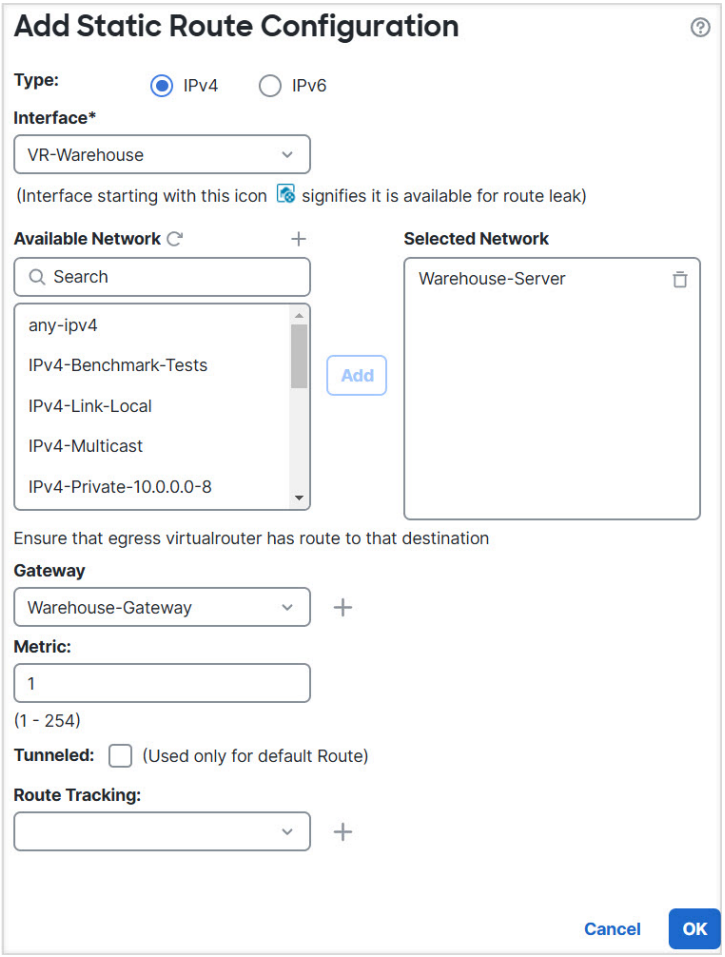
f) 点击**保存 (Save)**。

步骤 7 在“仓库”虚拟路由器中，定义指向仓库路由器 2 网关的路由：

a) 从下拉列表中选择“仓库”虚拟路由器，然后点击**静态路由**。

b) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口** - 选择“VR-Warehouse”。
- **网络** - 选择 Warehouse-Server 对象。
- **网关**-选择 Warehouse-Gateway 对象。



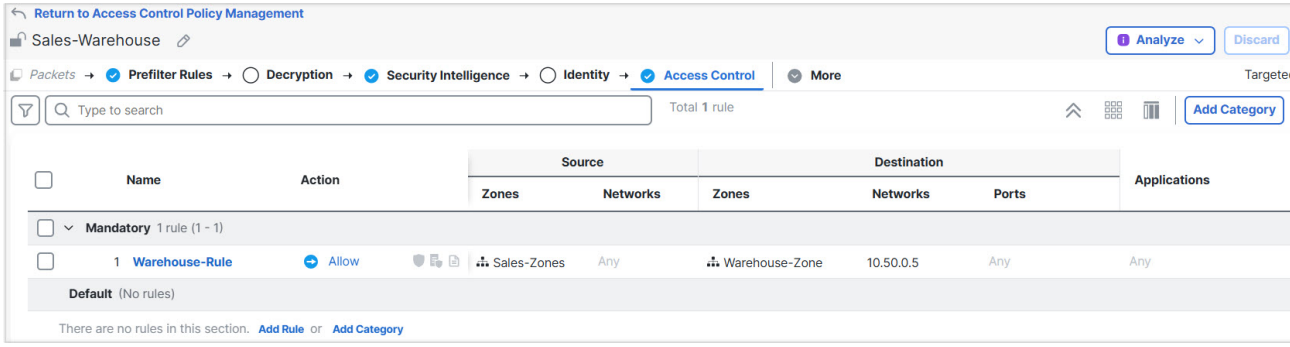
c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 8 配置允许访问仓库服务器的访问控制规则。要创建访问控制规则，您需要创建安全区域。使用。**对象** > **接口**依次选择**添加** > **安全区域**并为“VR-Sales”和“VR-Warehouse”创建安全区域；对于 Warehouse-Server 网络对象，创建 Warehouse-Server 接口组（依次选择**添加** > **接口组**）。

步骤 9 依次选择**策略** > **安全策略** > **访问控制**策略访问控制并配置访问控制规则，以允许流量从“销售”虚拟路由器中的源接口到流向目的 Warehouse-Server 网络对象的“仓库”虚拟路由器中的目的接口。

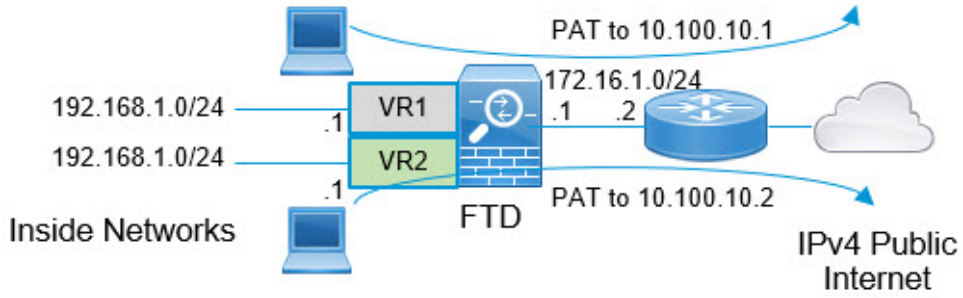
例如，如果“销售”虚拟路由器中的接口位于“销售区域”安全区域中，而“仓库”虚拟路由器中的接口位于“仓库区域”安全区域中，则访问控制规则将如下所述：



如何提供包含重叠地址空间的互联网访问权限

使用虚拟路由器时，您可以为驻留在单独路由器中的多个接口设置相同的网络地址。但是，由于在这些单独的虚拟路由器中路由的 IP 地址相同，因此请使用单独的 NAT/PAT 池为每个接口应用 NAT/PAT 规则，以确保返回流量到达正确的目的地。此示例提供了为管理重叠地址空间而配置虚拟路由器和 NAT/PAT 规则的程序。

例如，Firewall Threat Defense 上的接口 vr1-inside 和 vr2-inside 被定义为使用 IP 地址 192.168.1.1/24，从而将终端托管在其在 192.168.1.0/24 网络中的分段上。要允许通过两个使用相同地址空间的虚拟路由器访问互联网，您需要将 NAT 规则分别应用于每个虚拟路由器中的接口，最好使用单独的 NAT 或 PAT 池。可以使用 PAT 将 VR1 中的源地址转换为 10.100.10.1，并将 VR2 中的源地址转换为 10.100.10.2。下图显示了此设置，其中面向互联网的外部接口是全局路由器的一部分。您必须使用明确选择的源接口（vr1-inside 和 vr2-inside）来定义 NAT/PAT 规则 - 使用“任何”作为源接口将使系统无法识别正确源，这是因为两个不同的接口上可能存在相同的 IP 地址。



注释 即使您拥有不使用重叠地址空间的虚拟路由器中的一些接口，也要用源接口定义NAT规则，以便简化故障排除过程，并确保更加清楚地区分来自与互联网绑定的各虚拟路由器之间的流量。

过程

步骤 1 为 VR1 配置设备的内部接口：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击**接口**。

b) 编辑您要分配给 VR1 的接口：

- **名称 (Name)** - 在此示例中为 vr1-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 2 为 VR2 配置设备的内部接口：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击**接口**。

b) 编辑您要分配给 VR2 的接口：

- **名称 (Name)** - 在此示例中为 vr2-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 3 配置 VR1 和到外部接口的静态默认路由泄漏：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

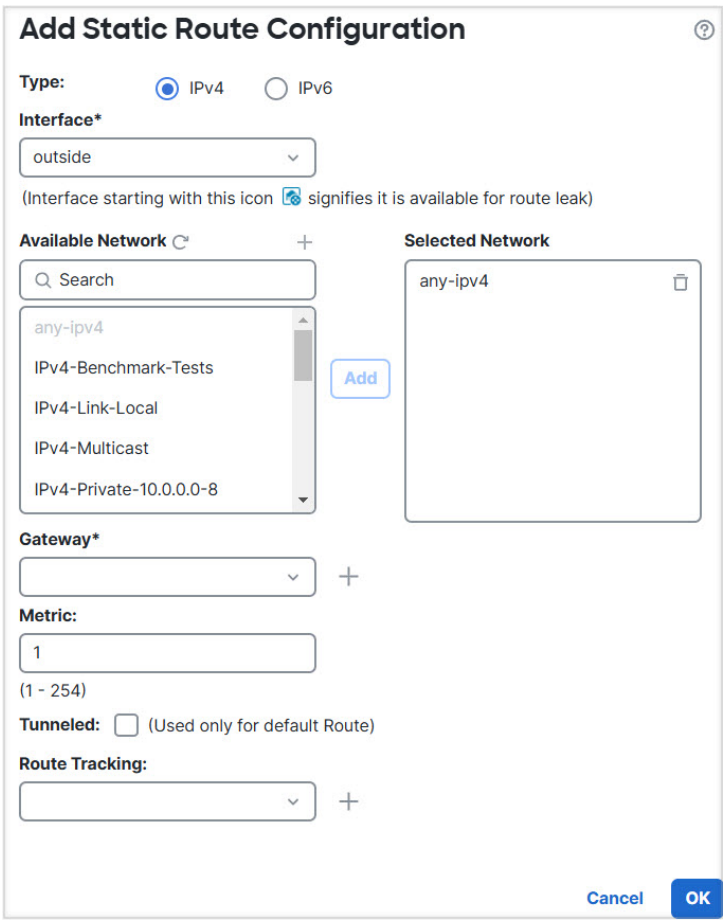
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR1。

c) 对于 VR1，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr1-inside 并保存。

d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR1 内路由的任何流量的默认路由。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿提供网关。



f) 点击**确定 (OK)**。

g) 点击**保存 (Save)**。

步骤 4 配置 VR2 和到外部接口的静态默认路由泄漏：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

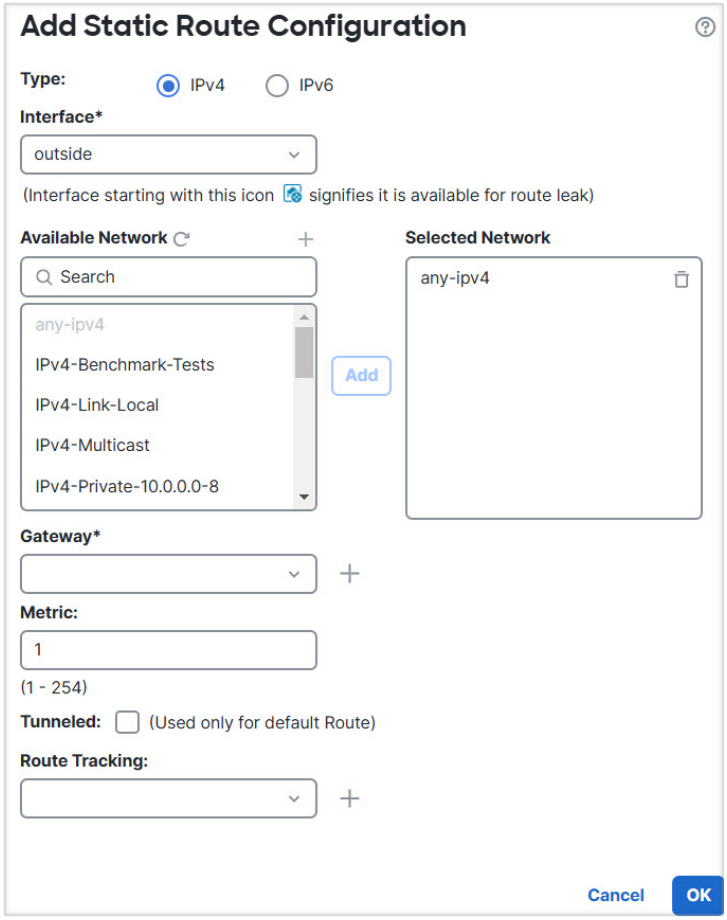
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR2。

c) 对于 VR2，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr2-inside 并保存。

d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR2 内路由的任何流量的默认路由。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



f) 点击**确定 (OK)**。

g) 点击**保存 (Save)**。

步骤 5 在全局路由器的外部接口上配置 IPv4 静态默认路由，即 172.16.1.2：

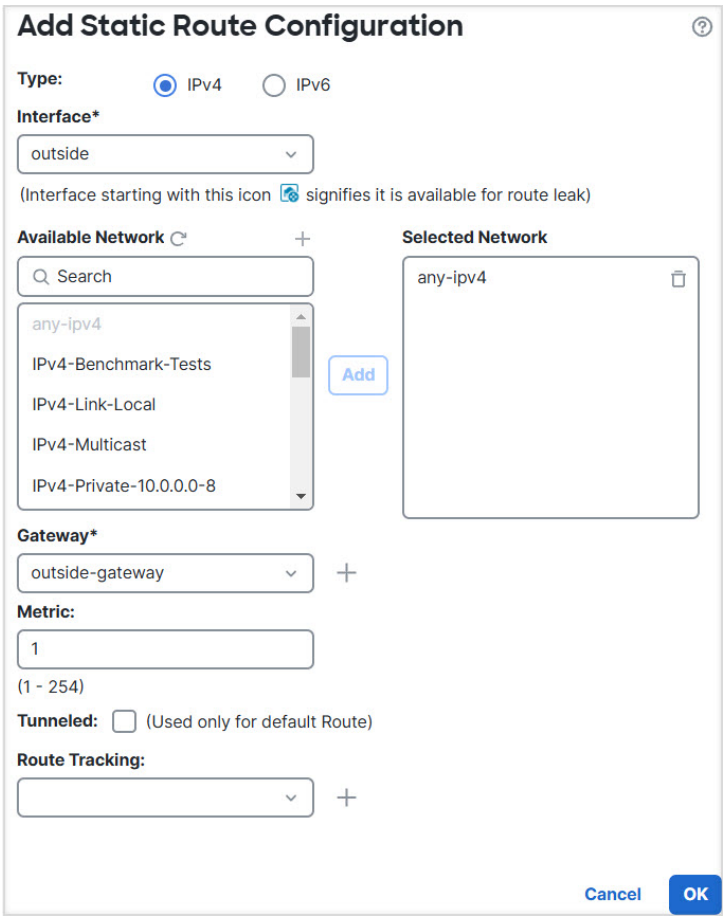
a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

b) 选择**路由 (Routing)** 并编辑全局路由器属性。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这将是用于任何 IPv4 流量的默认路由。
- **网关 (Gateway)** - 如果已创建，请从下拉列表中选择主机名。如果尚未创建对象，请点击**添加 (Add)**，然后为外部接口上网络链路另一端的网关的 IP 地址（在本例中为 172.16.1.2）定义主机对象。创建对象后，在“网关”(Gateway) 字段中选择该对象。



e) 点击**确定 (OK)**。

f) 点击**保存 (Save)**。

步骤 6 重新访问 vr2-inside 接口配置：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击**接口**。

b) 点击 vr2-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 vr1-inside 的相同 IP 地址进行配置。

c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 7 创建 NAT 规则，以将 VR1 的 PAT 内-外流量传输到 10.100.10.1。

a) 选择**策略** > **网络策略** > **NAT** 。

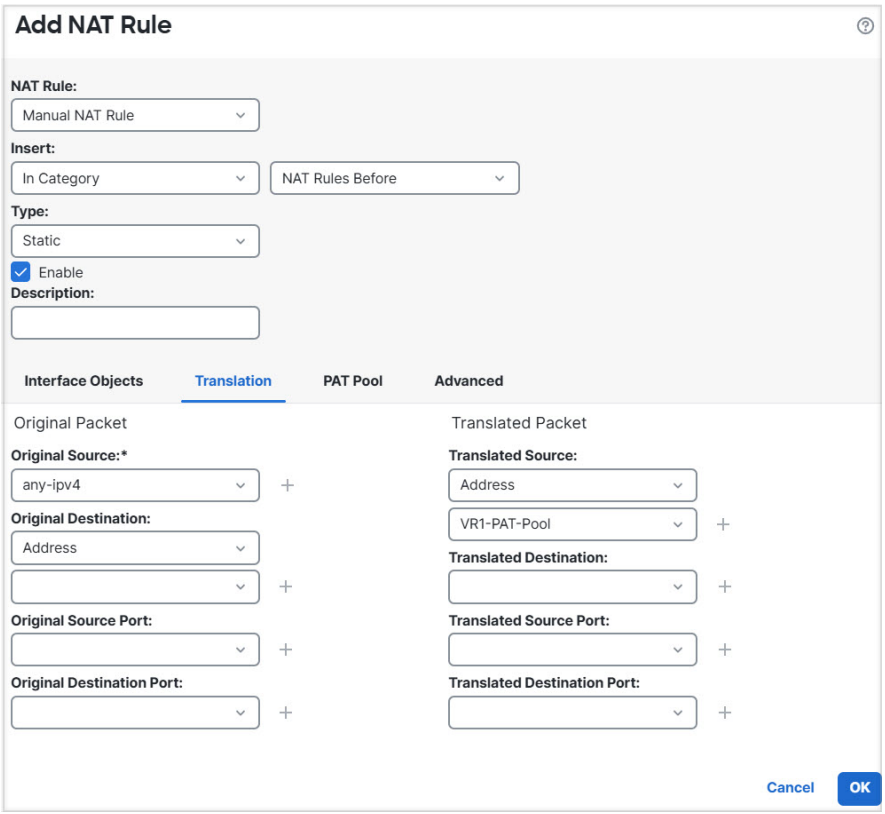
b) 点击**新策略 (New Policy)**。

c) 输入 InsideOutsideNATRule 作为 NAT 策略名称，然后选择 Firewall Threat Defense 设备。点击**保存**。

d) 在 InsideOutsideNATRule 页面中，点击**添加规则**并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“动态”(Dynamic)。

- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象**中，选择 vr1-interface 对象并点击**添加到源**（如果该对象不可用，请在 **对象** > **接口** 中创建一个），然后选择外部接口作为**添加到目标**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.1 来定义主机对象 VR1-PAT-Pool。选择 VR1-PAT-Pool，如下图所示：



e) 点击**确定 (OK)**。

f) 点击**保存 (Save)**。

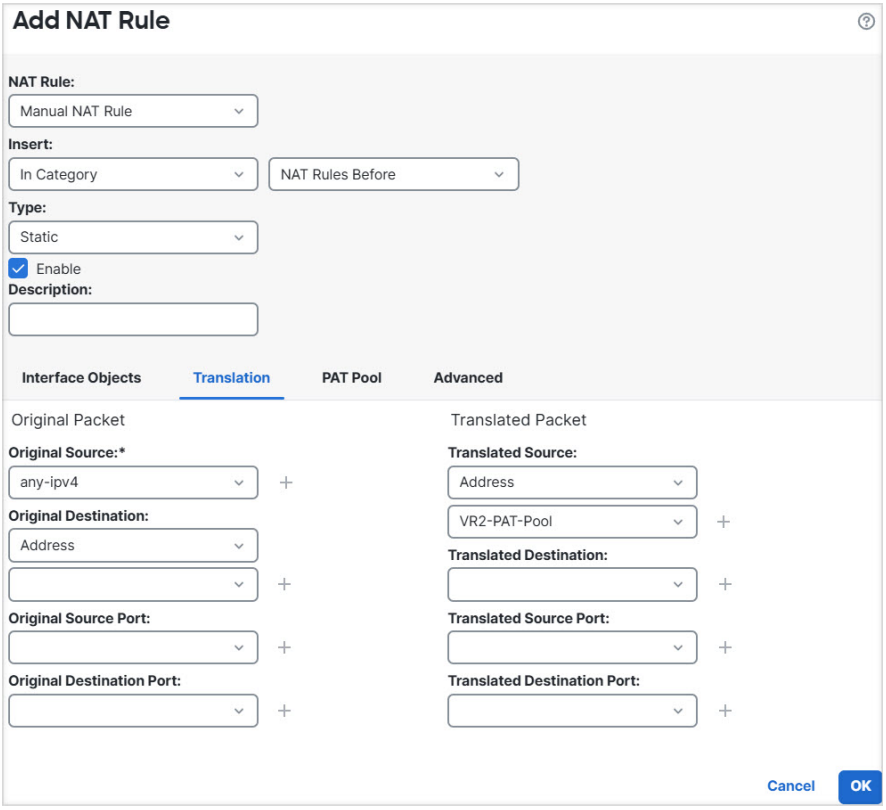
步骤 8 添加 NAT 规则，以将 VR2 的 PAT 内-外流量传输到 10.100.10.2。

a) 选择**策略** > **网络策略** > **NAT** 。

b) 编辑 InsideOutsideNATRule 以定义 VR2 NAT 规则：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“动态”(Dynamic)。
- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。

- 在**接口对象**中，选择 vr2-interface 对象并点击**添加到源**（如果该对象不可用，请在 **管理** > **配置** > **管理接口** 中创建一个），然后选择外部接口作为**添加到目标**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.2 来定义主机对象 VR2-PAT-Pool。选择 VR2-PAT-Pool，如下图所示：



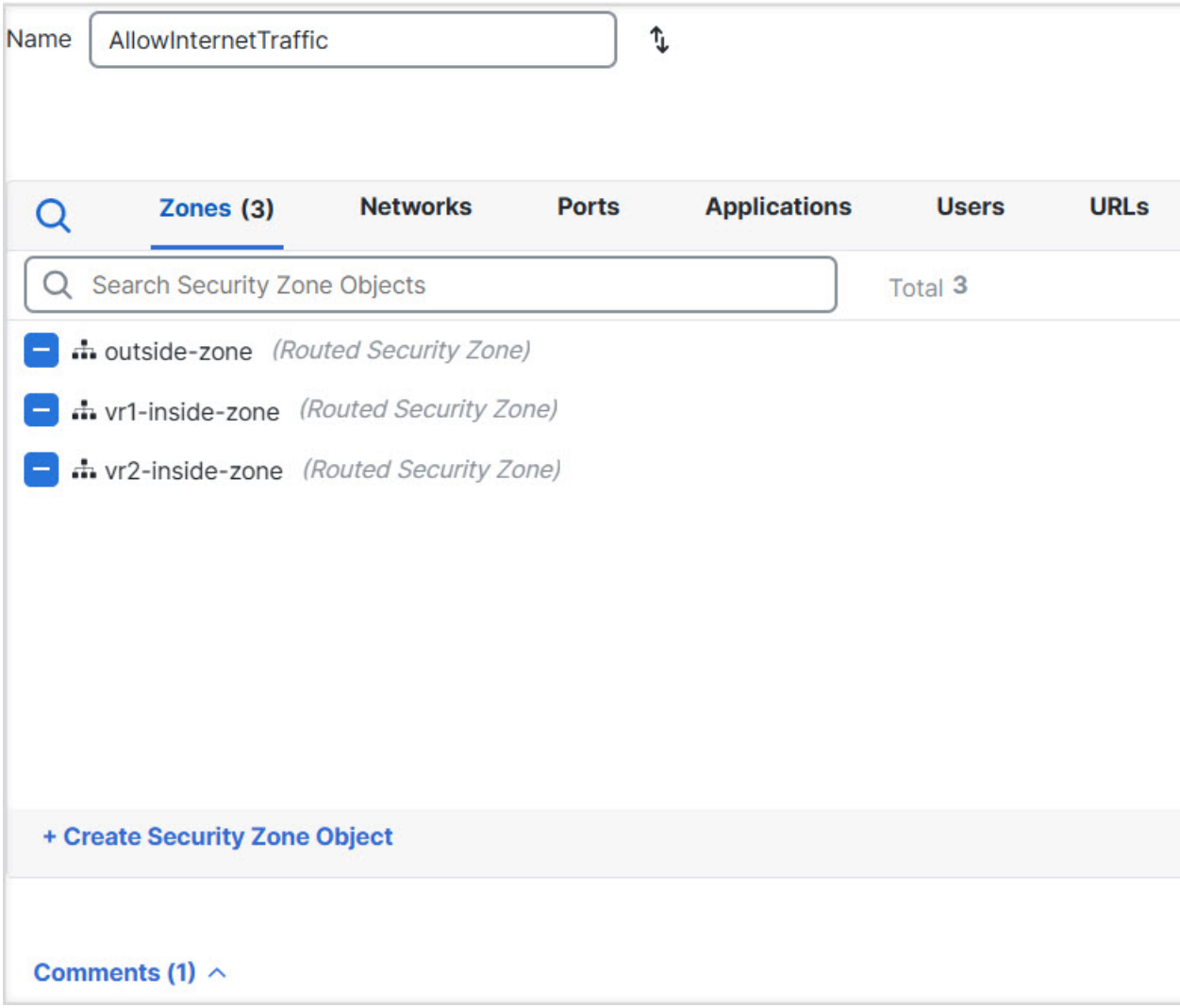
c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 9 要配置允许流量从 vr1-inside 和 vr2-inside 接口流向外部接口的访问控制策略，您需要创建安全区域。使用。**对象** > **接口**选择**添加 (Add)** > **安全区域 (Security Zone)** 并为 vr1-inside、vr2-inside 和外部接口创建安全区域。

步骤 10 选择**策略** > **安全策略** > **访问控制**，然后配置访问控制规则以允许将 vr1-inside-zone 和 vr2- inside-zone 中的流量传输到 outside-zone。

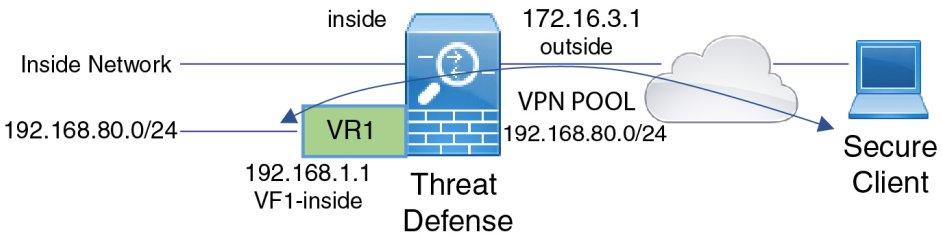
假设您创建了以接口命名的区域，则允许所有流量流向互联网的基本规则将如下所示：您可以将其他参数应用于此访问控制策略：



如何允许对虚拟路由中的内部网络进行 RA VPN 访问

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持 RA VPN。此示例提供允许 Secure Client 用户连接到用户定义的虚拟路由器网络的程序。

在下面的示例中，RA VPN（Secure Client）用户连接到地址为 172.16.3.1 的 Firewall Threat Defense 外部接口，并在 192.168.80.0/24 池中获得 IP 地址。该用户只能访问全局虚拟路由器的内部网络。要允许流量通过用户定义的虚拟路由器 VR1 的网络（即 192.168.1.0/24），请通过在全局和 VR1 上配置静态路由来泄漏路由。



开始之前

此示例假设您已配置 RA VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏。

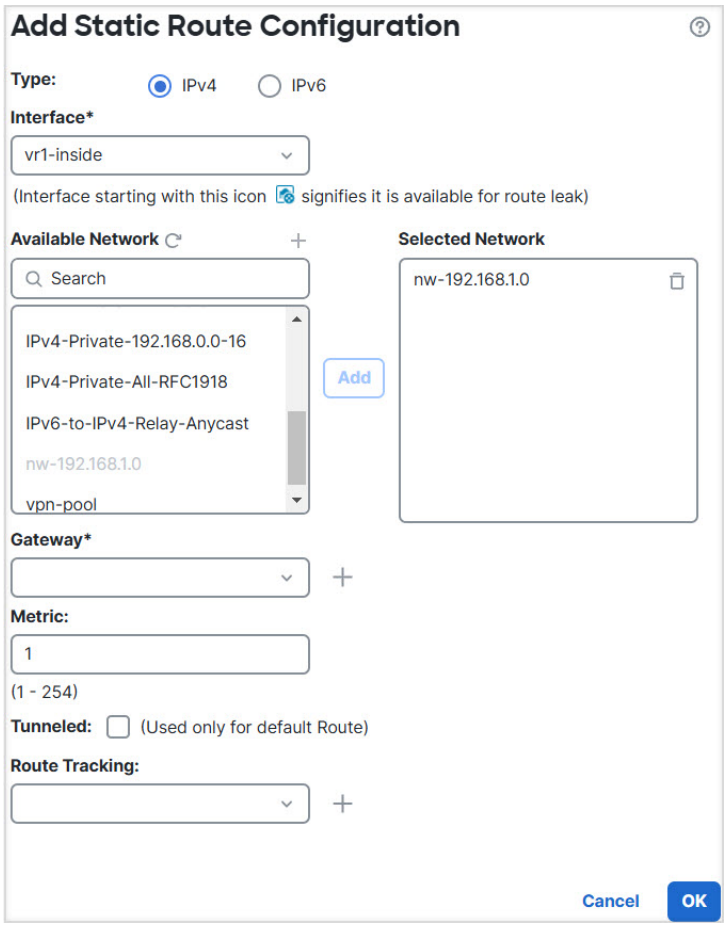
a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

b) 点击**路由 (Routing)**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



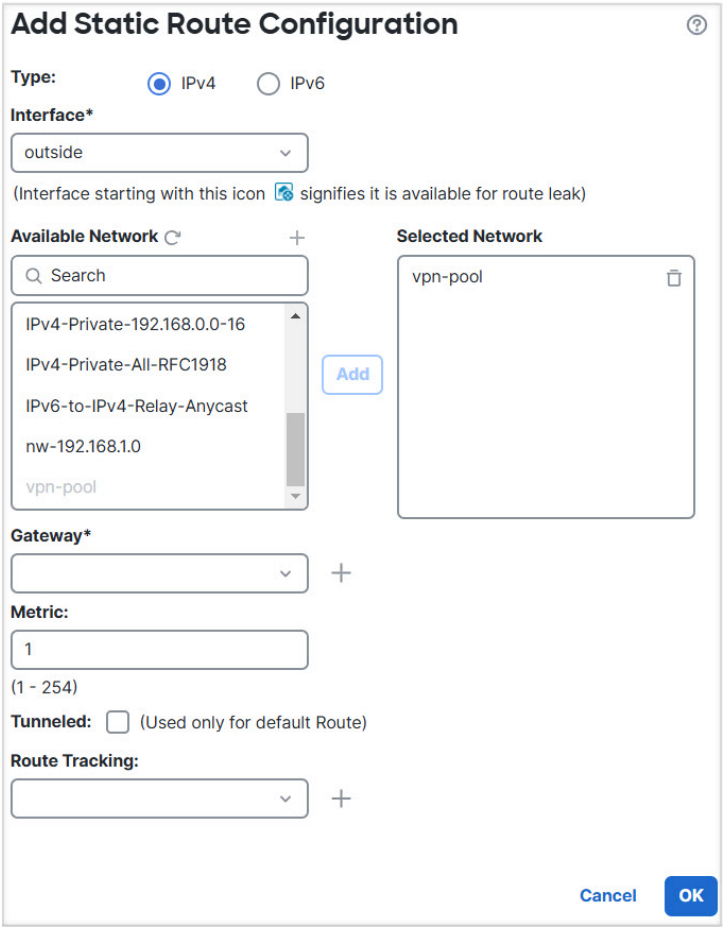
此路由泄露允许在 VPN 池中分配 IP 地址的 Secure Client 访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。
c) 点击**静态路由 (Static Route)**。
d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



配置的静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端向在 VPN 池中分配 IP 地址的 Secure Client 发起连接。

e) 点击**确定**。

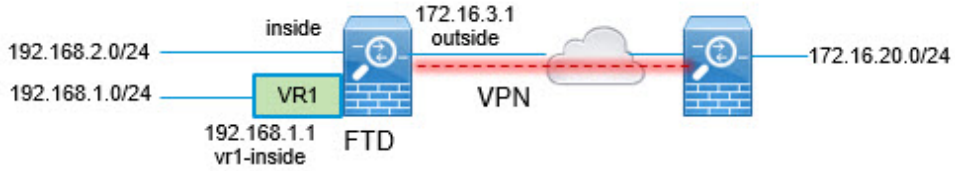
下一步做什么

如果 RA VPN 地址池与用户定义的虚拟路由器中的 IP 地址重叠，则还必须对 IP 地址使用静态 NAT 规则，以启用正确的路由。或者，您可以更改 RA VPN 地址池，以免出现重叠。

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持站点间 VPN。您不能在属于用户定义的虚拟路由器的接口上配置它。此示例提供的程序让您能够通过站点间VPN保护来自或到达用户定义的虚拟路由器内的网络的连接。您还需要更新站点间VPN连接，以包括这些用户定义的虚拟路由网络。

我们假设这样一个场景：在分支机构网络和公司总部网络之间配置站点间VPN；分支机构中的Firewall Threat Defense 具有虚拟路由器。在这种情况下，站点间 VPN 在 172.16.3.1 的分支机构外部接口上定义。此 VPN 包括内部网络 192.168.2.0/24，而无需进行额外配置，因为内部接口也是全局虚拟路由器的一部分。但是，要为 192.168.1.0/24 网络（其为 VR1 虚拟路由器的一部分）提供站点间 VPN 服务，则必须通过在全局和 VR1 上配置静态路由来泄露路由，并将 VR1 网络加入站点间的 VPN 配置中。



开始之前

此示例假设您已在本地网络 192.168.2.0/24 与外部网络 172.16.20.0/24 之间配置站点间 VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏：

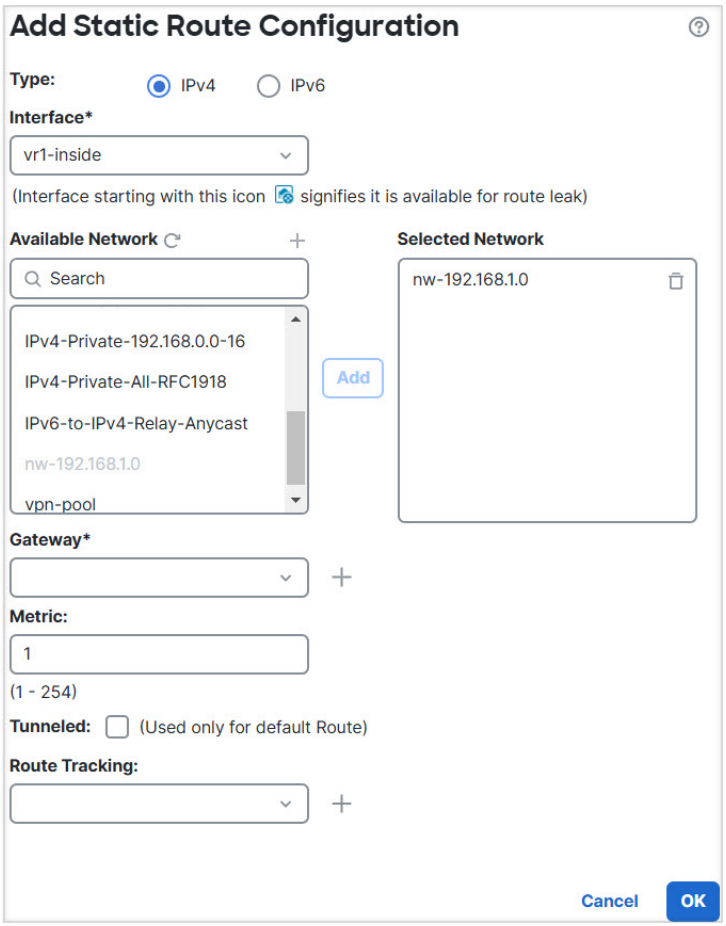
a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

b) 点击**路由 (Routing)**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此路由泄漏允许受站点间 VPN 的外部（远程）终端保护的终端访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

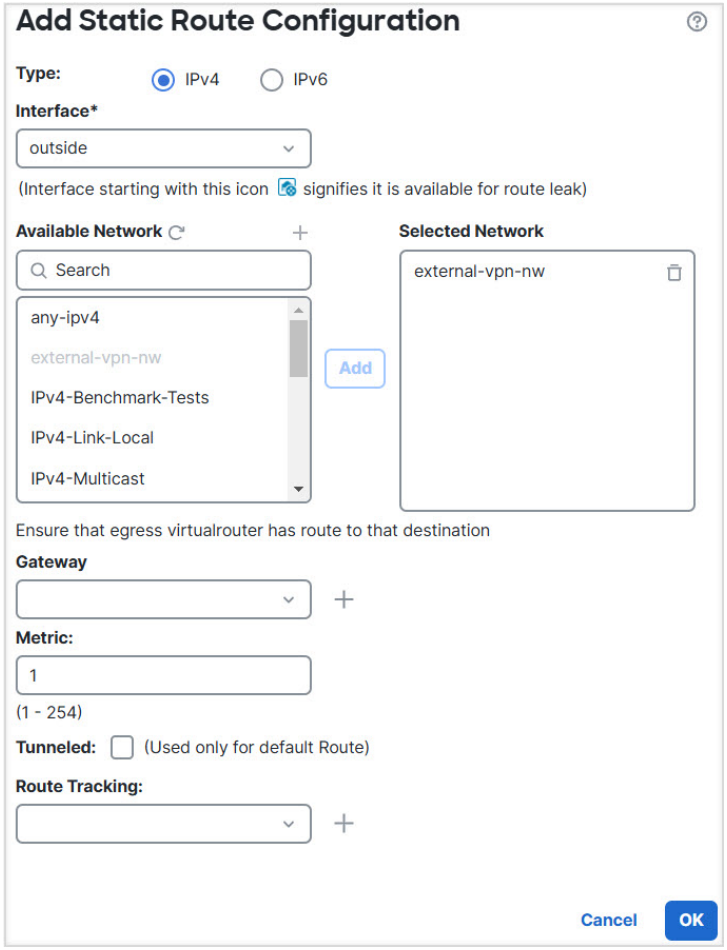
a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端发起流经站点间 VPN 隧道的连接。在本示例中，远程终端正在保护 172.16.20.0/24 网络。

e) 点击**确定**。

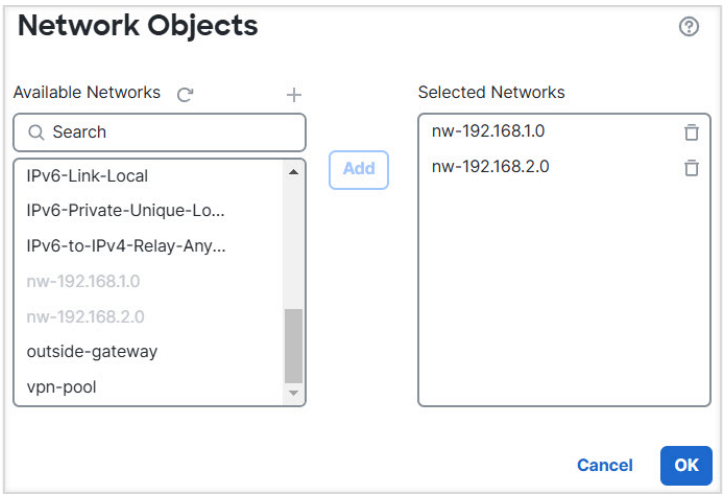
步骤 3 将 192.168.1.0/24 网络添加到站点间 VPN 连接配置文件中：

a) 选择**安全连接** > **站点间 VPN 和 SD-WAN**，然后编辑 VPN 拓扑。

b) 在**终端 (Endpoints)** 中，编辑节点 A 终端。

c) 在**编辑终端 (Edit Endpoint)** 的**受保护网络 (Protected Networks)** 字段中，点击**添加新网络对象 (Add New Network Object)**。

d) 添加网络为 192.168.1.0 的 VR1 网络对象：



e) 点击**确定 (Ok)** 并保存配置。

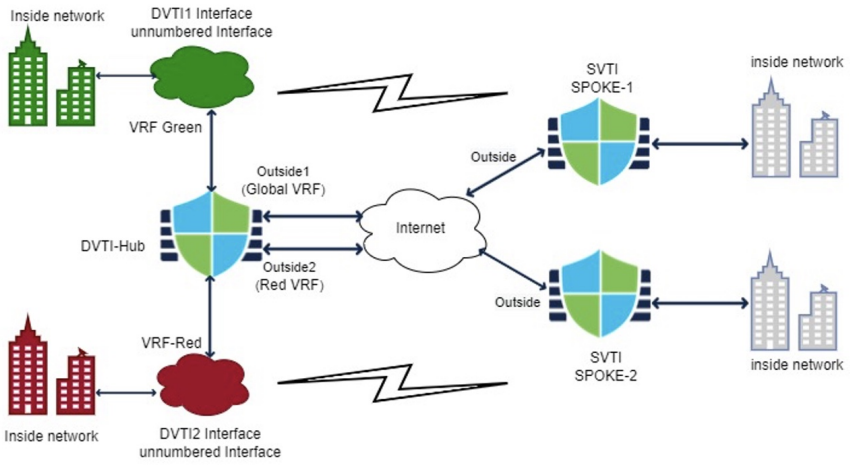
如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量

ISP 为不同的客户提供不同的分段网络。您可以创建虚拟路由器，将动态 VTI 与这些虚拟路由器关联，并在网络中扩展动态 VTI 的功能。可以将动态 VTI 与全局或用户定义的虚拟路由器关联。单个威胁防御设备可以充当具有全局或一个或多个用户定义的虚拟路由器的动态 VTI 中枢。每个用户定义的虚拟路由器都可以是一个客户网络。

让我们考虑在两个公司总部网络与其两个分支机构网络之间配置基于路由的站点间 VPN 的示例。ISP 的威胁防御是一个动态 VTI 集线器，它使用两个用户定义的虚拟路由器管理两个公司总部网络：VRF 绿色和 VRF 红色。动态 VTI 集线器在以下对象之间建立站点间 VPN：

- 客户 1（VRF 绿色）和分支机构 1（SVTI 分支 1）
- 客户 2（VRF 红色）和分支机构 2（SVT2 分支 2）

图 *392:* 具有多个虚拟路由器和动态 *VTI* 的站点间 *VPN*



此示例说明如何通过具有动态 VTI 的站点间 VPN 配置具有多个虚拟路由器的网络。

过程

步骤 1 在集线器上配置动态 VTI 接口。

a) 选择**设备** > **设备管理**，并且编辑威胁防御设备。
b) 选择 **添加接口** > **虚拟隧道接口**。
c) 选择 **动态** 作为**隧道类型** 。
d) 将接口名称指定为 DVTI1，并为动态 VTI 配置所有参数。
e) 点击**保存**
f) 重复步骤 1a - e，在集线器 DVTI2 上配置第二个动态 VTI。

步骤 2 在分支 1 上配置静态 VTI。

a) 选择**设备** > **设备管理**，并且编辑威胁防御设备。
b) 选择 **添加接口** > **虚拟隧道接口**。
c) 选择 **隧道类型** 作为 **静态**。
d) 将接口名称指定为 SVTI Spoke-1，并为静态 VTI 配置所有参数。
e) 点击**保存**
f) 重复步骤 2a - e，在分支 2 上配置静态 VTI：SVTI 分支 2。

步骤 3 为中心和 SVTI 1辐射型拓扑配置路由型站点间 VPN。

a) 选择**安全连接** > **站点间 VPN 和 SD-WAN**，然后点击 **+ 站点间 VPN**。
b) 在 **拓扑名称** 字段中，输入 VPN 拓扑的名称。
c) 选择 **基于路由 (VTI)** 并选择 **中心辐射型** 作为网络拓扑。
d) 点击 **终端** 选项卡。
e) 配置中心和分支（DVTI1 和 SVTI 分支 1）及其路由策略。
f) 如果需要，为 VPN 配置 **IKE**、 **IPsec**和 **高级** 选项。

g) 点击**保存**。
h) 重复步骤 3a - g，在中心 (DVTI2) 和 SVTI 分支 2 之间配置第二个基于路由的站点间 VPN 拓扑。

步骤 4 配置两个虚拟路由器。

a) 选择**设备** > **设备管理**，并且编辑威胁防御设备。
b) 点击**路由 (Routing)**。
c) 点击**管理虚拟路由器 (Manage Virtual Routers)**。
d) 点击 **Add Virtual Router**。

将名称指定为 VRF 绿色，并提供虚拟路由器的说明。

e) 重复步骤 4a-d，配置 VRF 红色。

步骤 5 将所有接口分配给虚拟路由器。

a) 从下拉列表中，选择虚拟路由器。
b) 在 **虚拟路由器属性** 页面中，选择 **可用接口** 框下列出的接口。

将动态 VTI 接口与其他接口一起分配。

c) 点击**添加 (Add)**。

步骤 6 对 VRF 红色重复步骤 5a-c。

步骤 7 配置虚拟路由器的路由策略。

a) 从下拉列表中，选择虚拟路由器。
b) 点击 **静态路由** 或其中一种动态路由协议。
c) 配置路由参数。
d) 点击**保存**。

下一步做什么

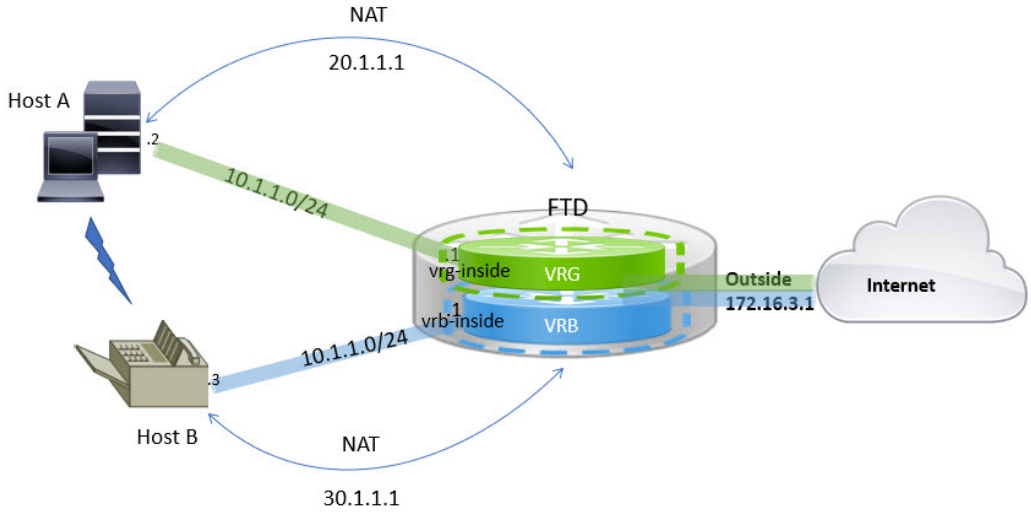
选择中心辐射型设备，然后点击 **部署**。部署后，您可以在站点间监控控制面板（**洞察和报告** > **VPN 控制面板** > **站点间 VPN**）中监控 VPN 隧道。

您还可以使用 监控虚拟路由器，第 1117 页 中列出的命令查看虚拟路由器并对其进行故障排除。

如何在虚拟路由中的两个重叠网络主机之间路由流量

您可以在具有相同网络地址的虚拟路由器上配置主机。如果主机想要通信，您可以配置两次 NAT。本示例提供了配置 NAT 规则以管理重叠网络主机的程序。

在下面的示例中，两台主机主机 A 和主机 B 属于不同的虚拟路由器：VRG（接口 vrg-inside）和 VRB（接口 vrb-inside），分别具有相同的子网 10.1.1.0/24。要让两台主机通信，请创建一个 NAT 策略，其中 VRG 主机接口对象将使用映射 NAT 地址 - 20.1.1.1，而 VRB 主机接口对象将使用映射 NAT 地址 - 30.1.1.1。因此，主机 A 会使用 30.1.1.1 与主机 B 通信；主机 B 会使用 20.1.1.1 访问主机 A。



开始之前

此示例假定您已：

- vrg-inside 和 vrb-inside 接口分别与虚拟路由器关联：VRG 和 VRB 以及配置了相同子网地址的 vrg-inside 和 vrb-inside 接口（例如 10.1.1.0/24）。
- 分别使用 vrg-inside 和 vrb-inside 接口创建的接口区域 VRG-Inf、VRB-Inf。
- VRG 中的主机 A，默认网关为 vrg-inside；主机 B 位于 VRB 中，vrb-inside 作为默认网关。

过程

步骤 1 创建 NAT 规则以处理从主机 A 到主机 B 的流量。选择**策略** > **网络策略** > **NAT** 。

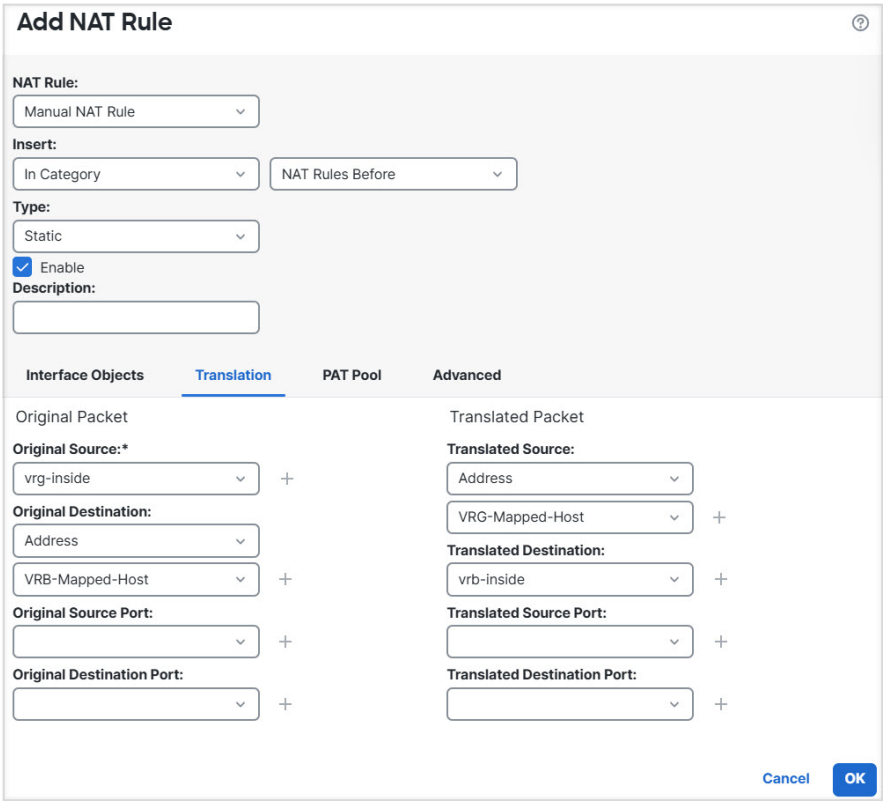
步骤 2 点击**新策略 (New Policy)**。

步骤 3 输入 NAT 策略名称，然后选择 Firewall Threat Defense 设备。点击**保存**。

步骤 4 在 NAT 页面中，点击**添加规则**并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象**中，选择 VRG-Inf 对象并点击**添加到源**（如果该对象不可用，请在 **对象** > **接口** 中创建一个），然后选择 VRB-Inf 对象并点击**添加到目标**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 vrg-inside。

- **原始目标 (Original Destination)**，点击**添加 (Add)** 并使用 30.1.1.1 定义对象 VRB-Mapped-Host。选择 VRB 映射主机。
- **转换后的源 (Translated Source)**，，点击**添加 (Add)** 并使用 20.1.1.1 定义对象 VRG-Mapped-Host。选择 VRG 映射主机。
- **转换后的目标 (Translated Destination)**，选择 vrb-inside，如下图所示：



在 Firewall Threat Defense 设备上运行 **show nat detail** 命令时，您将看到类似于以下内容的输出：

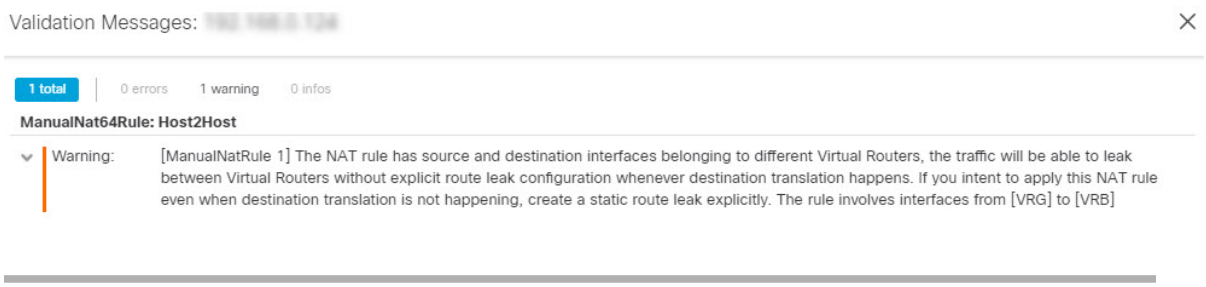
```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

NAT 规则如下所示：

在部署配置时会出现一条警告消息：

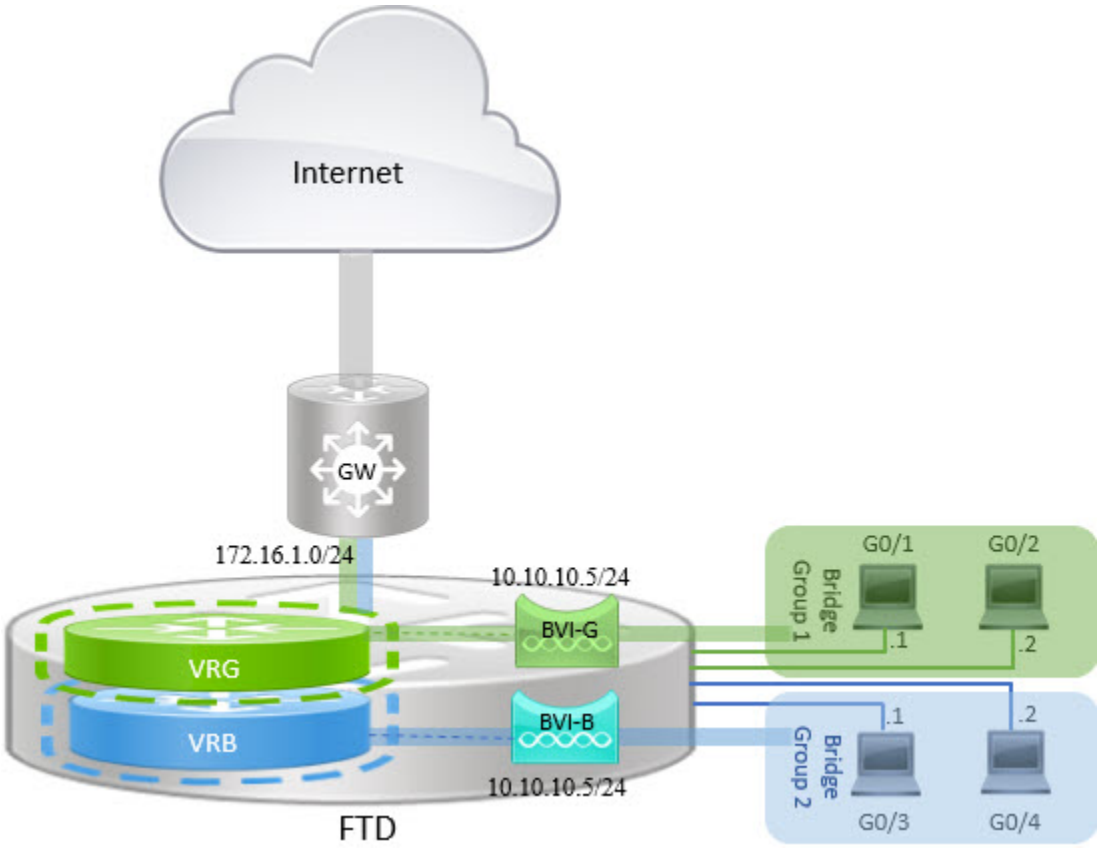


如何使用 BVI 接口在路由防火墙模式下管理重叠网段

您可以在多个重叠网络之间透明地部署单个 Firewall Threat Defense 和/或在同一网络的主机之间部署防火墙。要实现此部署，请按虚拟路由器来配置 BVI。下面介绍了在虚拟路由器中配置 BVI 的程序。

BVI 是路由器内的虚拟接口，其作用类似于普通路由接口。它不支持网桥，但表示路由器内路由接口的可比较网桥组。传入或传出这些桥接接口的所有数据包都会通过 BVI 接口。BVI 的接口编号是虚拟接口所代表的网桥组的编号。

在以下示例中，在 VRG 中配置了 BVI-G，而网桥组 1 是接口 G0/1 和 G0/2 的路由接口。同样，在 VRB 中配置了 BVI-B，网桥组 2 是接口 G0/3 和 G0/4 的路由接口。假设两个 BVI 具有相同的 IP 子网地址，例如 10.10.10.5/24。由于虚拟路由器，网络会在共享资源上被隔离。



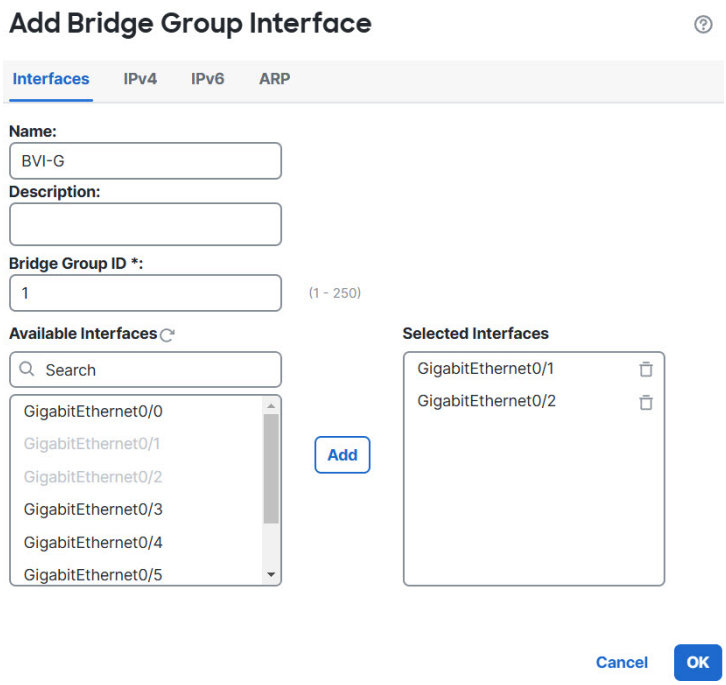
过程

步骤 1 选择设备 > 设备管理。编辑所需的设备。

步骤 2 在接口 (Interfaces) 中，选择添加接口 (Add Interfaces) > 网桥组接口 (Bridge Group Interface)。

a) 为 BVI-G 输入下列详细信息：

- 名称 (Name) - 在此示例中，为 BVI-G。
- 网桥组 ID (Bridge Group ID) - 在本例中为 1。
- 可用接口 (Available Interface) - 选择接口。
- 在 IPV4 中，对于 IP 类型，请选择使用静态 IP。
- IP 地址 (IP Address) - 输入 10.30.0.1/24。



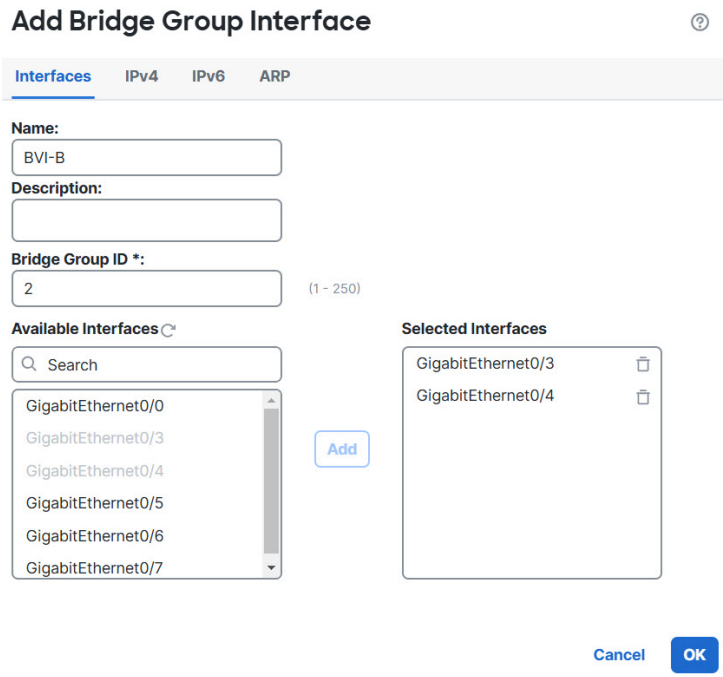
b) 点击确定 (OK)。

c) 点击保存 (Save)。

a) 为 BVI-B 输入下列详细信息：

- 名称 (Name) - 在此示例中，为 BVI-B。
- 网桥组 ID (Bridge Group ID) - 在本例中为 2。
- 可用接口 (Available Interface) - 选择子接口。
- 在 IPV4 中，对于 IP 类型，请选择使用静态 IP。

- **IP 地址 (IP Address)** - 将此字段留空，因为系统不允许两个接口具有重叠的 IP 地址。您可以重新访问网桥组并在虚拟路由器下对齐后提供相同的 IP 地址。



b) 点击**确定 (OK)**。

c) 点击**保存 (Save)**。

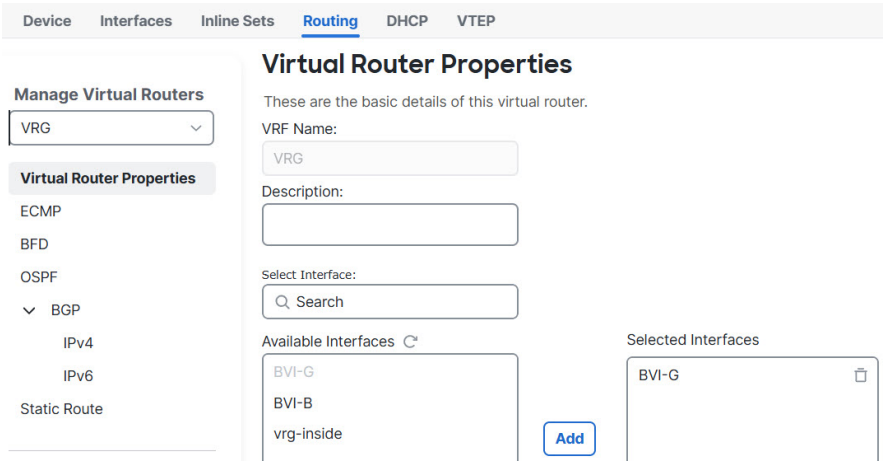
步骤 3 创建虚拟路由器，例如 VRG，然后选择 BVI-G 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-G**，然后点击**添加 (Add)**。



e) 点击**保存**。

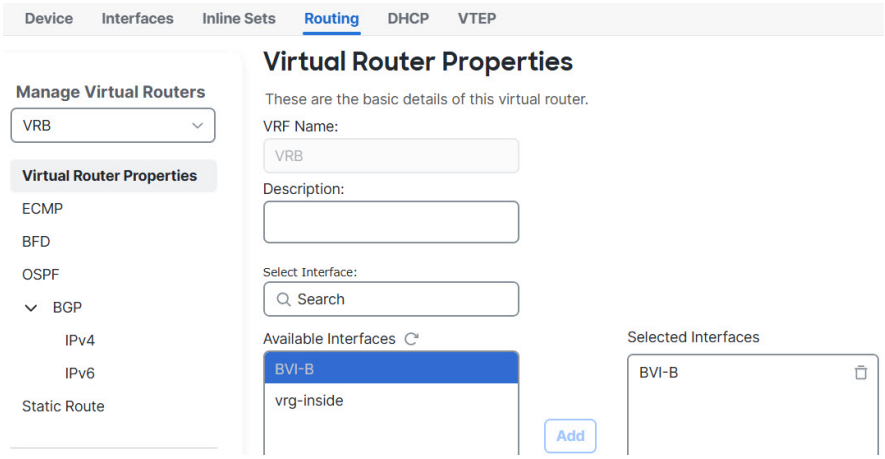
步骤 4 创建虚拟路由器，例如 VRB，然后选择 BVI-B 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-B**，然后点击**添加 (Add)**。



e) 点击**保存**。

步骤 5 重新访问 BVI-B 配置：

a) 选择 **设备** > **设备管理**，编辑设备，然后点击**接口**。

b) 点击 BVI-B 接口的**编辑 (Edit)**。将 IP 地址指定为 10.10.10.5/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 BVI-G 的同一 IP 地址进行配置。

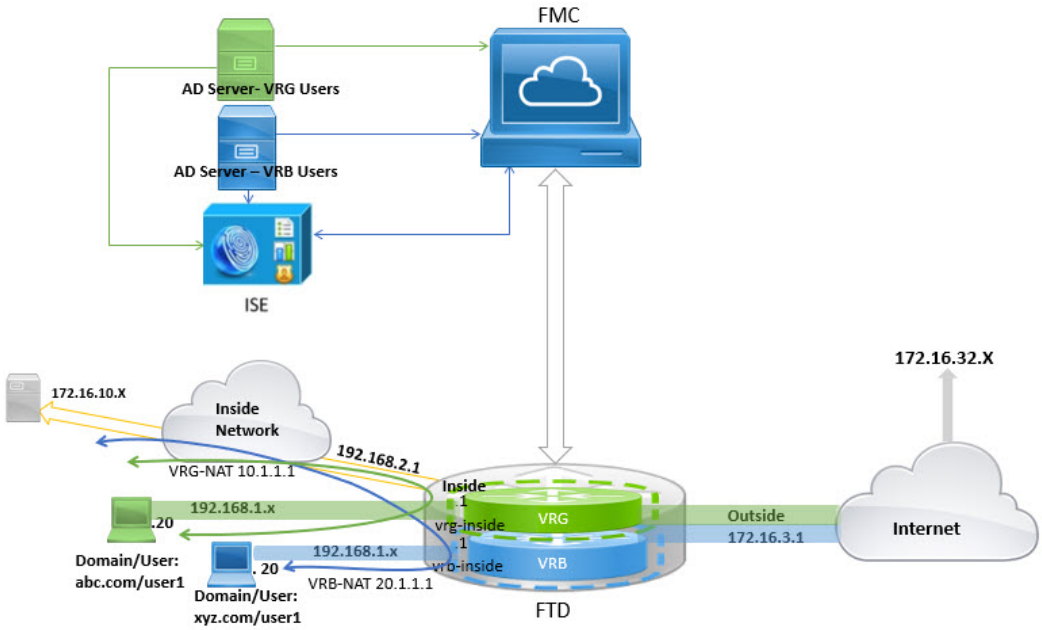
c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

如果要启用 BVI 间通信，请使用外部路由器作为默认网关。在重叠的 BVI 场景中，如本例所示，使用两次 NAT 外部路由器作为网关来建立 BVI 间流量。为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。

如何使用重叠网络来配置用户身份验证

在虚拟路由中，您可以配置多个具有重叠 IP 和重叠用户的虚拟路由器。在本例中，VRG 和 VRB 是具有重叠 IP - 192.168.1.1/24 的虚拟路由器。两个不同域上的用户也同样位于重叠的网络 IP 192.168.1.20 上。为了让 VRG 和 VRB 用户访问共享服务器 172.16.10.X，可将路由泄漏到全局虚拟路由器。使用源 NAT 来处理重叠 IP。为了控制 VRG 和 VRB 用户的访问，必须在 防火墙管理中心中设置用户认证。防火墙管理中心 会使用领域、Active Directory、身份源以及身份规则和策略来验证用户身份。由于 Firewall Threat Defense 在用户身份验证方面并不发挥直接作用，因此仅通过访问控制策略管理用户访问。要控制来自重叠用户的流量，请使用身份策略和规则来创建访问控制策略。



开始之前

此示例假定您已：

- VRG 和 VRB 用户的两台 AD 服务器。
- 添加了包含两台 AD 服务器的 ISE。

过程

步骤 1 为 VRG 配置设备的内部接口：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击**接口**。

b) 编辑您要分配给 VRG 的接口：

- **名称 (Name)** - 在此示例中为 VRG-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 2 为 VRB 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

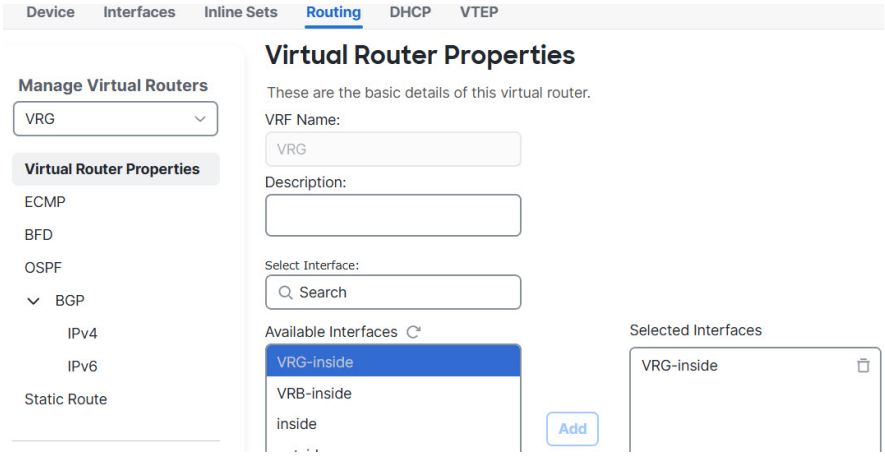
b) 编辑您要分配给 VRB 的接口：

- **名称 (Name)** - 在此示例中为 VRB-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定 (OK)**。
d) 点击**保存 (Save)**。

步骤 3 将 VRG 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRG 用户访问通用服务器 172.16.10.1：

a) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并且编辑 Firewall Threat Defense 设备。
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRG。
c) 对于 VRG，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRG-inside 并保存。



d) 点击**静态路由 (Static Route)**。
e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

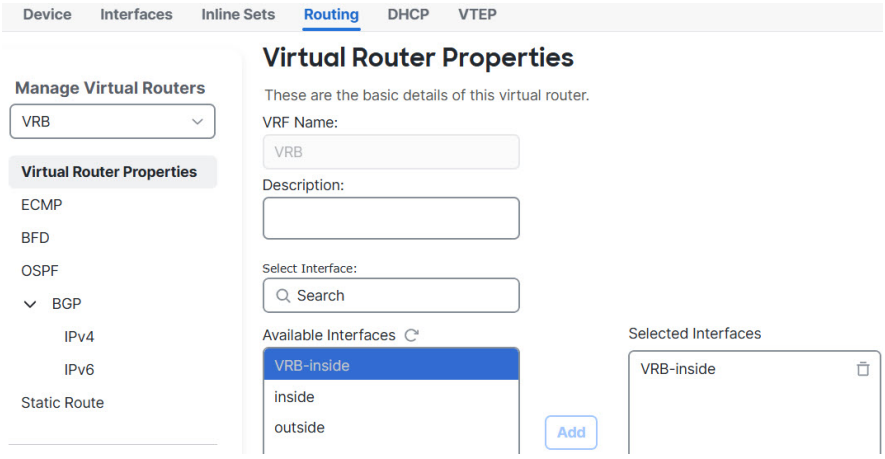
- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定 (OK)**。
g) 点击**保存 (Save)**。

步骤 4 将 VRB 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRB 用户访问共享服务器 172.16.10.x：

a) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并且编辑 Firewall Threat Defense 设备。
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRB。

c) 对于 VRB，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRB-inside 并保存。



d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定 (OK)**。

g) 点击**保存 (Save)**。

步骤 5 重新访问 VRB-inside 接口配置：

a) 选择 **设备** > **设备管理**，点击设备名称，然后点击**接口**。

b) 点击 VRB-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 VRG-inside 的相同 IP 地址进行配置。

c) 点击**确定 (OK)**。

d) 点击**保存 (Save)**。

步骤 6 为源对象 VRG 和 VRB 添加 NAT 规则。请点击 **策略** > **网络策略** > **NAT** 。

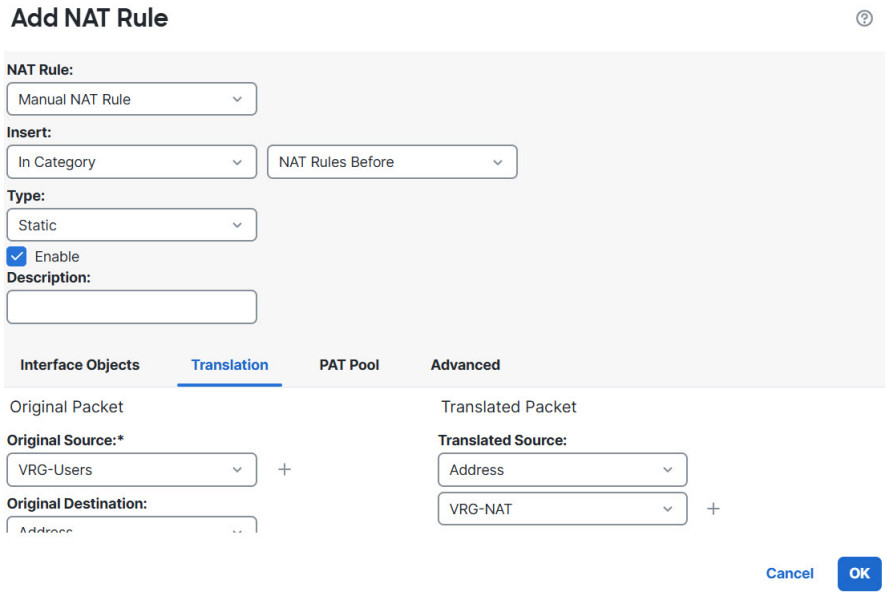
步骤 7 点击**新策略 (New Policy)**。

步骤 8 输入 NAT 策略名称，然后选择 Firewall Threat Defense 设备。点击**保存**。

步骤 9 在 NAT 页面中，点击**添加规则**并为 VRG 定义以下源 NAT：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象**中，选择 VRG-Inside 对象，然后点击**添加到源**（如果对象不可用，请在 **对象** > **接口** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标**。

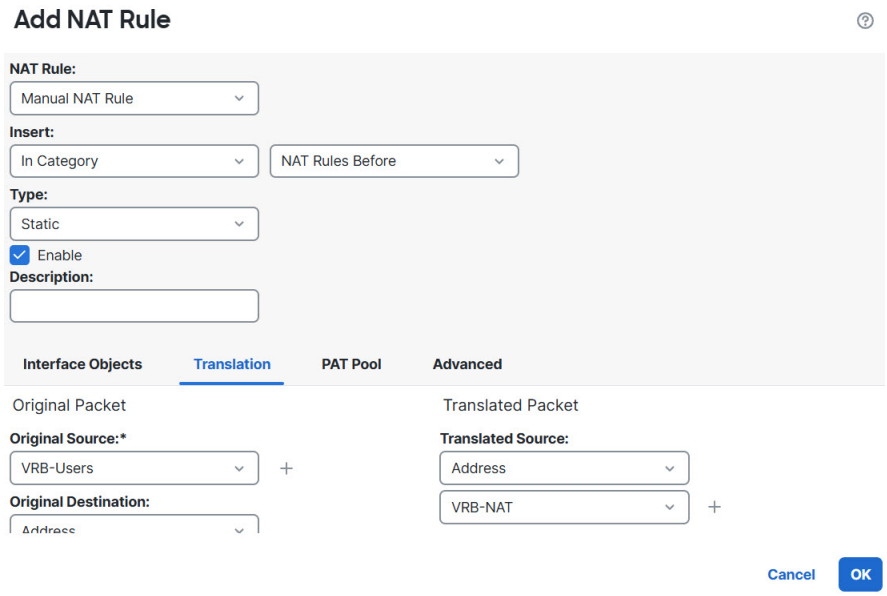
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRG-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 10.1.1.1 来定义对象 VRG-NAT。选择 VRG-NAT，如下图所示：



步骤 10 点击**确定**。

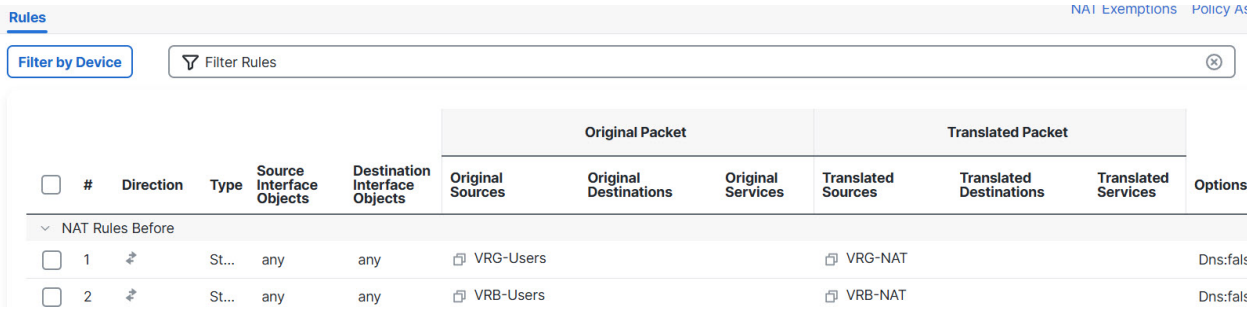
步骤 11 在 NAT 页面中，点击**添加规则**并为 VRB 定义以下源 NAT：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象**中，选择 VRB-Inside 对象，然后点击**添加到源**（如果对象不可用，请在 **对象** > **接口** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRB-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 20.1.1.1 来定义对象 VRB-NAT。选择 VRB-NAT，如下图所示：



步骤 12 点击**保存**。

NAT 规则如下所示：



步骤 13 在 防火墙管理中心 中为每个 VRG 和 VRB 用户添加两个唯一的 AD 服务器 - 选择**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**。

步骤 14 点击**新建领域**并填写字段。有关这些字段的详细信息，请参阅领域字段 ， 第 2029 页。

步骤 15 要控制来自 VRG 和 VRB 用户的访问，请定义 2 个 Active Directory，请参阅领域目录和同步字段 ， 第 2032 页请参阅创建 LDAP 领域或 Active Directory 领域和领域目录 ， 第 2019 页

步骤 16 在 防火墙管理中心 中添加 ISE - 选择**系统 (System)** > **集成 (Integration)** > **身份源 (Identity Sources)**。

步骤 17 点击**身份服务引擎 (Identity Services Engine)** 并填写字段。有关这些字段的详细信息，请参阅如何为无领域的用户控制配置 ISE/ISE-PIC ， 第 2085 页。

步骤 18 创建身份策略和规则，然后定义访问控制策略，以便控制来自 VRG 和 VRB 的重叠用户的访问。

如何使用 BGP 来互连虚拟路由器

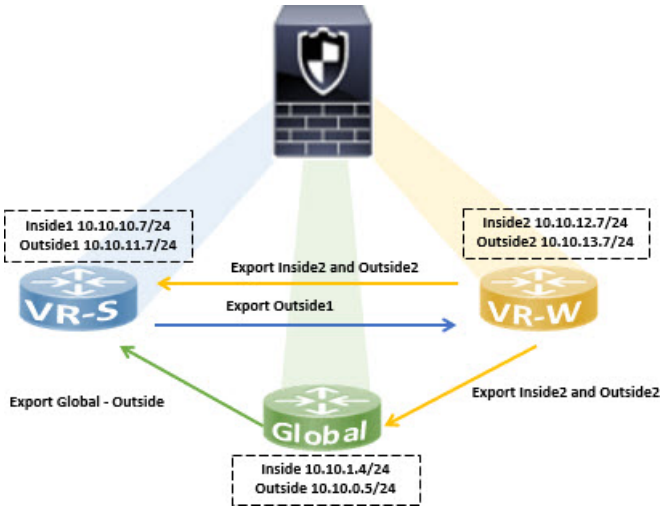
现在，您可以在设备上配置BGP设置，以便在虚拟路由器（全局和用户定义的虚拟路由器）之间泄漏路由。源虚拟路由器的路由目标会被导出到BGP表，而该表又会被导入到目的虚拟路由器。路由地图用于与用户定义的虚拟路由器共享全局虚拟路由，反之亦然。请注意，所有路由到BGP表的导入或导出都在用户定义的虚拟路由器上配置，包括全局虚拟路由。

假设工厂的防火墙设备配置了以下虚拟路由器和接口：

- 全局虚拟路由器配置了内部 (10.10.1.4/24) 和外部 (10.10.0.5/24)
- VR-S（销售）虚拟路由器配置了 Inside1 (10.10.10.7/24) 和 outside1 (10.10.11.7/24)
- VR-W（仓库）虚拟路由器配置了 Inside2 (10.10.12.7/24) 和 outside2 (10.10.13.7/24)

假设您想把仓库 (VR-W) 的路由泄漏给销售 (VR-S) 和全局，并将 VR-S 的外部接口路由到 VR-W。同样，您想把全局路由器的外部接口路由泄漏给销售 (VR-S)。此示例演示了实现路由器互连的BGP配置程序：

图 *393:* 使用 *BGP* 设置来互连虚拟路由器



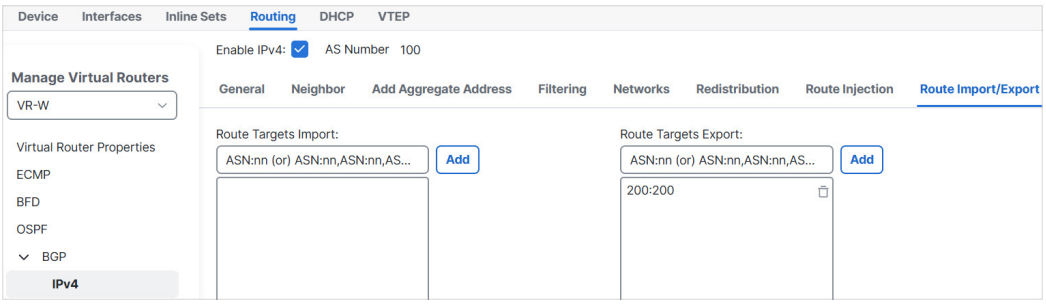
开始之前

- 创建虚拟路由器 (Create the virtual routers) - VR-S 和 VR-W。
- 启用 BGP，并为每个虚拟路由器选择配置 BGP 以重新分发连接的路由 (Configure BGP for redistribution of connected routes)。

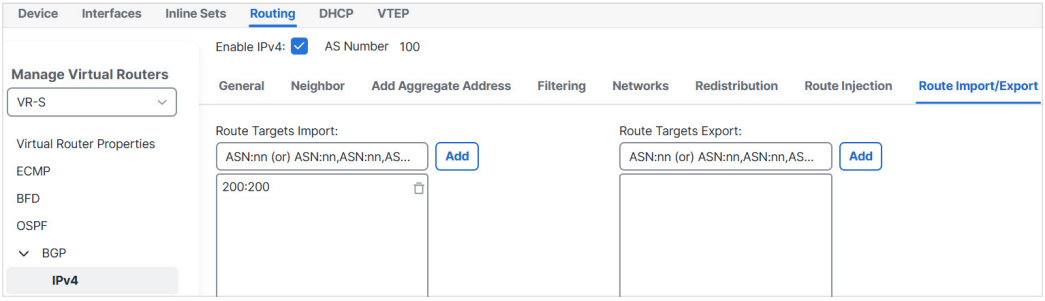
过程

步骤 1 配置 VR-W 以将其带有路由目标的路由导出至 VR-S：

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，编辑设备，然后点击**路由 (Routing)** 选项卡。
b) 在虚拟路由器下拉列表中选择 VR-W。
c) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。
d) 要将 VR-W 路由泄漏到 VR-S，请使用路由目标标记路由，以便将 VR-W 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *200:200*。点击**添加 (Add)**：



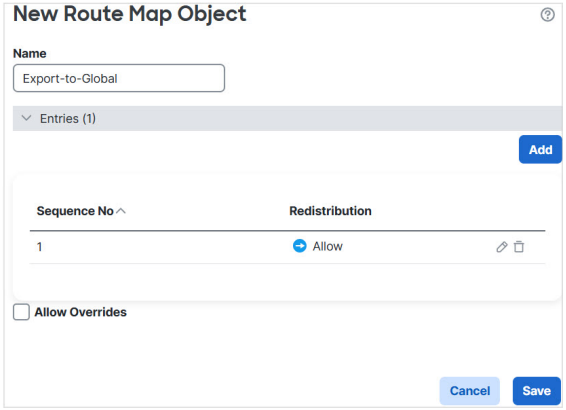
e) 从虚拟路由器下拉列表中选择 VR-S。
f) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。
g) 要从 VR-W 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-W 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入您为 VR-W 配置的相同路由目标值 *200:200*。点击**添加 (Add)**。



注释
如果要对从 VR-W 泄漏的路由进行条件化，可以在路由映射对象中指定匹配条件，并在**用户虚拟路由器导出路由地图 (User Virtual Router Export Route Map)** 中选择该匹配条件。同样，如果想对要从 BGP 表导入 VR-S 的路由进行条件化，您可以使用**用户虚拟路由器导入路由映射 (User Virtual Router Import Route Map)**。此程序在步骤 3 中进行了介绍。

步骤 2 配置 VR-W 以便将其路由导出到全局虚拟路由器：

a) 您需要创建一个允许将 VR-W 路由导出到全局路由表的路由地图。选择**对象** > **路由地图**。
b) 点击**添加路由地图 (Add Route Map)**，为其命名（如 *Export-to-Global*），然后点击**添加 (Add)**。
c) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)：

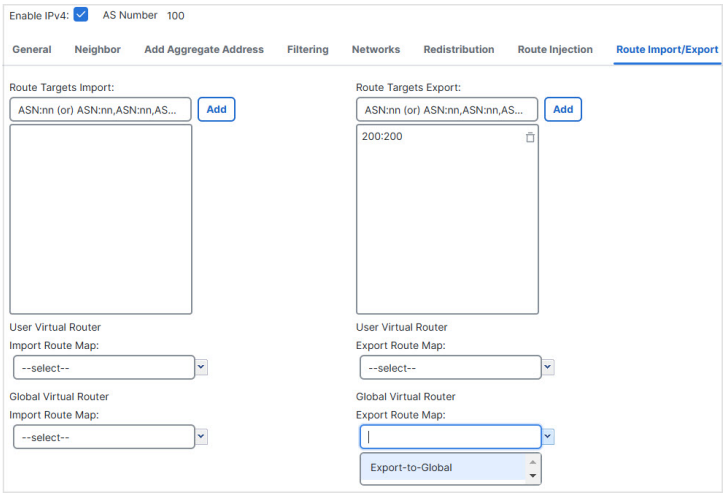


d) 点击**保存**。

在本例中，所有 VR-W 路由都会被泄漏到全局路由表。因此，没有为路由映射配置匹配条件。

e) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

f) 从**全局虚拟路由器导出路由地图 (Global Virtual Router Export Route Map)** 下拉列表中，选择 Export-to-Global：



步骤 3 要仅将 VR-S 的外部 1 路由泄漏到 VR-W，请执行以下操作：

a) 从虚拟路由器下拉列表中选择 VR-S。

b) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

c) 要将 VR-S 路由泄漏到 VR-W，请使用路由目标标记路由，以便将 VR-S 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *100:100*。点击**添加 (Add)**。

d) 从虚拟路由器下拉列表中，选择 VR-W，然后选择 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

e) 要从 VR-S 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-S 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入 VR-S 路由目标值 *100:100*。点击**添加 (Add)**。

f) 现在，您需要将 VR-S 的外部 1 路由限制为泄漏到 VR-W。选择**对象** > **前缀列表** > **IPv4 前缀列表** 。

g) 点击**添加 IPv4 前缀列表 (Add IPv4 Prefix List)**，提供名称（如 *VRS-Outside1-Only*），然后点击**添加 (Add)**。

h) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

i) 输入 VR-S outside1 接口的 IP 地址（前两个八位组）。

j) 点击**保存**。

k) 使用带前缀列表的 match 子句来创建路由地图。点击**路由地图 (Route Map)**。点击**添加路由映射 (Add Route Map)**，指定名称（如 *Import-from-VRS*），然后点击**添加 (Add)**。

l) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

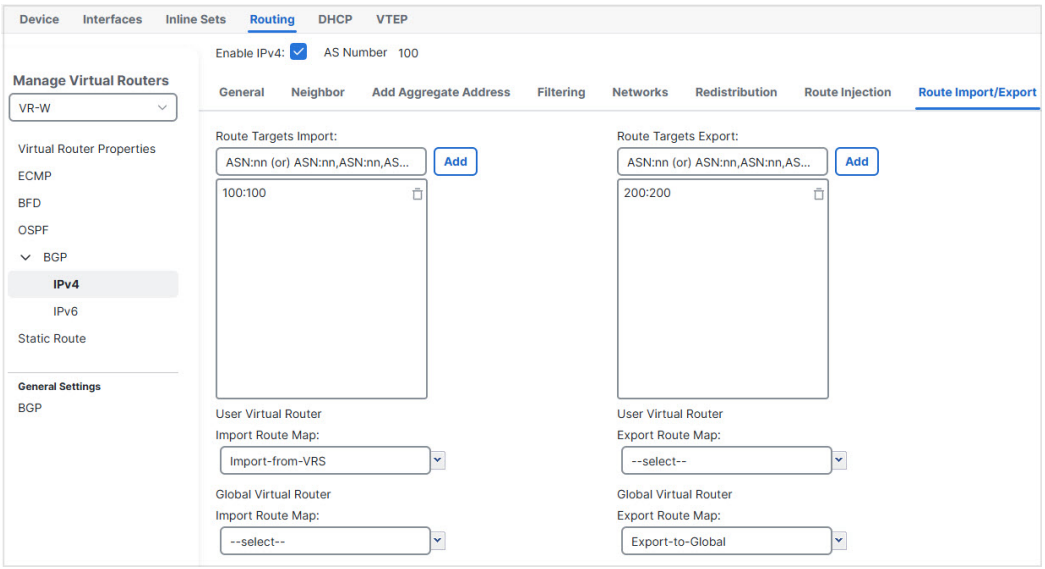
m) 在**匹配子句 (Match Clause)** 选项卡中，点击 **IPv4**。在**地址 (Address)** 选项卡下，点击**前缀列表 (Prefix List)**。

n) 在**可用 IPv4 前缀列表 (Available IPv4 Prefix List)** 下，选择 VRS-Outside1-Only，然后点击**添加 (Add)**。

o) 点击**保存**。

p) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

q) 从**全局虚拟路由器导入路由地图 (Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-VRS：



步骤 4 配置 VR-S 以便导入全局虚拟路由器的外部路由：

注释

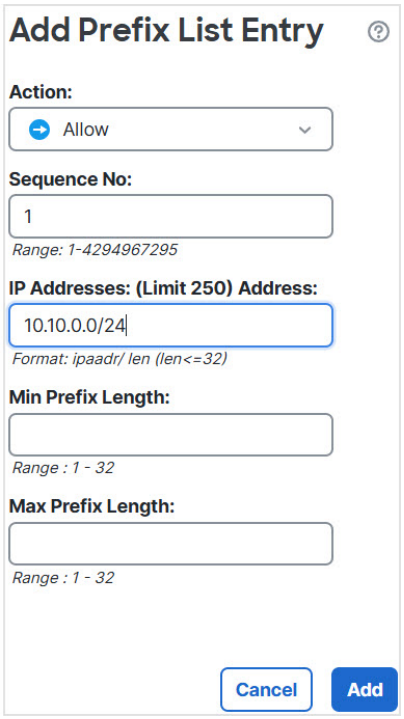
要从全局虚拟路由器泄漏路由，您必须分别配置源或目标用户定义的虚拟路由器。因此，在本例中，VR-S 是从全局虚拟路由器的外部接口导入路由的目的路由器。

a) 选择**对象** > **前缀列表** > **IPv4 前缀列表** 。

b) 点击**添加 IPv4 前缀列表 (Add IPv4 Prefix List)**，提供名称（如 *Global-Outside-Only*），然后点击**添加 (Add)**。

c) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

d) 输入 Global Outside 接口的 IP 地址（前两个八位组）：



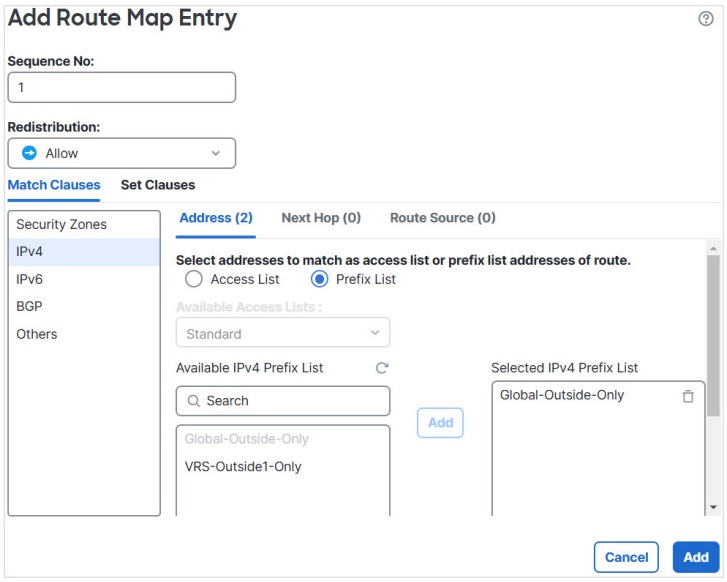
e) 点击**保存**。

f) 点击**路由地图 (Route Map)**。点击**添加路由映射 (Add Route Map)**，指定名称（如 *Import-from-Global*），然后点击**添加 (Add)**。

g) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

h) 在**匹配子句 (Match Clause)** 选项卡中，点击 **IPv4**。在**地址 (Address)** 选项卡下，点击**前缀列表 (Prefix List)**。

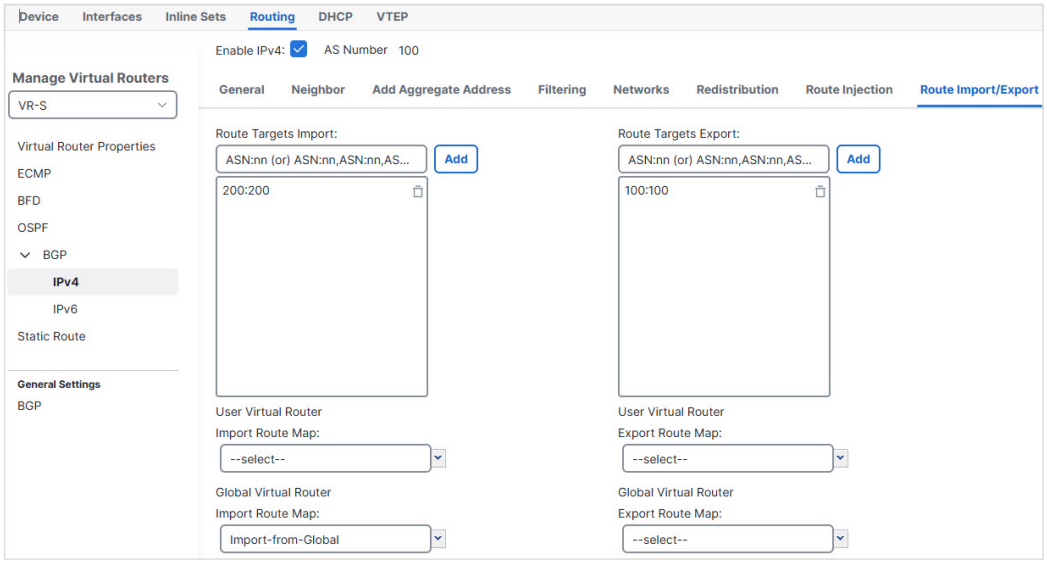
i) 在**可用 IPv4 前缀列表 (Available IPv4 Prefix List)** 下，选择 Global-Outside-Only，然后点击**添加 (Add)**。



j) 点击保存。

k) 导航到设备的路由 **(Routing)** 选项卡，然后选择 VR-S。点击 **BGP** > **IPv4** > 路由导入/导出 **(Route Import/Export)**。

l) 从全局虚拟路由器导入路由地图 **(Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-Global：

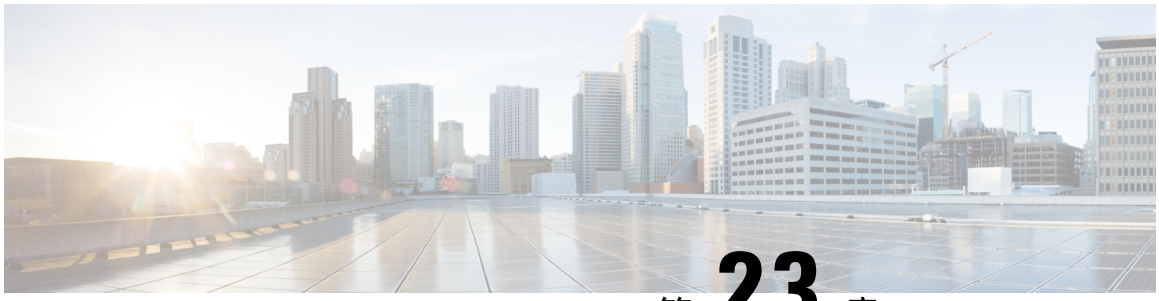


步骤 **5** 保存和部署。

虚拟路由器的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
用户定义的 VRF 接口上支持 AAA。	7.6	7.6	用户定义的虚拟路由和转发 (VRF) 接口现在支持设备身份验证、授权和记账 (AAA)。默认使用管理接口。 在设备平台设置中，现在可以将具有 VRF 接口的安全区域或接口组与已配置的外部身份验证服务器关联起来。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **外部身份验证 (External Authentication)**
具有动态 VTI 的虚拟路由。	7.4	7.4	现在，您可以为基于路由的站点间 VPN 配置具有动态 VTI 的虚拟路由器。 新增/修改的屏幕：**设备** > **设备管理** > **编辑设备** > **路由** > **虚拟路由器属性** > **可用接口下的动态 VTI 接口** 平台限制：仅支持本机模式独立设备或高可用性设备。不支持容器实例或集群设备。
对 ISA 3000 的虚拟路由器支持。	7.0	7.0	您可以在 ISA 3000 上最多配置 10 个虚拟路由器。
在用户定义的虚拟路由器上的 SNMP 支持	7.0	7.0	在用户定义的虚拟路由器上配置 SNMP。
批量删除虚拟路由器。	6.7	6.6	您可以从威胁防御一次删除多个虚拟路由器。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
用于威胁防御的虚拟路由器和 VRF-Lite。	6.6	6.6	现在可以创建多个虚拟路由器来为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。虚拟路由器将实施虚拟路由和转发功能的“轻型”版本（或VRF Lite），它不支持 BGP 的多协议扩展 (MBGP)。可以创建的最大虚拟路由器数量为 5-100，并取决于设备型号。 新增/修改的屏幕：**设备** > **设备管理** 编辑设备**路由**选项卡 新增/修改的CLI 命令： 。 • **show vrf** • 向以下 CLI 命令添加了 ［**vrf** *name* ｜ **all**］关键字集，并且在适用的情况下更改了指示虚拟路由器信息的输出：**clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters**。 平台限制：不支持 Firepower 1010 或 ISA 3000。



第 23 章

ECMP

本章介绍配置等价多路径 (ECMP) 路由的程序，该路由协议用于网络流量负载均衡。

- ECMP 路由方法， 第 1159 页
- ECMP 的准则和限制， 第 1160 页
- 管理虚拟路由器的 ECMP 区域， 第 1161 页
- 创建 ECMP 区域， 第 1161 页
- 配置等价静态路由， 第 1162 页
- 修改 ECMP 区域， 第 1163 页
- 删除 ECMP 区域， 第 1164 页
- 配置 ECMP， 第 1165 页
- Cisco Secure Firewall Threat Defense 中按时间顺序排列的 ECMP 发展历史记录， 第 1168 页

ECMP 路由方法

ECMP 是一种路由方法

- 支持在多个等价路径之间分配流量，
- 每个区域内最多支持 8 个接口上的 8 条等价静态或动态路由，并且
- 每个虚拟路由器使用流量区域来包含一组接口。

多个默认路由配置

此示例显示了在区域中的三个接口上配置的多条默认路由：

```
0.0.0.0 0.0.0.0 通过 outside1 到 10.1.1.2 的路由
0.0.0.0 0.0.0.0 通过 outside2 到 10.2.1.2 的路由
0.0.0.0 0.0.0.0 通过 outside3 到 10.3.1.2 的路由
```

ECMP 的准则和限制

遵循以下原则可有效配置 ECMP 区域：

防火墙模式限制

仅在路由防火墙模式下使用 ECMP 区域。

接口限制

请勿将 dVTI 或环回接口与 ECMP 区域一起使用。

ECMP 区域配置限制

配置 ECMP 区域时，请遵循以下限制：

- 设备最多可以有 256 个 ECMP 区域。
- 每个 ECMP 区域只能关联 8 个接口。
- 接口只能是一个 ECMP 区域的成员。

接口管理限制

请勿移除接口或删除正用于路由的区域：

- 不能从 ECMP 区域中删除与等价静态路由相关联的接口。
- 如果 ECMP 区域的接口具有与其关联的等价静态路由，则您无法删除该区域。

支持的接口类型

仅将路由接口用于 ECMP 区域。请勿将这些接口类型与 ECMP 区域关联：

- BVI 接口。
- EtherChannel 中的成员接口。
- 故障转移或状态链路接口。
- 管理专用接口或管理访问接口。
- 集群控制链路接口。
- VNI。
- VLAN 接口。
- 已启用 SSL 的远程接入 VPN 配置中的接口。

功能兼容性限制

使用 ECMP 区域时，请考虑以下功能限制：

- ECMP 区域中的接口不支持 DHCP 中继。
- 双 ISP/WAN Firewall Threat Defense 部署 — 为主数据接口和辅助数据接口创建单个 ECMP 区域，从而实现具有相同度量值的静态路由。
- Firewall Threat Defense 不支持在 IPsec 会话中使用 NAT 的 ECMP - 标准 IPsec 虚拟专用网络 (VPN) 隧道不适用于 IPsec 数据包传送路径中的 NAT 点。

管理虚拟路由器的 ECMP 区域

ECMP 页面提供管理与虚拟路由器链接的现有 ECMP 区域的功能。当您点击路由窗格中的 **ECMP** 时，ECMP 页面会显示虚拟路由器的当前 ECMP 区域，包括关联的接口。在此页面上，您可以向虚拟路由器添加新的 ECMP 区域。您还可以 **编辑** (✎) 和 **删除** (🗑) ECMP。

您可以执行以下操作：

- 创建 ECMP 区域，第 1161 页
- 配置等价静态路由，第 1162 页
- 修改 ECMP 区域，第 1163 页
- 删除 ECMP 区域，第 1164 页

创建 ECMP 区域

创建 ECMP 区域，以在虚拟路由器配置中跨多条等价路径启用负载均衡。

ECMP 区域会按虚拟路由器来创建。只有创建 ECMP 的虚拟路由器所属的接口才能与该 ECMP 关联。

过程

步骤 1 导航至 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 在虚拟路由器下拉列表中，选择要在其中创建 ECMP 区域的虚拟路由器。

您可以在全局虚拟路由器和用户定义的虚拟路由器中创建 ECMP 区域。有关创建虚拟路由器的信息，请参阅创建虚拟路由器，第 1114 页。

步骤 4 点击 **ECMP**。

步骤 5 点击**添加 (Add)**。

步骤 6 在**添加 ECMP (Add ECMP)** 框中，输入 ECMP 区域的名称。

注释

路由设备的 ECMP 名称必须是唯一的。

步骤 7 在**可用接口**框中，选择接口，然后点击**添加**。

- 只有属于您要创建 ECMP 的虚拟路由器的接口才能与它关联。接口必须具有逻辑名称才会显示；请编辑接口并保存以设置逻辑名称。
- 从版本 10.0 开始，SD-WAN VPN 拓扑中中心设备的动态 VTI (DVTI) 支持 ECMP。在 DVTI 上启用时，它会自动添加到系统生成的 ECMP 区域，因此 DVTI 不会显示在 **可用接口**下。

步骤 8 点击**确定**。

ECMP 页面现在会显示新创建的 ECMP 区域。

步骤 9 点击**保存 (Save)** 和**部署 (Deploy)** 以部署配置。

通过定义相同的目标网络和度量值但使用不同的网关，您可以将 ECMP 区域接口与等价静态路由相关联。

下一步做什么

- 配置等价静态路由，第 1162 页
- 修改 ECMP 区域，第 1163 页
- 删除 ECMP 区域，第 1164 页

配置等价静态路由

配置等价静态路由，以便在 ECMP 区域内多个具有相同目标网络和度量值的接口之间启用负载均衡。

智能许可证	经典许可证	支持的设备	支持的域	访问权限
任意	不适用	Firewall Threat Defense和Firewall Threat Defense Virtual	任意	管理员/网络管理员/安全审批人

您可以将虚拟路由器的接口（全局和用户定义）分配给设备的 ECMP 区域。

Before you begin

- 要为接口配置等价静态路由，请确保将其与ECMP区域关联。请参阅创建ECMP区域，第1161页。
- 非 VRF 设备的所有路由配置设置也可用于全局虚拟路由器。
- 如果没有将接口与 ECMP 区域关联，则无法为具有相同目标和指标的接口定义静态路由。

过程

步骤 1 从页面 **设备** > **设备管理** 中，编辑 Firewall Threat Defense 设备。 点击**路由 (Routing)**选项卡。

步骤 2 从下拉列表中，选择其接口与 ECMP 区域相关联的虚拟路由器。

步骤 3 要为接口配置等价静态路由，请点击**静态路由 (Static Route)**。

步骤 4 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑** (✎)。

步骤 5 从**接口 (Interface)** 下拉列表中，选择属于虚拟路由器的接口和 ECMP 区域。

步骤 6 从**可用网络 (Available Networks)** 框中选择目标网络，然后点击**添加 (Add)**。

步骤 7 输入网络的网关。

步骤 8 输入指标值。它可以是介于 1 和 254 之间的数字。

步骤 9 要保存设置，点击**保存 (Save)**。

步骤 10 要配置等价静态路由，请重复这些步骤，为同一 ECMP 区域中具有相同目的网络和指标值的另一个接口配置静态路由。请记住提供其他网关。

已为与 ECMP 区域关联的接口配置了等价静态路由，从而在多条路径之间启用了负载均衡。

下一步做什么

- 修改 ECMP 区域，第 1163 页
- 删除 ECMP 区域，第 1164 页

修改 ECMP 区域

当您需要更改设备上的现有 ECMP 区域配置时，请使用此过程。

按照以下步骤修改 ECMP 区域：

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击 **ECMP**。

系统将显示 ECMP 区域及其关联接口。

步骤 4 要修改 ECMP 区域，请点击所需 ECMP 区域旁边的 **编辑** (✎)。在**编辑 ECMP (Edit ECMP)** 框中，您可以执行以下操作：

- ECMP 名称 — 确保您的更改是唯一的。

- 接口 — 您可以添加或删除接口。

  注释
  一个接口不得属于多个 ECMP 区域，也不应链接到等价静态路由。

步骤 5 点击**确定**。

步骤 6 点击**保存**保存所做的更改。

ECMP 区域将反映您的更新设置。

下一步做什么

- 配置等价静态路由，第 1162 页
- 删除 ECMP 区域，第 1164 页

删除 ECMP 区域

用于等价多路径路由的 ECMP 区域组接口。在重新配置网络拓扑或不再需要该区域时，您可能需要删除 ECMP 区域。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击 **ECMP**。

系统将显示 ECMP 区域及其关联的接口。

步骤 4 要删除 ECMP 区域，请点击该区域旁的 **删除** ()。

注释
若 ECMP 区域有关联等价静态路由的接口，则无法删除该区域。

步骤 5 在确认邮件中点击**删除 (Delete)**。

步骤 6 点击**保存**以应用更改。

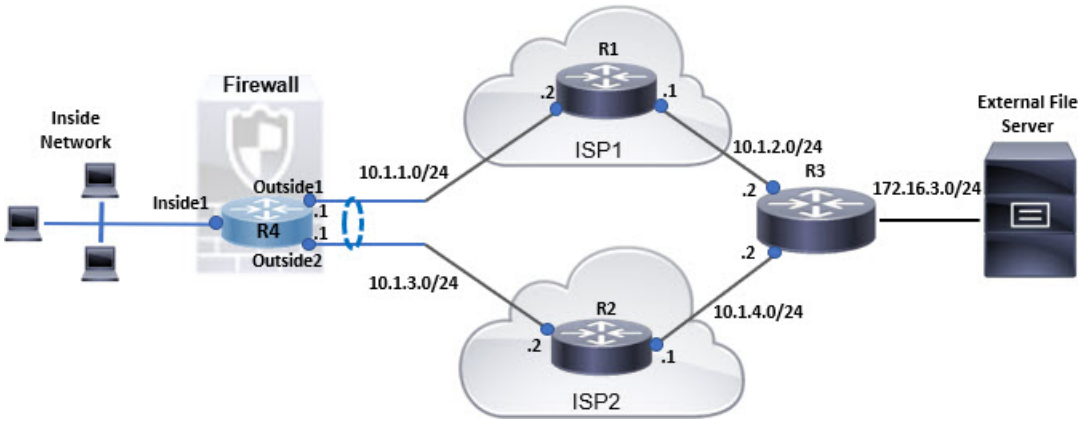
ECMP 区域将从设备配置中移除，并不再可用于路由操作。

配置 ECMP

配置ECMP，可通过设备实现高效的流量处理，支持不对称路由、负载均衡和无缝处理丢失的流量。

此示例演示了如何使用 防火墙管理中心 在 Firewall Threat Defense 上配置 ECMP 区域，以便有效地处理流经设备的流量。如果配置了 ECMP，Firewall Threat Defense 可逐个区域维护路由表，从而实现高效的数据包重新路由。因此，ECMP 支持非对称路由、负载均衡和无缝处理丢失的流量。在本例中，R4 会记录到达外部文件服务器的两个路径。

图 *394: ECMP* 的配置示例



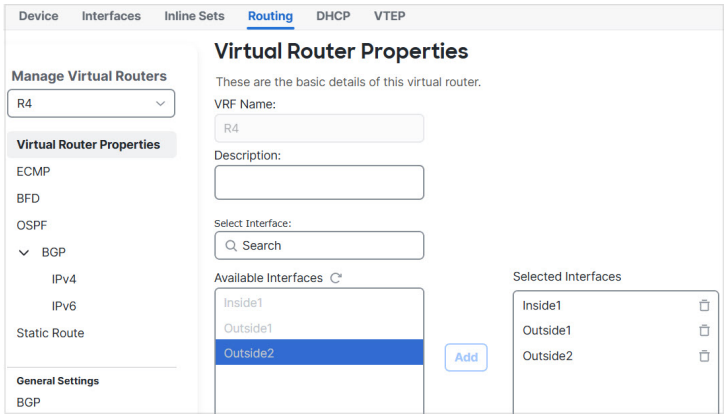
按照以下步骤在设备上配置 ECMP：

过程

步骤 1 创建虚拟路由器。

在 *R4* 上使用以下接口设定新路由器：*Inside1*、*Outside1* 和 *Outside2*。有关详细信息，请参阅创建虚拟路由器。

图 *395:* 配置 *R4* 虚拟路由器



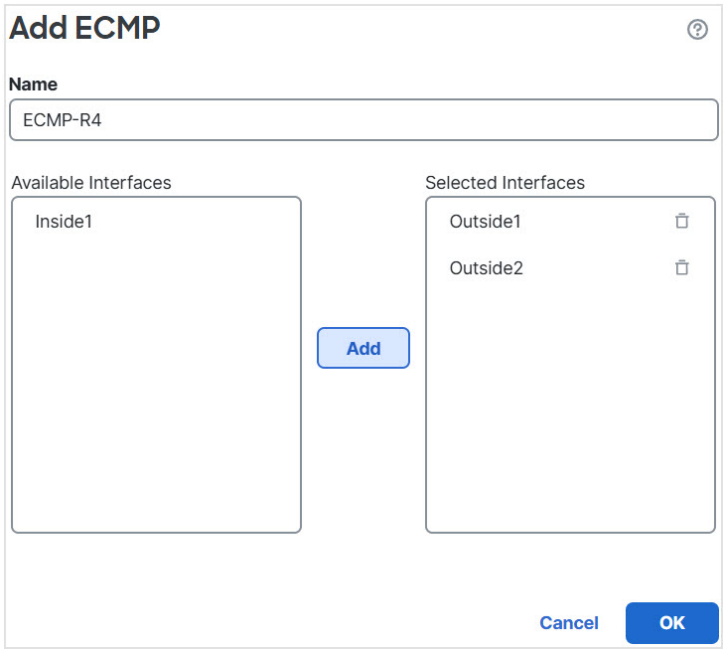
步骤 2 创建 ECMP 区域：

a) 在**路由 (Routing)** 选项卡中，选择 R4 用户定义的虚拟路由器，然后点击 **ECMP**。

b) 点击**添加 (Add)**。

c) 输入 ECMP 名称，然后从**可用接口 (Available Interfaces)** 列表中选择 *Outside1* 和 *Outside2*：

图 ***396:*** 创建 ***ECMP*** 区域



d) 点击**确定**，然后点击**保存**。

步骤 3 为区域接口创建静态路由：

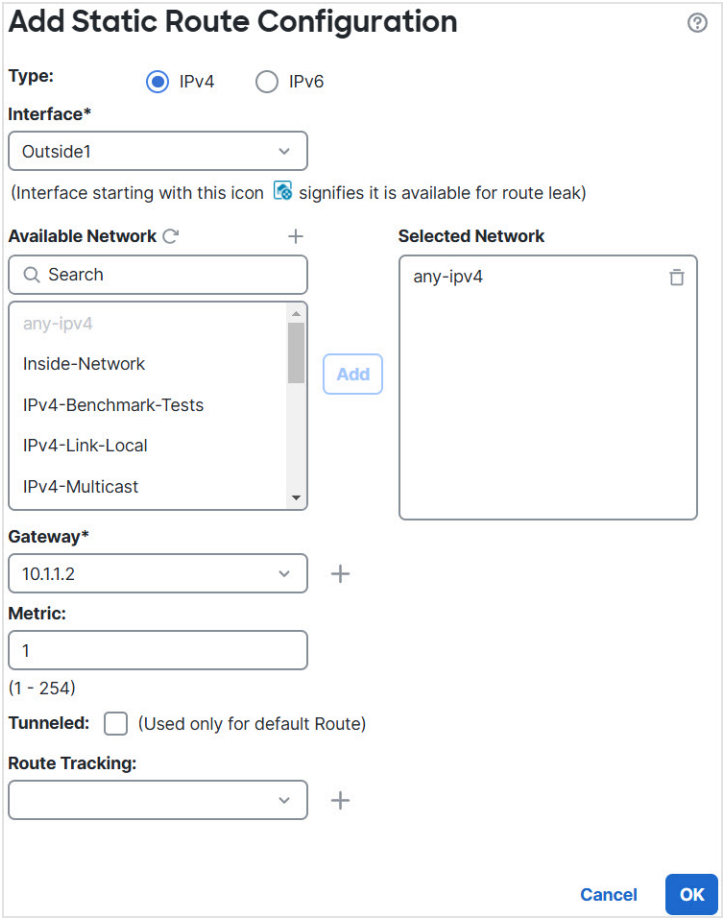
a) 在**路由 (Routing)** 选项卡中，点击**静态路由 (Static Route)**。

b) 在**接口 (Interface)** 下拉列表中，选择 Outside1。

c) 在**可用网络 (Available Network)** 下，选择 any-ipv4，然后点击**添加 (Add)**。

d) 在**网关**字段中指定下一跳地址：10.1.1.2。

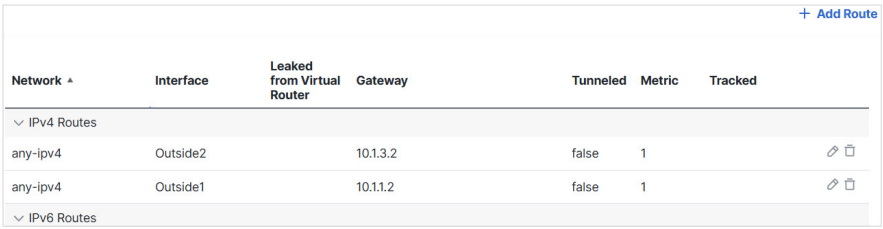
图 *397:* 为 *Outside1* 配置静态路由



e) 重复步骤 3b 到步骤 3d，为 Outside2 配置静态路由。

确保为静态路由指定相同的度量值但不同的网关：

图 *398:* 已配置的 *ECMP* 区域接口静态路由



步骤 4 保存配置并继续将其部署到网络上。

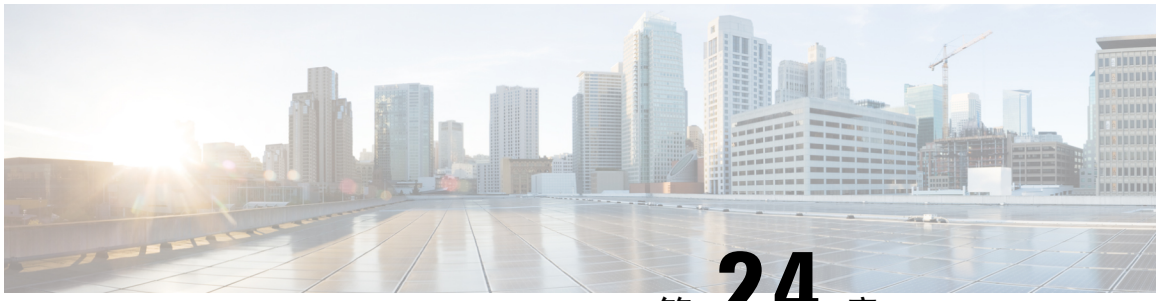
现在，网络数据包将遵循 ECMP 算法配置，利用高效的路由通过 R4>R1>R3 或 R4>R2>R3 到达其目标 R3。如果 R1>R3 路由不可用，流量将流经 R2，而不丢弃任何数据包。此外，虽然数据包是从

outside1 发送的，但来自 R3 的响应可被 *outside2* 接收。当网络流量很大时，R4 会在两个指定的路由之间分配网络负载，以保持流量均衡。

Cisco Secure Firewall Threat Defense 中按时间顺序排列的 ECMP 发展历史记录

本参考按时间顺序提供等价多路径 (ECMP) 功能的开发历史，重点关注各种版本中引入的关键增强功能及其实现细节。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
ECMP 支持作为路由策略	7.1	任意	Cisco Secure Firewall Threat Defense 通过 FlexConfig 策略支持 ECMP 路由。将接口分组到流量区域中，以在 Secure Firewall Management Center 中优化 ECMP 路由。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **ECMP**



第 24 章

双向转发检测路由

本章介绍如何配置 Firewall Threat Defense 以使用双向转发检测 (BFD) 路由协议。

- BFD 路由协议，第 1169 页
- BFD 路由准则，第 1169 页
- 配置 BFD，第 1171 页
- BFD 路由的历史记录，第 1174 页

BFD 路由协议

BFD 路由协议是一种检测协议

- 为媒体类型、封装、拓扑和路由协议提供快速转发路径故障检测时间
- 可以在单播、点对点模式下对正在两系统之间转发的任何数据协议上运行，并且
- 在适用于媒体和网络的封装协议负载中携带数据包。

为什么要使用 BFD？

除了快速转发路径故障检测外，BFD 还为网络管理员提供一致的故障检测方法。

网络管理员可以使用 BFD 以统一的速率检测转发路径故障，而不是像不同的路由协议 hello 机制那样以可变速率检测故障。这样可以简化网络分析和规划，而且重新收敛时间一致且可预测。

BFD 路由准则

上下文模式准则

所有 Firewall Threat Defense 平台均支持 BFD，且在多实例模式下可用。

防火墙模式准则

路由防火墙模式支持 BFD，透明模式不支持。

故障转移和集群准则

- 在故障转移接口上不支持 BFD。
- 在群集中，仅在控制节点上支持 BFD。

路由和协议准则

- 支持 OSPFv2、OSPFv3、IS-IS、BGP IPv4、和 BGP IPv6 协议。

  对于 IS-IS 上的 BFD 支持，使用 FlexConfig CLI 在 IS-IS 接口上配置 BFD（仅限物理接口、子接口、端口通道）：

```
For IPv6
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  ipv6 router isis
  isis ipv6 bfd
exit

For IPv4
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  isis
  isis bfd
exit
```

  不支持 EIGRP 协议。

- 不支持用于静态路由的 BFD。您可以在只属于虚拟路由器的接口上配置 BFD。
- 仅支持命名接口。
- 不支持 BVI、VTI 和 LoopBack 接口上的 BFD。

单跳准则

- 默认情况下，Echo 模式为禁用状态。您可以仅在单跳上启用回应。
- IPv6 不支持回送模式。
- 仅使用单跳模板来配置单跳策略。
- 单跳模板的身份验证为可选。
- 您不能在同一个接口上配置多个 BFD。

多跳准则

- 请勿将源 IP 地址也配置为目标 IP 地址。

- 源地址和目标地址应具有相同的 IP 类型 - IPV4 或 IPV6。
- 仅允许主机或网络类型的网络对象。
- 仅使用多跳模板配置多跳策略。
- 多跳模板必须进行身份验证。

升级准则

当您升级到版本 7.3 且先前版本有任何 FlexConfig BFD 策略时，管理中心会在部署期间显示警告消息。但是，它不会停止部署过程。在升级部署后，要从 UI（**设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** > **BFD**）管理 BFD 策略，则必须在 **设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** > **EIGRP** 页面中配置 BFD 策略，并从设备的 FlexConfig 策略中删除配置。

配置 BFD

此任务将在系统中启用和配置双向转发检测 (BFD) 路由策略，以提供对转发路径中故障的快速检测。

Before you begin

确保您有权访问要配置 BFD 的系统。

按照以下步骤配置 BFD：

过程

步骤 1 创建BFD 模板， 第 2632 页。

步骤 2 配置 BFD 策略， 第 1171 页。

步骤 3 在 BGP 邻居设置中配置 BFD 支持；请参阅配置 BGP 邻居设置。

已在系统上启用并配置 BFD。

配置 BFD 策略

BFD 策略用于为与虚拟路由器关联的接口提供快速故障检测。配置 BFD 模板可让您监控连接并快速识别链路故障。

- 启用路由接口的快速故障检测。
- 支持单跳和多跳 BFD 配置。

您可以将 BFD 模板绑定到属于虚拟路由器的接口，或者绑定到源地址和目标地址对。

Before you begin

- BFD 策略仅可在属于虚拟路由器的接口上进行配置。请参阅配置到虚拟路由器的接口。

按照以下步骤配置 BFD 策略：

过程

步骤 1 在**设备** > **设备管理**页面中，编辑虚拟路由器支持的设备。导航至**路由**。

步骤 2 从下拉列表中，选择所需的虚拟路由器，然后点击 **BFD**。

步骤 3 要在接口上配置 BFD，请点击**单跳 (Single-Hop)** 选项卡或**多跳 (Multi-Hop)** 选项卡。

注释
对于单跳策略，在接口上配置了 BFD 模板；对于多跳策略，在源地址和目标地址对上配置了 BFD 模板。

步骤 4 点击**添加 (Add)**。要修改已配置的 BFD 策略，请点击 **编辑** ()。

注释
在使用 BFD 模板编辑接口映射以将其替换为新的 BFD 模板时，防火墙管理中心 会使用 **no** 命令从接口中删除模板映射，并将新模板应用于接口，这会导致 BFD 摆动，也可能导致 OSPFv2 、OSPFv3 或 BGP 摆动。但是，如果 BFD 间隔较高，则可能不会发生 BFD 摆动。或者，为避免摆动，您可以删除现有的 BFD 模板映射；部署接口，然后将新的 BFD 模板添加到接口并部署配置。

- 请参阅配置单跳 BFD 策略，第 1172 页。
- 请参阅配置多跳 BFD 策略，第 1173 页。

完成此任务后，系统会在所选接口或地址对上配置 BFD 策略。

配置单跳 BFD 策略

您只能在属于虚拟路由器的接口上配置单跳 BFD 策略。当您需要在特定接口上应用 BFD 以进行快速链路故障检测时，此任务是相关的。

Before you begin

- 创建单跳 BFD 模板。您不能在将多跳模板的接口上配置单跳 BFD 策略。

按照以下步骤配置单跳 BFD 策略：

过程

步骤 1 在**单跳 (Single-Hop)** 选项卡中，点击**添加 (Add)** 或**编辑 (Edit)**。

步骤 2 在**添加 BFD 单跳 (Add BFD Single-Hop)** 对话框中，配置以下内容：

a) **接口**下拉列表显示属于虚拟路由器的接口。选择要使用 BFD 策略配置的接口。

b) **模板名称**下拉列表显示单跳模板。选择要应用的模板。

如果尚未创建单跳模板，请使用 **添加** (+) 并创建单跳 BFD 模板。

步骤 3 点击**确定**和**保存**以保存配置。

单跳 BFD 策略将应用于选定的接口。该接口现在将对单跳操作使用指定的 BFD 模板。

配置多跳 BFD 策略

配置多跳BFD策略，以启用对特定源地址和目标地址对之间连接的监控。此配置有助于监控经过网络中多个跃点的链路。

Before you begin

- 创建多跳 BFD 模板。您不能使用单跳模板来配置多跳 BFD 策略。

按照以下步骤配置多跳 BFD 策略：

过程

步骤 1 在**添加 BFD 多跳 (Add BFD Multi-Hop)** 对话框中，配置以下内容：

a) 点击 BFD 源地址类型：**IPv4** 或 **IPv6** 单选按钮。

b) **源地址**下拉列表中列出了网络对象。为 BFD 策略选择源地址；不要选择 *any-ipv4* 或 *any-ipv6*。

如果尚未创建所需的网络对象，请使用 **添加** (+) 并创建主机/网络对象。

注释
所创建的网络对象的 IP 类型应与所选的源 IP 类型匹配。

c) **目标地址**下拉列表中列出了网络对象。为 BFD 选择目标地址；不要选择 *any-ipv4* 或 *any-ipv6*。

如果尚未创建所需的网络对象，请使用 **添加** (+) 并创建主机/网络对象。

注释
所创建的网络对象的 IP 类型应与所选的源 IP 类型匹配。

注意
不要选择与源地址具有相同 IP 地址的网络对象。

d) **模板名称**下拉列表中列出了多跳模板。选择要应用于 BFD 政策的模板。

如果尚未创建多跳模板，请使用 **添加** (+) 并创建多跳 BFD 模板。

步骤 2 点击**确定**和**保存**以保存配置。

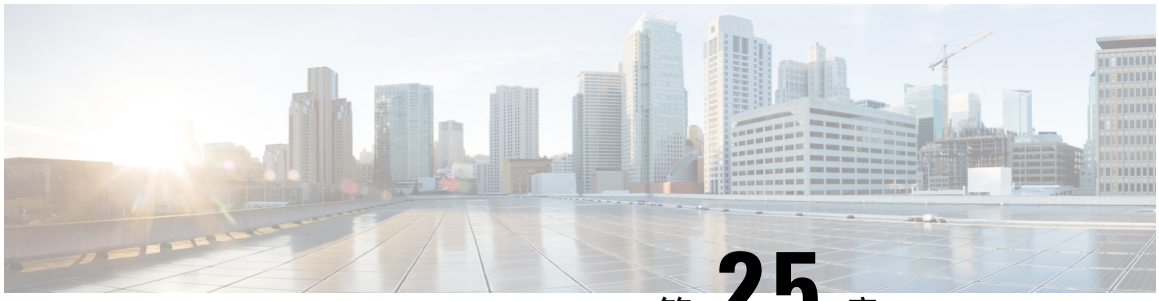
多跳映射（表视图）显示在**多跳 (Multi-Hop)** 选项卡页面上。

BFD 路由的历史记录

历史记录表总结了思科 防火墙管理中心 各版本中 BFD 路由的引入和发展，有助于快速跟踪功能可用性和变更。

表 *80: BFD* 路由的功能历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense** 最低版本	详细信息
IS-IS 的 BFD 支持	7.4	7.4	您可以使用 FlexConfig CLI 在 IS-IS 接口上配置 BFD。
OSPF 的 BFD 支持	7.4	7.4	您可以在使用 OSPF 版本 2 和 OSPF 版本 3 的接口上启用 BFD。 新增/修改的菜单项： • **配置** > **设备设置** > **路由** > **OSPFv2** • **配置** > **设备设置** > **路由** > **OSPFv3**
BFD 配置	7.4	7.4	在之前的版本中，BFD 只能通过 FlexConfig 在威胁防御上进行配置。FlexConfig 不再支持 BFD 配置。现在，您可以在管理中心 UI 中为威胁防御配置 BFD 策略。在威胁防御中，只有 BGP 协议支持 BFD。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **BFD**。



第 25 章

OSPF

本章介绍如何将Firewall Threat Defense配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

- OSPF，第 1175 页
- OSPF 的要求和前提条件，第 1178 页
- OSPF 准则，第 1178 页
- 配置 OSPFv2，第 1180 页
- 配置 OSPFv3，第 1192 页
- OSPF 的历史记录，第 1202 页

OSPF

本章介绍如何将Firewall Threat Defense配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

相比 RIP，OSPF 具有以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于开销，它表明通过特定接口发送数据包所需的开销。Firewall 威胁防御设备 根据链路带宽而非到目标的跃点数计算接口的开销。可以配置开销来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

Firewall 威胁防御设备 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠地址），则可能要运行两个进程。

或者，可能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

您可以将路由从一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

Firewall 威胁防御设备 支持以下 OSPF 功能：

- 区域内、区域间和外部（I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证（密码和 MD5 身份验证）。
- 将 Firewall 威胁防御设备 配置为指定路由器或指定备用路由器。Firewall 威胁防御设备 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议（如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 筛选，您可以具有单独的以 ASA 作为 ABR 的专用和公共区域。3 类 LSA（区域间路由）可以从一个区域筛选到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。

注释 只能筛选 3 类 LSA。如果在专用网络中将 Firewall 威胁防御设备 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将到公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 Firewall 威胁防御设备 保护的专用网络配置静态路由。此外，不应在同一 Firewall 威胁防御设备 接口上混用公用和专用网络。

您可以同时在 Firewall 威胁防御设备 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

OSPF 快速呼叫数据包支持功能提供了一种以短于一秒的间隔发送呼叫数据包的配置方式。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

OSPF 支持快速呼叫数据包的前提条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔（以秒为单位）进行发送。对于以太网链路，默认值为10秒；对于非广播链路，默认值为30秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔（以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF快速呼叫数据包是指按照小于1秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 OSPF 呼叫间隔和停顿间隔，第 1177 页。

通过使用 ospf dead-interval 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该1秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为1秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF快速呼叫数据包功能的优势是OSPF网络将比没有快速呼叫数据包的情况更快收敛。通过此功能，您可以在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 按链路进行协议处理。
- 删除寻址语义。
- 添加泛洪范围。
- 支持每条链路多个实例。

- 使用 IPv6 链路本地地址执行网络发现和其他功能。
- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 的要求和前提条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

OSPF 准则

防火墙模式准则

OSPF 仅支持路由防火墙模式。OSPF 不支持透明防火墙模式。

准则

OSPFv2 和 OSPFv3 支持状态 。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。
- OSPFv3 使用 IPv6 进行身份验证。
- Firewall 威胁防御设备 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。

OSPFv3 Hello 数据包和 GRE

通常，OSPF流量不会通过 GRE 隧道。当 IPv6 上的 OSPFv3 封装在 GRE 内时，安全检查（例如组播目标）的IPv6报头验证失败。由于隐式安全检查验证，数据包被丢弃，因为此数据包具有目标 IPv6 组播。

您可以定义预过滤器规则来绕过GRE流量。但是，使用预过滤器规则，检测引擎不会询问内部数据包。

集群准则

- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式下，仅管理接口上不支持动态路由。
- 在单个接口模式下，确保已作为 OSPFv2 或 OSPFv3 邻居建立控制和数据单元。
- 在单个接口模式下，只能在控制单元共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 当集群中的控制角色发生变化时，会发生以下行为：
  - 在跨接口模式中，路由器进程仅在控制单元上处于活动状态，在数据单元上处于暂停状态。各集群设备具有同一路由器 ID，因为已从控制单元对配置进行同步。因此，在角色更改过程中，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
  - 在单个接口模式中，路由器进程在所有单个集群设备上都处于活动状态。各集群设备从已配置的集群池中选择其自己独特的路由器 ID。集群中的控制角色更改不会以任何方式更改路由拓扑。

多协议标签交换 (MPLS) 和 OSPF 准则

如果 MPLS 配置的路由器发送的链路状态 (LS) 更新数据包包含不透明 Type-10 链路状态通告 (LSA)，而且其中包括 MPLS 报头，则身份验证会失败且设备会自动丢弃更新数据包，而不是确认它们。最终，对等路由器将终止邻居关系，因为它没有收到任何确认。

确保在设备上禁用了不间断转发 (NSF)，以确保邻居关系保持稳定：

- 导航到 防火墙管理中心 中的**不间断转发 (Non Stop Forwarding)** 页面（**设备 (Devices)** > **设备管理 (Device Management)**（选择所需的设备） > **路由 (Routing)** > **OSPF** > **高级 (Advanced)** > **不间断转发 (Non Stop Forwarding)**）。

  确保未选中“**不间断转发功能**”复选框。



注释 Firepower 4100/9300 型号在使用 MPLS 时可能具有高延迟，因为它们缺乏跨多个接收队列的负载均衡。

双向和转发检测 (BFD)及 OSPF 准则

- 您可以在 OSPFv2 和 OSPFv3 接口（物理接口、子接口和端口通道）上启用 BFD。
- VTI 隧道、DVTI 隧道、环回接口、交换机端口、VNI、VTEP 和 IRB 接口不支持 BFD。

路由重分布准则

- 支持在 OSPFv2 上重新分配带有 IPv4 前缀列表的路由映射。但是，不支持在 OSPFv3 上重新分配带有 IPv6 前缀列表的路由映射。 使用 OSPF 上的路由映射中的访问列表进行重新分发。
- 在属于 EIGRP 网络的设备上配置 OSPF 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 尚不支持路由标记）。

  将 OSPF 重新分发到 EIGRP 并将 EIGRP 重新分发到 OSPF 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。
- 可分发的区域内（类型 1）路由数具有限制。对于这些路由，单一 1 类 LSA 包含所有前缀。由于系统的数据包大小限制为 35 KB，所以 3000 个路由会导致数据包超出该限制。考虑设置 2900 个 1 类路由作为支持的最大数量。
- 对于使用虚拟路由的设备，可以为全局虚拟路由器配置 OSPFv2 和 OSPFv3。但是，只能为用户定义的虚拟路由器配置 OSPFv2。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 如果数据包大小超过 8190，OSPFv3 会放弃 LS 更新。因此，邻接关系将终止。因此，使用“ospfv3 mtu-ignore”命令来配置交换机，以避免邻接关系终止。

配置 OSPFv2

本节介绍配置 OSPFv2 路由进程所涉及的任务。对于使用虚拟路由的设备，可以为用户定义的虚拟路由器配置 OSPFv2。

配置 OSPF 区域、范围和虚拟链路

可以配置多个 OSPF 区域参数，包括设置身份验证、定义末节区域以及将特定成本分配给默认摘要路由。您最多可以启用两个 OSPF 进程实例。每个 OSPF 进程具有其自己的关联区域和网络。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选中 **过程 1** 的复选框。对于每个 context/virtual router，最多可以启用两个 OSPF 进程实例。您必须选择 OSPF 进程才能配置区域参数。

如果设备使用的是虚拟路由，则 ID 字段会显示为所选虚拟路由器生成的唯一进程 ID。

步骤 6 从下拉列表中选择**OSPF 角色**，然后在下一字段中为其输入说明。这些选项是“内部”、“ABR”、“ASBR” 和 “ABR 和 ASBR”。有关 OSPF 角色的说明，请参阅关于 OSPF，第 1175 页。

步骤 7 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8 为每个 OSPF 进程配置以下区域选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **区域 ID** - 要汇总其路由的区域的资格。
- **区域类型** - 选择以下选项之一：
  - **普通 (Normal)** -（默认）标准 OSPF 区域。
  - **末节** - 末节区域之外没有任何路由器或区域。末节区域防止自制系统 (AS) 外部 LSA（5 类 LSA）泛洪至末节区域中。创建末节区域时，可以通过取消选中**摘要末节**复选框来防止摘要 LSA（3 类和 4 类）泛洪至该区域中。
  - **NSSA** - 使该区域成为次末节区域 (NSSA)。NSSA 接受 7 类 LSA。您也可以通过取消选中**重新分发** 复选框并选中 **默认信息来源** 复选框来禁用路由重新分发。可以通过取消选中**摘要 NSSA** 复选框来防止摘要 LSA 泛洪至该区域中。
- **指标值** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 至 16777214。

- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **可用网络** - 选择可用网络之一并点击**添加**，或点击 **添加** (+) 以添加新网络对象。有关添加网络的过程，请参阅网络，第 2658 页。
- **身份验证** - 选择 OSPF 身份验证：
  - **无** -（默认）禁用 OSPF 区域身份验证。
  - **密码** - 为区域身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。
- **默认成本** - OSPF 区域的默认开成本，用于确定到目标的最短路径。有效值范围为 0 至 65535。默认值为 1。

步骤 9 点击**确定 (OK)** 以保存区域配置。

步骤 10 选择**范围 (Range)** > **添加 (Add)**。

- 选择可用网络之一，以及是否进行通告，或者，
- 点击 **添加** (+) 以添加新网络对象。有关添加网络的过程，请参阅网络，第 2658 页。

步骤 11 点击**确定 (OK)** 以保存范围配置。

步骤 12 选择**虚拟链路 (Virtual Link)**，点击**添加 (Add)** (+)，并为每个 OSPF 进程配置以下选项：

- **对等体路由器** - 选择对等体路由器的 IP 地址。要添加新的对等体路由器，请点击 **添加** (+)。有关添加网络的过程，请参阅网络，第 2658 页。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。有效值范围为 1 至 65535。默认值为 10。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。
- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 至 8192。默认值为 1。

  更新数据包中的LSA在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑LSA通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送LSA时，它将保留该LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。

- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍（或40秒）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 至 65535。
- **身份验证** - 从以下选项中选择 OSPF 虚拟链路身份验证：
  - **无** -（默认）禁用虚拟链路区域身份验证。
  - **区域身份验证** - 使用 MD5 启用区域身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。

    注释
    确保仅输入数字作为 MD5 密钥 ID。
  - **密钥链** - 允许密钥链身份验证。点击**添加**并创建的密钥链，然后点击**保存**。有关详细操作步骤，请参阅创建密钥链对象，第2656页。为对等体使用相同的身份验证类型（MD5或密钥链）和密钥 ID 以建立成功的邻接关系。

步骤 13 点击**确定 (OK)** 以保存虚拟链路配置。

步骤 14 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPF 重新分发。

配置 OSPF 重新分发

Firewall Threat Defense设备可以控制路由在OSPF路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 EIGRP、RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 从 **OSPF 角色** 下拉列表中，选择角色。

步骤 6 点击 **重新分发** > **添加**。

您可以点击 **编辑** (✎)，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 7 为每个 OSPF 进程配置以下重新分发选项：

- **OSPF 进程 (OSPF Process)**- 选择进程 ID。对于使用虚拟路由的设备，该下拉列表会显示为所选虚拟路由器生成的唯一进程 ID。
- **路由类型** - 选择下列类型之一：
  - **静态** - 将静态路由重新分发到 OSPF 路由过程。
  - **已连接** - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 OSPF 路由过程。已连接路由会作为设备的外部路由重新分发。您可以在“可选”列表下选择是否使用子网。
  - **OSPF** - 重新分发来自另一个 OSPF 路由过程（例如内部、外部 1 和 2、NSSA 外部 1 和 2）的路由，或选择是否使用子网。您可以在“可选”列表下选择以下选项。
  - **BGP** - 重新分发来自 BGP 路由过程的路由。添加 AS 编号以及选择是否使用子网。
  - **RIP** - 重新分发来自 RIP 路由过程的路由。您可以在“可选”列表下选择是否使用子网。

    注释
    由于用户定义的虚拟路由器不支持 RIP，因此您无法从 RIP 重新分发路由。

  - **EIGRP**- 重新分发来自 EIGRP 路由进程的路由。添加 AS 编号以及选择是否使用子网。
- **指标值** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **标签值** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 检查对于从源路由协议到当前路由协议的路由导入的过滤。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标记，则不会导入任何路由。也可以通过点击 **添加** (+) 来添加新的路由映射。请参阅配置路由映射条目以添加新的路由映射。

步骤 8 点击**确定 (OK)** 以保存重新分发配置。

步骤 9 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 区域间过滤，第 1185 页。

配置 OSPF 区域间过滤

ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。配置前缀列表后，便会仅将指定的前缀从一个 OSPF 区域发送到另一个 OSPF 区域。所有其他前缀都限用于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。默认情况下，序列号从 5 开始并以 5 为增量自动生成。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**区域间 (InterArea)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域间。

步骤 6 为每个 OSPF 进程配置下列区域间过滤选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **区域 ID** - 要汇总其路由的区域。
- **前缀列表** - 前缀的名称。要添加新的前缀列表对象，请参阅步骤 5。
- **流量方向** - 入站或出站。选择 Inbound 以筛选传入 OSPF 区域的 LSA，或者选择 Outbound 以筛选传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 7 点击 **添加** ()，然后输入新前缀列表的名称，以及是否允许重写。

配置前缀规则之前，必须先配置前缀列表。

步骤 8 点击**添加**以配置前缀规则，并配置以下参数：

- **操作** - 针对重新分发访问，选择**阻止**或**允许**。
- **序列号** - 路由序列号。默认情况下，序列号从 5 开始并以 5 为增量自动生成。
- **IP 地址** - 以 IP 地址/掩码长度格式指定前缀数字。

- **最小前缀长度** -（可选）最小前缀长度。
- **最大前缀长度** -（可选）最大前缀长度。

步骤 9 点击**确定 (OK)** 以保存区域间过滤配置。

步骤 10 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 过滤规则，第 1186 页。

配置 OSPF 过滤规则

您可以为每个 OSPF 进程配置 ABR 3 类 LSA 过滤器。ABR 3 类 LSA 过滤器仅允许将指定的前缀从一个区域发送到另一个区域，并会限制其他所有前缀。此类型的区域过滤可以应用在特定 OSPF 区域外、应用到特定 OSPF 区域中，或者同时在相同 OSPF 区域的内外进行应用。OSPF ABR 3 类 LSA 过滤可提高对 OSPF 区域之间路由重新分发的控制。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**过滤规则 (Filter Rule)** > **添加 (Add)**。

您可以点击 **编辑** ()，或使用右击菜单剪切、复制、粘贴、插入和删除过滤器规则。

步骤 6 为每个 OSPF 进程配置以下过滤规则选项:

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **访问列表** - 针对此 OSPF 进程的访问列表。若要添加新的标准访问列表对象，请点击 **添加** () 并参阅配置标准 ACL 对象，第 2629 页。
- **流量方向** - 为要过滤的流量方向选择 In 或 Out。选择 In 以过滤传入 OSPF 区域的 LSA，或者选择 Out 以过滤传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。
- **接口** - 此过滤规则的接口。

步骤 7 点击**确定**保存过滤规则配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 汇总地址，第 1187 页。

配置 OSPF 汇总地址

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。但是，您可以将 Firewall Threat Defense设备配置为对于为指定网络地址和掩码包含的所有重新分发的路由通告单个路由。此配置可减小 OSPF 链路状态数据库的大小。可以抑制与指定 IP 地址/掩码对相匹配的路由。标记值可用作用于通过路由映射控制重新分发的值。

可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**摘要地址 (Summary Address)** > **添加 (Add)**。

可以点击 **编辑** (✎) 进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除汇总地址。

步骤 6 为每个 OSPF 进程配置以下汇总地址选项：

- **OSPF 进程 (OSPF Process)**- 对于使用虚拟路由的设备，下拉列表会列出为所选虚拟路由器生成的唯一进程 ID。
- **可用网络** - 汇总地址的 IP 地址。从“可用网络”(Address) 列表中选择一项然后点击**添加**，或者要添加新网络，请点击 **添加** (+)。有关添加网络的程序，请参阅网络，第 2658 页。
- **标记** - 附加到每个外部路由的 32 位十进制值。OSPF 本身未使用此值，但是其可能用于在 ASBR 之间传达信息。
- **通告 (Advertise)** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 7 点击**确定 (OK)** 以保存汇总地址配置。

步骤 8 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPF 接口和邻居，第 1188 页。

配置 OSPF 接口和邻居

如有必要，您可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：呼叫间隔、停顿间隔和身份验证密钥。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF**。

步骤 5 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 为每个 OSPF 进程配置以下接口选项：

- **接口** - 要配置的接口。

  注释
  如果设备使用的是虚拟路由，则此下拉列表只会显示属于路由器的接口。

- **默认成本** - 通过接口发送数据包的成本。默认值为 10。
- **优先级**-为网络指定的路由器。有效值范围为 0 到 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。此设置不适用于配置为点对点接口的接口。

- **MTU 忽略 (MTU Ignore)** - OSPF 检查邻居在公用接口上是否使用的是同一 MTU。在邻居交换 DBD 数据包时会执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，则不建立 OSPF 邻接。
- **数据库过滤器** - 使用此设置在同步和泛洪过程中筛选传出 LSA 接口默认情况下，OSPF 会在同一区域中的所有接口上泛洪新 LSA，但 LSA 到达的接口除外。在全网状拓扑中，此泛洪可能会浪费带宽并产生过多的链路和 CPU 使用情况。选中此复选框可防止 OSPF 在所选接口上进行 LSA 泛洪。

- **呼叫间隔** - 用于指定在接口上发送的呼叫数据包之间的间隔（以秒为单位）。有效值的范围为 1-8192 秒。默认值为 10 秒。

  呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。

- **传输延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。有效值的范围为 1-65535 秒。默认值为 1 秒。

  更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。

- **停顿间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：网络上所有节点的值必须相同，范围可以是 1-65535。

- **呼叫乘数** - 指定每秒要发送的呼叫数据包的数量。有效值为 3 - 20.

- **点对点** - 允许您通过 VPN 隧道传输 OSPF 路由。

- **身份验证** - 从以下选项中选择 OSPF 接口身份验证：

  - **无** -（默认）禁用接口身份验证。
  - **区域身份验证** - 使用 MD5 启用接口身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。
  - **密码** - 为虚拟链路身份验证提供明文密码，在需要考虑安全性的情景下，建议不要选择此选项。
  - **MD5** - 允许 MD5 身份验证。点击**添加**按钮，输入密钥 ID、密钥、确认密钥，然后点击**确定**。

    注释
    只能为 MD5 密钥标识符输入字母、数字和特殊字符。请勿输入空格；空格在管理中心中会被截断。

  - **密钥链** - 允许密钥链身份验证。点击**添加**并创建的密钥链，然后点击**保存**。有关详细操作步骤，请参阅创建密钥链对象，第 2656 页。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID 以建立成功的邻接关系。

- **启用 BFD**-允许您在此接口上启用 BFD。

- **输入密码** - 配置的密码，如果选择“密码”作为身份验证类型。

- **确认密码 (Confirm Password)** - 确认选择的密码。

步骤 7 选择**邻居 (Neighbor)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 8 为每个 OSPF 进程配置以下参数：

- **OSPF 进程** - 选择1或2。
- **邻居** - 在下拉列表中选择一个邻居，或点击 **添加** () 以添加新的邻居；输入名称、说明、网络、是否允许重写，然后点击**保存**。
- **接口** - 选择与邻居关联的接口。

步骤 9 点击**确定 (OK)** 以保存邻居配置。

步骤 10 点击“路由”页面上的**保存**以保存更改。

配置 OSPF 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、LSA 计时器和平稳重启。

平稳重启

Firewall Threat Defense设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。通过使用NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。

注释 NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF功能的设备可以向邻居表明其自己的重启活动，而支持NSF感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**。

步骤 3 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 OSPF 的虚拟路由器。

步骤 4 点击 **OSPF** > **高级设置**。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **路由器 ID** - 选择自动或手动（对于非集群和跨区以太网通道模式下的集群显示）或集群池（对于单个接口模式下的集群显示）。如果选择 IP 地址，在邻接字段中输入 IP 地址。如果选择集群池，请在相邻的下拉字段中选择 IPv4 集群池值。有关创建集群池地址的信息，请参阅地址池，第 2630 页。
- **忽略 LSA MOSPF** - 在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时，抑制系统日志消息。
- **RFC 1583 兼容** - 将 RFC 1583 兼容性配置为用于计算摘要路由成本的方法。在启用了 RFC 1583 兼容性的情况下，可能会出现路由环路。禁用它可以防止路由环路的出现。OSPF 路由域中的所有 OSPF 路由器都应设置相同的 RFC 兼容性。
- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在 OSPF 邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在 OSPF 邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **日志邻接更改** - 使 Firewall Threat Defense设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **日志邻接更改详细信息** - 使 Firewall Threat Defense设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。

- **管理路由距离**-允许您修改用于为 **区域间**、 **区域内**和 **外部** IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **LSA 组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **启用默认信息来源** - 选中**启用**复选框可将默认外部路由生成到OSPF 路由域中并配置以下选项：
  - **始终通告默认路由** - 确保始终通告默认路由。
  - **指标值 (Metric Value)** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
  - **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。

- **路由映射 (RouteMap)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击 **添加** (+) 以添加新路由。请参阅配置路由映射条目以添加新的路由映射。

步骤 6 点击**确定 (OK)** 以保存常规配置。

步骤 7 选择**非停止转发 (Non Stop Forwarding)**，并为支持 NSF 或识别 NSF 的设备配置 OSPFv2 的思科 NSF 平稳重启：

注释
对于 OSPFv2、思科 NSF 和 IETF NSF，存在两种平稳重启机制。一次只能为 OSPF 实例配置其中一种平稳重启机制。支持 NSF 感知的设备既可以配置为思科 NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在思科 NSF 或 IETF NSF 模式中为 OSPF 实例配置支持 NSF 功能的设备。

a) 选中**启用思科非停止转发功能**复选框。
b) （可选）如果需要，请选中**当检测到无法识别 NSF 的邻居设备时取消 NSF 重启**复选框。
c) （可选）确保取消选中**启用思科非停止转发助手模式**复选框，以便在识别 NSF 的设备上禁用助手模式。

步骤 8 为 OSPFv2 配置思科 IETF NSF 平稳重启（支持 NSF 功能的设备或 NSF 感知的设备）。

a) 选中**启用 IETF 非停止转发功能**复选框。
b) 在**平稳重启间隔的长度 (秒)** 字段中，以秒为单位输入重启间隔。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。
c) （可选）确保取消选中**针对助手模式启用 IETF 非停止转发 (NSF)** 复选框，以便在识别 NSF 的设备上禁用 IETF NSF 助手模式。
d) **启用严格链路状态通告检查** - 启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。
e) **启用 IETF 非停止转发** - 启用非停止转发，这样将允许在状态切换后恢复路由协议信息时，转发数据包以沿已知路由继续。OSPF 使用 OSPF 协议的扩展来从相邻的 OSPF 设备恢复其状态。要进行恢复，相邻的路由器必须支持 NSF 协议扩展，并愿意充当重启设备的“助手”。邻居还必须继续在进行协议状态恢复时将数据流量转发到正在重启的设备。

配置 OSPFv3

本节介绍配置 OSPFv3 路由进程所涉及的任务。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 OSPFv3，而不能为其用户定义的虚拟路由器配置 RIP。

配置 OSPFv3 区域、路由摘要和虚拟链路

要启用 OSPFv3，您需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**选项卡。在选项卡的左窗格上，点击 **OSPFv3**。

步骤 3 默认情况下，**启用进程 1** 处于选中状态。您最多可以启用两个 OSPF 进程实例。

步骤 4 从下拉列表中选择OSPFv3 角色，并为其输入说明。这些选项是“内部”、“ABR”、“ASBR”以及“ABR 和 ASBR”。有关 OSPFv3 角色的说明，请参阅关于 OSPF，第 1175 页。

步骤 5 选择**区域 (Area)** > **添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 6 选择**常规 (General)**，然后为每个 OSPF 进程配置以下选项：

- **区域 ID** - 要汇总其路由的区域。
- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。
- **类型** - 指定“普通”、“NSSA”或“末节”。如果选择“普通”，则没有其他参数要配置。如果选择“末节”，则可以选择在区域中发送摘要 LSA。如果选择“NSSA”，则可以配置下面的三个选项：
  - **允许将摘要 LSA 发送到该区域** - 允许将摘要 LSA 发送到该区域。
  - **将路由导入到普通和 NSSA 区域**-允许重新分发以将路由导入到正常区域，而不是末节区域。
  - **默认信息源** - 在 OSPFv3 路由域中生成默认的外部路由。
- **指标** - 用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 到 16777214。
- **指标类型** - 指标类型是与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。

步骤 7 点击**确定 (OK)** 以保存常规配置。

步骤 8 （不适用于内部 OSPFv3 角色）选择 **路由摘要** > **添加路由摘要**。

您可以点击 **编辑** ()，或使用右键点击菜单剪切、复制、粘贴、插入和删除路由摘要。

步骤 9 为每个 OSPF 进程配置以下路由摘要选项：

- **IPv6 前缀/长度** - IPv6 前缀。要添加新的网络对象，请点击 **添加** ()。有关添加网络的过程，请参阅网络，第 2658 页。
- **成本** - 汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。

- **通告** - 通告摘要路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

步骤 10 点击**确定 (OK)** 以保存路由摘要配置。

步骤 11 （不适用于 OSPFv3 角色）选择**虚拟链接 (Virtual Link)**，点击**添加虚拟链接 (Add Virtual Link)**，并为每个 OSPF 进程配置以下选项：

- **对等体路由器 ID (Peer RouterID)** - 选择对等体路由器的 IP 地址。要添加新的网络对象，请点击 **添加** (+)。有关添加网络的过程，请参阅网络，第 2658 页。
- **TTL 安全** - 启用 TTL 安全检查。hop-count 的值是一个介于 1 到 254 之间的数字。默认值为 1。

  OSPF 发送使用 IP 报头生存时间 (TTL) 值 255 来发送传出数据包，并丢弃 TTL 值小于可配置阈值的传入数据包。由于转发 IP 数据包的每个设备都会使 TTL 递减，因此通过直接（一跳）连接接收的数据包的值为 255。跨越两跳的数据包的值为 254，以此类推。接收阈值根据数据包可能已移动的最大跳数来配置。
- **停顿间隔** - 在邻居指示路由器关闭之前呼叫数据包不可见的时间（以秒为单位）。默认值是呼叫间隔的四倍（或 40 秒）。有效值范围为 1 到 65535。

  停顿间隔是无符号整数。对于连接到公用网络的所有路由器和接入服务器，值必须相同。
- **呼叫间隔** - 在接口上发送的呼叫数据包的间隔时间（以秒为单位）。有效值范围为 1 到 65535。默认值为 10。

  呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。该值对特定网络上的所有路由器和访问服务器必须相同。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 65535。默认值为 5。

  当一台路由器向其邻居发送 LSA 时，它将保留该 LSA，直至收到确认消息。如果路由器没有接收到确认，则重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。
- **传送延迟** - 在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。整数值必须大于零。有效值范围为 1 到 8192。默认值为 1。

  更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。

步骤 12 点击**确定**保存虚拟链路配置。

步骤 13 点击“路由”页面上的**保存**以保存更改。

下一步做什么

继续配置 OSPFv3 重新分发。

配置 OSPFv3 重新分发

Cisco Secure Firewall Threat Defense设备可以控制路由在 OSPF 路由过程之间的重新分发。将路由从一个路由过程重新分发到 OSPF 路由过程的规则将会显示。可以将 EIGRP、RIP 和 BGP 发现的路由重新分发到 OSPF 路由过程中。还可以将静态路由和已连接路由重新分发到 OSPF 路由过程中。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPF**。

步骤 3 选择**重新分发 (Redistribution)** 并点击**添加 (Add)**。

您可以点击 **编辑** ()，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPF 进程配置以下重新分发选项：

- **源协议** - 从中重新分发路由的源协议。支持的协议为“已连接”、“静态”、“OSPF”和“BGP”。如果选择“OSPF”，则必须在**过程 ID** 字段中输入过程 ID。如果选择“BGP”，则必须在 **AS 编号**字段中添加 AS 编号。
- **指标** - 正在分发的路由的指标值。默认值为 10。有效值范围为 0 到 16777214。

  在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到OSPF进程时，如果未指定指标值，则默认指标为 20。
- **指标类型 (Metric Type)** - 指标类型是与通告到OSPF路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- **标签** - 标签指定附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- **路由映射** - 选中以过滤从源路由协议到当前路由协议的路由的导入。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标记，则不会导入任何路由。也可以通过点击 **添加** () 来添加新的路由映射。请参阅路由映射，第 2685 页了解添加新路由映射的过程。
- **过程 ID** - OSPF 过程 ID，即 1 或 2。

  注释
  过程 ID 已启用，OSPFv3 过程正在重新分发由另一个 OSPFv3 过程获悉的路由。
- **匹配** - 启用要重新分发到其他路由域的 OSPF 路由：
  - **内部**，表示特定自治系统的内部路由。
  - **外部 1**，表示自治系统的外部路由，但会作为 1 类外部路由导入 OSPFv3。

- **外部 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入 OSPFv3。
- **NSSA 外部 1**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类外部路由导入到 OSPFv3 中。
- **NSSA 外部 2**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 2 类外部路由导入到 OSPFv3 中。

步骤 5 点击**确定 (OK)** 以保存重新分发配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 摘要前缀，第 1196 页。

配置 OSPFv3 摘要前缀

您可以配置 Firewall Threat Defense设备以通告与指定的 IPv6 前缀和掩码对匹配的路由。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPFv3** 。

步骤 3 选择**摘要前缀 (Summary Prefix)** > **添加 (Add)**。

您可以点击 **编辑** ()，或使用右键点击菜单剪切、复制、粘贴、插入和删除摘要前缀。

步骤 4 为每个 OSPF 进程配置以下摘要前缀选项：

- **IPv6 前缀/长度** - IPv6 前缀和前缀长度标签。从列表中选择一个或点击 **添加** () 以添加新的网络对象。有关添加网络的过程，请参阅网络，第 2658 页。
- **通告** - 通告与指定前缀/掩码对匹配的路由。取消选中此复选框以抑制与指定前缀/掩码对匹配的路由。
- （可选）**标记** - 可用作通过路由映射控制重新分发的匹配值的值。

步骤 5 点击**确定 (OK)** 以保存摘要前缀配置。

步骤 6 点击“路由”页上的 **保存**以保存更改。

下一步做什么

继续执行配置 OSPFv3 接口、身份验证和邻居，第 1197 页。

配置 OSPFv3 接口、身份验证和邻居

如有必要，您可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：hello-interval 和 dead-interval。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

要与 Nexus 交换机成功实现 OSPFv3 身份验证，请确保您拥有兼容版本的交换机，例如 Nexus 3000、7000 和 9000 系列交换机。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由** > **OSPFv3**。

步骤 3 选择**接口 (Interface)** > **添加 (Add)**。

您可以点击**编辑**以进行编辑，或者使用右键点击菜单剪切、复制、粘贴、插入和删除区域。

步骤 4 为每个 OSPFv3 进程配置以下接口选项：

- **接口** - 正在配置的接口。
- **启用 OSPFv3** - 启用 OSPFv3。
- **OSPF 进程** - 选择 1 或 2。
- **区域** - 此进程的区域 ID。
- **实例** - 指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。您可以在多个接口上使用同一区域，并且每个接口可以使用不同的区域实例 ID。

步骤 5 选择**属性 (Properties)**，并为每个 OSPFv3 进程配置以下选项：

- **过滤传出链路状态通告** - 过滤到 OSPFv3 接口的传出 LSA。默认情况下，所有传出 LSA 都泛洪至该接口。
- **禁用 MTU 不匹配检测** - 收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测。默认情况下，OSPF MTU 不匹配检测已启用。
- **泛洪减少** - 将普通 LSA 更改为“不老化”LSA，以使它们不会每 3600 秒就出现跨区域泛洪。

  OSPF LSA 每 3600 秒刷新一次。在大型 OSPF 网络中，这可能导致区域间出现大量不必要的 LSA 泛洪。
- **点对点网络** - 允许您通过 VPN 隧道传送 OSPF 路由。当接口配置为点对点非广播时，以下限制适用：
  - 只能为接口定义一个邻居。
  - 需要手动配置邻居。
  - 您无需定义指向加密终端的静态路由。

- 如果通过隧道执行的 OSPF 是在接口上运行，则上游路由器的常规 OSPF 不能在同一接口上运行。
- 在指定 OSPF 邻居之前应将加密映射绑定到接口，以确保通过 VPN 隧道传递 OSPF 更新。如果在指定 OSPF 邻居之后将加密映射绑定到接口，请使用 **clear local-host all** 命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接。

- **广播** - 指定接口为广播接口。默认情况下，对于以太网接口会选中此复选框。取消选中此复选框以将接口指定为点对点非广播接口。将接口指定为点对点非广播可以通过VPN隧道传输OSPF路由。
- **成本** - 指定在接口上发送数据包的成本。此设置的有效值范围为 0 至 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。此设置不适用于配置为点对点非广播接口的接口。

  当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。
- **优先级** - 确定为网络指定的路由器。有效值范围为 0 到 255。
- **死间隔** - 在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。
- **Hello 间隔** - 在与邻居建立邻接关系之前，路由器将发送的 OSPF 数据包之间的时间段（以秒为单位）。路由设备检测到活动邻居，呼叫数据包间隔将从轮询间隔中指定的时间更改为呼叫间隔中指定的时间。有效值的范围为 1 到 65535 秒。
- **重新传送间隔** - 属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- **传送延迟** - 在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。
- **启用 BFD**-允许您在此接口上启用 BFD。

步骤 6 点击**确定 (OK)** 以保存属性配置。

步骤 7 选择**身份验证 (Authentication)**，并为每个 OSPFv3 进程配置以下选项：

- **类型** - 身份验证类型。可用选项为 Area、Interface 和 None。None 选项表示未使用身份验证。
- **安全参数索引** - 从 256 到 4294967295 的一个数字。如果选择“接口”作为类型，请配置此选项。
- **身份验证** - 身份验证算法的类型。支持的值为 SHA-1 和 MD5。如果选择“接口”作为类型，请配置此选项。
- **身份验证密钥** - 使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
- **加密身份验证密钥** - 启用身份验证密钥的加密。

- **包括加密** - 启用加密。
- **加密算法** - 加密算法的类型。支持的值为 DES。NULL 条目表示不加密。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 输入加密密钥。密钥长度必须是十六进制字符串。使用 AES-256-CBC 身份验证时，密钥长度必须为 130 位十六进制数字。如果选择**包括加密**，请配置此选项。
- **加密密钥** - 使密钥被加密。

步骤 8 点击**确定 (OK)** 以保存身份验证配置。

步骤 9 选择**邻居 (Neighbor)**，点击**添加 (Add)**，并为每个 OSPFv3 进程配置以下选项：

- **链路本地地址** - 静态邻居的 IPv6 地址。
- **成本** - 启用成本。在**成本**字段中输入成本，如果需要通告，请选中**过滤传出链路状态通告**。
- （可选）**轮询间隔** - 启用轮询间隔。以秒为单位输入**优先级**级别和**轮询间隔**。

步骤 10 点击**添加**以添加帐户。

步骤 11 点击**确定 (OK)** 以保存接口配置。

配置 OSPFv3 高级属性

“高级属性”(Advanced Properties) 允许您配置选项，如系统日志消息生成、管理路由距离、被动 OSPFv3 路由、LSA 计时器和平稳重启。

平稳重启

Firewall Threat Defense设备可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。当有计划的无中断软件升级时，此功能非常有用。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

注释 NSF 功能在 HA 模式和集群中也很有用。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持NSF功能的设备可以向邻居表明其自己的重启活动，而支持NSF感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。

- 为使设备支持NSF功能或NSF感知，应将其配置为能够根据需要处理不透明链路状态通告(LSA)/本地链路信令 (LLS) 块。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **路由** > **OSPFv3** > **高级**。

步骤 3 对于 **路由器 ID**，选择自动或手动（对于非集群和跨区以太网通道模式下的集群显示）或集群池（对于单个接口模式下的集群显示）。如果选择 IP 地址，在 **IP 地址** 字段中输入 IPv6 地址。如果选择集群池，请在 **集群池**下拉列表中选择 IPv6 集群池值。有关创建集群池地址的信息，请参阅地址池，第 2630 页。

步骤 4 如果您希望在路由收到不受支持的 LSA 类型 6 组播 OSPF (MOSPF) 数据包时抑制系统日志消息，请选中**忽略 LSA MOSPF** 复选框。

步骤 5 选择**常规 (General)**，然后配置以下选项：

- **邻接更改** - 定义将导致发送系统日志消息的邻接更改。

  默认情况下，在OSPF邻居启动或关闭时会生成系统日志消息。您可以将路由器配置为在OSPF邻居关闭时发送一个系统日志消息，并为每个状态发送系统日志。

  - **邻接更改** - 使 Firewall Threat Defense设备每当在 OSPF 邻居启动或关闭时都会发送系统日志消息。默认情况下，此设置处于选中状态。
  - **包括详细信息** - 使 Firewall Threat Defense设备每当在发生任何状态更改时都会发送系统日志消息，而不只是在邻居启动或关闭时发送。默认情况下，此设置处于未选中状态。

- **管理路由距离** - 允许您修改用于为区域间、区域内和外部 IPv6 路由配置管理路由距离的设置。管理路由距离是从 1 至 254 的整数。默认值为 110。
- **默认信息来源** - 选中**启用**复选框可将默认外部路由生成到 OSPFv3 路由域中并配置以下选项：
  - **始终通告** - 将会始终通告默认路由（无论其是否存在）。
  - **指标** - 用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
  - **指标类型** - 与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值为 1（1 类外部路由）和 2（2 类外部路由）。默认为 2 类外部路由。
  - **路由地图 (Route Map)** - 选择在路由映射符合条件时生成默认路由的路由过程，或者点击**添加** (+) 以添加新路由。请参阅路由映射，第 2685 页以添加路由映射。

步骤 6 点击**确定 (OK)** 以保存常规配置。

步骤 7 选择**被动接口 (Passive Interface)**，从“可用接口”(Available Interfaces) 列表中选择要在其上启用被动 OSPFv3 路由的接口，然后点击**添加 (Add)** 将它们移动到“选定的接口”(Selected Interfaces) 列表中。

备用路由帮助控制 OSPFv3 路由信息的通告并禁用在接口上发送和接收 OSPFv3 路由更新。

步骤 8 点击**确定 (OK)** 以保存被动接口配置。

步骤 9 选择**计时器 (Timer)**，并配置以下 LSA 步调设置和 SPF 计算计时器：

- **到达** - 指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围是从 0 到 6000,000 毫秒。默认值为 1000 毫秒。
- **泛洪步调设置** - 指定泛洪队列中的 LSA 在两次更新之间定步的时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。
- **组步调设置** - 指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **重新传输步调设置** - 指定重新传输队列中 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。
- **LSA 调速** - 指定生成第一次出现的 LSA 时的延迟（以毫秒为单位）。默认值为 0 毫秒。最小值指定发起同一 LSA 所需的最小延迟（以毫秒为单位）。默认值为 5000 毫秒。最大值指定发起同一 LSA 所需的最大延迟（以毫秒为单位）。默认值为 5000 毫秒。

  注释
  对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

- **SPF 调速** - 指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。默认值为 5000 毫秒。最小值指定第一次和第二次 SPF 计算之间的延迟（以毫秒为单位）。默认值为 10000 毫秒。最大值指定 SPF 计算的最长等待时间（以毫秒为单位）。默认值为 10000 毫秒。

  注释
  对于 SPF 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

步骤 10 点击**确定 (OK)** 以保存 LSA 计时器配置。

步骤 11 选中**非停止转发 (Non Stop Forwarding)**，并选中**启用稳定重启助手 (Enable graceful-restart helper)** 复选框。默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用平稳重启助手模式。

步骤 12 选中**启用链路状态通告**复选框以启用严格链路状态通告检查。

启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。

步骤 13 选中**启用稳定重启 (配置了跨区集群或故障切换时使用)**，然后以秒为单位输入稳定重启间隔。范围为 1-1800。默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

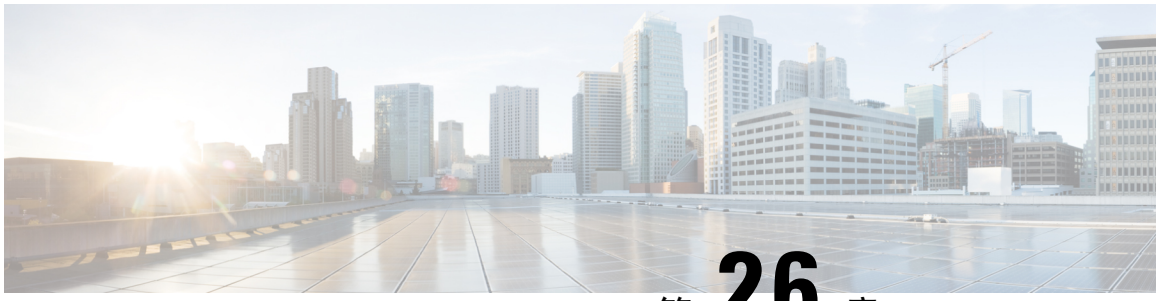
步骤 14 点击**确定 (OK)** 以保存平稳重启配置。

步骤 15 点击“路由”页面上的**保存**以保存更改。

OSPF 的历史记录

表 *81: OSPF* 的功能历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
OSPF v2 和 v3 的 BFD 支持	7.4	7.4	您可以在 OSPFv2 和 OSPFv3 接口上启用 BFD。 新增/修改的菜单项： • **配置 > 设备设置 > 路由 > OSPFv2** • **配置 > 设备设置 > 路由 > OSPFv3**



第 26 章

EIGRP

本部分介绍如何使用增强型内部网关路由协议 (EIGRP) 配置 Firewall Threat Defense，以路由数据、执行身份验证以及重新分发路由信息。

- 关于 EIGRP 路由， 第 1203 页
- EIGRP 的要求和前提条件， 第 1204 页
- EIGRP 路由的准则和限制， 第 1204 页
- 配置 EIGRP， 第 1206 页
- EIGRP 的历史记录， 第 1212 页

关于 EIGRP 路由

思科开发的增强型内部网关路由协议 (EIGRP) 是 IGRP 的增强版本。与 IGRP 和 RIP 不同，EIGRP 不发送定期路由更新。仅在网络拓扑发生更改时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速收敛、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器会存储所有邻居路由表，以便可以迅速适应备用路由。如果不存在合适的路由，则 EIGRP 会查询其邻居以发现备用路由。这些查询会被传播直至找到备用路由为止。EIGRP 对可变长度子网掩码功能的支持允许在网络边界自动汇总路由。此外，还可以将 EIGRP 配置为在任何接口的任何位边界汇总。

EIGRP 不会定期更新。相反，它会在路由指标发生更改时发送部分更新。部分更新的传播是自动绑定的，因此只有需要该信息的路由器才会更新。得益于这两项功能，EIGRP 与 IGRP 相比可显著减少占用的带宽。

要动态地了解直接连接网络上的其他路由器，威胁防御会使用邻居发现。EIGRP 路由器发出组播 Hello 数据包，通告其在网络中的存在状态。当 EIGRP 设备收到来自新邻居的 Hello 数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到设备。

Hello 数据包作为组播消息发出。预期不会对 Hello 消息作出响应。静态定义的邻居不在此规则的范围内。如果手动配置邻居，则 Hello 消息、路由更新和确认将作为单播消息发送。

一旦邻居关系建立后，除非网络拓扑发生更改，否则便不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。保持时间是威胁防御预期收到该邻

居的 Hello 数据包的时间。如果设备在保持时间内未收到由该邻居通告的 Hello 数据包，则设备会将该邻居视为不可用。

EIGRP 会使用邻居发现/恢复、可靠传输协议 (RTP) 和扩散更新算法 (DUAL) 进行路由计算。DUAL 将目标的所有路由都保存在拓扑表中，而不只是保存最低成本路由。最低成本路由会插入到路由表中。其他路由则保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于进行数据包转发的具有到达目标的最低成本路径的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果在拓扑表中找不到可行后继路由，则会重新计算路由。在路由重新计算期间，DUAL 会查询 EIGRP 邻居以获取路由。查询会被传播到连续的邻居。如果找不到可行的后继邻居，则会返回不可达消息。

在路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，威胁防御会等待三分钟接收来自其邻居的响应。如果设备未收到来自邻居的响应，则会将路由标记为陷入主动状态。系统会删除拓扑表中作为可行性后继路由指向无响应邻居的所有路由。

EIGRP 的要求和前提条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

EIGRP 路由的准则和限制

防火墙模式指导原则

仅支持路由防火墙模式。

设备准则

- 每台设备仅允许有一个 EIGRP 进程。
- 可以通过 Firewall Threat Defense 6.6 及更高版本上的管理中心 UI 来配置 EIGRP。

接口指导原则

- 只有具有逻辑名称和 IP 地址的路由接口才能与 EIGRP 路由进程相关联。
- 只有属于全局虚拟路由器的接口才能成为 EIGRP 的一部分。EIGRP 可以在全局虚拟路由器中跨路由协议获知、过滤和重新分发路由。
- 仅支持物理、EtherChannel、冗余、子接口。但是，不支持 EtherChannel 接口的成员。
- BVI 和 VNI 不能是 EIGRP 的一部分。
- 被动接口不能被配置为邻居接口。

IP 地址和网络对象支持

- 仅支持 IPv4 地址。
- 不支持范围、FQDN 和通配符掩码。
- 仅支持标准访问列表对象。

重新分配准则

- 全局虚拟路由器中的 BGP、OSPF 和 RIP 可以重新分配到 EIGRP。
- EIGRP 可以重新分配到全局虚拟路由器中的 BGP、OSPF、RIP、静态和已连接。
- 在属于 OSPF 网络的设备上配置 EIGRP 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 不支持路由标记）。

  将 EIGRP 重新分发到 OSPF 并将 OSPF 重新分发到 EIGRP 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

部署流程准则

如果要更改已部署 EIGRP 配置的现有 AS 编号，您必须禁用 EIGRP 并进行部署。此步骤将清除威胁防御上已部署的 EIGRP 配置。接下来使用新的 AS 编号重新创建 EIGRP 配置，然后进行部署。因此，此过程可防止由于在威胁防御上部署相同的 EIGRP 配置而导致任何部署失败。

升级准则

如果您升级到版本 7.2 和更新版本具有任何 FlexConfig EIGRP 策略，则管理中心会在部署期间显示警告消息。但是，它不会停止部署过程。但在部署后，要从 UI (**设备** > **设备管理**) 管理 EIGRP 策略，然后点击 **编辑** (✎) 图标。然后，点击**路由>EIGRP**），您必须在 **EIGRP** 页面中重新进行配置，并从 FlexConfig 中删除配置。要在 UI 中自动创建策略，防火墙管理中心 提供了将策略从 FlexConfig 迁移到 UI 的选项。有关详细信息，请参阅迁移 FlexConfig 策略，第 1080 页。

配置 EIGRP

您可以在**路由 (Routing)** 选项卡中启用和配置防火墙设备上的 EIGRP。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由**选项卡。

步骤 3 在“全局”(Global) 下，点击 **EIGRP**.

步骤 4 选中 **启用 EIGRP** 复选框以启用 EIGRP 路由进程。

步骤 5 在 **AS 编号**字段中，输入 EIGRP 进程的自治系统 (AS) 编号。AS 编号包含多个自主编号。AS 编号可从 1 到 65535，并且是分配的唯一值，用于在互联网上标识各个网络。

步骤 6 要配置其他 EIGRP 属性，请参阅以下主题：

1. 配置 EIGRP 设置， 第 1206 页。
2. 配置 EIGRP 邻居设置， 第 1207 页。
3. 配置 EIGRP 过滤器规则设置， 第 1207 页。
4. 配置 EIGRP 重新分发设置， 第 1208 页。
5. 配置 EIGRP 摘要地址设置， 第 1209 页。
6. 配置 EIGRP 接口设置， 第 1209 页。
7. 配置 EIGRP 高级设置， 第 1210 页。

配置 EIGRP 设置

过程

步骤 1 在 **EIGRP** 页面上，点击**设置 (Setup)** 选项卡。

步骤 2 选中 **自动汇总** 复选框，使 EIGRP 能够汇总网络编号边界。

注释
如果存在非连续网络，启用自动汇总这可能会引起路由问题。

步骤 3 在**可用网络/主机 (Available Networks/Hosts)** 框中，点击应参与 EIGRP 路由进程的网络或主机，然后点击**添加 (Add)**。要添加新的网络对象，请点击 **添加** (+)。有关添加网络的过程，请参阅网络， 第 2658 页。

步骤 4 要配置被动接口，请选中 **被动接口** 复选框。在 EIGRP 中，被动接口既不发送也不接收路由更新。

a) 要将选择性接口指定为被动接口，请点击**选定接口 (Selected Interface)** 单选按钮。在**可用接口 (Available Interfaces)** 框中，选择接口，然后点击**添加 (Add)**。

b) 要将所有接口指定为被动，点击**所有接口 (All Interfaces)** 单选按钮。

步骤 5 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 邻居设置

您可以为 EIGRP 进程定义静态邻居。在手动定义 EIGRP 邻居时，Hello 数据包会单播至该邻居。

过程

步骤 1 在 **EIGRP** 页面上，点击**邻居 (Neighbors)** 选项卡。

步骤 2 点击**添加 (Add)**。

步骤 3 从**接口 (Interface)** 下拉列表中选择可通过其访问邻居的接口。

步骤 4 从**邻居 (Neighbor)** 下拉列表中选择静态邻居的 IP 地址。要添加网络对象，请点击 **添加** (+)。有关添加网络对象的过程，请参阅网络，第 2658 页。

步骤 5 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 过滤器规则设置

您可以为 EIGRP 路由进程配置路由过滤规则。过滤规则让您能够控制 EIGRP 路由进程接受或通告的路由。

过程

步骤 1 在 **EIGRP** 页面上，点击**过滤器规则 (Filter Rules)** 选项卡。

步骤 2 请点击 **添加** (+)。

步骤 3 在**添加过滤器规则 (Add Filter Rules)** 对话框中，从**过滤器方向 (Filter Direction)** 下拉列表中选择规则的方向：

- 入站 (Inbound) - 规则过滤来自传入 EIGRP 路由更新的默认路由信息。
- 出站 (Outbound) - 规则过滤来自传出 EIGRP 路由更新的默认路由信息。

步骤 4 要选择应用过滤规则的接口，请点击**接口 (Interface)** 单选按钮，然后从下拉列表中选择接口。

注释

您不能在 VTI 接口上应用 EIGRP 过滤规则。

步骤 5 要选择应用过滤规则的协议，请点击**协议 (Protocol)** 单选按钮，然后从下拉列表中选择协议 - BGP、RIP、静态、已连接或 OSPF。对于 BGP 和 OSPF 协议，您可以指定相关的进程 ID。

步骤 6 从**访问列表 (Access List)** 下拉列表中选择访问列表。此列表定义了要在路由更新中接收的网络和要抑制的网络。若要添加新的标准访问列表对象，请点击**添加** (+) 并参阅配置标准 ACL 对象，第 2629 页了解详细程序。

步骤 7 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 重新分发设置

您可以定义将来自其他路由协议的路由重新分发到 EIGRP 路由进程的规则

过程

步骤 1 在 **EIGRP** 页面上，点击**重新分配 (Redistribution)** 选项卡。

步骤 2 请点击 **添加** (+)。

步骤 3 在**添加重新分配 (Add Redistribution)** 对话框中，从**协议 (Protocol)** 下拉列表选择要从其重新分配路由的源协议：

- BGP - 将 BGP 路由进程发现的路由重新分配给 EIGRP。
- RIP - 将 RIP 路由进程发现的路由重新分配给 EIGRP。
- 静态 - 将静态路由重新分布到 EIGRP 路由过程中。位于 network 语句范围内的静态路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。但是，在 EIGRP 中重新分发指向 VTI 接口的静态路由时，必须指定指标。对于指向其他类型接口的静态路由，不需要指定指标。
- 已连接 - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 EIGRP 路由进程。位于 network 语句范围内的已连接路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- OSPF - 将由 OSPF 路由进程发现的路由重新分发到 EIGRP。如果选择此协议，则此对话框中的“匹配”(Match) 选项将在**可选 OSPF 重新分配 (Optional OSPF Redistribution)** 下变得可见：
  - 内部 - 特定 AS 的内部路由。
  - External1 - AS 外部的路由，会作为 1 类外部路由导入OSPF。
  - External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程。
  - Nsaa-External1 - AS 外部的路由，会作为第 1 类外部路由导入所选进程的次末节区域 (NSSA)。
  - Nsaa-External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程的 (NSSA)。

注释

当重新分发静态、已连接、RIP 或 BGP 路由时，这些选项不可用。

步骤 4 在**可选指标 (Optional Metrics)** 下输入相关值：

- **带宽 (Bandwidth)** - 路由的最小带宽（以千比特/秒为单位）。有效值范围为 1 到 4294967295。
- **延迟时间 (Delay Time)** - 路由延迟（以十微秒为单位）。有效值范围为 0 到 4294967295。
- **可靠性 (Reliability)** - 数据包成功传输的可能性（以 0 到 255 的数字表示）。值 255 表示 100% 可靠；0 表示不可靠。
- **正在加载 (Loading)** - 路由的有效带宽。有效值范围为 1 到 255。255 表示 100% 加载。
- **MTU** - 路径的最大传输单位允许的最小值。有效值范围为 1 到 65535。

步骤 5 从**路由地图 (Route Map)** 下拉列表中选择要应用于重新分配条目的路由映射。要创建新的路由映射对象，请点击 **添加** (+)。请参阅程序的配置路由映射条目以添加新的路由映射。

步骤 6 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 摘要地址设置

您可以为每个接口配置汇总地址。如果要创建不会出现在网络边界上的汇总地址，或者要在自动路由汇总禁用的情况下在威胁防御上使用汇总地址，则需要手动定义汇总地址。如果路由表中有任何更具体的路由，则 EIGRP 会使用与所有更具体路由的最小值相等的指标来通告汇总地址。

过程

步骤 1 在 **EIGRP** 页面上，点击**汇总地址 (Summary Address)** 选项卡。

步骤 2 点击**添加 (Add)**。

步骤 3 从**接口 (Interface)** 下拉列表中，选择从其通告汇总地址的接口。

步骤 4 从**网络 (Network)** 下拉列表中，选择具有要汇总的特定 IP 地址和网络掩码的网络对象。要添加新的网络，请点击 **添加** (+)。有关添加网络的过程，请参阅网络，第 2658 页。

步骤 5 在 **管理距离** 字段中，输入汇总路由的管理距离。有效值范围为 1 到 255。

步骤 6 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 接口设置

您可以在“接口”(Interfaces) 选项卡中配置接口特定的 EIGRP 路由属性。

过程

步骤 1 在 **EIGRP** 页面上，点击**接口 (Interfaces)** 选项卡。

步骤 2 请点击 **添加** (+)。

步骤 3 从**接口 (Interface)** 下拉列表中，选择要应用配置的接口的名称。

步骤 4 在 **Hello 间隔 (Hello Interval)** 字段中，输入在接口上发送 EIGRP 呼叫数据包的间隔（以秒为单位）。有效值范围为 1 到 65535。默认值为 5 秒。

步骤 5 在**保持时间 (Hold Time)** 字段中，输入设备在 EIGRP Hello 数据包中进行通告的保持时间。有效值范围为 3 到 65535。默认值为 15 秒。

步骤 6 要在接口上启用 EIGRP 水平分割，请点击**水平分割 (Split Horizon)** 复选框。

步骤 7 在**延迟时间 (Delay Time)** 字段中输入延迟时间，以十微秒为单位。有效值范围为 1 至 16777215。在多情景模式下，设备不支持此选项。

步骤 8 指定身份验证属性的值：

- **启用 MD5 身份验证**-选中此复选框可使用 MD5 散列算法对 EIGRP 数据包进行身份验证。
- **密钥类型 (Key Type)** - 从下拉列表中选择以下任一密钥类型：
  - “无”(None) - 表示无需身份验证。
  - “未加密”(Unencrypted) - 指示要使用的密钥字符串是用于身份验证的明文密码。
  - “已加密”(Encrypted) - 指示要使用的密钥字符串是用于身份验证的加密密码。
  - “身份验证密钥”(Auth Key) - 指示要使用的密钥字符串是 EIGRP 身份验证密钥。
- **密钥 ID (Key ID)** - 用于对 EIGRP 更新进行身份验证的密钥的 ID。输入数字密钥标识符。有效值范围为 0 到 255。
- **密钥 (Key)** - 最多包含 17 个字符的字母数字字符串。对于加密身份验证类型，此字段应至少包含 17 个字符。
- **确认密钥 (Confirm Key)** - 重新输入密钥。

步骤 9 点击**确定**和**保存**以保存这些设置。

配置 EIGRP 高级设置

您可以配置 EIGRP 高级设置，例如路由器 ID、末节路由和邻接更改。

过程

步骤 1 在 **EIGRP** 页面上，点击**高级 (Advanced)** 选项卡。

步骤 2 在**默认路由器信息 (Default Route Information)** 下，您可以指定 EIGRP 更新中默认路由信息的发送和接收。

- 在跨区以太网通道模式中出现在非集群和集群中**路由器 ID**-输入用于标识外部路由的始发路由器的 ID。 如果收到的外部路由具有本地路由器 ID，该路由将被丢弃。要防止出现此问题，请为路由器 ID 指定全局地址。应该为每台 EIGRP 路由器配置一个唯一值。
- （仅针对处于单个接口模式的集群显示）**IPv4 地址池**—选择相关集群池值（IPv4 地址池对象）。要创建 IP 地址池，请参阅地址池，第 2630 页。
- **接受默认路由信息**-选中此复选框可将 EIGRP 配置为接受外部默认路由信息。
  - **访问列表 (Access List)** - 从**访问列表 (Access List)** 下拉列表中，指定一个标准访问列表，该列表定义接收默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加** (+) 并参阅配置标准 ACL 对象，第 2629 页了解详细程序。
- **发送默认路由信息**-选中此复选框可将 EIGRP 配置为通告外部默认路由信息。
  - **访问列表 (Access List)** - 从**访问列表 (Access List)** 下拉列表中，指定一个标准访问列表，该列表定义发送默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加** (+) 并参阅配置标准 ACL 对象，第 2629 页了解详细程序。

步骤 3 在**管理距离 (Administrative Distance)** 下，指定：

- **内部距离 (Internal Distance)** - EIGRP 内部路由的管理距离。内部路由是从同一自主系统中的其他实体学习的路由。有效值范围为 1 到 255。默认值为 90。
- **外部距离 (External Distance)** - EIGRP 外部路由的管理距离。外部路由是为其从自主系统外部的邻居学习最佳路径的路由。有效值范围为 1 到 255。默认值为 170。

步骤 4 在**邻接更改 (Adjacency Changes)** 下，指定：

- **记录邻居更改 (Log Neighbor Changes)** - 点击此复选框可启用 EIGRP 邻居邻接更改的日志记录。
- **记录邻居警告 (Log Neighbor Warnings)** - 点击此复选框可启用 EIGRP 邻居警告消息的日志记录。
- （可选）输入重复的邻居警告消息之间的时间间隔（以秒为单位）。有效值范围为 1 到 65535。系统不会记录在此间隔期间重复出现的警告。

步骤 5 在**末节 (Stub)** 下，要启用设备作为 EIGRP 末节路由进程，请选中以下一个或多个 EIGRP 末节路由进程复选框：

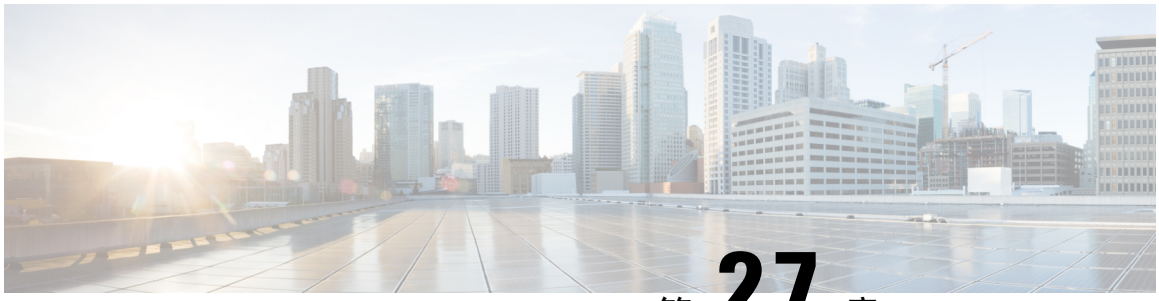
- **仅接收**-将 EIGRP 末节路由进程配置为接收来自相邻路由器的路由信息，但不向邻居发送路由信息。如果选中此选项，则不能选择任何其他末节路由选项。
- **已连接**-通告已连接路由。
- **已重新分发**-通告已连接路由。
- **静态**-通告静态路由。
- **汇总**-通告汇总路由。

步骤 6 在**默认指标 (Default Metrics)** 下，定义重分布到 EIGRP 路由进程中的路由的默认指标：

- **带宽**-路由的最小带宽（以千比特/秒为单位）。有效值范围为 1 到 4294967295。
- **延迟时间**-路由延迟（以十微秒为单位）。有效值范围为 0 到 4294967295。
- **可靠性**-数据包成功传输的可能性（以 0 到 255 的数字表示）。值 255 表示 100% 可靠；0 表示不可靠。
- **正在加载**-路由的有效带宽。有效值范围为 1 到 255；255 表示已 100% 加载。
- **MTU**-路径的最大传输单位允许的最小值，以字节表示。有效值范围为 1 到 65535。

EIGRP 的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
EIGRP 配置	7.2	任意	在之前的版本中，EIGRP 只能通过 FlexConfig 在威胁防御上进行配置。FlexConfig 不再支持 EIGRP 配置。现在，您可以在管理中心 UI 中为威胁防御配置 EIGRP 设置。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **EIGRP**。



第 27 章

BGP

本节介绍如何配置 Firewall Threat Defense，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

- 关于 BGP，第 1213 页
- BGP 的要求和前提条件，第 1216 页
- BGP 准则，第 1217 页
- 配置 BGP，第 1217 页
- BGP 的历史记录，第 1231 页

关于 BGP

BGP 是一种外部和内部自主系统路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。



注释 系统通过扫描完整的 AS 路径（在 AS_PATH 属性中指定）并检查本地系统的 AS 编号是否未出现在 AS 路径中来完成 AS 环路检测。默认情况下，EBGP 将获知的路由通告给同一对等体，以防止在执行环路检查时设备上出现额外的 CPU 周期，并避免现有传出更新任务中出现延迟。

当存在多个到达某个特定目标的路由时，通过BGP获悉的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可在路由选择过程中使用：

- 权重 - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。

- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能具有下面三个可能值中的一个，用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP，EBGP 下一跳地址会携带至本地 AS 中。但是，当下一个跃点与 eBGP 对等体的对等地址位于同一子网时，下一个跃点不会被修改。此行为称为第三方下一个跃点。

  在将 VPN 通告的路由重新分发到 iBGP 对等体时，请使用 **next-hop-self** 命令，以确保使用正确的下一跳 IP 重新分发路由。
- 社区 - 社区属性提供一种目标（称为社区）的分组方式，可对社区应用路由决策（例如，接受、首选项和重新分发）。路由映射用于设置社区属性。预定义的社区属性如下：
  - no-export - 不向 EBGP 对等体通告相应路由。
  - no-advertise - 不向任何对等体进行通告。
  - internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

BGP 也可用于通过 IPv6 网络承载有关 IPv6 前缀的路由信息。

BGP 路径选择

BGP 可能会从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径后，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。
- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 在 BGP 多路径，第 1215 页的路由表中确定是否需要安装多个路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径（最早的路径）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 多路径

BGP 多路径允许将多个等成本 BGP 路径的 IP 路由表安装到相同的目标前缀。然后，跨安装的所有路径共享到目标前缀的流量。

这些路径连同最佳路径一起安装在表中，以实现负载共享。BGP 多路径不影响最佳路径选择。例如，路由器仍会根据算法将其中一个路径指定为最佳路径，并将此最佳路径通知其 BGP 对等体。

要想成为多路径的候选对象，指向同一目标的路径需要具有与最佳路径特性相同的以下特性：

- 重量
- 本地优先级
- AS-PATH 长度
- 源代码
- 多出口鉴别器 (MED)

- 以下选项之一：
  - 相邻的 AS 或子 AS（在添加 BGP 多路径之前）
  - AS 路径（在添加 BGP 多路径之后）

某些 BGP 多路径功能对多路径候选对象有一些额外要求：

- 此路径应从外部或联盟外部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标。

这些是内部 BGP (iBGP) 多路径候选对象的额外要求：

- 此路径应从内部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标，除非路由器是面向非等成本 iBGP 多路径配置的。

BGP 可将最多 *n* 个最近收到的路径从多路候选对象插入到 IP 路由表中，其中 *n* 是要安装到路由表的路由数，如配置 BGP 多路径时所指定的那样。禁用多路径时的默认值为 1。

对于非等成本的负载平衡，您还可以使用 BGP 链路带宽。



注释 等效的下一自跳将在从 eBGP 中选择的最佳路径上执行，并且是在最佳路径转发至内部对等体之前执行。

BGP 的要求和前提条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

BGP 准则

防火墙模式准则

不支持透明防火墙模式。仅在路由模式下支持 BGP。

IPv6 准则

支持 IPv6。

其他准则

- 对于 BGP，路由的下一跳 IP 地址是网络 IP 地址，而不是 0.0.0.0。
- 系统不会在 CP 路由表中为通过 PPPoE 接收的 IP 地址添加路由条目。BGP 始终查看用于发起 TCP 会话的 CP 路由表，因此 BGP 不会形成 TCP 会话。

  因此，不支持通过 PPPoE 发送 BGP。
- 仅管理或 BVI 接口不支持 BGP。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 如果 MTU 发现失败，使用 PATH MTU (PMTU) 的 BGP 可能会导致邻接失效，特别是在 ECMP 路由情况下。因此，在使用 BGP、PMTU 和 ECMP 时一定要谨慎，因为如果 MTU 发现因任何原因失败，都可能导致数据包丢弃。
- 成员设备的 BGP 表未与控制设备表同步。仅其路由表与控制单元路由表同步。
- 使用静态或动态 VTI 接口配置基于路由的站点间 VPN 时，如果使用 BGP 作为路由协议，请确保 TTL 跳的值大于 1。

配置 BGP

要配置 BGP，请参阅下列主题：

过程

步骤 1 配置 BGP 基本设置， 第 1218 页
步骤 2 配置 BGP 常规设置， 第 1220 页
步骤 3 配置 BGP 邻居设置， 第 1221 页
步骤 4 配置 BGP 汇聚地址设置， 第 1225 页
步骤 5 配置 BGPv4 过滤设置， 第 1226 页

注释
“过滤”部分仅适用于 IPv4 设置

步骤 6 配置 BGP 网络设置，第 1227 页
步骤 7 配置 BGP 重新分发设置，第 1227 页
步骤 8 配置 BGP 路由注入设置，第 1228 页
步骤 9 配置 BGP 路由导入/导出设置，第 1229 页

配置 BGP 基本设置

可为 BGP 设置很多基本设置。

对于使用虚拟路由的设备，必须在 **BGP** 页面的**常规设置 (General Settings)** 下配置此部分中描述的基本设置。有关详细信息，请参阅 防火墙管理中心 Web 界面 - 路由页面修改，第 1113 页。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
步骤 2 选择**路由**。
步骤 3 （对于虚拟路由器感知设备）在**常规设置**下，点击 **BGP**。
步骤 4 选中**启用 BGP (Enable BGP)** 复选框以启用 BGP 路由进程。
步骤 5 在 **AS 编号**字段中，输入 BGP 进程的自治系统 (AS) 编号。AS 编号内部包含多个自主编号。AS 编号范围为从 1 至 4294967295，或从 1.0 至 65535.65535。AS 编号是一个唯一分配的值，用于在互联网上标识各个网络。
步骤 6 在**路由器 ID (Router ID)** 下拉列表中，选择自动或手动（对于非集群和跨区以太网通道模式下的集群显示）或集群池（对于单个接口模式下的集群显示）。如果选择了“自动”，则会将 Firewall Threat Defense设备上的最高级别的 IP 地址用作路由器 ID。如果选择手动，在 **IP 地址 (IP Address)** 字段中输入 IP 地址。如果选择集群池，请在**集群池 (Cluster Pool)** 字段中输入集群池值。有关创建集群池地址的信息，请参阅地址池，第 2630 页。
步骤 7 要使用固定路由器 ID，请选择“手动”，然后在 **IP 地址** 字段中输入一个 IPv4 地址。默认值是自动。对于虚拟路由器感知设备，您可以覆盖**虚拟路由器 (Virtual Routers)** > **BGP** 页面中的路由器 ID 设置。
步骤 8 （可选）从**常规**开始，编辑各项 BGP 设置。这些设置的默认值适用于大多数情况，但也可以调整它们，以适应您的网络的需求。点击 **编辑** (✎) 以编辑组中的设置：

a) 为下一跳验证输入 BGP 路由器的**扫描间隔**。有效值范围为 5 至 60 秒。默认值为 60。
b) 输入 **AS_PATH 属性中 AS 编号的数量**。AS_PATH 属性是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。有效值介于 1 与 254 之间。默认值为“无”。
c) 选中**记录邻居更改**复选框，启用对 BGP 邻居更改（向上或向下）和重置的日志记录。这有助于解决网络连接问题并衡量网络稳定性。默认情况下，此选项已启用。

d) 选中**使用 TCP 路径 MTU 发现**复选框，使用路径 MTU 确定方法确定两个 IP 主机之间网络路径上的最大传输单位 (MTU) 大小。这可以避免 IP 分片。默认情况下，此选项已启用。

e) 选中**在故障转移时重置会话**复选框，在出现链路故障后立即重置外部 BGP 会话。默认情况下，此选项已启用。

f) 选中**执行第一个 AS 作为对等体的 AS 用于 EBGP 路由**复选框，放弃从未在 AS_PATH 属性中将其 AS 编号列为首个分段的外部 BGP 对等体接收的传入更新。这可以防止错误配置或未经授权的对等体通过通告路由（如同其源自另一个自治系统）来错误定向流量。默认情况下，此选项已启用。

g) 选中**将点分表示法用于 AS 编号**复选框，将完整的二进制 4 字节 AS 编号拆分为两个单词，每个单词 16 位，以点分隔。0-65553 的 AS 编号以十进制数字表示，大于 65535 的 AS 编号使用点分表示法来表示。默认情况下将禁用此复选框。

h) 点击**确定 (OK)**。

步骤 9 （可选）编辑**最佳路径选择**部分：

a) 为 **默认本地首选项** 输入一个介于 0 与 4294967295 之间的值。默认值为 100。值越大，表示优先级越高。此首选项会发送到本地自治系统中的所有路由器和接入服务器。

b) 选中**允许比较来自不同邻居的MED**复选框，允许比较来自不同自治系统中不同邻居的路径的多出口鉴别器 (MED)。默认情况下将禁用此复选框。

c) 选中**比较相同 EBGP 路径的路由器 ID** 复选框，在最佳路径选择过程中，比较从外部 BGP 对等体接收的类似路径，并将最佳路径切换到路由器 ID 最低的路由。默认情况下将禁用此复选框。

d) 选中**在邻居 AS 通告的路径之间选择最佳 MED 路径**复选框，启用从联盟对等体获悉的路径之间的MED比较。仅当路径中没有外部自治系统时，才会比较MED。默认情况下将禁用此复选框。

e) 选中**将缺失 MED 的路径视为最不推荐的路径**复选框，将缺失 MED 的属性视为具有无穷值，从而使此路径成为最不需要使用的路径；因此，缺失 MED 的路径最不优先考虑。默认情况下将禁用此复选框。

f) 点击**确定 (OK)**。

步骤 10 （可选）编辑**邻居计时器**部分：

a) 在**保持连接时间间隔 (Keep alive interval)** 字段中，输入 BGP 邻居在不发送保持连接消息后保持活动状态的时间间隔。在此 keepalive 时间间隔结束时，如果未发送消息，则声明 BGP 对等体处于失效状态。默认值为 60 秒。

b) 在**保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的时间间隔。默认值为 180 秒。指定一个从 0 至 65535 的值。

c) （可选）在**最小保持时间**字段中，输入在发起和配置 BGP 连接期间 BGP 邻居保持活动状态的最小时间间隔。指定一个从 3 至 65535 的值。

注释
保持时间小于 20 秒会增加对等体振荡的可能性。

d) 点击**确定 (OK)**。

步骤 11 在**下一跃点**部分中，选择地选中**启用地址跟踪**复选框，以启用BGP下一跃点地址跟踪，并输入检查路由表中所安装的更新后下一跃点路由的**延迟间隔**。点击**确定 (OK)**。

注释
下一跃点部分仅适用于 IPv4 设置。

步骤 12 （可选）编辑**无中断重启**部分：

注释
仅当 Firewall Threat Defense 设备处于故障转移或跨集群模式下时，此部分才可用。此操作已经完成，以便在处于故障转移设置中的某一设备发生故障时，流量中的数据包不会被丢弃。

a) 选中 **启用无中断重启** 复选框，使 Firewall Threat Defense 对等体能在状态切换后避免路由抖动。
b) 在**重启时间**字段中，指定在收到 BGP 开放消息之前，Firewall Threat Defense对等体删除过时路由的持续时间。默认值为 120 秒。有效值介于 1 至 3600 秒之间。
c) 在 **过时路径时间** 字段中，输入 Firewall Threat Defense 在从重启 Firewall Threat Defense 收到记录终止 (EOR) 消息之后，删除过时路由之前等待的持续时间。默认值为 360 秒。有效值介于 1 至 3600 秒之间。
d) 点击**确定**。

步骤 13 点击**保存**。

步骤 14 要查看 BGP 基本设置，请从虚拟路由器下拉列表中选择所需的路由器，然后点击 **BGP**。

此页面显示在**设置 (Settings)** 页面中配置的基本设置。您可以在此页面上编辑路由器 ID 设置。

步骤 15 要编辑路由器ID设置，请修改 **IP 地址**字段中的 IP 地址。修改后的值会覆盖在 **BGP** 页面中**常规设置 (General Settings)** 下配置的路由器 ID 设置。

配置 BGP 常规设置

配置路由映射、管理路由距离、同步、下一跃点和数据包转发。这些设置的默认值适用于大多数情况，但也可以调整它们，以适应您的网络的需求。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4** 或 **IPv6**。

步骤 4 点击**常规 (General)**。

步骤 5 在**常规 (General)**选项卡中，更新以下部分：

a) 在**设置 (Settings)** 部分中，输入或选择**路由映射 (Route Map)** 对象，然后点击**确定 (OK)**。

注释
路由映射 (Route Map) 字段仅适用于 IPv4 设置。

b) 在**管理路由距离 (Administrative Route Distances)** 部分，根据需要更新以下内容，然后点击**确定 (OK)**：

- **外部** - 输入外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。此参数值的范围为 1 至 255。默认值为 20。

- **内部** - 输入内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。此参数值的范围为 1 至 255。默认值为 200。
- **本地** - 输入本地 BGP 路由的管理距离。本地路由是指通过网络路由器显示命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数值的范围为 1 至 255。默认值为 200。

c) 在 **路由和同步** 部分中，根据需要更新以下内容，然后点击 **确定**：

- （可选） **生成默认路由 (Generate default routes)** - 选择此选项的复选框以配置默认信息来源。
- （可选） **汇总子网路由至网络级路由 (Summarize subnet routes into network-level routes)** - 选中该复选框，以将子网路由配置为自动汇总到网络级路由中。此复选框仅适用于 IPv4 设置。
- （可选） **通告非活动路由 (Advertise inactive routes)** - 选中该复选框，以通告未装载至路由信息库 (RIB) 中的路由。
- （可选） **在 BGP 和 IGP 系统之间同步 (Synchronise between BGP and IGP system)** - 选择该复选框，以启用 BGP 和内部网关协议 (IGP) 系统之间的同步。通常，BGP 发言方不会向外部邻居通告路由，除非路由是本地路由或存在于 IGP 中。使用此功能，自治主系统中的路由器和接入服务器可在 BGP 将某个路由分配给其他自治系统之前获得该路由。
- （可选） **将 iBGP 重新分发到 IGP 中 (Redistribute IBGP into IGP)** - 选中该复选框，以将 iBGP 配置为重新分发到内部网关协议 (IGP) 中，例如 OSPF。

d) 在**在多个路径上转发数据包**部分中，根据需要更新以下内容，并点击**确定**：

- （可选）**路径数 (Number of Paths)** - 输入可以安装在路由表中的边界网关协议路由的最大数量。值的范围是从 1 到 8。默认值为 1。
- （可选）**IBGP 路径数 (IBGP Number of Paths)** - 输入可以安装在路由表中的并行内部边界网关协议 (iBGP) 路由的最大数目。值的范围是从 1 到 8。默认值为 1。

步骤 6 点击**保存**。

配置 BGP 邻居设置

在交换更新之前，BGP 路由器必须与其每个对等体连接。这些对等体称为 BGP 邻居。执行此程序以定义 BGP IPv4 或 IPv6 邻居及邻居设置。

过程

步骤 1 在“设备管理”(Device Management) 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击 **Neighbor**。

步骤 5 点击**添加**以定义 BGP 邻居及邻居设置。

步骤 6 输入 BGP 邻居的 **IP 地址**。此 IP 地址会添加到 BGP 邻居表。在静态 VTI 上配置 BGP IPv6 时，请输入邻居的虚拟隧道 IP 地址。

步骤 7 选择 BGP 邻居**接口**。

注释
接口字段仅适用于 IPv6 设置。

步骤 8 在**远程 AS** 字段中，输入 BGP 邻居所属的自治系统。

步骤 9 选中**启用地址 (Enabled address)** 复选框以启用与此BGP邻居的通信。仅当选中“已启用地址”复选框时，才会配置进一步的邻居设置。

步骤 10 (仅当路由不会导致环路时，才使用此选项。) 选中 **AS 覆盖 (AS Override)** 复选框，以使用发送 BGP 路由器的 AS 编号覆盖源路由器的 AS 编号。

注释
BGP 中的环路预防是通过验证 AS 路径中的 AS 号来实现的。当 AS 路径属性包含自己的 AS 号时，BGP 会拒绝路由更新。但是，在不连续网段使用相同 ASN 的情况下，为了建立端到端的可达性，可以选择用发送 BGP 路由器的 AS 号覆盖 AS 号。

步骤 11 （可选）选中**以管理员身份关闭 (Shutdown administratively)** 复选框，以禁用邻居或对等体组。

步骤 12 （可选）选中**配置平稳重启（故障转移 / 跨区模式）(Configure graceful restart [failover / spanned mode])** 复选框，以为此邻居启用 BGP 平稳重启功能的配置。选择此选项后，必须选中 **启用平稳重启 (Enable graceful restart)** 复选框来指定对此邻居启用还是禁用平稳重启。

注释
- 仅当设备处于 HA 模式或配置了 L2 集群（来自同一网络的所有节点）时，才会启用平稳重启。
- BGPv6 的平稳重启选项仅在 Firewall Threat Defense 版本 7.3 上启用。
- 如果仅在常规设置而不是 BGP IPv6 中配置平稳重启，则全局常规设置配置仍然存在。
- 如果在常规设置和 BGP IPv6 中配置平稳重启，则全局常规设置配置将被 BGP IPv6 配置设置覆盖。

步骤 13 （可选）要为 BGP 启用 BFD 支持配置，请从 **BFD 故障转移 (BFD Fallover)** 下拉列表中选择 BFD 类型 - 单跳、多跳或自动检测跳。该选择会注册 BGP 邻居以接收来自 BFD 的转发路径检测失败消息。如果您不想获得 BFD 支持，请选择“无”(None)。

步骤 14 （可选）输入 BGP 邻居的**说明**。

步骤 15 （可选）从**更新源 (Update Source)** 下拉列表中选择 BGP 数据包源接口。

您可以选择环回地址作为此接口，以克服路径故障。您还可以选择任何物理接口、端口通道或子接口。

步骤 16 （可选）在**过滤路由**中，根据需要使用访问列表、路由映射、前缀列表和AS路径过滤器来分发BGP邻居信息。更新以下部分：

a) 选择适当的传入或传出**访问列表**以分发 BGP 邻居信息。

注释
访问列表仅适用于 IPv4 设置。

b) 选择适当的传入或传出**路由映射**以将路由映射应用到传入或传出路由。

c) 选择适当的传入或传出**前缀列表**以分发 BGP 邻居信息。

d) 选择适当的传入或传出**AS 路径过滤器**以分发 BGP 邻居信息。

e) 选中**限制允许从邻居接收的前缀数量 (Limit the number of prefixes allowed from the neighbor)** 复选框，以控制可以从邻居接收的前缀的数量。

- 在**最大前缀数**字段中，输入允许从特定邻居接收的前缀的最大数量。
- 在**阈值级别**字段中，输入路由器开始生成警告消息时所处的（最大值的）百分比。有效值是介于 1 和 100 之间的整数。默认值为 75。

f) 选中**控制从对等体接收的前缀 (Control prefixes received from the peer)** 复选框，以指定对从对等体接收的前缀的额外控制。执行以下操作之一：

- 选中**超出前缀限制时终止对等 (Terminate peering when prefix limit is exceeded)** 复选框，以在达到前缀限制时停止 BGP 邻居。在 **Restart interval** 字段中，指定 BGP 邻居重新启动前的间隔。
- 选中**仅在超出前缀限制时发出警报消息 (Give only warning message when prefix limit is exceeded)** 复选框，以在达到最大前缀限制时生成日志消息。此时将不会终止 BGP 邻居。

g) 点击**确定 (OK)**。

步骤 17 （可选）在**路由**中，指定其他邻居路由参数。继续更新以下内容：

a) 在**Advertisement Interval**字段中，输入前后两次发送BGP路由更新的最小间隔（以秒为单位）。有效值介于 1 与 600 之间。

b) 选中**删除传出路由更新中的专用 AS 编号 (Remove private AS numbers from outbound routing updates)** 复选框，以阻止在出站路由上通告专用 AS 编号。

c) 选中**生成默认路由 (Generate default routes)** 复选框，以允许本地路由器将默认路由 0.0.0.0 发送到邻居，以用作该邻居的默认路由。在**路由映射**字段中输入或选择允许有条件地注入路由0.0.0.0的路由映射。

d) 要添加有条件通告的路由，请点击“添加行”+。在“添加通告路由”对话框中，执行以下操作：

1. 在**通告映射 (Advertise Map)** 字段中添加或选择路由映射，如果满足现有映射或非现有映射的条件，则会通告该映射。
2. 点击**现有映射 (Exist Map)**，然后从“路由映射对象选择器”(Route Map Object Selector) 中选择路由映射。此路由映射与 BGP 表中的路由进行比较，以确定是否对通告映射路由进行通告。

3. 点击**非现有映射 (Non-Exist Map)**，然后从“路由映射对象选择器”(Route Map Object Selector)中选择路由映射。此路由映射与BGP表中的路由进行比较，以确定是否对通告映射路由进行通告。
4. 点击**确定 (OK)**。

步骤 18 在**计时器 (Timers)** 中，选中**设置 BGP 对等体的计时器 (Set timers for the BGP peer)** 复选框，以设置保持连接频率、保持时间和最小保持时间。

- **保持连接间隔 (Keep alive interval)** - 输入 Firewall Threat Defense 向邻居发送保持连接消息的频率（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 60 秒。
- **保持时间 (Hold time)** - Firewall Threat Defense 在未接收到保持连接消息后声明对等体处于失效状态的间隔（以秒为单位）。有效值介于 0 与 65535 之间。默认值为 180 秒。
- **最小保持时间** -（可选）Firewall Threat Defense 在未接收到保持连接消息后声明对等体处于失效状态的最小间隔（以秒为单位）。有效值介于 3 与 65535 之间。默认值为 3 秒。

  注释
  保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 19 在**高级**中，更新以下内容：

a) （可选）选中 **Enable Authentication** 复选框，以在两个 BGP 对等体之间的 TCP 连接上启用 MD5 身份验证。

1. 从**启用加密类型**下拉列表中选择加密类型。
2. 在**密码 (Password)** 字段中输入密码。在**确认密码 (Confirm Password)** 字段中重新输入密码。密码区分大小写，当启用 service password-encryption 命令时，长度最大为 25 个字符；未启用 service password-encryption 命令时，长度最大为 81 个字符。此字符串包含任意字母数字字符，包括空格。

   注释
   不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

b) （可选）选中**将社区属性发送到此邻居 (Send Community attribute to this neighbor)** 复选框，以指定应将社区属性发送到 BGP 邻居

c) （可选）选中**使用 FTD 作为此邻居的下一跳**复选框，将路由器配置为 BGP 发言邻居或对等体组的下一跳。

d) 选中**禁用连接验证 (Disable Connection Verification)** 复选框可为可通过单跳访问但在环回接口上配置或通过非直接连接 IP 地址配置的 eBGP 对等会话禁用连接验证过程。取消选中（默认设置）时，BGP 路由过程将验证单跳 eBGP 对等会话 (TTL=254) 的连接，以确定 eBGP 对等体在默认情况下是否直接连接到相同的网段。如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。

e) 选择**允许连接未直接连接的邻居**，以接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接。（可选）在 **TTL hops** 字段中输入生存时间。有效值介于 1 与 255 之间。但是，对于 eBGP 多跳邻居配置，您必须输入 **TTL 跳数**值。或者，选择**有限的 TTL 跳数到邻居**，以保护 BGP 对

等会话。在 **TTL hops** 字段中，输入用于分隔 eBGP 对等体的最大跳数。有效值介于 1 与 254 之间。

f) （可选）选中**使用 TCP MTU 路径发现**复选框，为 BGP 会话启用 TCP 传输会话。

g) 从 **TCP 传输模式** 下拉列表中选择 TCP 连接模式。选项包括“默认”、“主动”或“被动”。

h) （可选）输入 BGP 邻居连接的**权重**。

i) 从下拉列表中选择 Firewall Threat Defense 将接受的 **BGP 版本**。版本可以设置为“仅限 4”，以强制软件仅对指定邻居使用版本 4。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

步骤 20 仅当考虑进行 AS 迁移时，才更新**迁移**。

注释
在过渡完成后，应删除 AS 迁移自定义。

a) （可选）选中 **Customize the AS number for routes received from the neighbor** 复选框，为从 eBGP 邻居接收的路由自定义 AS_PATH 属性。

b) 在**本地 AS 编号**字段中输入本地自治系统编号。有效值是从 1 到 4294967295 或 1.0 到 65535.65535 之间的任何有效自治系统编号。

c) （可选）选中**不将本地 AS 编号附加到从邻居接收的路由前 (Do not prepend local AS number to routes received from neighbor)** 复选框，以防止将本地 AS 编号附加到从 eBGP 对等体接收的任何路由前。

d) （可选）选中**将实际 AS 编号替换为从邻居接收的路由中的本地 AS 编号 (Replace real AS number with local AS number in routes received from neighbor)** 复选框，将实际自治系统编号替换为 eBGP 更新中的本地自治系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。

e) （可选）选中 **接受实际 AS 编号或从邻居接收的路由中的本地 AS 编号 (Accept either real AS number or local AS number in routesreceived from neighbor)** 复选框，将 eBGP 邻居配置为使用实际自治系统号（来自本地 BGP 路由过程）或使用本地自治系统编号建立对等会话。

步骤 21 点击**确定**。

步骤 22 点击**保存**。

配置 BGP 汇聚地址设置

BGP邻居存储和交换路由信息，随着配置的BGP发言方的增加，路由信息的量也随之增加。路由聚合是将多个不同路由的属性组合在一起的过程，以便仅通告一个路由。聚合前缀使用无类别域内路由 (CIDR) 原则将相邻的网络合并成一个可在路由表中汇总的无类别 IP 地址集。因此，通告的路由更少。使用“添加/编辑汇聚地址”对话框可将特定路由的聚合定义到一个路由中。

过程

步骤 1 编辑 Firewall Threat Defense 设备时，点击 **路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击添加汇聚地址 **(Add Aggregate Address)**。

步骤 5 在**聚合计时器**字段中，为聚合计时器指定一个值（以秒为单位）。有效值为 0 或介于 6 与 60 之间的任意值。默认值为 30。

步骤 6 点击 (+)**添加 (Add)** 并更新 **添加聚合地址 (Add Aggregate Address)** 对话框：

a) **网络** - 输入 IPv4 地址或选择所需的网络/主机对象。
b) **属性映射** -（可选）输入或选择用于设置聚合路由属性的路由映射。
c) **通告映射** -（可选）输入或选择用于选择路由的路由映射，以创建 AS_SET 源社区。
d) **隐含映射** -（可选）输入或选择用于选择要隐含的路由的路由映射。
e) **生成 AS 设置路径信息** -（可选）选中该复选框以生成自动系统设置路径信息。
f) **从更新中过滤所有路由** -（可选）选中该复选框可从更新中过滤所有更加特定的路由。
g) 点击**确定 (OK)**。

下一步做什么

- 对于 BGPv4 设置，请继续配置 BGPv4 过滤设置，第 1226 页。
- 对于 BGPv6 设置，请继续配置 BGP 网络设置，第 1227 页。

配置 BGPv4 过滤设置

过滤设置用于过滤传入的 BGP 更新中接收的路由或网络。过滤用于限制路由器所获悉或通告的路由信息。

开始之前

过滤仅适用于 BGP IPv4 路由策略。

过程

步骤 1 在“设备管理”(Device Management) 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**。

步骤 4 点击 **Filtering**。

注释
过滤 (Filtering) 字段仅适用于 IPv4 设置。

步骤 5 点击 (+)**添加 (Add)** 并更新**添加过滤器 (Add Filter)** 对话框：

a) **访问列表 (Access List)** - 选择定义在路由更新中要接收和抑制哪些网络的访问控制列表。
b) **方向 (Direction)** -（可选）选择指定是否应将过滤器应用于入站更新或出站更新的方向。

c) **协议 (Protocol)** -（可选）选择要过滤的路由进程：“无”、“BGP”、“已连接”、“OSPF”、“RIP”或“静态”。
d) **进程 ID** -（可选）输入 OSPF 路由协议的进程 ID。
e) 点击**确定**。

步骤 6 点击**保存**。

配置 BGP 网络设置

网络设置用于添加将由BGP路由过程通告的网络，以及将被检查以过滤要通告的网络的路由映射。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。
步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。
步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。
步骤 4 点击 **Networks**。
步骤 5 点击**添加 (Add)** 并更新**添加网络 (Add Networks)** 对话框：
a) **网络 (Network)** - 选择将由 BGP 路由过程通告的网络：

注释
要通告网络前缀，路由表中必须存在通往设备的路由。

要添加新的网络对象，请请参阅创建网络对象，第 2660 页。

b) （可选） **路由映射 (Route Map)** - 输入或选择应被检查以过滤要通告的网络的路由映射。如果未指定，则重新分发所有网络。要添加新的路由映射对象，请参阅路由映射，第 2685 页。
c) 点击**确定**。

步骤 6 点击**保存**。

配置 BGP 重新分发设置

重新分发设置可定义将其他路由域中的路由重新分发到 BGP 的条件。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。
步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4** 或 **IPv6**。

步骤 4 点击 **Redistribution**。

步骤 5 点击**添加**并更新**添加重新分发**对话框：

a) **源协议** - 从“源协议”下拉列表中选择要将路由重新分发到 BGP 域所使用的协议。

注释
用户定义的虚拟路由器不支持从 RIP 重新分发流量。

b) **进程 ID** - 输入所选源协议的标识符。应用至 OSPF 协议。对于使用虚拟路由的设备，此下拉列表列出了为您为其配置 BGP 设置的虚拟路由器分配的进程 ID。

c) **指标** -（可选）为重新分配的路由输入一个指标。

d) **路由映射** - 输入或选择应检查的路由映射，以便过滤要重新分发的网络。如果未指定，则重新分发所有网络。要创建新的路由映射对象，请点击 **添加** (+)。请参阅程序的配置路由映射条目以添加新的路由映射。

e) **匹配** - 用于将路由从一个路由协议重新分发到另一个路由协议的条件。路由必须与要重新分发的所选条件相匹配。您可以选择以下一个或多个匹配条件。只有在选择 OSPF 作为源协议时，才会启用这些选项。

- 内部
- 外部 1
- 外部 2
- NSSA 外部 1
- NSSA 外部 2

f) 点击**确定 (OK)**。

配置 BGP 路由注入设置

路由注入设置使您可以定义有条件地注入 BGP 路由表中的路由。

过程

步骤 1 在**设备管理 (Device Management)** 页面中，点击**路由 (Routing)**。

步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4**或 **IPv6**。

步骤 4 点击**路由注入 (Route Injection)**。

步骤 5 点击**添加 (Add)** 并更新**添加路由注入 (Add Route Injection)** 对话框：

a) **注入映射** - 输入或选择指定要注入本地 BGP 路由表的前缀的路由映射。要创建新的路由映射对象，请点击 **添加** (+)。有关添加新的路由映射的程序，请参阅配置路由映射条目。
b) **现有映射** - 输入或选择包含 BGP 发言者将跟踪的前缀的路由映射。
c) **已注入的路由将继承聚合路由的属性 (Injected routes will inherit the attributes of the aggregate route)** - 选中复选框可将已注入的路由配置为继承聚合路由的属性。
d) 点击**确定**。

步骤 6 点击**保存**。

配置 BGP 路由导入/导出设置

在BGP中，可以通过分别使用目的和源虚拟路由器的路由目标扩展社区导入或导出路由来实现虚拟路由器间路由泄漏。您可以使用路由映射来过滤所需的路由目标，而不是泄漏整个路由表。您还可以将全局虚拟路由器的路由泄漏到用户定义的虚拟路由器，反之亦然。

- 您可以将 BGP 配置为使用路由目标扩展社区在两个用户定义的虚拟路由器之间泄漏路由：
  - 使用路由目标导出，使用来自源虚拟路由器的路由目标标记路由。
  - 使用路由目标导入，将与路由目标匹配的路由导入到目的虚拟路由器。
  - 或者，您可以分别使用导出或导入路由映射来过滤来自源虚拟路由器或到目的虚拟路由器的路由。您可以通过匹配扩展社区列表来配置路由映射，以过滤路由。同样，您可以通过设置扩展社区路由目标来配置路由映射，以使用路由目标扩展社区标记路由。
- 要将路由从全局虚拟路由器导入到用户定义的虚拟路由器，需要在全局虚拟路由器导入路由映射中指定 IPv4/IPv6 路由映射，以导入到用户定义的虚拟路由器。
- 要将路由从用户定义的虚拟路由器导出到全局虚拟路由器，除了导出路由目标外，还可以指定全局虚拟路由器导出路由映射，以从用户定义的虚拟路由器导出。

BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

开始之前

- 创建虚拟路由器。
- 在虚拟路由器上启用 BGP。
- 配置 BGP ， 第 1217 页。

过程

步骤 1 在“设备管理”(Device Management) 页面中，点击**路由 (Routing)**。
步骤 2 （对于虚拟路由器感知设备）在虚拟路由器下拉列表中，选择要为其配置 BGP 的虚拟路由器。

步骤 3 选择 **BGP** > **IPv4** 或 **IPv6**。

步骤 4 （仅虚拟路由器支持）点击**路由导入/导出 (Route Import/Export)**。

步骤 5 在**路由目标导入**字段中，输入要与待导入的路由匹配的路由目标扩展社区。在部署时，与此值匹配的目标虚拟路由器的路由将导入到源虚拟路由器的 BGP 表中。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 6 在**路由目标导出**字段中，输入路由目标扩展社区，以使用路由目标值标记源虚拟路由器的路由。部署时，源虚拟路由器的路由使用此值进行标记。

注释
- 路由目标必须采用 **ASN:nn** 格式。
- 您可以以逗号分隔值的形式输入多个路由目标。
- 此值的范围为 0:1 到 65534:65535。

步骤 7 路由映射可帮助您缩小要共享的路由的范围，而不是泄漏整个路由表。路由映射过滤应用于使用指定路由目标值获取的路由列表：

a) （可选）在**用户虚拟路由器**下，从**导入路由映射**下拉列表中选择路由映射，以过滤目的虚拟路由器上的路由。

注释
用户虚拟路由器导入路由映射只有在配置了路由目标导入时才有效。

b) （可选）在**用户虚拟路由器 (User Virtual Router)** 下，从**导出路由映射 (Export Route Map)** 下拉列表中选择路由映射，以在将路由导出到其他虚拟路由器之前过滤源虚拟路由器上的路由。

注释
您可以将路由映射中的 match 和 set 子句与路由目标扩展社区列表一起使用，以根据其他条件进行过滤或使用路由目标社区值标记路由。有关详细信息，请参阅路由映射，第 2685 页。

步骤 8 要在用户定义的虚拟路由器和全局虚拟路由器之间共享路由，请在**全局虚拟路由器**下指定路由映射：

a) 要将全局虚拟路由器路由泄漏到用户定义的虚拟路由器，请从**导入路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导入用户定义的虚拟路由器。

b) 要将用户定义的虚拟路由器路由泄漏到全局虚拟路由器，请从**导出路由映射**下拉列表中选择路由映射。将 IPv4 或 IPv6 路由映射导出到全局虚拟路由器。

注释
除了指定路由映射之外，您还必须指定导出的路由目标。

注释

您可以使用路由映射对象的 match 子句过滤路由以进行泄漏。有关详细信息，请参阅路由映射，第 2685 页。

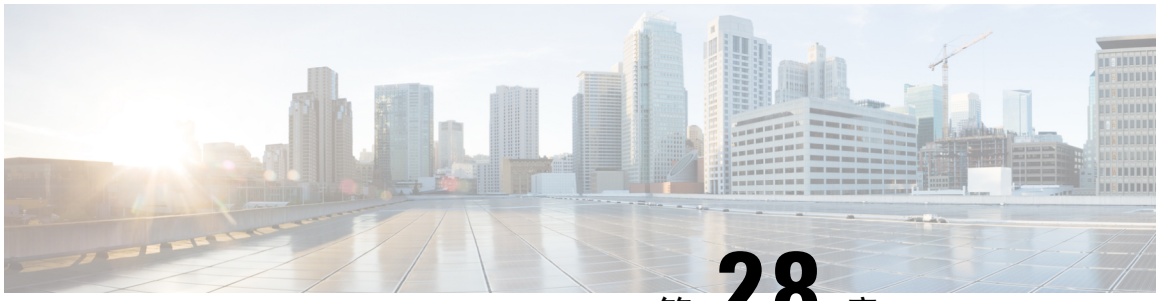
步骤 9 按照步骤（步骤 3 到步骤 8）为其他虚拟路由器配置相关的 BGP 路由导入和导出设置。

步骤 10 点击**保存 (Save)**，然后点击**部署 (Deploy)**。

当数据包流入入口虚拟路由器时，BGP 会从具有匹配路由目标值的目的虚拟路由器导入路由，如果还配置了路由映射，则会进一步过滤路由并使用这些路由来识别用于路由数据包的最佳路径路由。

BGP 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
BGP AS 覆盖	7.77.6.1	7.77.6.1	如果不连续网段使用相同的 AS 编号，则可以启用接收 BGP 路由器用发送 BGP 路由器的 AS 编号覆盖发端路由器（与接收路由器相同）的 AS 编号。 新增/修改的屏幕：**路由 (Routing)** > **BGP** > **IPv4 或 IPv6 (IPv4 or IPv6)** > **添加/编辑邻居 (Add/Edit Neighbor)**。
BGPv6 上的平稳重启支持	7.4	任意	您可以在 BGPv6 上为 Cisco Secure Firewall Threat Defense 7.3 及更高版本配置平稳重启。 新增/修改的屏幕： **路由** > **BGP** > **IPv6** > **添加/编辑邻居**。
BGP 的环回接口支持	7.4	任意	您可以将环回接口用于 BGP。 新增/修改的屏幕： **路由** > **BGP** > **IPv4 或 IPv6** > **添加/编辑邻居** 。
用于互连虚拟路由器的 BGP 配置	7.1	任意	可以将 BGP 设置配置为在用户定义的虚拟路由器之间以及全局虚拟路由器和用户定义的虚拟路由器之间动态泄漏路由。引入和导出路由功能是为了在虚拟路由器之间交换路由，方法是为它们标记路由目标，并选择性地使用路由映射过滤匹配的路由。仅当您选择用户定义的虚拟路由器时，才能访问此 BGP 功能。 新增/修改的屏幕：对于选定的用户定义的虚拟路由器，**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **BGPv4/v6** > **路由导入/导出 (Route Import/Export)** 选项卡。
BGPv6 支持用户定义的虚拟路由器	7.1	任意	Cisco Secure Firewall Threat Defense 现在支持在用户定义的虚拟路由器上配置 BGPv6。 新增/修改的屏幕：对于选定的用户定义的虚拟路由器，**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **BGPv6** 页面。



第 28 章

RIP

本章介绍如何配置 Firewall Threat Defense，以使用路由信息协议 (RIP) 来路由数据、执行身份验证以及重新分发路由信息。对于使用虚拟路由的设备，只能为其全局虚拟路由器配置 RIP，不能为其用户定义的虚拟路由器配置 RIP。

- 关于 RIP，第 1233 页
- RIP 的要求和前提条件，第 1235 页
- RIP 准则，第 1235 页
- 配置 RIP，第 1236 页

关于 RIP

路由信息协议 (RIP) 是所有路由协议中最常见的协议。RIP 有四基本组成部分：路由更新过程、RIP 路由指标、路由稳定性和路由计时器。支持 RIP 的设备将定期以及在网络拓扑更改时发送路由更新消息。这些 RIP 数据包包括有关设备可到达的网络的信息，以及数据包必须经过才能到达目标地址的路由器或网关的数量。RIP 产生的流量比 OSPF 多，但更易于配置。

RIP 是一种使用跳数作为路径选择指标的距离矢量路由协议。当在某接口上启用 RIP 时，该接口会交换与相邻设备的 RIP 广播，以动态了解和通告路由。

Cisco Secure Firewall Threat Defense 设备支持 RIP 版本 1 和 RIP 版本 2。RIP 版本 1 不通过路由更新发送子网掩码。RIP 版本 2 通过路由更新发送子网掩码，并支持可变长度的子网掩码。此外，交换路由更新时，RIP 版本 2 支持邻居身份验证。此身份验证可确保 Cisco Secure Firewall Threat Defense 设备从受信任的源接收可靠的路由信息。

RIP 比静态路由更有优势，因为初始配置比较简单，并且您不需要在拓扑更改时更新配置。RIP 的缺点是网络和处理开销比静态路由大。

路由更新过程

RIP 会定期以及在网络拓扑更改时发送路由更新消息。当路由器接收到包含对某个条目的更改的路由更新时，它将更新其路由表以反映新路由。路径的指标值增加 1，而发送器被指示为下一跳。RIP 路由器只维护到目标的最佳路由（指标值最低的路由）。更新其路由表后，路由器立即开始传输路由更新，以将此更改通知到其他网络路由器。这些更新独立于 RIP 路由器发送的定期计划更新发送。

RIP 路由指标

RIP 使用单个路由指标（跃点数）来测量源和目标网络之间的距离。从源到目标的路径中的每个跃点都分配了跃点数值，通常为 1。当路由器接收到包含新的或已更改的目标网络项的路由更新时，路由器会向更新中指示的指标数值增加 1，并将网络输入到路由表中。发送器的 IP 地址被用作下一个跃点。

RIP 稳定性功能

RIP 通过对源到目标的路径中允许的跃点数施加限制，防止无限期地执行路由循环。路径中的最大跃点数量为 15 个。如果路由器接收到包含新项或已更改项的路由更新，并且如果将跃点数增加 1 会导致跃点数无穷大（即 16），则认为网络目标不可访问。此稳定性功能的缺点是，它将 RIP 网络的最大直径限制为少于 16 个跃点。

RIP 具有许多其他路由协议所共有的一些稳定性功能。这些功能旨在提供稳定性，尽管网络拓扑可能会发生快速变化。例如，RIP 实施水平分割和抑制机制，以防止传播不正确的路由信息。

RIP 计时器

RIP 使用多个计时器来调节性能。以下是 RIP 的计时器阶段：

- 更新 - 路由更新计时器会记录定期路由更新之间的时间间隔。这是设备发送路由更新的频率。通常情况下，此间隔设置为 30 秒，每次计时器复位会随机增加少量的时间。这样做是为了防止由所有路由器同时试图更新邻居而造成的拥塞。
- 无效 - 每个路由表条目都有一个与之关联的路由超时计时器。这是设备自上次收到有效更新以来经过的秒数。路由超时计时器过期后，路由将被标记为无效，但会保留在表中，直到路由刷新计时器过期。此计时器到期后，路由将进入抑制状态。默认值为 3 分钟（180 秒）。
- 抑制 - 抑制周期是指系统在接受处于抑制状态的路由（即已标记为无效的路由）的任何新更新之前等待的秒数。默认值为 3 分钟（180 秒）。
- 刷新 - 路由刷新计时器是指从系统收到上次有效更新到路由被丢弃并从路由表中删除之前所经过的秒数。默认值为 240 秒（4 分钟）。

例如，当相邻路由器上的接口关闭时，系统不会再从相邻路由器接收路由更新。此时，无效和刷新计时器会开始计数。在前 180 秒内，什么都不会发生。180 秒后，无效计时器到期，从而让路由无效，同时抑制计时器启动并将路由额外保持 60 秒。如果仍然没有关于相邻路由器上的接口状态的更新（即它仍处于关闭状态），则该路由会进入刷新状态，其中系统从上次更新开始总共等待了 240 秒（无效计时器等待了 180 秒，抑制计时器等待了 60 秒），系统将刷新路由。即使相邻路由器的接口立即启动，系统也不会接受路由更新，直到抑制计时器完成剩余的 120 秒。

RIP 的要求和前提条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

RIP 准则

IPv6 准则

不支持 IPv6。

其他准则

以下信息仅适用于 RIP 版本 2：

- 如果适用邻居身份验证，则在为接口提供 RIP 版本 2 更新的所有邻居设备上，身份验证密钥和密钥 ID 都必须相同。
- 通过 RIP 版本 2，Cisco Secure Firewall Threat Defense 设备 将使用组播地址 224.0.0.9 传输和接收默认路由更新。在被动模式下，它将在该地址接收路由更新。
- 在接口上配置 RIP 版本 2 时，将在该接口上注册组播地址 224.0.0.9。在从接口上删除 RIP 版本 2 配置时，将取消注册该组播地址。

限制

- Cisco Secure Firewall Threat Defense 设备 不能在两个接口之间传递 RIP 更新。
- RIP 版本 1 不支持可变长度的子网掩码。
- RIP 的最大跳数为 15。跳数大于 15 的路由将被视为无法访问。
- 与其他路由协议相比，RIP 融合的速度相对较慢。
- 只能在 Cisco Secure Firewall Threat Defense 设备上启用单个 RIP 进程。

配置 RIP

RIP 是一种使用跳数作为路径选项指标的距离矢量路由协议。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由**。

步骤 3 从目录中选择 **RIP**。

步骤 4 选中 **启用 RIP** 复选框以配置 RIP 设置。

步骤 5 从 **RIP 版本** 下拉列表中选择用于发送和接收 RIP 更新的 RIP 版本。

步骤 6 （可选）选中 **生成默认路由** 复选框，以根据您指定的路由映射生成用于分发的默认路由。

a) 在**路由映射**字段中，指定要用于生成默认路由的路由映射名称。
当在**路由映射**字段中指定的路由映射存在时，将生成默认路由 0.0. 0.0/0 以便通过特定接口进行分发。

步骤 7 当发送和接收版本 2 为所选的 RIP 版本时，**启用自动摘要**选项将可用。选中 **启用自动摘要** 复选框后，将启用自动路由汇总。如果您必须在已断开连接的子网之间执行路由，则禁用自动汇总。当禁用自动汇总时，会通告子网。

注释
RIP 版本 1 始终使用自动汇总，您无法将其禁用。

步骤 8 点击 **Networks**。定义一个或多个用于 RIP 路由的网络。输入 IP 地址，或者输入或选择所需的网络/主机对象。可添加到安全设备配置的网络数量没有限制。属于此命令定义的网络的任何接口都将参与 RIP 路由过程。RIP 路由更新仅通过指定网络上的接口发送和接收。此外，如果未指定接口的网络，则在不会在任何 RIP 更新中通告该接口。

注释
RIP 仅支持 IPv4 对象。

步骤 9 （可选）点击**被动接口 (Passive Interface)**。使用此选项可以指定设备上的被动接口，以及通过扩展指定主动接口。该设备监听被动接口上的 RIP 路由广播，使用该信息填充其路由表，但不在被动接口上广播路由更新。未指定为被动的接口会接收和发送更新。

步骤 10 点击**重新分发 (Redistribution)** 可管理重新分发路由。这些路由将从其他路由进程重新分发到 RIP 路由进程。

a) 点击**添加**以指定重新分发路由。

b) 在 **协议** 下拉列表中选择要重新分发到 RIP 路由进程中的路由协议。

注释
对于 OSPF 协议，指定进程 ID。类似地，指定 BGP 的 AS 路径。在**协议**下拉列表中选择“已连接”选项时，可以将直接连接的网络重新分发到 RIP 路由进程中。

c) （可选）如果要将OSPF路由重新分发到RIP路由进程，可以在**匹配**下拉列表中选择要重新分发的特定类型的 OSPF 路由。按住 Ctrl 键并点击以选择多个类型：

- **内部** - 重新分发自治系统 (AS) 内部的路由。
- **外部 1** - 重新分发 AS 外部的类型 1 路由。
- **外部 2** - 重新分发 AS 外部的类型 2 路由。
- **NSSA 外部 1** - 重新分发末节区域 (NSSA) 外部的类型 1 路由。
- **NSSA 外部 2** - 重新分发 NSSA 外部的类型 2 路由

注释
默认设置为匹配内部、外部 1 和外部 2

d) 在**指标**下拉列表中选择要应用于重新分发的路由的 RIP 指标类型。两个选择包括：

- **透明** – 使用当前路由指标
- **指定的值** - 分配特定的指标值。在**指标值**字段中输入一个特定的值（从 0 到 16）。
- **无** - 不指定指标。不将任何指标值应用于重新分发的路由。

注释
无选项仅适用于静态和已连接协议。

e) （可选）在**路由映射**字段中输入必须满足的路由映射的名称，然后才能将路由重新分发到RIP路由进程中。只有当 IP 地址与路由映射地址列表中的允许语句匹配时，才会重新分发路由。要创建新的路由映射对象，请点击**添加**(+)。请参阅程序的配置路由映射条目以添加新的路由映射。

f) 点击**确定**。

步骤 11 （可选）点击**过滤 (Filtering)** 以管理 RIP 策略的过滤器。在本部分中，过滤器用于避免通过接口路由更新、控制路由更新中的路由通告、控制路由更新的处理以及过滤路由更新的源。

a) 点击**添加**添加 RIP 选项。

b) 在**流量方向**字段中，选择要过滤的流量类型：入站或出站。

注释
如果流量方向为入站，则只能定义接口过滤器。

c) 通过在**过滤方式 (Filter On)** 字段中进行相应的选择，指定过滤器是基于“接口”(Interface) 还是“路由”(Route)。如果点击 **接口**，则输入或选择要过滤其路由更新的接口的名称。如果点击 **路由**，则选择路由类型：

- **静态** - 仅过滤静态路由。
- **已连接** - 仅过滤连接的路由。
- **OSPF** - 仅过滤由指定的 OSPF 进程发现的 OSPFv2 路由。输入要过滤的 OSPF 进程的进程 ID。
- **BGP** - 仅过滤由指定的 BGP 进程发现的 BGPv4 路由。输入要过滤的 BGP 进程的 AS 路径。

d) 在 **访问列表** 字段中，输入或选择定义要在 RIP 路由通告中允许或删除的网络的一个或多个访问控制列表 (ACL) 的名称。若要添加新的标准访问列表对象，请点击 **添加** (+) 并参阅配置标准 ACL 对象，第 2629 页。

e) 点击**确定**。

步骤 12 （可选）点击**广播 (Broadcast)** 以添加或编辑接口配置。使用“广播”，可以覆盖要按接口发送或接收的全局 RIP 版本。如果要实施身份验证以确保有效的 RIP 更新，则还可以定义每个接口的身份验证参数。

a) 点击**添加**添加接口配置。

b) 在 **接口** 字段中输入或选择在此设备上定义的接口。

c) 在“发送”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 发送更新。这些选项使您可以为指定的接口覆盖指定的全局发送版本。

d) 在“接收”选项中，选择相应的框以指定使用 RIP **版本 1** 和/或**版本 2** 接受更新。这些选项使您可以为指定的接口覆盖指定的全局接收版本。

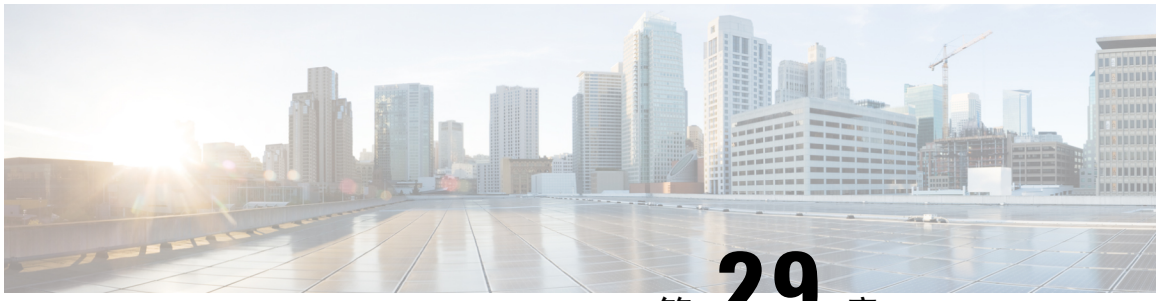
e) 选择此接口上用于 RIP 广播的**身份验证**。

- **无** - 无身份验证
- **MD5** - 使用 MD5
- **清除文本** - 使用明文身份验证

如果选择 MD5 或明文，则还必须提供以下身份验证参数。

- **密钥 ID** - 身份验证密钥的 ID。有效值为 0 至 255。
- **密钥** - 所选身份验证方法使用的密钥。最多可以包含 16 个字符。
- **确认** - 再次输入身份验证密钥以进行确认

f) 点击**确定**。



第 29 章

组播

本章介绍如何将 Cisco Secure Firewall Threat Defense 设备配置为使用组播路由协议。

- 关于组播路由，第 1239 页
- 组播路由的先决条件，第 1243 页
- 组播路由准则，第 1244 页
- 配置 IGMP 功能，第 1245 页
- 配置 PIM 功能，第 1249 页
- 配置组播路由，第 1255 页
- 配置组播边界过滤器，第 1256 页

关于组播路由

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传递给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的 Firewall 威胁防御设备 在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

Firewall 威胁防御设备 支持末节组播路由和 PIM 组播路由。但是，不能在一个 Firewall 威胁防御设备 上都配置这两种路由。

注释 组播路由同时支持 UDP 和非 UDP 传输。但是，非 UDP 传输没有进行快速路径优化。

IGMP 协议

IP 主机使用互联网组管理协议 (IGMP) 将其组成员身份报告给直连组播路由器。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

IGMP 将组地址（D 类 IP 地址）用作组标识符。主机组地址的范围可以是 224.0.0.0 到 239.255.255.255。地址 224.0.0.0 不分配给任何组。地址 224.0.0.1 分配给子网上的所有系统。地址 224.0.0.2 分配给子网上的所有路由器。



注释 如果在 Firewall Threat Defense设备上启用组播路由，IGMP V2 将会在所有接口上自动启用。

发送到组播组的查询消息

Firewall Threat Defense设备发送查询消息，以发现哪些组播组有成员位于与接口连接的网络上。成员以 IGMP 报告消息作出响应，以表明自己想要接收特定组的组播数据包。查询消息会发送到全系统组播组，该组的地址为 224.0.0.1，生存时间值为 1。

这些消息会定期发送，从而刷新Firewall Threat Defense设备上存储的成员身份信息。如果Firewall Threat Defense设备发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时，IGMP查询中通告的最大查询响应时间为10秒。如果Firewall Threat Defense设备不在此时间内接收对主机查询的响应，它就会删除该组。

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置，Firewall威胁防御设备 将用作 IGMP 受托代理。Firewall 威胁防御设备 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。Firewall 威胁防御设备 在为末节组播路由而配置后，就不能为 PIM 稀疏模式或双向模式而配置。您必须在参与 IGMP 末节组播路由的接口上启用 PIM。

Firewall 威胁防御设备 同时支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。该协议会按组播组构建以单个交汇点 (RP) 为根的单向共享树，并且可以选择性地按组播源创建最短路径数。

PIM 组播路由

双向 PIM 是 PIM-SM 的一个变体，用于构建连接组播源和接收器的双向共享树。双向树使用每个组播拓扑链路上运行的专用转发器 (DF) 选择流程构建借助 DF，组播数据从源转发至交汇点 (RP)，然后联通共享树一起发送至接收器，而无需源特定的状态。DF 选择发生在 RP 发现期间，提供至 RP 的默认路由。



注释 如果 Firewall 威胁防御设备 是 PIM RP，请使用 Firewall 威胁防御设备 的未被转换的外部地址作为 RP 地址。

PIM 稀疏模式

PIM 稀疏模式 (PIM-SM) 是一种仅在接收器明确请求时才转发流量的 PIM 模式。它使用中央交汇点 (RP) 来协调组播源与目标之间的组播流量转发。RP 是充当组播源和接收器交汇点的路由器。组播源通过其第一跳路由器注册到 RP，并通过 RP 将组播流量的副本发送给接收器。

PIM 源特定组播支持

Firewall 威胁防御设备 可以转发源特定的组播流量（例如，对于 232.x.x.x 范围中的组），即使它们不支持 PIM-SSM 配置或互联网组管理协议版本 3 (IGMPv3)。

SSM 被分类为数据传递机制，适用于一对多应用，如 IPTV。SSM 模型使用“通道”的概念，以 (S,G) 对表示，其中 S 表示源地址，G 表示 SSM 目标地址。通过使用组管理协议（如 IGMPv3）来实现订用通道。一旦SSM获悉某一特定的组播源，它将使接收客户端能直接从该源接收多播流，而不是从共享交汇点 (RP) 接收。SSM 中引入了访问控制机制，提供当前稀疏或疏-密模式实施无法提供的安全增强功能。

限制：

- Firewall 威胁防御设备 不能用作 SSM 组播的最后一跳路由器，因为它不支持 IGMPv3（接收器用于加入 SSM 组）。

  如果 Firewall 威胁防御设备 是最后一跳，它将忽略来自 SSM 组接收器的 IGMPv3 加入消息，且 SSM 转发将不起作用。

- Firewall 威胁防御设备 上的组播路由不适用于 SSM 范围 (232.x.x.x)。

解决办法

要使思科 Firewall 威胁防御设备 防火墙转发 SSM 相关的组播流量，您必须添加一台具有组播功能的第 3 层设备（例如路由器或交换机），且该第 3 层设备要在与接收器相同的网段上支持 PIM 和 IGMPv3。

工作原理：

- 接收器向此第 3 层设备注册其 SSM 组加入 (IGMPv3)。
- 此第 3 层设备会向 Firewall 威胁防御设备 发送 PIM 加入消息。
- Firewall 威胁防御设备 将接收这些 PIM 消息并动态获知组播路由。
- 然后，SSM 组播流量由 Firewall 威胁防御设备 正确转发，因为它不再是最后一跳设备。

PIM-SSM 与 PIM-SM 不同，前者不使用 RP 或共享树。相反，组播组源地址上的信息将由接收方通过本地接收协议 (IGMPv3) 提供，并且用于直接构建源特定树。

组播双向 PIM

对于有多个源和接收器相互同步交互的网络，以及每个参与者都可以同时成为多播流量的源和接收器的网络而言，多播双向 PIM （例如在视频会议、Webex 会议和分组聊天中）非常有用。当使用

PIM 双向模式时，RP 仅会为共享树创建 (*,G) 条目。没有 (S,G) 条目。这节省了 RP 上的资源，因为这样不用维护每个 (S,G) 条目的状态表。

在 PIM 稀疏模式下，流量仅会沿共享树向下流动。在 PIM 双向模式下，流量沿共享树向上和向下流动。

PIM 双向模式也不使用 PIM 寄存器/寄存器停止机制来向 RP 注册源。每个源随时都可以开始发送到源。当多播数据包到达 RP 时，这些数据包将向下转发到共享树（如果有接收器）或被丢弃（如果没有接收器）。但是，RP 无法告知源停止发送多播流量。

从设计角度看，您必须考虑在网络中放置 RP 的位置，因为该位置应为网络中源和接收器之间的中间位置。

PIM 双向模式没有反向路径转发 (RPF) 检查。相反，它使用指定转发器 (DF) 的概念来防止循环。此 DF 是网段上唯一允许向 RP 发送多播流量的路由器。如果每个网段只有一个路由器转发多播流量，则没有循环。使用以下机制选择 DF：

- 具有最低 RP 指标的路由器是 DF。
- 如果指标相等，则具有最高 IP 地址的路由器将成为 DF。

PIM 自举路由器 (BSR)

PIM 自举路由器 (BSR) 是一个动态交汇点 (RP) 选择模型，它使用候选路由器执行 RP 功能以及中继组的 RP 信息。RP 功能包括 RP 发现并向 RP 提供默认路由。它执行此操作的方式是将一组设备配置为候选 BSR (C-BSR)，它们参与 BSR 选举过程，以从它们自身中选出一个 BSR。选择 BSR 后，配置为候选交汇点 (C-RP) 的设备将开始向选出的 BSR 发送其组映射。然后，BSR 会将组与 RP 的映射信息通过基于跳从 PIM 路由器传送至 PIM 路由器的 BSR 消息发至组播树下的其他所有设备。

此功能提供了一种动态获悉 RP 的方法，这在 RP 可能会定期关闭和启动的大型负载网络中非常重要。

PIM 引导程序路由器 (BSR) 术语

以下术语经常在 PIM BSR 配置中引用：

- 自举路由器 (BSR) - BSR 通过 PIM 逐跳向其他路由器通告交汇点 (RP) 信息。在多个候选 BSR 中，在选举过程后会选择单个 BSR。此自举路由器的主要目的是将所有候选 RP (C-RP) 通告收集到称为 RP-set 的数据库中，并以 BSR 消息的形式定期（每 60 秒）将此数据库发送到该网络中的其他路由器。
- 自举路由器 (BSR) 消息— BSR 消息会组播到 TTL 为 1 的 All-PIM-Routers 组。收到这些消息的所有 PIM 邻居会将它们重新传输（TTL 同样为 1）到除收到消息的接口之外的所有接口。BSR 消息包含 RP 集合和当前活动 BSR 的 IP 地址。这是 C-RP 了解在何处单播其 C-RP 消息的方式。
- 候选自举路由器 (C-BSR) - 配置为候选 BSR 的某个设备会参与 BSR 选举机制。具有最高优先级的 C-BSR 会被选举作为 BSR。C-BSR 的最高 IP 地址作为决定因素。BSR 选举过程是优先的，例如，如果出现具有更高优先级的新 C-BSR，它会触发新的选举过程。

- 候选交汇点 (C-RP) - RP 作为组播数据源和接收器的交汇场所。配置为 C-RP 的设备会通过单播定期将组播组映射信息直接通告到选举的BSR。这些消息包含组范围、C-RP地址和保持时间。当前 BSR 的 IP 地址从网络中所有路由器收到的定期 BSR 消息获取。这样，BSR 可了解当前正在运行且可访问的 RP。



注释 Firewall 威胁防御设备 不充当 C-RP，即使 C-RP 是 BSR 流量的强制性要求也是如此。仅路由器可以充当 C-RP。因此，对于 BSR 测试功能，您必须将路由器添加到拓扑。

- BSR 选举机制 - 每个 C-BSR 都会生成包含 BSR 优先级字段的引导程序消息 (BSM)。该域中的路由器会在整个域中泛洪传播 BSM。C-BSR 收到具有比自身优先级更高的 C-BSR 时，会在特定时间内抑制进一步发送 BSM。剩余的单个 C-BSR 会成为选举的 BSR，而且其 BSM 会通知域中的所有其他路由器它是选举的 BSR。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。要接收数据流，主机必须是该组的成员。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到此组的流量。

集群

组播路由支持集群。在跨网络 EtherChannel 集群中，在快速路径转发建立之前，控制单元会发送所有的组播数据包和数据包。在建立快速路径转发后，数据单元可能会转发组播数据包。所有数据流都是全流量。同时还支持末节转发流。由于跨网络 EtherChannel 集群中仅有一台设备接收组播数据包，因此，重定向到控制单元较为常见。

组播路由的先决条件

型号支持

Firewall Threat Defense

Firewall Threat Defense Virtual

支持的域

任意

用户角色

- 管理员
- 网络管理员

组播路由准则

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

IPv6

不支持 IPv6。

组播组

保留 224.0.0.0 和 224.0.0.255 之间的地址范围用于路由协议和其他拓扑发现或维护协议，例如网关发现和组成员报告。因此，不支持来自地址范围 224.0.0/24 的互联网组播路由；为保留地址启用组播路由时，未创建 IGMP 组。

集群

在集群中，对于 IGMP 和 PIM，仅在主设备上支持此功能。

其他准则

- 必须针对入站安全区配置访问控制或预过滤器规则的，以允许流量到达组播主机（如224.1.2.3）。但不能为该规则指定目标安全区，或者不能使其在初始连接验证过程中适用于组播连接。
- 不能禁用配置了 PIM 的接口。如果已在接口上配置 PIM（请参阅配置 PIM 协议，第 1250 页），则禁用组播路由和 PIM 不会删除PIM配置。您必须移除（删除）PIM配置才能禁用接口。
- 流量区域中的接口上不支持 PIM/IGMP 组播路由。
- 请勿将 Firewall Threat Defense 同时配置为交汇点 (RP) 和第一跳路由器。
- HSRP 备用 IP 地址不参与 PIM 邻居关系。因此，如果通过 HSRP 备用 IP 地址路由 RP 路由器 IP，则 Firewall Threat Defense中组播路由不起作用。因此，要使组播流量成功通过，请确保 RP 地址的路由不是 HSRP 备用 IP 地址，而是将路由地址配置为接口 IP 地址。
- 对于使用虚拟路由的设备，只能为其全局虚拟路由器配置组播，不能为其用户定义的虚拟路由器配置组播。

配置 IGMP 功能

IP 主机使用 IGMP 向直接连接的组播路由器报告其组成员身份。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

本节介绍如何为逐个接口配置可选的 IGMP 设置。

过程

步骤 1 启用组播路由，第 1245 页。
步骤 2 配置 IGMP 协议，第 1246 页。
步骤 3 配置 IGMP 访问组，第 1247 页。
步骤 4 配置 IGMP 静态组，第 1248 页。
步骤 5 配置 IGMP 加入组，第 1248 页。

启用组播路由

默认情况下，在 Firewall Threat Defense设备上启用组播路由可以在所有接口上启用 IGMP 和 PIM。IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。PIM 用于维护转发表，以转发组播数据报。



注释 组播路由仅支持 UDP 传输层。

下表列出了特定组播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

- MFIB - 30,000
- IGMP 组 - 30,000
- PIM 路由 - 72,000

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
步骤 2 依次选择**路由** > **组播路由** > **IGMP**。
步骤 3 选中**启用组播路由**复选框。

选中此复选框可在设备上启用 IP 组播路由。取消选中此复选框将禁用 IP 组播路由。默认情况下，组播已禁用。启用组播路由可在所有接口上启用组播。

您可以逐个接口禁用组播。如果知道特定接口上没有组播接口，并且希望防止Firewall Threat Defense设备通过该接口发送主机查询消息，则此操作很有用。

配置 IGMP 协议

您可以为每个接口配置 IGMP 参数，如转发接口、查询消息和时间间隔。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **路由** > **组播路由** > **IGMP**。

步骤 3 点击**协议**选项卡，然后点击**添加**，或者编辑接口。

在**添加 IGMP 参数**对话框中，为 Firewall Threat Defense 设备配置新的 IGMP 参数。使用**编辑 IGMP 参数**对话框更改现有参数。

步骤 4 配置这些参数：

- **接口**-从下拉列表中选择要为其配置 IGMP 协议的接口。
- **启用 IGMP** - 选中该复选框可启用 IGMP。

  注释
  如果知道特定接口上没有组播主机，并且想要防止设备通过该接口发送主机查询消息，则在特定接口上禁用 IGMP 很有用。

- **转发接口**-从下拉列表中，选择要从其中转发 IGMP 消息的特定接口。

  此选项可将 Cisco Secure Firewall Threat Defense设备配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。

- **版本** - 选择 IGMP 版本 1 或 2。

  默认情况下，Firewall Threat Defense设备运行 IGMP 版本 2，这将启用多个附加功能。

  注释
  子网上所有的组播路由器必须支持同一版本的 IGMP。Firewall Threat Defense设备不会自动检测 IGMP 版本 1 路由器并切换到版本 1。但是，可以在子网上结合使用 IGMP 版本 1 和版本 2 主机；当存在 IGMP 版本 1 主机时，运行 IGMP 版本 2 的 Firewall Threat Defense设备可正常工作。

- **查询间隔** - 指定的路由器发送 IGMP 主机查询消息的间隔（以秒为单位）。范围为 1 到 3600。默认值为 125。

  注释

如果 Firewall Threat Defense 设备不能在指定超时值内在接口上收到查询消息，设备将会成为指定路由器并开始发送查询消息。

- **响应时间** - 在 Firewall Threat Defense设备删除组之前的间隔（以秒为单位）。范围为 1 到 25。默认值为 10。

  如果 Firewall Threat Defense设备未在此时间内收到对主机查询的响应，它会删除该组。

- **组限制** - 可在接口上加入的最大主机数。范围为 1 到 500。默认值为 500。

  您可以对每个接口限制 IGMP 成员身份报告造成的 IGMP 状态数量。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发

- **查询超时** - 在上一请求者停止后，Firewall Threat Defense设备成为接口请求者之前需经过的时间（以秒为单位）。范围为 60 到 300。默认值为 255。

步骤 5 点击**确定 (OK)** 以保存 IGMP 协议配置。

配置 IGMP 访问组

您可以通过使用访问控制列表控制对组播组的访问。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **路由** > **组播路由** > **访问组**。

步骤 3 在**访问组 (Access Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 访问组参数**对话框可以将新的 IGMP 访问组添加到访问组表中。使用**编辑 IGMP 访问组参数**对话框可更改现有的参数。

步骤 4 配置以下选项：

a) 从 **接口** 下拉列表中，选择与访问组关联的接口。编辑现有访问组时，不能更改相关的接口。

b) 点击以下选项之一：

- **标准访问列表**-从 **标准访问列表** 下拉列表中，选择标准 ACL 或点击 **添加** (+) 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 2629 页了解相关程序。
- **扩展访问列表**-从 **扩展访问列表** 下拉列表中，选择扩展 ACL 或点击 **添加** (+) 创建新的扩展 ACL。请参阅配置扩展 ACL 对象，第 2625 页了解相关程序。

步骤 5 点击**确定 (OK)** 以保存访问组配置。

配置 IGMP 静态组

有时，组成员无法在组中报告其成员身份，或者网络段上没有组的成员，但仍希望将该组的组播流量发送到该网络段。您可以通过配置静态加入的 IGMP 组将该组的组播流量发送到网段。使用此方法时，Firewall Threat Defense设备不会接受数据包本身，只会转发它们。因此，此方法可用于快速切换。传出接口显示在 IGMP 缓存中，但此接口不是组播组的成员。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 **路由** > **组播路由** > **IGMP**。

步骤 3 在**静态组 (Static Group)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 IGMP 静态组参数**对话框可以将组播组静态地分配给接口。使用**编辑 IGMP 静态组参数**对话框可以更改现有的静态组分配。

注释
IGMP 静态组使 PIM 能够向源或汇聚点 (RP) 发送 加入 请求，前提是使用此命令的防火墙是应用该命令的接口上的 PIM 指定路由器 (DR)。

步骤 4 配置以下选项：

- 从 **接口** 下拉列表中，选择要向其静态分配组播组的接口。如果编辑的是现有条目，则无法更改此值。
- 从 **组播组** 下拉列表中，选择要为其分配接口的组播组，或点击 **添加** (+) 创建新的组播组。有关过程，请参阅创建网络对象。

步骤 5 点击**确定 (OK)** 以保存静态组配置。

配置 IGMP 加入组

您可以将接口配置成为组播组的成员。配置 Firewall Threat Defense设备加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。

注释 如果要将特定组的组播数据包转发给接口，且无需 Firewall Threat Defense设备将这些数据包接受为该组的一部分，请参阅配置 IGMP 静态组，第 1248 页。

过程

步骤 1 选择 设备 > 设备管理，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择 路由 > 组播路由 > IGMP。

步骤 3 在加入组 (Join Group) 上，点击添加 (Add) 或编辑 (Add)。

使用添加 IGMP 加入组参数对话框可以将 Firewall Threat Defense设备配置为组播组的成员。使用编辑 IGMP 加入组参数对话框可更改现有参数。

注释
IGMP 加入组使 PIM 能够向源或汇聚点 (RP) 发送 加入 请求，前提是使用此命令的防火墙是应用该命令的接口上的 PIM 指定路由器 (DR)。

步骤 4 配置以下选项：

- 从 接口 下拉列表中，选择要作为组播组成员的接口。如果编辑的是现有条目，则无法更改此值。
- 从 加入组 下拉列表中，选择要为其分配接口的组播组，或点击 加号 创建新的组播组。有关过程，请参阅创建网络对象。

配置 PIM 功能

路由器使用 PIM 来维护转发表，以便用于转发组播图。如果在 Cisco Secure Firewall Threat Defense 设备 上启用组播路由，PIM 和 IGMP 将会在所有接口上自动启用。

注释 PAT 不支持 PIM。PIM 协议不使用端口，PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

过程

步骤 1 配置 PIM 协议，第 1250 页。

步骤 2 配置 PIM 邻居过滤器，第 1251 页。

步骤 3 配置 PIM 双向邻居过滤器，第 1251 页。

步骤 4 配置 PIM 交汇点，第 1252 页。

步骤 5 配置 PIM 路由树，第 1253 页。

步骤 6 配置 PIM 请求过滤器，第 1254 页。

步骤 7 配置组播边界过滤器，第 1256 页。

配置 PIM 协议

可以在特定接口上启用或禁用 PIM。

还可以配置指定的路由器 (DR) 优先级。指定路由器 (DR) 负责将 PIM 注册消息、加入消息和删除消息发送到 RP。如果网段上有多个组播路由器，将会根据 DR 优先级来选择 DR。如果多台设备具有同样的 DR 优先级，则具有最高 IP 地址的设备将会成为 DR。默认情况下，Firewall Threat Defense设备 的 DR 优先级为 1。

路由器查询消息用于选择 PIM DR。PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外，Firewall Threat Defense设备每隔 60 秒发送一次 PIM 加入消息或删除消息。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由 (Routing)** > **组播路由 (Multicast Routing)** > **PIM**。

步骤 3 点击**协议**选项卡，然后点击**添加**，或者编辑接口。

在**添加 PIM 参数**对话框中，为接口添加新的 PIM 参数。使用**编辑 PIM 参数**对话框可以更改现有的参数。

步骤 4 配置这些选项：

- **接口** - 从下拉列表中，选择要为其配置 PIM 协议的接口。
- **启用 PIM** - 选中该复选框以启用 PIM。
- **DR 优先级** - 所选接口的 DR 值。子网上具有最高 DR 优先级的路由器将成为指定路由器。有效值范围为 0 到 4294967294。默认 DR 优先级为 1。将此值设置为 0 会使 Firewall Threat Defense 设备接口没有资格成为指定路由器。
- **呼叫间隔** - 接口发送 PIM 呼叫消息的时间间隔（以秒为单位）。范围为 1 到 3600。默认值为 30。
- **加入删除间隔** - 接口发送 PIM 加入和删除通告的间隔（以秒为单位）。范围为 10 到 600。默认值为 60。

步骤 5 点击**确定 (OK)** 以保存 PIM 协议配置。

配置 PIM 邻居过滤器

可以定义和过滤成为协议无关组播 (PIM) 邻居的路由器，以便：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **路由** > **组播路由** > **PIM**。

步骤 3 点击**邻居过滤器**选项卡，然后点击**添加**，或者编辑接口。

在**添加 PIM 邻居过滤器**对话框中，将新的 PIM 邻居过滤器添加到接口。使用**编辑 PIM 邻居过滤器**对话框更改现有参数。

步骤 4 配置这些选项：

- 从 **接口** 下拉列表中，选择要向其添加 PIM 邻居过滤器的接口。
- **标准访问列表**- 从 **标准访问列表** 下拉列表中，选择标准 ACL 或点击 **添加** (+) 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 2629 页了解相关程序。

  注释
  在**添加标准访问列表条目**对话框上选择**允许**可以使组播组通告通过该接口。选择**阻止**将会禁止指定的组播组通告通过接口。在接口上配置组播边界时，会阻止所有的组播流量通过接口，除非使用邻居过滤器条目允许通过。

步骤 5 点击**确定**保存 PIM 邻居过滤器配置。

配置 PIM 双向邻居过滤器

PIM 双向邻居过滤器是定义可参与指定转发器 (DF) 选择的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参与 DF 选择过程。

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须双向启用分片中的所有组播路由器。

如果启用了 PIM 双向邻居过滤器，ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支双向模式，将不会发生 DF 选择。
- 如果一个被拒绝的邻居支持双向模式，将不会发生 DF 选择。

- 如果一个被拒绝的邻居不支持双向模式，可能会发生 DF 选择。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**组播路由** > **PIM**。

步骤 3 在**双向邻居过滤器 (Bidirectional Neighbor Filter)** 上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加 PIM 双向邻居过滤器**对话框可以为 PIM 双向邻居过滤器 ACL 创建 ACL 条目。使用**编辑 BFD 双向邻居过滤器**对话框可更改现有的参数。

步骤 4 配置以下选项：

- 从**接口**下拉列表中，选择要配置 PIM 双向邻居过滤器 ACL 条目的接口。
- **标准访问列表 (Standard Access List)** - 从**标准访问列表 (Standard Access List)**下拉列表中，选择标准 ACL 或点击 **添加** (+) 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 2629 页了解相关程序。

  注释
  在**添加标准访问列表条目**对话框上选择**允许**可以使指定的设备参与 DR 选择过程。选择**阻止**可阻止指定设备参与 DR 选择过程。

步骤 5 点击**确定 (OK)** 以保存 PIM 双向邻居过滤器配置。

配置 PIM 交汇点

可以将 Firewall Threat Defense设备配置为用作多个组的 RP。ACL 中指定的组范围确定 PIM RP 组映射。如果未指定 ACL，则一个组的 RP 将应用于整个组播组范围 (224.0.0.0/4)。有关双向 PIM 的更多信息，请参阅组播双向 PIM，第 1241 页。

以下限制适用于 RP：

- 一个 RP 地址不能用两次。
- 不能为多个 RP 指定所有组。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **路由** > **组播路由** > **PIM**。

步骤 3 在**交汇点 (Rendezvous Points)** 选项卡上，点击**添加 (Add)** 或**编辑 (Edit)**。

使用**添加交汇点**对话框为“交汇点”表创建新条目。使用**编辑交汇点**对话框以更改现有参数。

步骤 4 配置以下选项：

- 从 **交汇点 IP 地址** 下拉列表中，选择希望添加为 RP 的 IP 地址，或者点击 **添加** (+) 以创建新网络对象。请参阅创建网络对象了解相关程序。
- 如果指定的组播组要在双向模式下运行，请选中 **Use bi-directional forwarding** 复选框。在双向模式下，如果 Firewall Threat Defense设备接收组播数据包，且没有直连成员或 PIM 邻居，则会将删除消息发送回源。
- 点击 **将此 RP 用于所有组播组** 以便将指定的 RP 用于该接口上的所有组播组。
- 点击 **将此 RP 用于下面指定的所有组播组** ，以指定组播组与指定 RP 一起使用，然后从 **标准访问列表** 下拉列表中，选择标准 ACL，或者点击 **添加** (+) 以创建新的标准 ACL。请参阅配置标准 ACL 对象 ， 第 2629 页了解相关程序。

步骤 5 点击**确定 (OK)** 以保存交汇点配置。

配置 PIM 路由树

默认情况下，PIM 叶子路由器在第一个数据包从新源到达后会立即加入到最短路径树。此方法可降低延迟，但需要的内存比共享树多。您可以将 Firewall Threat Defense设备配置为对于所有组播组或仅对于特定组播地址加入到最短路径树或者使用共享树。

最短路径树用于未在 Multicast Groups 表中指定的任何组。“组播组”表显示与共享树配合使用的组播组。表条目按自上而下的顺序进行处理。您可以通过以下方法来创建包含一系列组播组但不包含该系列中特定组的条目：将特定组的拒绝规则放置在表的顶部，并将该系列组播组的允许规则放置在拒绝语句下面。

注释 这种行为称为最短路径状态切换 (SPT)。建议您始终使用“共享树”选项。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **路由** > **组播路由** > **PIM**。

步骤 3 在**路由树 (Route Tree)** 上，选择路由树的路径：

- 点击**最短路径 (Shortest Path)** 可为所有组播组使用最短路径树。
- 点击**共享树 (Shared Tree)** 可为所有组播组使用共享树。

- 点击**提到的以下组的共享树 (Shared tree for below mentioned group)** 以指定在“组播组”表中指定的组，然后从**标准访问列表 (Standard Access List)** 下拉列表中选择一个标准 ACL 或点击**添加** (+) 以创建新的标准 ACL。请参阅配置标准 ACL 对象，第 2629 页了解相关程序。

步骤 4 点击**确定 (OK)** 以保存路由树配置。

配置 PIM 请求过滤器

当 Firewall Threat Defense设备作为 RP 时，您可以禁止特定的组播源注册到该设备，以防止未授权的源注册到 RP。您可以定义 Firewall Threat Defense设备从其接受 PIM 寄存器消息的组播源。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择 **路由** > **组播路由** > **PIM**。

步骤 3 在**请求过滤器 (Request Filter)** 上，定义允许在 Firewall Threat Defense设备充当 RP 时向其注册的组播源：

- 从**筛选 PIM 寄存器消息使用:** 下拉列表中选择**无**、**访问列表**或**路由映射**。
- 如果从下拉列表中选择**访问列表 (Access List)**，请选择扩展 ACL 或点击 **添加** (+) 以创建新的扩展 ACL。请参阅配置扩展 ACL 对象，第 2625 页了解相关程序。

  注释
  在 **添加扩展访问列表项** 对话框中，从下拉列表中选择 **允许** 以创建允许指定的组播通信的指定源注册到 Firewall Threat Defense 设备的规则，或选择 **阻止** 以创建阻止指定的组播通信的指定源注册到设备的规则。

- 如果选择**路由地图 (Route Map)**，请从**路由地图 (Route Map)** 下拉列表中选择一个路由映射，或点击 **添加** (+) 以创建新的路由映射。有关过程请参阅创建网络对象。

步骤 4 点击**确定 (OK)** 以保存请求过滤配置。

将 Cisco Secure Firewall Threat Defense设备配置为候选自举路由器

可将 Firewall Threat Defense设备配置为候选 BSR。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择**路由** > **组播路由** > **PIM**。

步骤 3 在**引导程序路由器 (Bootstrap Router)** 上，选中**将此 FTD 配置为候选自举路由器 (C-BSR) (Configure this FTD as a Candidate Bootstrap Router [C-BSR])** 复选框，以执行 C-BSR 设置。

a) 从**接口**下拉列表中，选择 Firewall Threat Defense 设备上要从其派生 BSR 地址以使其成为候选者的接口。

此接口必须使用 PIM 启用。

b) 在**散列掩码长度**字段中，输入将在调用散列函数之前与组地址进行与运算的掩码的长度（最多 32 位）。所有具有相同种子的组都将散列（对应）到同一 RP。例如，如果此值为 24，则组地址只有前 24 位起作用。这种情况允许您为多个组获取一个 RP。范围为 0 到 32。

c) 在**优先级**字段中，输入候选 BSR 的优先级。优先选择优先级高的 BSR。如果优先级值相同，则 IP 地址较大的路由器是 BSR。范围为 0 到 255。默认值为 0。

步骤 4 （可选）在**将此 FTD 配置为边界自举路由器 (BSR)** 部分中点击 **添加** (+)，选择不会在其上发送或接收 PIM BSR 消息的接口。

- 从**接口**下拉列表中，选择不会在其上发送或接收 PIM BSR 消息的接口。

  RP 或 BSR 通告将被有效过滤，从而隔离两个域的 RP 信息交换。

- 选中**启用边界 BSR**复选框以启用 BSR。

步骤 5 点击**确定 (OK)** 以保存自举路由器配置。

配置组播路由

配置静态组播路由可以将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用GRE隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时，Firewall Threat Defense设备期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下（例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 选择**路由 (Routing)** > **组播路由 (Multicast Routing)** > **组播路由 (Multicast Routes)** > **添加或编辑 (Add or Edit)**。

使用**添加组播路由**对话框可将新的组播路由添加到 Firewall Threat Defense设备。使用**编辑组播路由**对话框可更改现有的组播路由。

步骤 3 从 **源网络** 下拉框中，选择一个现有网络或点击 **添加** (+) 以添加新网络。有关过程，请参阅创建网络对象。

步骤 4 要配置接口以转发路由，请点击**接口 (Interface)** 并配置以下选项：

- 从 **源接口** 下拉列表中，为组播路由选择传入接口。
- 从 **输出接口/密集** 下拉列表中，选择路由转发到的目标接口。
- 在**距离**字段中，输入组播路由的距离。范围为 0 到 255。

步骤 5 要配置 RPF 地址以转发路由，请点击**地址 (Address)** 并配置以下选项：

- 在 **RPF 地址**字段中，输入组播路由的 IP 地址。
- 在**距离**字段中，输入组播路由的距离，范围为 0 到 255。

步骤 6 点击**确定 (OK)** 以保存组播路由配置。

配置组播边界过滤器

地址范围定义了域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

可以在接口上为组播组地址设置管理权限界定的边界过滤器。IANA 已将 239.0.0.0 到 239.255.255.255 的组播地址范围指定为可使用管理性界定的地址。此地址范围可在不同组织管理的域中重复使用。此类地址被视为本地地址，而不是全局唯一地址。

标准ACL定义受影响地址的范围。在设置边界过滤器后，不允许组播数据包从任一方向流经边界。边界过滤器允许同一个组播组地址在不同的管理域中重复使用。

可在使用管理权限界定的边界配置、检查和过滤 Auto-RP 发现消息和通知消息。Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被删除。仅在 Auto-RP 组范围中的所有地址获得边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界过滤器。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 依次选择**路由** > **组播路由** > **组播边界过滤器**，然后点击**添加**或**编辑**。

使用**添加组播边界过滤器**对话框向设备添加新的组播边界过滤器。使用**编辑组播边界过滤器**对话框更改现有参数。

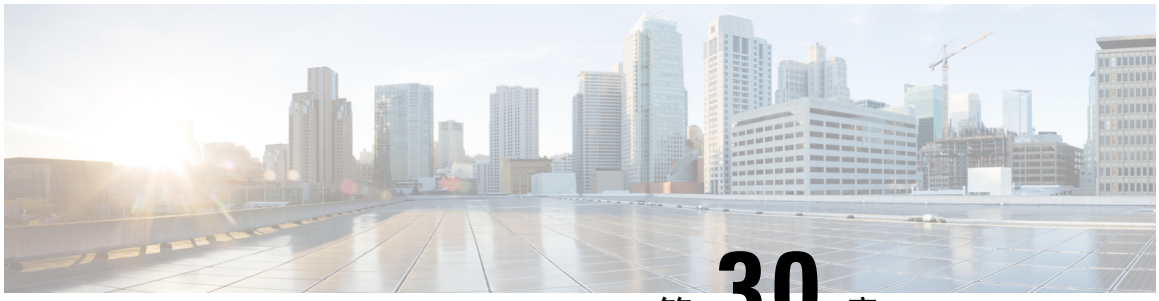
可为使用管理权限界定的组播地址配置组播边界。组播边界限制组播数据包流，并允许在不同的管理域中重复使用相同的组播组地址。在接口上定义了组播边界后，只有过滤器ACL允许的组播流量可通过接口。

步骤 3 从**接口**下拉列表中，选择为其配置组播边界过滤器 ACL 的接口。

步骤 4 从**标准访问列表**下拉列表中，选择要使用的标准 ACL，或者点击 **添加** (+) 创建新的标准 ACL。请参阅配置标准 ACL 对象，第 2629 页了解相关程序。

步骤 5 选中**删除 Auto-RP 数据包中被边界拒绝的任意 Auto-RP 组范围通知**复选框，从被边界 ACL 拒绝的源中过滤 Auto-RP 消息。如果未选中此复选框，则将允许所有 Auto-RP 消息通过。

步骤 6 点击**确定**，以保存组播边界过滤器配置。



第 30 章

策略型路由

本章介绍如何通过 防火墙管理中心 的策略型路由页面来配置 Firewall Threat Defense 以支持策略型路由 (PBR)。以下部分介绍策略型路由、PBR 的准则和 PBR 的配置。

- 策略型路由， 第 1259 页
- 策略型路由的许可证， 第 1261 页
- 策略型路由的最佳实践， 第 1261 页
- 用于确定最佳路径路由的路径监控指标， 第 1263 页
- 配置策略型路由策略， 第 1266 页
- 配置策略型路由， 第 1276 页
- 配置具有路径监控的 PBR， 第 1281 页
- 用于监控 PBR 的有用 CLI， 第 1283 页
- 对PBR进行故障排除， 第 1286 页
- 策略型路由的历史记录， 第 1288 页

策略型路由

策略型路由 (PBR) 扩展了传统路由协议，可增强对流量的控制。它支持根据目标 IP 以外的条件做出路由决策，例如源和目标端口、协议和应用。此外，PBR 可在大规模网络部署中实现安全的特定应用的流量分支。

策略型路由特征

在传统路由中，数据包会根据目的 IP 地址进行路由。在基于目的地的路由系统中，更改特定流量的路由并非易事。策略型路由 (PBR) 扩展并补充了路由协议提供的机制。

PBR 允许您设置 IP 优先。它还允许为某些流量指定路径，例如高成本链路上的优先级流量。通过 PBR，您可以定义基于目的网络以外的标准的路由，如源端口、目的地址、目的端口、协议、应用，或者这些对象的组合。

您可以使用 PBR 根据应用、用户名、组成员身份和安全组关联对网络流量进行分类。此路由方法适用于大型网络部署中众多设备访问应用程序和数据的场景。在大规模部署中，网络流量通常会通过基于路由的 VPN 以加密流量的形式回传到中心服务器。这些拓扑通常会导致诸如数据包延迟、带宽降低和数据丢包等问题。解决这些问题需要昂贵且复杂的部署和管理。

PBR 策略让您能够安全地中断指定应用的流量。您可以在 Secure Firewall Management Center 用户界面中配置 PBR 策略，以允许直接访问应用。

假设一家公司在不同位置之间有两条链路：一条是高带宽、低延迟、较为昂贵的链路，而另一条是低带宽、高延迟、不太昂贵的链路。使用传统路由协议时，高带宽链路将基于通过该链路的带宽、延迟或两者（使用 EIGRP 或 OSPF）特性所实现的指标节约而获得大部分（如果不是全部）跨该链路发送的流量。通过 PBR，您可以通过高带宽/低延迟的链路来路由优先级较高的流量，而通过低带宽/高延迟链路发送其他所有流量。

这些场景演示了基于策略的路由应用：

- **直接互联网访问**：在此拓扑中，来自分支机构的应用流量可以被直接路由到互联网，而不是通过连接到总部的 VPN 隧道。分支机构 Firewall Threat Defense 配置了互联网出口点。在入口接口（内部 *1*）上应用 PBR 策略，以便根据 ACL 中定义的应用、用户身份（用户名和组成员身份）和安全组标记（安全组关联）来识别流量。相应地，流量会通过出口接口直接转发到互联网或 IPsec VPN 隧道。
- **平等访问和源敏感路由**：在此拓扑中，来自 HR 和管理管理网络的流量可配置为通过 ISP-1，来自工程网络的流量可配置为通过 ISP-2。因此在本例中，策略型路由支持网络管理员提供同等访问权限和源敏感路由。
- **负载共享**：除 ECMP 负载均衡提供的动态负载共享功能外，网络管理员现在还可以实施策略来根据流量特征在多个路径之间分发流量。例如，在同等访问和基于源的路由场景所描绘的拓扑中，管理员可以配置策略型路由来路由从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量，从而实现负载共享。

图 *399:* 直接互联网接入场景

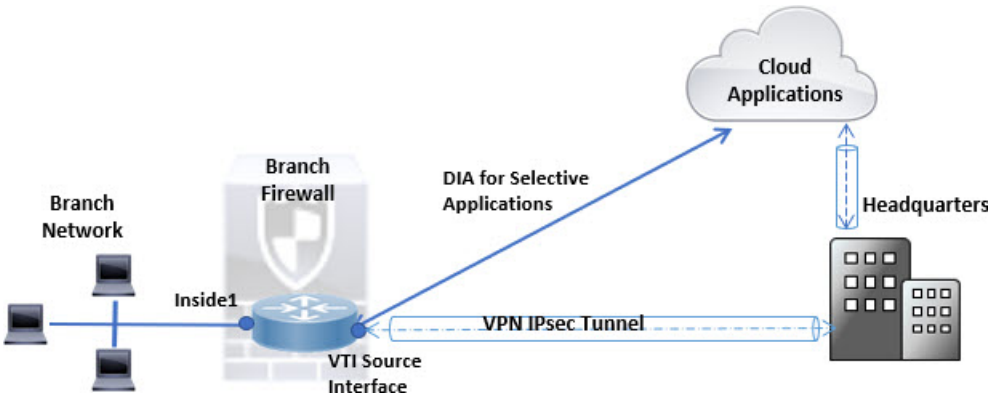
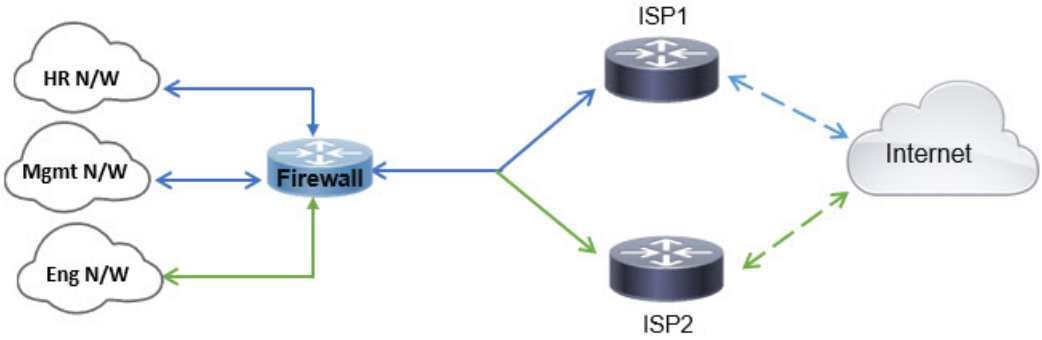


图 *400:* 平等访问场景



策略型路由的许可证

策略型路由 (PBR) 有特定的许可要求，具体取决于您的配置中使用的功能和服务。

- 所有 PBR 策略功能均受 基础版 Firewall Threat Defense 智能软件许可的支持。
- 如果要为通过 RA VPN 隧道接口来为路由流量配置 Cisco Secure 客户端，则必须拥有 PBR 许可。
- 要在 PBR 策略中使用 ISE，需要 Cisco ISE 许可证。

策略型路由的最佳实践

设备准则

在实施策略型路由时，确保版本兼容性和设备特定配置正确。

- PBR 至 防火墙管理中心 的“策略型路由”页面仅在 7.1 及更高版本的 防火墙管理中心 和 Firewall Threat Defense 设备上受支持。
- 当您将 防火墙管理中心 或 防火墙威胁防御 升级到版本 7.1 及更高版本时，设备中的 PBR 配置将被删除。您必须使用策略型路由页面再次配置 PBR。如果托管设备的版本低于 7.1，则必须使用 FlexConfig 再次配置 PBR，并将部署选项设置为“每次”。
- 在集群设备上，请勿配置基于应用、用户身份和安全组标签 (SGT) 的 PBR 策略，因为集群设备不支持这些策略。
- 在 Cisco Secure Firewall 200 型号设备上，请勿配置基于用户身份或安全组标记 (SGT) 的 PBR 策略，因为这些设备不支持这些策略。

接口准则

为 PBR 策略配置适当的接口类型和设置。

- 仅将全局虚拟路由器中的路由模式接口和非仅管理接口配置为 PBR 策略的入口或出口接口。您不能为该策略配置用户定义的虚拟路由器接口。
- 要在策略中定义的接口必须具有逻辑名称。
- 仅将静态 VTI 配置为出口接口。
- 请勿选择动态 VTI 来配置 PBR 出口接口。

您可以应用 PBR 来管理 IPv4 和 IPv6 流量。

基于应用的 PBR 和 DNS 配置

确保基于应用的 PBR 功能配置正确。

- 基于应用的 PBR 使用 DNS 监听进行应用检测。仅当 DNS 请求以明文格式通过 Firewall Threat Defense 时，应用检测才会成功； DNS 流量不会被加密。
- 您必须配置受信任的 DNS 服务器，应用检测才能成功。

有关配置 DNS 服务器的详细信息，请参阅DNS，第 977 页。

未对输出路由查询应用的 PBR 策略

策略型路由是一种仅入口功能；系统仅会将 PBR 应用于新传入连接的第一个数据包，并在此时选择连接转发支路的出口接口。请注意，如果传入数据包属于现有连接，则不会触发 PBR，或者已应用 NAT，则 NAT 选择出口接口。

PBR 策略不适用于初期流量

初期连接是指源与目标之间尚未完成必要握手的连接。在添加新的内部接口并使用唯一地址池来创建新的 VPN 策略时，PBR 将应用于与新客户端池的源匹配的外部接口。因此，PBR 会将流量从客户端发送到新接口上的下一跳。但是，在新的内部接口与客户端建立连接之前，PBR 不会处理来自主机的返回流量。因此，从主机到 VPN 客户端的返回流量（具体而言，VPN 客户端响应）会由于缺少有效路由而被丢弃。为防止响应丢失，请在内部接口上配置具有更高度量值的加权静态路由。

基于 HTTP 的路径监控准则

通过适当的接口类型和版本注意事项来配置基于 SSL 的路径监控。

- 仅在物理接口、端口通道接口、子接口和静态隧道接口上配置基于 HTTP 的路径监控。请勿在集群设备上进行配置。
- HTTP 仅使用 IPv4 对应用执行 ping 操作。IPv4 指标同时用于路由和转发 IPv4 和 IPv6 流量。
- Secure Firewall Management Center 7.4 及更高版本默认启用基于 HTTP 的应用监控。但是，从以前的版本升级时，默认情况下不启用此选项。您必须手动启用它。

其他准则

请按照以下其他配置注意事项来有效实施 PBR。

- 所有现有的配置限制和路由映射限制仍然有效。

- 在定义策略匹配条件的ACL时，您可以从列表中选择多个预定义的应用程序来形成访问控制条目 (ACE)。在 Firewall Threat Defense 中，预定义应用会被作为网络服务对象进行存储，而应用组会作为网络服务组 (NSG) 进行存储。最多可以创建 1024 个此类 NSG。应用或网络服务组会通过第一个数据包分类来检测。目前，您无法添加或修改预定义应用列表。但是，您可以创建自定义应用检测器。请参阅为 PBR 创建自定义应用检测器，第 1269 页。
- 单播反向路径转发 (uRPF) 会根据路由表而不是 PBR 路由映射来验证接口上接收的数据包的源 IP 地址。启用 uRPF 时，通过 PBR 在接口上接收的数据包将被丢弃，因为它们没有特定路由条目。因此，在使用 PBR 时，请确保禁用 uRPF。

用于确定最佳路径路由的路径监控指标

用于确定最佳路径路由的路径监控指标是一种使用各种监控方法（例如ICMP和HTTP）来收集性能指标并确定最佳路径的动态路由方法。

路径监控方法和操作

PBR 使用静态开销或路径监控（动态指标）来路由其流量。

路径监控（在接口上配置）会派生指标，例如往返时间 (RTT)、抖动、平均意见得分 (MOS) 和每个接口的丢包。这些指标会被用于确定路由 PBR 流量的最佳路径。

基于 ICMP 的路径监控方法

接口上的指标会使用 ICMP 探测消息动态收集到接口的默认网关或指定的远程对等体。

基于 HTTP 的路径监控方法

路径监控会计算与接口关联的每个远程对等体的动态指标。在监控多个应用程序并确定分支防火墙策略的最佳路径时，HTTP 比 ICMP 更受青睐，原因如下：

- HTTP-ping 可以派生到服务器的应用层的路径的性能指标，其中应用托管。
- 由于跟踪的是应用域而不是 IP 地址，因此当应用程序服务器 IP 地址更改时，无需更改防火墙配置。



注释 可以在同一接口上同时配置 ICMP 和 HTTP。如果策略中的目的地与任何域 IP 匹配，则使用相应的指标。如果目的地与任何已配置的域都不匹配，则 PBR 将使用 ICMP 中的指标来选择传出接口。

用于指标收集的默认监控计时器

对于指标收集和监控，使用以下计时器：

- 接口监控的平均间隔时间为 30 秒。此间隔时间表示探测平均值的频率。
- 接口监控器更新间隔时间为30秒。此时间间隔表示计算所收集的值的平均值并使其可用于PBR以确定最佳路由路径的频率。

- ICMP 的接口监控器探测间隔时间为一秒。此间隔时间表示发送 ICMP ping 的频率。
- HTTP 的应用监控探测间隔为 10 秒。此间隔时间表示发送 HTTP ping 的频率。路径监控使用 HTTP ping 的最后 30 个样本来计算平均指标。

注释 您不能配置或修改任何计时器的间隔时间。

PBR 和路径监控集成

在 PBR 中，流量通常会根据出口接口上配置的优先级值（接口成本）进行转发。从管理中心版本 7.2，PBR 使用基于 IP 的路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。PBR 会使用指标来确定转发流量的最佳路径（出口接口）。路径监控会定期向 PBR 通知其指标已更改的受监控接口。PBR 会从路径监控数据库中检索受监控接口的最新指标值，并更新数据路径。

只有在接口上设置了 RTT、抖动、丢包或 MOS 变量时，路径监控功能才会使用动态指标。路径监控对静态指标-接口成本（在接口中设置的成本）不起作用。

您必须为接口启用路径监控并配置监控类型。PBR 策略页面允许您为确定路径指定所需的指标。参阅配置策略型路由策略，第 1266 页。

PBR 和基于 HTTP 的路径监控

从管理中心版本 7.4 开始，可以将 PBR 配置为使用基于 HTTP 的路径监控来收集应用域的性能指标，而不仅仅是一个目的 IP 地址。仅在检测到域的 DNS 条目后才开始路径监控；配置基于 HTTP 的应用监控时，监控不会立即启动。在获取域的已解析 IP 地址后，路径监控会发送一个 HTTP 请求并接收响应。如果 DNS 为一个域解析出多个 IP 地址，则路径监控探测会使用第一个解析出的 IP 地址来监控应用。路径监控将持续进行，直到 IP 地址发生变化或基于 HTTP 的监控被禁用为止。

根据 HTTP 请求和响应持续时间，路径监控计算应用的性能指标。路径监控会定期向 PBR 发送收集的指标，以便 PBR 可以为来自已配置入口接口的流量做出路由和转发决策。如果在路径监控向 PBR 发送指标之前流量到达，则路由表决定流量流向。一旦指标可用，PBR 会使用它们为后续流量制定路由决策。

注释 根据策略的匹配 ACL 中的网络服务组，您可以对具有多个 IP 地址的多个域应用 PBR。

管理中心仅在 PBR 配置满足以下条件时才将应用和 NSG 与出口接口关联：

- 匹配 ACL 包含受监控的应用。
- 使用任一接口排序值（度量类型）配置 PBR 策略：
  - 最小抖动
  - 最大平均意见得分
  - 最短往返时间
  - 最小丢包率

配置路径监控设置

配置路径监控以收集指定接口上的RTT、抖动、MOS和丢包等指标，以便进行有效的流量管理和路由优化。

PBR 策略依靠灵活的指标（例如往返时间（RTT）、抖动、平均意见评分（MOS）和接口丢包率）来确定流量的最佳路由路径。路径监控收集指定接口上的这些指标。在**接口**页面上，您可以配置接口的路径监控设置，以发送 ICMP 探测或 或 HTTP ping 来收集指标。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击要编辑的接口的 **编辑** (✎)。

步骤 3 点击 **路径监控 (Path Monitoring)** 选项卡。

步骤 4 要配置基于 ICMP 的接口监控，请点击**启用基于 IP 的监控 (Enable IP based Monitoring)** 复选框。

步骤 5 从 **监控类型** 下拉列表中，选择相关选项：

- **自动**— 将 ICMP 探测发送到接口的 IPv4 默认网关。如果 IPv4 网关不存在，路径监控会将探测发送到接口的 IPv6 默认网关。
- **对等体 IPv4**— 将 ICMP 探测发送到指定的对等 IPv4 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv4 地址。
- **对等体 IPv6**— 将 ICMP 探测发送到指定的对等 IPv6 地址（下一跳 IP）以进行监控。如果选择此选项，请在**要监控的对等体 (Peer IP To Monitor)** 字段中输入 IPv6 地址。
- **自动 IPv4**— 将 ICMP 探测发送到接口的默认 IPv4 网关。
- **自动 IPv6**— 将 ICMP 探测发送到接口的默认 IPv6 网关。

注释

- 自动选项不适用于 VTI 接口。您必须指定对等体地址。
- 只有一个下一跳被监控到目的地。也就是说，不能为一个接口指定多个对等体地址。

步骤 6 默认情况下，**启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框处于选中状态。如果此接口配置为策略中的出口接口，则列出在 PBR 策略的匹配 ACL 中选择用于路径监控的所有应用。要禁用基于 HTTP 的接口监控，请清除此复选框。

步骤 7 点击**确定 (OK)**。

步骤 8 要保存设置，点击**保存 (Save)**。

路径监控已使用指定设置在接口上配置完毕。系统将根据您的配置使用 ICMP 探测或 HTTP Ping 收集指标，以优化路由路径。

添加路径监控控制面板

添加路径监控控制面板，以便通过预定义的关联和构件管理使用可自定义的显示选项查看路径监控指标。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

步骤 2 选择设备，然后点击**添加控制面板** (+)。

步骤 3 输入自定义控制面板的名称。

步骤 4 在**指标**区域中，点击**从预定义关联添加**按钮。

步骤 5 从列表中，点击**接口 - 路径指标**。

默认情况下，所有四个指标和一个附加指标字段均被选中，以构件的形式显示在控制面板中。要排除任何内容，请点击 **删除** (🗑)。

步骤 6 点击**添加控制面板**。

配置策略型路由策略

此任务使您能够配置策略型路由 (PBR)，以根据特定条件来控制流量路由，而不是仅仅依靠路由表来控制流量路由。

您可以通过指定入口接口，匹配条件（扩展访问控制列表）和出口接口，在“策略型路由”(Policy Based Routing) 页面中配置 PBR 策略。PBR

Before you begin

要使用路径监控指标配置出口接口上的流量转发优先级，必须为接口配置路径监控设置。请参阅配置路径监控设置 ， 第 1265 页。

按照这些步骤来配置策略型路由策略：

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 点击**策略型路由**。

在“策略型路由”页面上，您可以查看配置的策略。网格显示入口接口以及策略型路由访问列表和出口接口的组合。

步骤 4 要配置策略，请点击 **添加**。

步骤 5 在 **添加策略型路由** 对话框中，从下拉列表中选择 **入口接口** 。

注释
您只能从下拉列表中选择属于全局虚拟路由器的逻辑名称的接口。您不能将具有逻辑名称的 VLAN 接口配置为源（入口）接口。

步骤 6 要在策略中指定匹配条件和转发操作，请点击 **添加**。

步骤 7 在 **添加转发操作** 对话框中，执行以下操作：

a) 从 **Match ACL** 下拉列表中，选择扩展访问控制列表对象。您可以预定义 ACL 对象（请参阅 配置扩展 ACL 对象，第 2625 页）或点击 **添加**(+)图标创建对象。在**新建扩展访问列表对象**框中，输入名称，点击**添加**以打开**添加扩展访问列表条目**对话框，您可以在其中为 PBR 策略定义网络，端口、用户身份、SGT 或应用匹配条件。有关创建要与 PBR同步的自定义域的信息，请参阅 为 PBR 创建自定义应用检测器，第 1269 页。

注释
您可以在 ACE 中定义目的地址或应用/用户身份/SGT。

要选择性地在传入接口上应用 PBR，可以在 ACE 中定义阻止条件。当流量匹配 ACE 的阻止规则时，流量将根据路由表转发到出口接口。

b) 从 **发送至** 下拉列表：

- 要选择配置的接口，请选择 **出口接口**。
- 要指定 IPv4 / IPv6 下一跳地址，请选择 **IP 地址**。继续步骤 7.e，第 1268 页

c) 如果已选择 **出口接口**，请从 **接口顺序** 下拉列表中选择相关选项：

- 按**接口优先级 (Interface Priority)** - 按接口的优先级转发流量。流量首先路由到具有最低优先级值的接口。当接口不可用时，流量会转发到具有下一个最低优先级值的接口。例如，假设 *Gig0/1*、 *Gig0/2*和 *Gig0/3* 分别配置了优先级值 *0*、*1*和 *2* 。流量被转发到 *Gig0/1*。如果 *Gig0/1* 变得不可用，流量将被转发到 *Gig0/2*。

  注释
  要配置接口的优先级，请点击策略型路由页面上的**配置接口优先级**。在对话框中，提供接口的优先级编号，然后点击 **保存**。您还可以在 接口设置中配置接口的优先级。

  当所有接口的优先级值相同时，流量在接口之间均衡。默认情况下，设备优先级会被设为 0。PBR优先使用具有最低优先级值的接口来进行流量转发。

- 按**顺序 (Order)** - 按此处指定的接口顺序转发流量。例如，假设 *Gig0/1*、 *Gig0/2*和 *Gig0/3* 是按此顺序选择的：*Gig0/2*、*Gig0/3*、*Gig0/1*。流量首先转发到 *Gig0/2*，然后转发到 *Gig0/3*，无论其优先级值如何。
- 按**最小抖动 (Minimal Jitter)** - 流量转发到抖动值最低的接口。您需要在接口上启用路径监控，以使 PBR 获取抖动值。
- 按**最大平均意见评分 (Maximum Mean Opinion Score)** - 按流量转发到具有最大平均意见评分（MOS）的接口。您需要在接口上启用路径监控，以便 PBR 获取 MOS 值。

- 按**最小往返时间 (Minimal Round Trip Time)** - 将流量转发到具有最小往返时间 (RTT) 的接口。您需要在接口上启用路径监控，以便 PBR 获取 RTT 值。
- 按**最小数据包丢失 (Minimal Packet Loss)** - 将流量转发到具有最小数据包丢失的接口。您需要在接口上启用路径监控，以使 PBR 获取丢包值。

d) 在 **可用接口框** 中，列出所有接口及其优先级值。从接口列表中，点击 **添加** (+) 按钮以添加到所选出口接口。继续步骤 7.k，第 1269 页

注释
路由表中必须存在通往所选接口的路由。

e) 如果选择了 **IP 地址 (IP Address)**，请在 **IPv4 地址 (IPv4 Addresses)** 和 **IPv6 地址 (IPv6 Addresses)** 字段中输入用逗号分隔的 IP 地址。流量根据指定 IP 地址的顺序转发。

注释
当提供多个下一跳 IP 地址时，将按照指定 IP 地址的顺序转发流量，直至找到有效的可路由下一跳 IP 地址。所配置的下一跳应为直连式。

f) 从**不分段 (Don't Fragment)** 下拉列表中选择“是”(Yes)、“否”(No) 或“无”(None)。如果 DF（不分段）标志设置为是 *(Yes)*，则中间路由器从不执行数据包分段。

g) 要将当前接口指定为默认转发接口，请选中默认接口 (Default Interface) 复选框。

h) **IPv4 设置**和 **IPv6 设置**选项卡允许您指定递归和默认设置：

注释
对于路由映射，您只能指定 IPv4 或 IPv6 下一跳设置。

- **递归 (Recursive)** - 只有当在直连子网上找到指定的下一跳地址和默认下一跳地址时，才会应用路由映射配置。但是，您可以使用递归选项，其中的下一跳地址不需要直接连接。在这里，会对下一跳地址进行递归查询，根据路由器的当前路由路径，将匹配的流量转发到该路由条目使用的下一跳中。
- **默认 (Default)** - 如果正常路由查询无法匹配流量，则流量会被转发到此指定的下一跳 IP 地址。

i) 选中**对等体地址 (Peer Address)** 复选框，以便使用下一跳地址作为对等体地址。

注释
您不能同时使用默认下一跳地址和对等体地址配置路由映射。

j) 对于 IPv4 设置，您可以在**验证可用性 (Verify Availability)**下检查路由映射的下一跳是否可用 - 点击 **添加** (+) 按钮并添加下一跳 IP 地址条目：

- **IP Address** - 输入下一跳 IP 地址。
- **顺序 (Sequence)** - 使用序列号按顺序来评估条目。确保没有输入重复的序列号。有效范围为 1 至 65535。
- **跟踪 (Track)** - 输入有效的 ID。有效范围为 1 至 255。

k) 点击保存。

步骤 8 要保存策略，点击 **保存** 和 **部署**。

Firewall Threat Defense 使用 ACL 来匹配流量，并对流量执行路由操作。典型地，配置指定用于进行匹配的ACL的路由映射，然后为该流量指定一个或多个操作。通过使用路径监控，PBR现在可以选择最佳出口接口来路由流量。最后，将路由映射与接口相关联，在该接口上要对所有传入流量应用 PBR 。

为 PBR 创建自定义应用检测器

此任务使您能够创建自定义应用检测器并配置基于应用的PBR 策略，以增强流量控制和路由决策。

自定义应用检测器允许您识别可能未被默认检测方法涵盖的特定应用。然后，这些检测器可用于PBR策略中，以基于应用识别做出路由决策。

过程

步骤 1 为用户定义的应用创建自定义检测器，如 创建用户定义的应用。 ，第 2573 页中所述。

注释
创建用户定义的应用时，请确保从 **标记 (Tag)** 下拉列表中选择 NSG。

步骤 2 通过选择适当的检测器类型和配置方法来定义检测模式。

要手动定义检测模式，请选择 **基本** 检测器类型 (Basic Detector Type) 并继续定义检测模式，如 指定基本检测器中的检测模式，第2574 页中所述。或者，如果要使用 .lua 文件创建检测模式，请选择 **高级** 检测器类型并按照 指定高级检测器中的检测条件 ，第 2575 页中提供的说明进行操作。

步骤 3 激活自定义检测器。

步骤 4 使用自定义应用 ACE 配置 PBR 的ACL 策略（扩展）。

有关创建 ACL 的程序，请参阅 配置扩展 ACL 对象 ，第 2625 页。

步骤 5 在 PBR 策略中，选择与所需转发操作匹配的 ACL。

有关详细操作创建PBR策略，请参阅配置策略型路由策略 ，第 1266 页。

您已成功创建自定义应用检测器并配置了基于应用的PBR 策略。系统现在可以根据您的配置识别自定义应用并应用适当的路由决策。

配置带有自定义应用检测器的 PBR（基本）

此任务使用自定义应用检测器配置PBR 策略，以便使用已定义域的自定义检测器根据特定应用流量模式做出路由决策。

本示例演示了使用特定域的自定义应用检测器配置策略型路由 (PBR)，例如：

- amazon123.com
- flipkart.com
- hamleysonline.com

Before you begin

- 本示例假定您了解配置 PBR 策略和自定义应用检测器的基本步骤。
- 您应已使用逻辑名称来配置入口和出口接口。本示例中，入口接口名为 *Inside1*，而出口接口名为 *eBuy*。

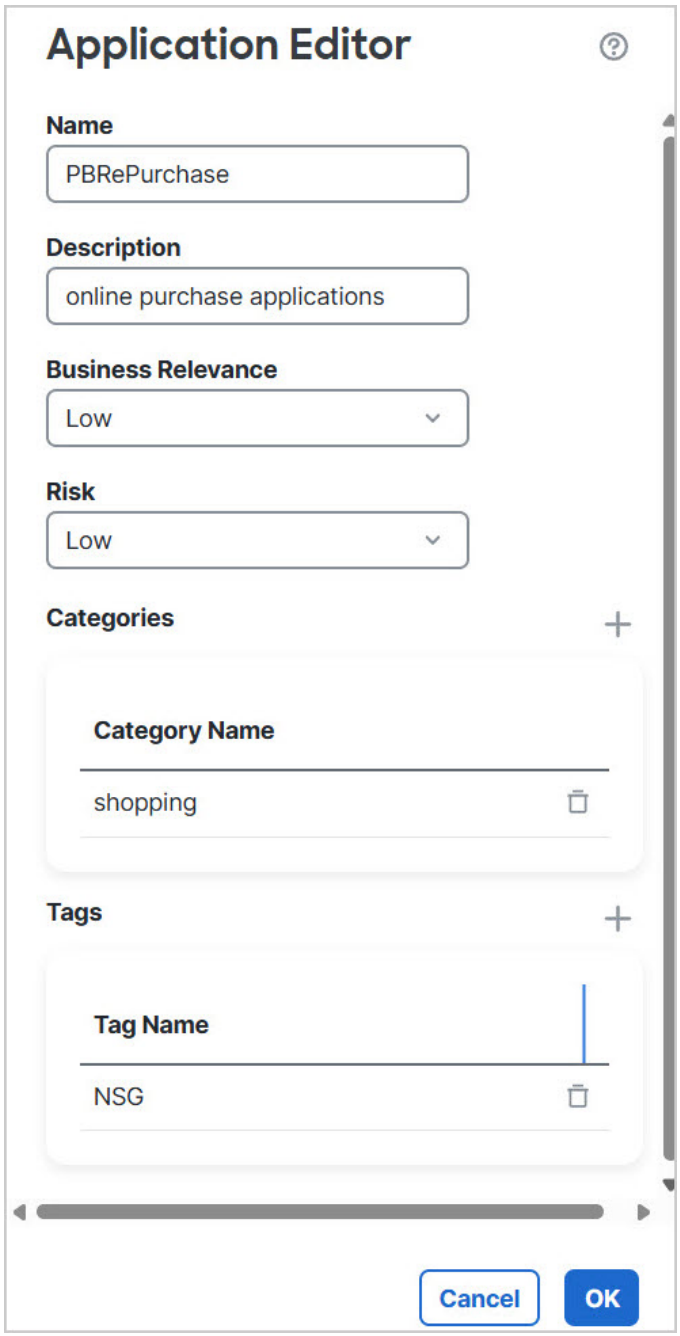
请按照以下步骤使用自定义应用检测器来配置 PBR：

过程

步骤 1 创建自定义检测器 *PBRePurchase*：

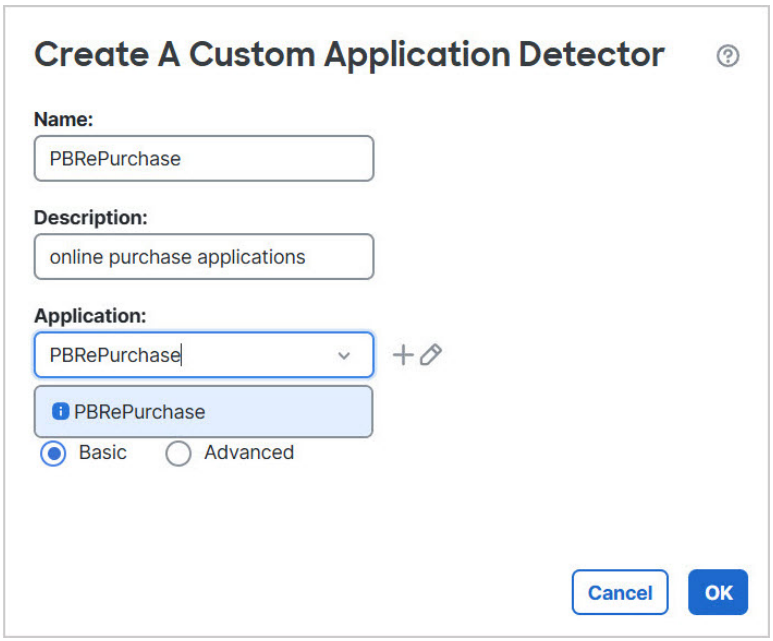
a) 选择 **策略** > **+ 显示更多** > **高级** > **自定义应用检测器**，然后点击**创建自定义检测器**。
b) 在**创建自定义应用检测器**字段中，输入名称（本示例中为 *PBRePurchase*）和说明。
c) 要创建自定义应用，请点击 (+)。
d) 在**应用编辑器**对话框的字段中输入相关值。有关每个字段的详细描述，请参阅创建用户定义的应用。，第 2573 页。

注释
要使自定义应用可被 PBR 检测到，请从**标记**下拉列表中选择 **NSG**：



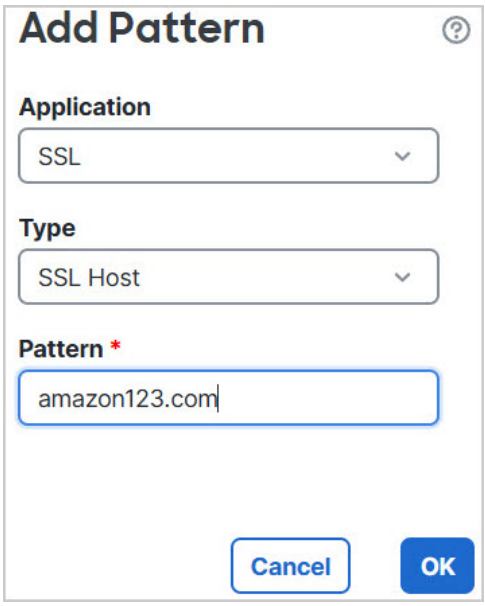
e) 点击**确定**。

f) 从**应用**下拉列表中选择 *PBRePurchase*。



注释
可以在 PBR 策略中使用**基本**或**高级**检测器类型。本示例使用**基本** 检测器类型。

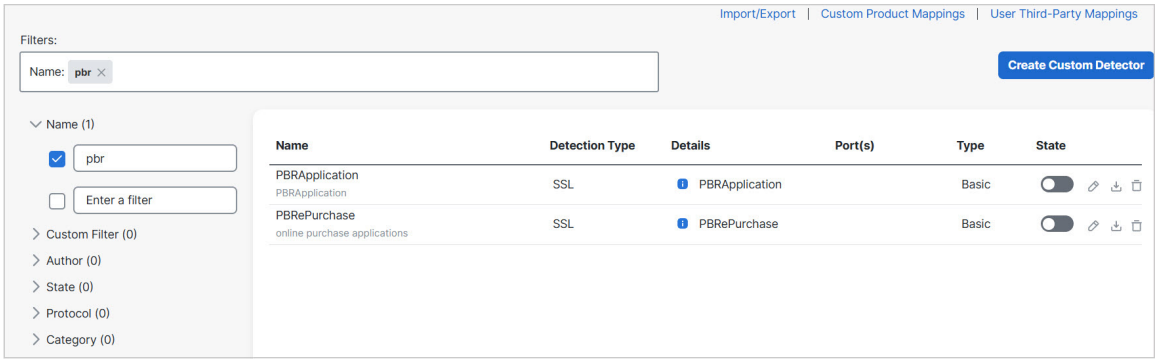
a) 点击**基本**单选按钮，然后点击**确定**。
b) 在**应用检测器**页面上，点击**检测模式**区域中的**添加**按钮以添加模式。
c) 从**应用**下拉列表中，选择 **SSL** 作为协议类型，然后选择适当的模式类型。输入与所选类型匹配的模式字符串（在本例中，输入 *amazon123.com*），然后点击**确定**。



d) 重复此过程，为自定义域 *flashing.com* 和 *hanleysonline.com* 创建另外两个模式。
e) 点击**保存**。

步骤 2 在应用检测器仪表盘中，使用过滤器搜索刚刚创建的自定义应用检测器。

步骤 3 要启用自定义检测器，请点击相应应用检测器旁边的**状态**切换按钮 ( )。



步骤 4 在显示的对话框中，点击**是**。

应用检测器激活后，将显示成功消息：



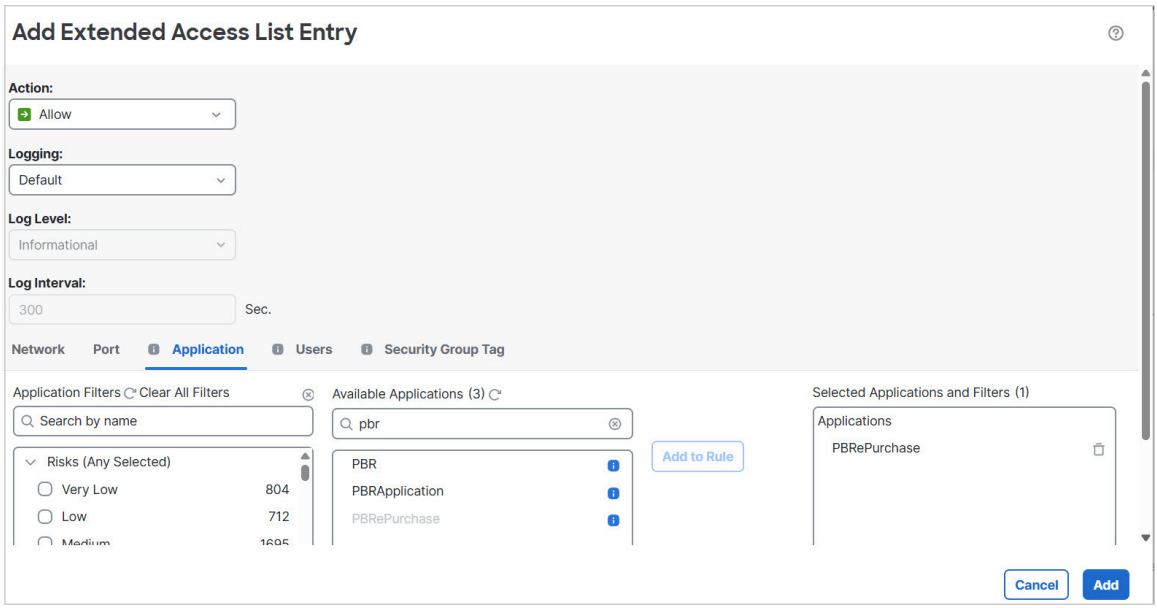
步骤 5 要使用自定义应用检测器创建 ACL 以与 PBR 策略同步：

a) 选择**对象** > **访问列表** > **扩展**。

b) 点击**添加扩展访问列表**。

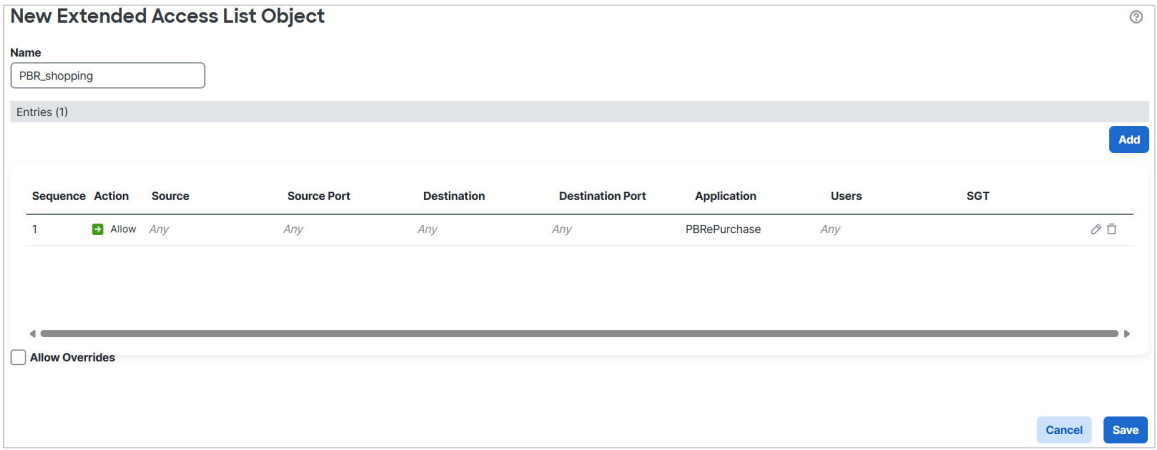
c) 为列表输入名称（例如 *PBR_sending*），然后点击**添加**为列表创建 ACE。

d) 在**添加扩展访问列表条目**对话框中，点击**应用**选项卡，选择应用名称 *PBRePurchase*，然后点击**添加到规则**。



e) 点击添加 **(Add)**。

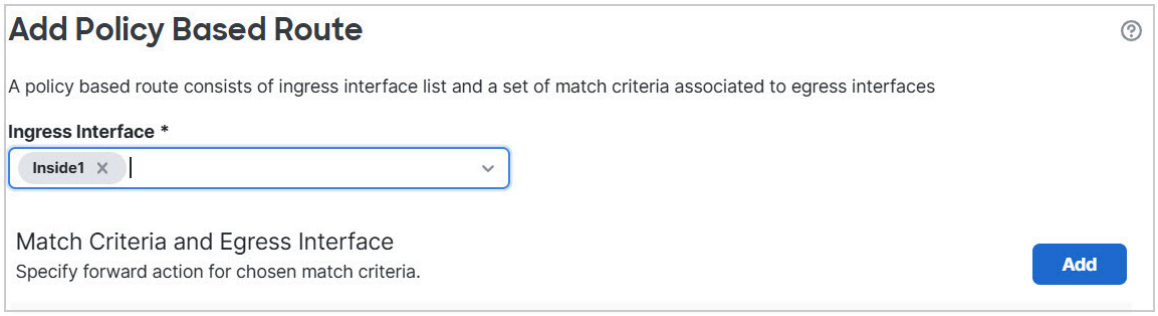
f) 点击保存。



步骤 6 选择路由 > 策略型路由。

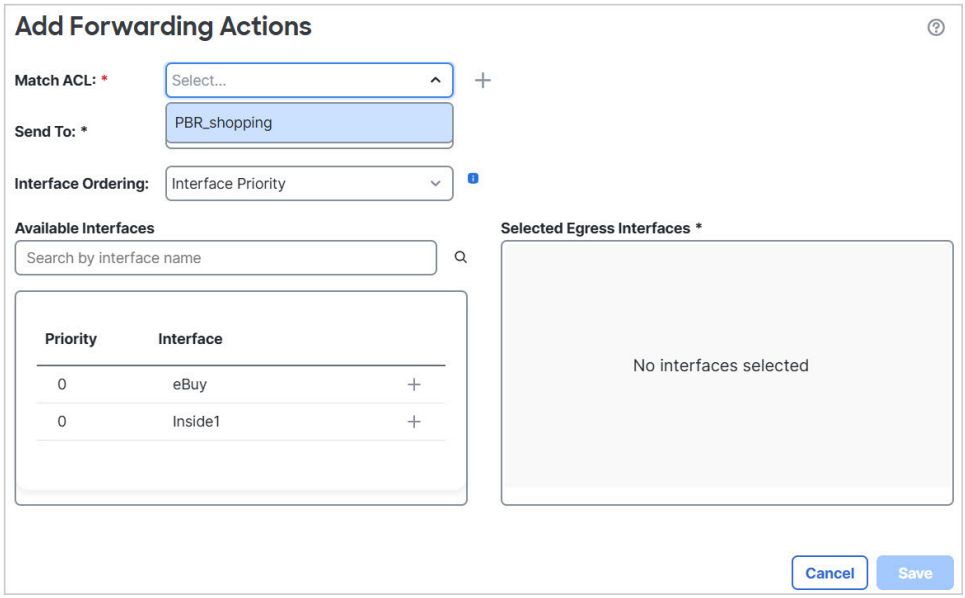
步骤 7 在显示的策略型路由页面上，点击添加。

步骤 8 在添加策略型路由对话框中，从入口接口下拉列表中选择内部 *1*。



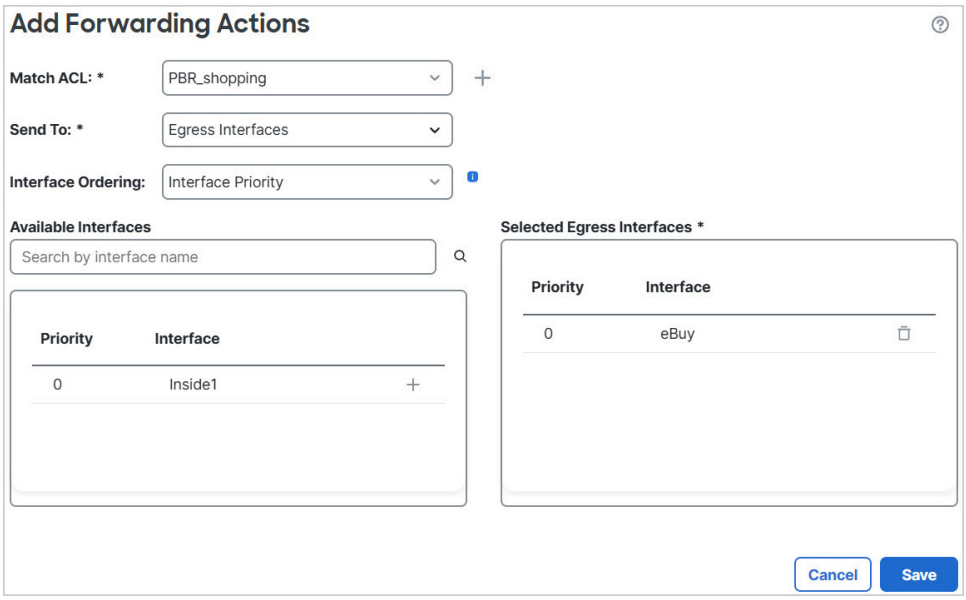
步骤 9 从**匹配 ACL** 下拉列表中，选择已创建的 ACL，在本示例中为 *PBR_sending*。

注释
在 Firewall Threat Defense 中，ACL 中的应用组配置为网络服务组。这就是我们将自定义应用标记为 **NSG** 的原因。

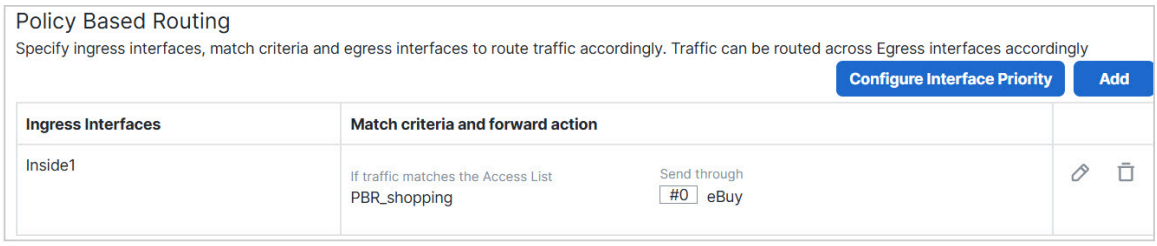


步骤 10 指定出口接口：

a) 在**发送到**下拉列表中，选择**出口接口**。
b) 从**接口排序**下拉列表中选择适当的顺序。
c) 在**可用接口**下，点击相应接口（即 *eBuy*）旁边的（+）。



d) 点击**保存**。



步骤 11 **保存**和**部署**。

使用自定义应用检测器配置和部署了 PBR 策略。与指定域匹配的流量将通过已定义的出口接口进行路由。

配置策略型路由

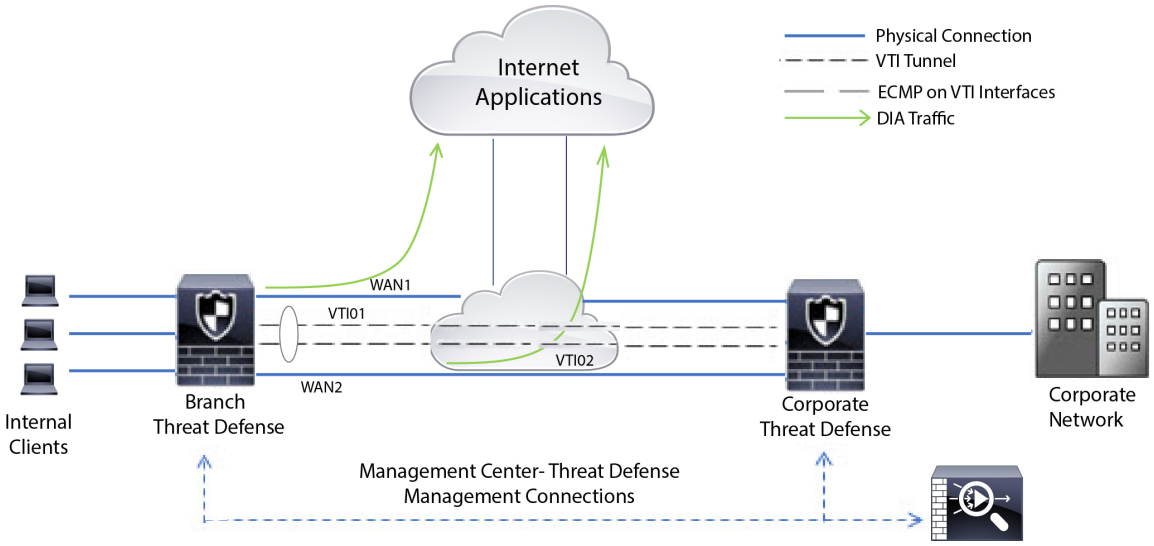
配置 PBR，为特定的基于 Web 的应用启用直连互联网访问，优化流量，并在 WAN 和 VTI 接口之间实现负载均衡。

假设一个典型的企业网络场景，其中所有分支机构网络流量都通过企业网络的基于路由的 VPN，并在需要时分流到外联网。通过企业网络访问支持日常运营的 Web 应用可能会导致网络规模扩大和维护成本增加。本示例说明如何配置 PBR 以实现直接互联网访问。

下图描述了企业网络的拓扑。分支机构网络通过基于路由的 VPN 连接到企业网络。传统上，公司 Firewall Threat Defense 会被配置为处理分支机构的内部和外部流量。通过 PBR 策略，分支机构 Firewall Threat Defense 会配置将特定流量路由到 WAN 网络而不是虚拟隧道的策略。其余流量会照常流经基于路由的 VPN。

此示例还说明了如何配置 WAN 和 VTI 接口与 ECMP 区域以实现负载均衡。

图 *401:* 在 防火墙管理中心 中的分支机构 ***Firewall Threat Defense*** 上配置策略型路由



Before you begin

此示例假定您已为 防火墙管理中心 中的分支机构 Firewall Threat Defense 配置 WAN 和 VTI 接口。

过程

步骤 1 为分支机构 Firewall Threat Defense 配置策略型路由，选择入口接口：

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。

c) 在 **添加策略型路由 (Add Policy Based Route)** 对话框中，从 **入口接口 (Ingress Interface)** 下拉列表中选择接口（也就是， 内部 *1 (Inside 1)* 和 内部 *2 (Inside 2)*）。

步骤 2 指定匹配条件：

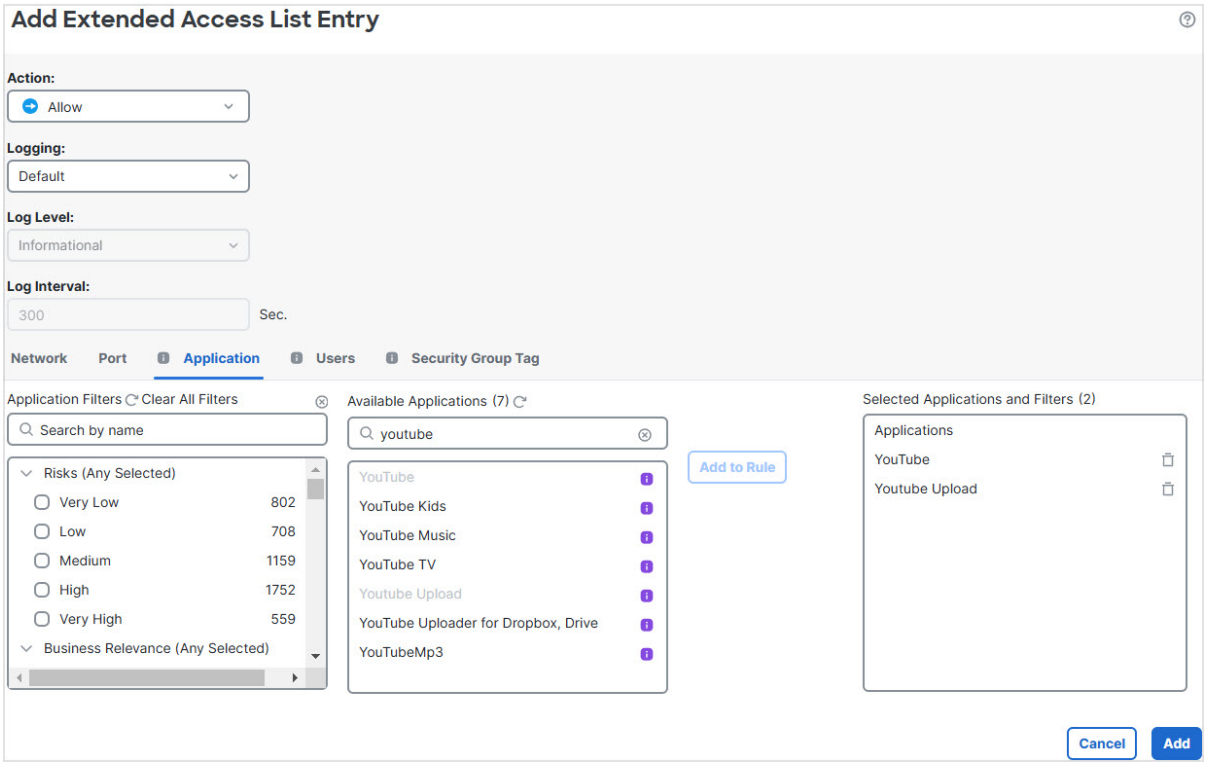
a) 点击**添加 (Add)**。

b) 要定义匹配条件，请点击 **添加** (+) 按钮。

c) 在**新建扩展访问列表对象**中，输入 ACL 的名称（例如 *DIA-FTD-Branch*），然后点击**添加**。

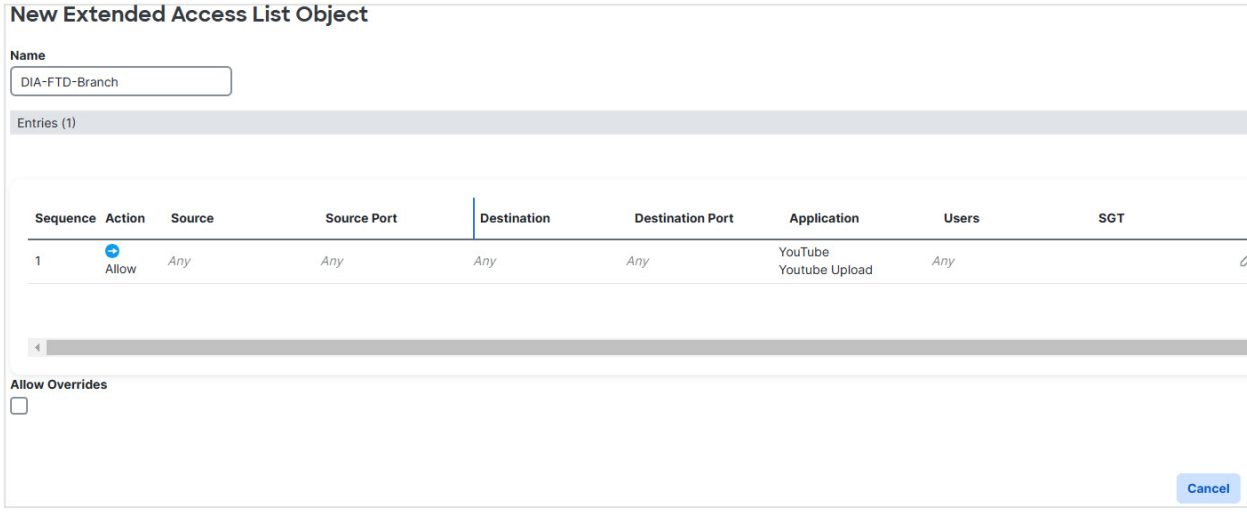
d) 在**添加扩展访问列表条目 (Add Extended Access List Entry)** 对话框中，从**应用 (Application)** 选项卡中选择所需的基于 Web 的应用：

图 *402:* “应用”选项卡



在 Firewall Threat Defense 上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

图 *403:* 扩展 *ACL*



e) 点击**保存**。

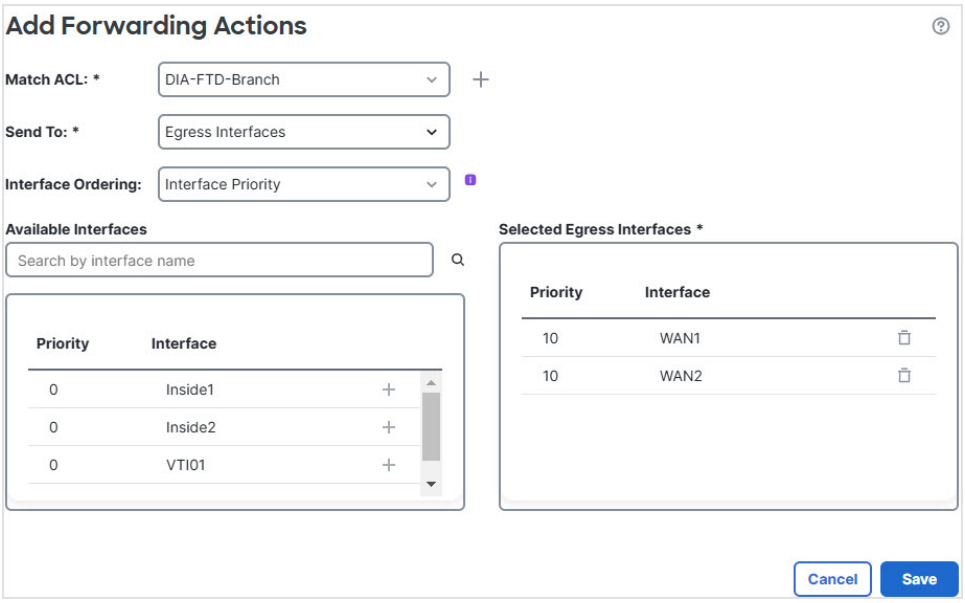
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *DIA-FTD-Branch*。

步骤 3 指定出口接口：

a) 从**发送到 (Send To)** 和**和接口排序 (Interface Ordering)** 下拉列表中，分别选择“出口接口”(Egress Interfaces) 和“接口优先级”(Interface Priority)。

b) 在 Available Interfaces 下，点击相应接口名称的 按钮以添加 WAN1 和 WAN2：在**可用接口 (Available Interfaces)** 下，再次点击相应接口名称的 ⊕ 按钮以便添加 *WAN1* 和 *WAN2*：

图 ***404:*** 配置策略型路由



c) 点击**保存**。

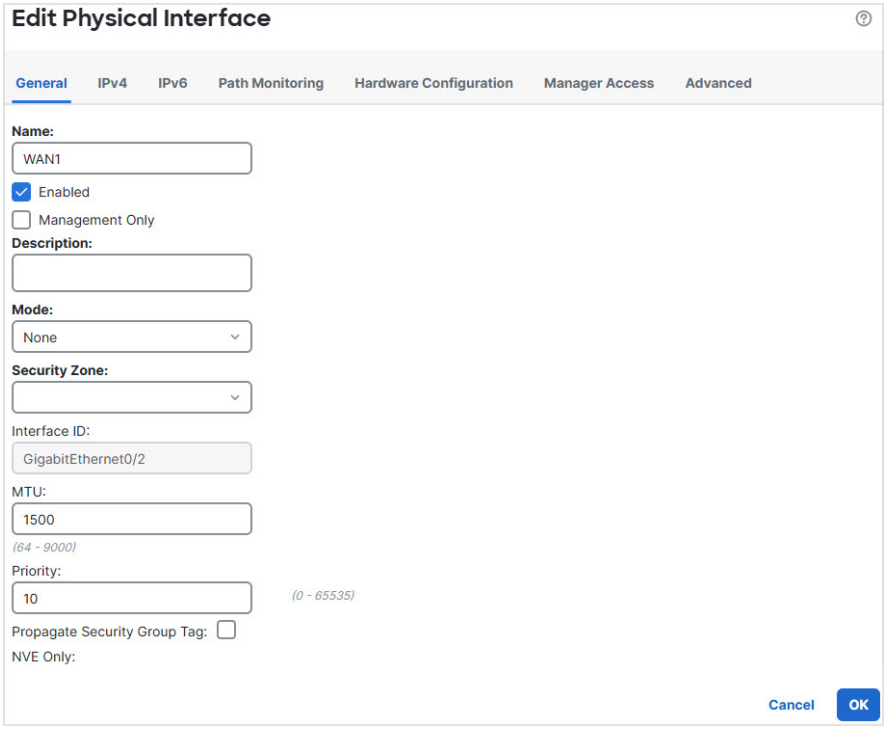
步骤 4 配置接口优先级

您可以在**编辑物理接口 (Edit Physical Interface)** 页面或**策略型路由 (Policy Based Routing)** 页面（**配置接口优先级**）中设置接口的优先级值。在本示例中，将介绍“编辑物理接口”方法。

a) 选择 **设备** > **设备管理**，然后编辑分支 Firewall Threat Defense。

b) 设置接口的优先级。点击接口的**编辑 (Edit)**，然后输入优先级值：

图 *405:* 设置接口优先级



c) 点击**确定** 和**保存**。

步骤 5 创建用于负载均衡的 ECMP 区域：

a) 在**路由 (Routing)** 页面中，点击 **ECMP**。

b) 要将接口关联到 ECMP 区域，请点击**添加 (Add)**。

c) 选择 *WAN1* 和 *WAN 2*，然后创建一个 ECMP 区域 — *ECMP-WAN*。同样，添加 *VTI01* 和 *VTI02*，然后创建一个 ECMP 区域 — *ECMP-VTI*：

图 *406:* 将接口与 ***ECMP*** 区域相关联

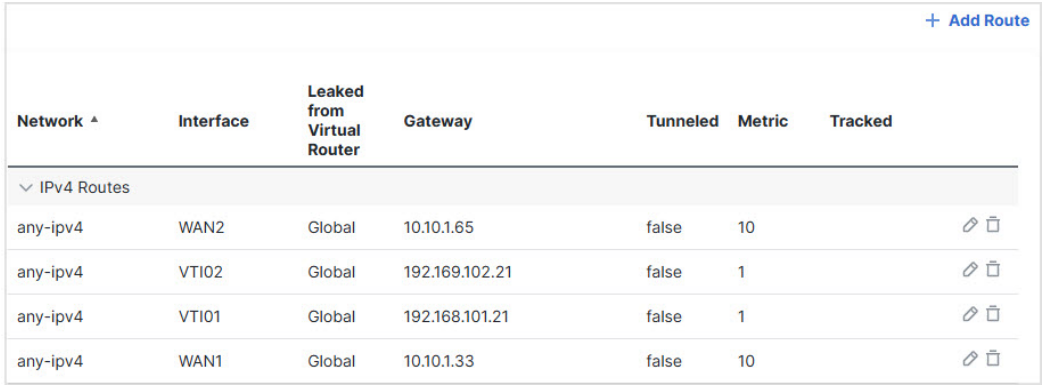


步骤 6 为区域接口配置静态路由以实现负载均衡：

a) 在**路由 (Routing)** 页面中，点击**静态路由 (Static Route)**。

b) 点击**添加 (Add)** 并为 *WAN1*、*WAN2*、*VTI01* 和 *VTI02* 指定静态路由。确保为属于相同 ECMP 区域的接口指定相同的指标值（步骤 5）：

图 *407:* 为 *ECMP* 区域接口配置静态路由



注释
确保区域接口具有相同的目的地址和指标，但网关地址不同。

步骤 7 在分支机构 Firewall Threat Defense 的 WAN 对象上配置受信任的 DNS，以确保流量安全地流向互联网：

a) 选择 **设备** > **平台设置**，然后在分支 Firewall Threat Defense 上创建 DNS 策略。
b) 要指定受信任的 DNS，请编辑策略，然后点击 **DNS**。
c) 要为 WAN 对象使用的 DNS 解析指定 DNS 服务器，请在 **DNS 设置 (DNS Settings)** 选项卡中提供 DNS 服务器组详细信息，然后从接口对象中选择 WAN。
d) 使用**受信任 DNS 服务器 (Trusted DNS Servers)** 选项卡为 DNS 解析提供您信任的特定 DNS 服务器。

步骤 8 点击**保存**，然后点击**部署**。

来自分支机构内部网络 *INSIDE1* 或 *INSIDE2* 的任何 *YouTube* 相关访问请求都会被路由到 *WAN1* 或 *WAN2*，因为它们将与 *DIA-FTD-Branch* ACL 匹配。任何其他请求（例如 *google.com*）都会通过在站点间 VPN 设置中配置的 *VTI01* 或 *VTI02* 进行路由。

如果配置了 ECMP，就可以无缝地平衡网络流量。

配置具有路径监控的 PBR

配置具有路径监控的 PBR，通过基于性能指标（例如抖动、往返时间和丢包）动态选择最佳出口接口来优化应用流量路由。

本示例描述了如何为以下应用配置具有路径监控的 PBR，并使用灵活的指标：

- 具有抖动的音频或视频敏感应用（例如，WebEx Meetings）。
- 使用 RTT 的基于云的应用（例如 Office365）。
- 具有丢包的基于网络的访问控制（具有特定的源和目标）。

Before you begin

1. 此示例假定您知道 PBR 的基本配置步骤。
2. 您已使用逻辑名称来配置入口和出口接口。在本示例中，入口接口命名为 *Inside1*，而出口接口命名为 *ISP01*、*ISP02* 和 *ISP03*。

按照以下步骤配置具有路径监控的 PBR：

过程

步骤 1 接口 *ISP01*、*ISP02* 和 *ISP03* 上的路径监控配置：

对于出口接口上的指标收集，您必须在它们上面启用并配置路径监控。

a) 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense。
b) 在**接口 (Interfaces)** 选项卡下，编辑接口（在我们的示例中为 *ISP01*）
c) 点击**路径监控 (Path Monitoring)** 选项卡，选中**启用路径监控 (Enable Path Monitoring)** 复选框，然后指定监控类型（请参阅配置路径监控设置，第 1265 页）。
d) 点击**确定** 和**保存**。
e) 重复这些步骤以便为 *ISP02* 和 *ISP03* 配置路径监控设置。

步骤 2 为组织 Firewall Threat Defense 中的分支机构配置策略型路由，选择入口接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 Firewall Threat Defense 设备。
b) 选择**路由 (Routing)** > **策略型路由 (Policy Based Routing)**，然后在**策略型路由 (Policy Based Routing)** 页面上，点击**添加 (Add)**。
c) 在**添加策略型路由 (Add Policy Based Route)** 对话框中，从**入口接口 (Ingress Interface)** 下拉列表中选择内部 *1 (Inside 1)*。

步骤 3 指定匹配条件：

a) 点击**添加 (Add)**。
b) 要定义匹配条件，请点击 **添加** (+) 按钮。
c) 在**新建扩展访问列表对象 (New Extended Access List Object)** 中，输入 ACL 的名称（例如 *PBR-WebEx*），然后点击**添加 (Add)**。
d) 在**添加扩展访问列表条目** 对话框中，从**应用**选项卡中选择基于 Web 的必要应用（例如 WebEx 会议）。

记住
在 Firewall Threat Defense上，ACL 中的应用组被配置为网络服务组，并且每个应用被配置为网络服务对象。

e) 点击**保存**。
f) 从**匹配 ACL (Match ACL)** 下拉列表中选择 *PBR-WebEx*。

步骤 4 指定出口接口：

a) 在**发送到 (Send To)** 下拉列表中，选择“出口接口”(Egress Interfaces)。

b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小抖动”(By Minimal Jitter)。
c) 在**可用接口 (Available Interfaces)** 下，点击相应接口名称对应的 **右箭头**（ ） 按钮，以便添加 *ISP01*、*ISP02* 和 *ISP03*。
d) 点击**保存**。

步骤 5 重复步骤 2 和步骤 3，为 *Inside1* 接口创建 PBR，以便路由 Office365 和基于网络的访问控制流量：
a) 创建匹配条件对象（例如 *PBR-Office365*），然后从**应用 (Application)** 选项卡中选择 Office365 应用。
b) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最短往返时间”(By Minimal Round Trip Time)。
c) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存**。
d) 现在，创建匹配条件对象（例如 *PBR-networks*），并在**网络 (Network)** 选项卡中指定源接口和目标接口。
e) 从**接口排序 (Interface Ordering)** 下拉列表中，选择“按最小丢包”(By Minimal Packet Loss)。
f) 指定出口接口 *ISP01*、*ISP02* 和 *ISP03*，然后点击**保存**。

步骤 6 点击**保存**，然后点击**部署**。

步骤 7 要查看路径监控指标，请选择**设备 (Devices)** > **设备管理 (Device Management)**，然后在 **更多** (⋮) 中点击**运行状况监控 (Health Monitor)**。要查看设备接口的指标详细信息，您必须添加路径指标控制面板。有关详细信息，请参阅添加路径监控控制面板 ， 第 1266 页。

WebEx、Office365 和基于网络的 ACL 流量会通过从 *ISP01*、*ISP02* 和 *ISP03*上收集的指标值得出的最佳路由进行转发。

用于监控 PBR 的有用 CLI

从 Firewall Threat Defense 设备 CLI 运行本主题中所述的监控命令。

接口配置

要查看设备的接口配置，请运行 `show run interface` 命令：

```
> show run interface
!
interface Ethernetl/l
 description Outside ispl handoff
 nameif outside1
 security-level 0
 zone-member ECMP-WAN
 ip address dhcp setroute
 policy-route cost 10
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
interface Ethernet1/2
 description Outside isp2 handoff
 nameif outside2
 security-level 0
```

```
 zone-member ECMP-WAN
 ip address 192.133.243.240 255.255.255.192
 policy-route cost 20
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
```

DNS 配置

基于应用的路由仅使用受信任的 DNS 服务器来解析域。要查看设备的 DNS 配置，请运行 `show run DNS` 命令：

```
> show run dns
DNS server-group DefaultDNS
dns trusted-source 10.100.0.5
dns trusted-source 10.200.0.5
```

路由地图配置

当您在设备上配置PBR时，管理中心会自动生成路由映射并将其应用到指定入口接口。要查看设备的路由映射，请运行 `show run route-map` 命令：

```
> show run route-map
!
route-map FMC_VPN_CONNECTED_DIST_RMAP_1000 permit 10
 match interface inside-employee
 set community 1000
!
route-map FMC GENERATED PBR 1729024850865 permit 5
 match ip address Cloud-storage-apps-acl
  set adaptive-intertace cost outside1 outside2

!
route-map FMC_GENERATED PBR 1729024850865 permit 10
match ip address Social-media-apps-acl
set adaptive-interface rtt outsidel outside2

!
route-map FMC GENERATED PBR 1729024850865 permit 15
match ip address Conferencing-apps-acl
set adaptive-interface jitter outside1 outside2

!
route-map FMC_GENERATED_PBR_1729024850865 permit 20
match ip address Corp-internal-apps-acl
set adaptive-interface cost outsidel_static_vti_1 outside2_static_vti_4
```

访问列表和网络服务组配置

应用到入口接口的路由映射可以引用扩展访问控制列表。要查看 PBR 的访问列表的详细信息，请运行 `show run access list <access list_name>` 命令：

```
> show run access-list Cloud-storage-apps-acl
access-list Cloud-storage-apps-acl extended permit ip any object-group-network-service
FMC_NSG_4295470562
```

网络服务对象和对象组在扩展访问控制列表中进行配置，并在策型路由路由地图和访问控制组中引用。要查看 NSG 配置，请运行 `show object-group network-service <network-service-groups-name>` 命令。*network-service-groups-name* 派生自上述访问列表的 show 命令。

```
> show object-group network-service FMC_NSG_4295470562
 object-group network-servire FMC_NSG_4295470562 (id=@xfdff0000)
 network-service-member "Box" dynamic
 description File storage and transfer site.
 app-id 1326
 domain box.com (bid=436735707) ip (hitcnt=0)
 domain boxcloud.com (bid=436924171) ip (hitcnt=0)
 domain box.net (bid=437080553) ip (hitcnt=0)
 domain box.org (bid=437174273) ip (hitcnt=0)
 domain boxcdn.net (bid=437272231) ip (hitcnt=0)
 domain boxrelay.com (bid=437481703) ip (hitcnt=0)
 domain boxenterprise.net (bid=437626005) ip {hitcnt=0)
 domain boxinvestorrelations.com (bid=437672765) ip (hitcnt=0)
 domain segment-box.com (bid=437886771) ip (hitcnt=0)
 domain box-corp.com (bid=437924995) ip (hitcnt=0)
 domain boxcn.net (bid=438072833) ip (hitcnt=0)
network-service-member "Dropbox" dynamic
 description Cloud based tile storage.
 app-id 125
 domain dropbox.com (bid=24259639) ip (hitcnt=0)
 domain cfl.dropboxstatic.com (bid=24495525) ip (hitcnt=0)
 domain dl.dropboxusercontent.com (bid=24596237) ip (hitcnt=0)
 domain dropboxapi.com (bid=24694467) ip (hitcnt=0)
 domain dropboxbusiness.com (bid=24859859) ip (hitcnt=0)
 domain dropboxcaptcha.com (bid=25008145) ip {hitcnt=0)
 domain dropbox-dns.com (bid=25087753) ip (hitcnt=0)
 domain dropboxer.net (bid=25236751) ip (hitcnt=0)
 domain dropboxusercontent.com (bid=25324335) ip (hitcnt=0)
 domain getdropbox.com (bid=25437501) ip (hitcnt=0)
 domain cloudon.com (bid=25580229) ip (hitcnt=0)
```

路径监控配置

要查看在出口接口上收集的路径监控指标，请运行 `show path-monitor` 命令：

```
> show path-monitor
Interface: outside2 (Ethernetl/2)
Remote peer: 8.8.8.8
    Remote peer reachable: Yes
    RTT average: 9138 microsecondes) Jitter: 1093 microsecond(s)
    Packet loss: 0% MOS: 4.39
    Last updated: 12 second(s) ago
Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470581
    Network Service: Facebook Domain name: fbsbx.com Remote peer reachable: Yes
    RTT average: 17460 microsecond(s) Jitter: 911 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago

    Network Service: Facebook
    Domain name: facebook.net
    Remote peer reachable: Yes
    RTT average: 17444 microsecondes)
    Jitter: 836 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
```

```
    Network Service: Instagram
    Domain name: instagram.com Remote peer reachable: Yes
    RTT average: 17576 microsecondes)
    Jitter: 429 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 secondes) ago

Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470600
    Network Service: WebEx
    Domain name: webex.com Remote peer reachable: Yes RTT average: 18537 microsecond(s)
Jitter: 318 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
    Network Service: Zoom Domain name: zoom.com Remote peer reachable: Yes
    RTT average: 98196 microsecond(s) Jitter: 4120 microseconde)
    Packet loss: 0%
    MOS: 4.34
    Last updated: 12 second(s) ago
```

对PBR进行故障排除

当数据包被丢弃时，此任务可以通过验证路由、监控指标和验证接口选择来调试 PBR 配置。

当 PBR 未按预期工作时，您需要系统地验证包括路由映射、路径监控和接口选择在内的配置组件，以确定数据包的根本原因。

Before you begin

当数据包被丢弃时，请按照以下步骤来排除 PBR 配置故障：

过程

步骤 1 在相应的表中使用 show route 或 show ipv6 route 命令，检查是否存在进行递归解析的所有必要路由。

除非使用正确的路由更新参与 PBR 中接口的路由映射，否则 PBR 将无法按预期工作。

步骤 2 通过使用 **show running-config interface** 命令来显示路径监控用于监控指标的远程地址。

示例：

```
interface GigabitEthernet0/0
nameif outside_0
security-level 0
zone-member ecmp-zone
ip address 20.0.0.3 255.255.255.0 -> This is egress interface "show running-config" output,
 the monitored address and cost metric value is determined in this output.
policy-route cost 1
policy-route path-monitoring
20.0.0.4
!
int GigabitEthernet 0/3
!
interface GigabitEthernet0/3
nameif outside_3
```

```
security-level 0
ip address 11.1.1.2 255.255.255.0 -> This is ingress interface "show running-config" output,
 the specific route-map will be used by PBR to determine the next route.
policy-route route-map rtt-tes
```

此命令通过发送 ICMP 数据包或 HTTP ping 显示路径监控的受监控地址和开销指标值。

步骤 3 检查 **show path-monitoring** 和 **show run route-map** 输出是否存在丢包。

示例：

```
ciscoasa(config)# show path-monitoring
Interface: outside_0  -> The remote address used for ICMP monitoring
Remote peer: 20.0.0.4
Version: 6223
Remote peer reachable: Yes -> If this value turns "No", then the ICMPv4/v6 packet is not
reaching the required remote address.
RTT average: 1920 microsecond(s)
Jitter: 394 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago -> The data should be updated by path monitoring after every
 30 seconds. The 'show route-map' would show the
updated metric values.
Interface: outside_2
Remote peer: 40.0.0.4
Version: 6223
Remote peer reachable: Yes
RTT average: 1935 microsecond(s)
Jitter: 433 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago
```

示例：

```
ciscoasa(config)# show route-map
route-map rtt-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface rtt outside_0 (1920) outside_2 (1935) outside_1 (1971) -> Displays the
metric type (rtt) that is used by the policy route to select the adequate interface to send
 the packet. The interface list where cost of each interface is given. As the metric type
is "rtt" and considering the minimum rtt value, the "outside_0" interface route will be
selected by PBR.
route-map mos-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface mos outside_0 (378) outside_1 (390) outside_2 (440) - > As the metric
type is "mos", considering the maximum value of mos, the "outside_2" interface will be
selected by PBR.
```

指标类型（丢失、rtt、抖动、成本）应选择具有最小指标值的接口进行路由。

指标类型“MOS”应选择具有最大指标值的接口进行路由。

步骤 4 使用 **packet-tracer** 命令根据 PBR 中定义的指标类型验证接口选择。

示例：

```
packet-tracer input <interface> icmp <src ip address> 8 0 <dst ip
address> detailed
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
```

```
Result: ALLOW
Elapsed time: 60656 ns
Config:
route-map rtt-test permit 10
match ip address allow_101_1_1_2
set adaptive-interface rtt outside_0 outside_2
Additional Information:
Matched route-map rtt-test, sequence 10, permit
Found next-hop 40.0.0.4 using egress ifc outside_2 -> PBR selects the adequate interface
from adaptiveinterface list given in "rtt-test" route-map.
```

步骤 5 使用类似 **debug policy-route** 命令的 **packet-tracer** 命令。

当 PBR 成功选择路由后，数据包跟踪器输出将如下所示：

```
pbr: policy based route lookup called for 101.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 20.0.0.4
```

当 PBR 无法找到适当的路由时，它会回退到正常路由查找，数据包跟踪器输出如下所示：

```
pbr: policy based route lookup called for 100.1.1.1/0 to 100.1.1.2/0 proto 1 sub_proto 8
received on interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map mos-test, sequence 10, permit; proceed with policy routing
pbr: no route to 100.1.1.2 on adaptive-interface outside_2
pbr: no route to 100.1.1.2 on adaptive-interface outside_1
pbr: no route to 100.1.1.2 on adaptive-interface outside_0
pbr: policy based routing could not be applied; proceeding with normal route lookup
```

当受监控的远程地址断开，并且路径监控将该地址的**远程对等体可访问**标记为**否**时，PBR 会显示日志，以从自适应接口列表中排除该接口。

```
pbr: policy based route lookup called for 100.1.1.1/0 to 101.1.1.2/0 proto 1 sub_proto 8
received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: Path Monitoring Ifc Down : adaptive-interface outside_1 Excluded from PBR routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 40.0.0.4
```

注释
当接口在路径监控模块中报告为可访问时，该接口就符合自适应 PBR 路由的条件。

策略型路由的历史记录

本参考提供了全面的历史记录表，总结了思科 Secure Firewall Management Center 各版本中策略型路由功能的介绍和演变，支持快速跟踪功能的可用性和变更。

表 *82:* 历史记录表

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
PBR中的自定义应用检测器支持	10.0.0	10.0.0	通过使用高级检测器类型选项，可以使用包含检测器模式的 .lua 文件创建自定义检测器。创建的自定义检测器模式然后可以在基于应用的PBR策略的扩展 ACL 中使用。 新增/修改的屏幕：未添加新的或修改的屏幕。
PBR中的自定义应用检测器支持	7.7	7.7	现在可以创建具有自定义应用域的PBR策略。用户定义的域创建为自定义检测器模式，可以在基于应用的 PBR 策略的扩展 ACL 中使用。 新增/修改的屏幕：未添加新的或修改的屏幕。
基于身份和 SGT 的 PBR 策略	7.4.0	7.4.0	现在，您可以根据用户和用户组以及 PBR 策略中的 SGT 对网络流量进行分类。您可以在定义 PBR 策略的扩展 ACL 时选择身份和 SGT 对象。 新增/修改的屏幕：扩展访问列表对象中添加的新选项卡，用于配置策略型路由策略：**对象 (Objects)** > **对象管理 (Object Management)** > **访问控制列表 (Access Control Lists)** > **添加扩展 (Add Extended)** 页面，**用户 (Users)** 和 **安全组标记 (Security Group Tag)**。
基于 HTTP 的路径监控	7.4.0	7.2.0	PBR 现在可以使用通过应用域上的 HTTP 客户端进行路径监控收集的性能指标（RTT、抖动、丢包和 MOS），而不是特定目标 IP 上的指标。默认情况下，为接口启用基于 HTTP 的应用监控选项。您可以使用匹配 ACL 配置 PBR 策略，该 ACL 具有用于确定路径的受监控应用和指标类型。 新增/修改的屏幕：接口页面中用于启用路径监控的新选项：**设备 (Devices)** > **设备管理 (Device Management)** > **编辑接口 (Edit Interfaces)** > **路径监控 (Path Monitoring)** > **启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框。
双 WAN/ISP 威胁防御管理支持	7.3.0	7.3.0	在启用双 WAN 的威胁防御中，配置了一个数据接口来与管理中心进行通信。现在提供了对配置辅助数据接口的支持，以便在主数据接口发生故障时维持通信通道。管理中心会自动配置PBR，以根据优先级和SLA指标将SF隧道流量从 *tapnlp*（内部）接口路由到其中一个可用的数据接口。
PBR路由映射的下一跳设置	7.3.0	7.1.0	您可以在启用数据包转发操作的同时，为 PBR 路由映射配置下一跳。 新增/修改的屏幕：添加/编辑转发操作页面中用于配置出口接口的新字段：**设备管理 (Device Management)** > **路由 (Routing)** > **策略型路由 (Policy Based Routing)** > **添加转发操作 (Add Forwarding Actions)** 页面。

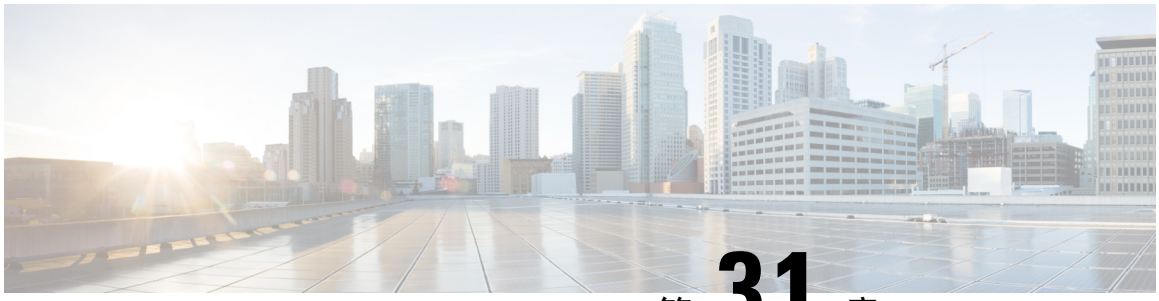
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
PBR 和路径监控	7.2.0	7.2.0	PBR 使用路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。您必须为接口启用路径监控并配置监控类型。您可以通过路径确定所需的指标来配置 PBR 策略。 新增/修改的屏幕：接口页面中用于启用路径监控的新选项卡：**设备 (Devices)** > **设备管理 (Device Management)** > **编辑接口 (Edit Interfaces)** > **路径监控 (Path Monitoring)** 选项卡。
从 FMC Web 界面配置策略型路由。	7.1.0	7.1.0	**升级影响。升级后重新设置 FlexConfig**。 您现在可以从 FMC Web 界面配置策略型路由 (PBR)。您可以根据应用对网络流量进行分类，并实施直接互联网接入 (DIA) 以将流量从分支机构部署发送到互联网。您可以定义PBR策略并在入口接口上进行配置，从而指定匹配条件和出口接口。根据策略中配置的优先级或顺序，通过出口接口转发与访问控制策略匹配的网络流量。 此功能需要 FMC 和设备上的版本 7.1+。将 FMC 升级到版本 7.1+ 时，将删除现有的策略型路由 FlexConfig。将设备升级到版本 7.1+ 后，请在 FMC Web 界面中重新执行策略型路由配置。对于未升级到版本 7.1+ 的设备，请重做 FlexConfig 并将其配置为“每次”部署。 新增/修改的屏幕： **设备** > **设备管理** > **路由** > **策略型路由**



第 V 部分

网络策略

- 网络地址转换， 第 1293 页
- 服务质量， 第 1413 页



第 31 章

网络地址转换

以下主题介绍网络地址转换 (NAT) 以及在 Firewall Threat Defense设备上配置网络地址转换的方法。

- 为何使用 NAT？ ，第 1293 页
- NAT 基础知识 ，第 1294 页
- NAT 策略的要求和先决条件 ，第 1302 页
- NAT 准则 ，第 1303 页
- 管理 NAT 策略 ，第 1309 页
- 配置用于威胁防御的 NAT ，第 1310 页
- 转换 IPv6 网络 ，第 1348 页
- 监控 NAT ，第 1361 页
- NAT 示例 ，第 1362 页
- Firewall Threat Defense NAT 的历史记录 ，第 1411 页

为何使用 NAT？

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。

- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。



注释 不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

NAT 基础知识

以下主题介绍一些 NAT 基础知识。

NAT 术语

本文档使用以下术语：

- 实际地址/主机/网络/接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换连接到设备的任何网络，而不是只在网络内部转换。因此，如果配置 NAT 以转换外部地址，“实际”可以是指访问内部网络时的外部网络。
- 映射地址/主机/网络/接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。



注释 在地址转换过程中，不会转换为设备接口配置的 IP 地址。

- 双向发起 - 静态 NAT 允许双向发起连接，意味着可发起到主机的连接和从主机发起连接。
- 源 NAT 和目的 NAT - 对于任何给定数据包，将源 IP 地址和目标 IP 地址与 NAT 规则进行比较，转换/不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。

NAT 类型

可以使用以下方法实施 NAT：

- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅动态 NAT，第 1316 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅动态 PAT，第 1321 页。

- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅静态 NAT，第 1331 页。
- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想豁免一小部分地址时，可能就要这样配置 NAT。请参阅身份 NAT，第 1339 页。

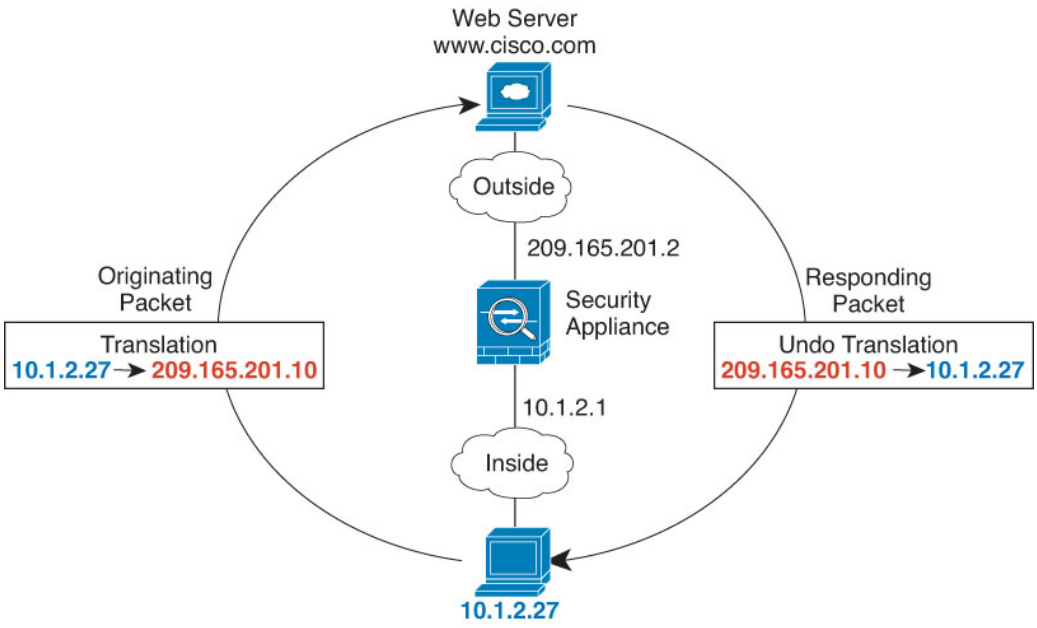
路由和透明防火墙模式下的 NAT

可以在路由和透明防火墙模式下配置 NAT。您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。以下部分介绍每种防火墙模式的典型用法。

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 *408: NAT* 示例：路由模式



1. 当位于 10.1.2.27 的内部主机向 Web 服务器发送数据包时，数据包的实际源地址 10.1.2.27 会转换为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，Firewall Threat Defense 接收数据包，因为 Firewall Threat Defense 执行代理 ARP 以认领数据包。
3. 接下来，Firewall Threat Defense 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

透明模式下的 NAT 或网桥组内的 NAT

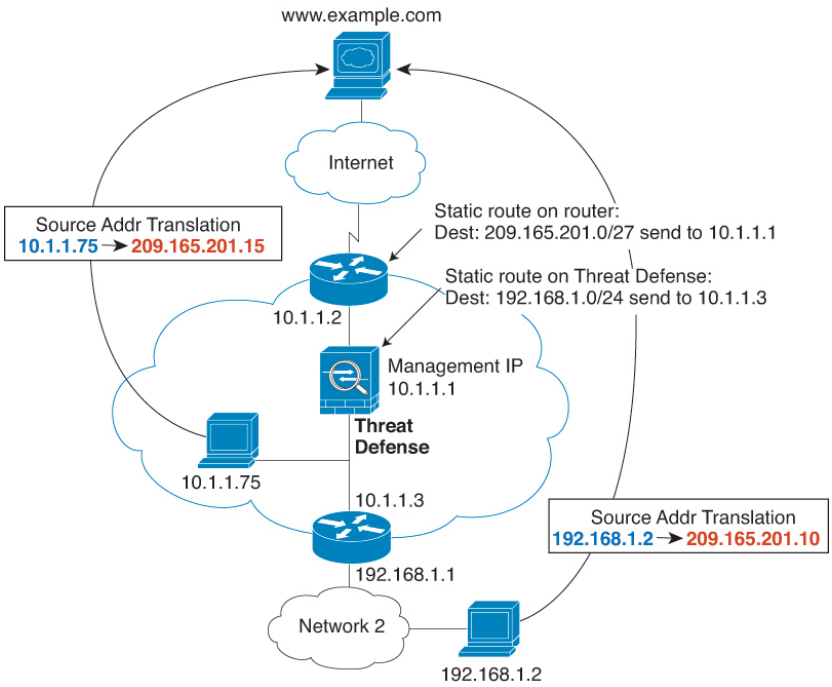
在透明模式下使用NAT可以消除上游或下游路由器为其网络执行NAT的需求。在路由模式下，NAT可以执行与桥接组内类似的功能。

透明模式下的 NAT或在路由模式下同一桥接组的成员之间具有以下要求和局限性：

- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 不支持 ARP 检测。此外，如果由于某种原因，Firewall 威胁防御 一端的主机向 Firewall 威胁防御 另一端的主机发送ARP请求，而且发起主机实际地址被映射到同一子网的不同地址，则实际地址在 ARP 请求中依然可见。
- 不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

下图显示透明模式下的典型NAT场景，内部接口和外部接口上的网络相同。在此场景中，透明防火墙执行 NAT 服务，因此上游路由器不必执行 NAT。

图 *409: NAT* 示例：透明模式



1. 当位于 10.1.1.75 的内部主机将数据包发送到 Web 服务器时，数据包的实际源地址 10.1.1.75 被更改为映射地址 209.165.201.15。
2. 当服务器响应时，它将响应发送到映射地址 209.165.201.15，Firewall 威胁防御 接收数据包，因为上游路由器将此映射网络包含在定向到 Firewall 威胁防御 管理 IP 地址的静态路由中。
3. 然后，Firewall 威胁防御 取消映射地址 209.165.201.15 回到实际地址 10.1.1.1.75 的转换。因为实际地址是直接连接的，所以 Firewall 威胁防御 将实际地址直接发送到主机。

4. 对于主机 192.168.1.2，发生相同流程，但返回流量除外，Firewall 威胁防御 在其路由表中查询路由，根据 192.168.1.0/24 的 Firewall 威胁防御 静态路由，将数据包发送到位于 10.1.1.3 的下游路由器。

自动 NAT 和手动 NAT

可以通过以下两种方法实施地址转换：自动 *NAT* 和手动 *NAT*。

我们建议使用自动 NAT，除非您需要手动 NAT 提供的额外功能。自动 NAT 更容易配置，而且可能对应用（例如 IP 语音 [VoIP]）更加可靠。（对于 VoIP，对不属于规则中使用的任何对象的间接地址进行转换可能会失败。）

自动 NAT

配置为网络对象参数的所有 NAT 规则都被视为自动 *NAT* 规则。这是一种为网络对象配置 NAT 的快捷方法。但是，您无法为对象组创建这些规则。

尽管这些规则配置为对象的一部分，但是您通过对象管理器无法看到对象定义中的 NAT 配置。

当数据包进入接口时，系统会根据自动 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。手动 NAT 用于实现这样的功能：您可以识别单个规则中的源和目标地址。

手动 NAT

手动 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目标地址，可以让您指定源 A/目的 A 有不同于源 A/目的 B 的转换。



注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

比较自动 NAT 和手动 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
    - 自动 NAT - NAT 规则成为网络对象的参数。网络对象 IP 地址用作原始（实际）地址。

- 手动 NAT- 标识实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是NAT配置的参数。能够使用实际地址的网络对象组意味着手动 NAT 更具可扩展性。

- 实施源和目标 NAT 的方法。
  - 自动 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源IP地址，一条用于目标IP地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
  - 手动 NAT- 单一规则可以同时转换源和目标。数据包仅匹配一条规则，且不再检查其他规则。即使您不配置可选目标地址，匹配的数据包仍仅匹配一个 手动 NAT 规则。源和目的绑在一起，使您可以根据源/目的组合进行不同的转换。例如，源 A/目的 A 可以有不同于源 A/目的 B 的转换。

- NAT 规则顺序。
  - 自动 NAT- 在 NAT 表中自动排序。
  - 手动 NAT - 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。

NAT 规则顺序

自动 NAT 和手动 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

注释 还有一个第 0 部分，其中包含系统创建供自己使用的任何 NAT 规则。这些规则优先于所有其他规则。系统会自动创建这些规则并根据需要清除 xlate。您不能在第 0 部分中添加、编辑或修改规则。

表 *83: NAT* 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	手动 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，手动 NAT 规则会添加到第 1 部分。 “具体规则优先”是指： • 静态规则应放在动态规则前面。 • 包含目的地转换的规则应仅放在具有源转换的规则前面。 如果无法消除重叠规则（其中可能有多个规则基于源或目标地址而应用），请特别注意遵循这些建议。 如果您不遵循上述建议，请确保为映射地址配置准确的路由，以匹配正确的 NAT 规则。
第 2 部分	自动 NAT	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第 3 部分	手动 NAT	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）

- 172.16.1.0/24（动态）（对象 def）
- 172.16.1.0/24（动态）（对象 abc）

结果排序可能是：

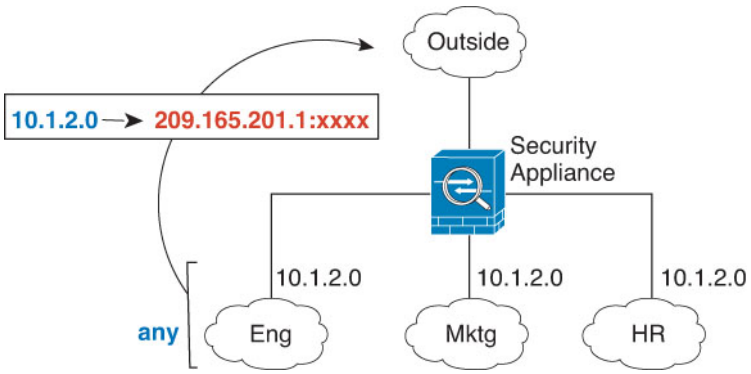
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了网桥组成员接口，您可以将NAT规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则可能要为实际地址指定任何接口，并且为映射地址指定外部接口。

图 *410:* 指定任何接口



然而，“任何”接口的概念不适用于网桥组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口(BVI)本身配置NAT，只能为成员接口配置NAT。

注释 您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。在指定接口时，请通过选择包含该接口的接口对象间接指定。

NAT 免除

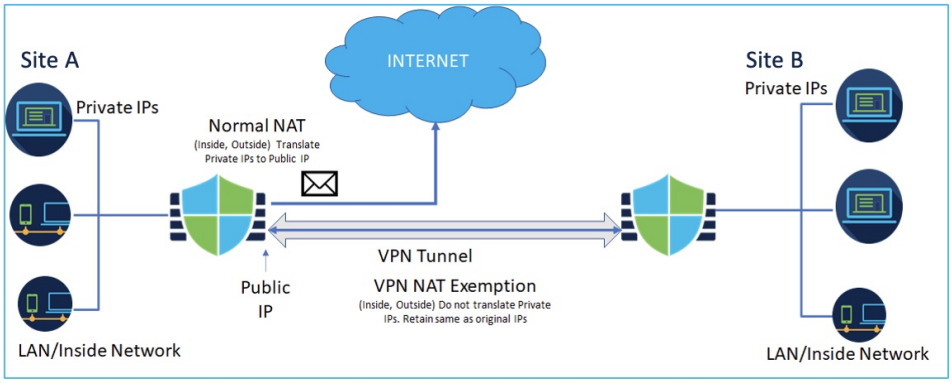
当互联网边缘设备在一个接口上配置了一个站点间 VPN，并且该接口也有 NAT 规则时，您必须将 VPN 流量从 NAT 规则中豁免。如果不让 VPN 流量免于 NAT 转换，流量将被丢弃或不会通过 VPN 隧道路由到远程对等体。

NAT 豁免允许您排除 NAT 规则转换的流量。使用 防火墙管理中心 VPN 向导创建基于策略的站点间 VPN 时，可以选择 **NAT 免除**选项以自动创建规则（**安全连接 > 站点间 VPN 和 SD-WAN**）。默认情况下，此选项处于已启用状态。您可以在 NAT 策略页面中查看设备的 NAT 豁免（**策略 > 网络策略 > NAT**，然后点击 **NAT 豁免**）。

防火墙管理中心 支持所有基于策略的站点间 VPN 拓扑类型的 NAT 豁免。有关详细信息，请参阅配置策略型站点间 VPN，第 1449 页。

请考虑以下示例，该示例显示连接站点 A 和站点 B 的站点间 VPN 隧道。对于必须流向互联网的流量，NAT 会将私有 IP 地址转换为公共 IP 地址以访问互联网。对于必须通过 VPN 隧道的流量，必须在 VPN 向导中为设备配置 NAT 豁免。

图 *411:* 具有 *NAT* 豁免的站点间 *VPN* 拓扑



请注意，当您从 7.4 之前的版本升级时，如果您已启用 NAT 豁免，防火墙管理中心 会禁用此选项。您必须在基于策略的站点间 VPN 向导中启用此选项。

为 NAT 配置路由

Firewall Threat Defense 设备需要成为发送到转换（映射）地址的所有数据包的目标。

在发送数据包时，设备使用目标接口（如果指定了接口）或路由表查找（如果未指定接口）来确定出口接口。对于身份 NAT，即使指定了目标接口，您也可以选择使用路由查找。

所需的路由配置类型取决于映射地址的类型，以下主题对此进行了说明。

地址与映射接口在相同的网络中

如果使用与目标（映射）接口在同一网络中的地址，Firewall Threat Defense使用代理 ARP 应答映射地址的任何 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 Firewall Threat Defense 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使

用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可显著增加您可以通过少量地址实现的转换数量，因此即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，甚至可以使用映射接口的 IP 地址。



注释 如果将映射接口配置为任何接口，而且在与其中一个映射接口相同的网络中指定映射地址，那么如果从其他接口传入对此映射地址的 ARP 请求，则需要在入口接口上为该网络手动配置 ARP 条目，并指定其 MAC 地址。通常，如果该映射接口指定任何接口，则将唯一网络用于此映射地址，避免此类情况发生。在入口接口的**高级**设置中配置 ARP 表。

唯一网络上的地址

如果需要比目标（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 Firewall Threat Defense 的映射地址进行静态路由。

或者，对于路由模式，可以将目标网络上的任何 IP 地址用作网关，为映射地址配置 Firewall Threat Defense 上的静态路由，然后使用路由协议重新分配路由。例如，如果您将 NAT 用于内部网络 (10.1.1.0/24)，并且使用映射 IP 地址 209.165.201.5，则可以为 10.1.1.99 网关配置 209.165.201.5 255.255.255.255（主机地址）的可重新分发静态路由。

对于透明模式，如果真实主机是直接连接的，请在上游路由器上配置静态路由以指向 Firewall Threat Defense：指定桥组 IP 地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，您也可以指定下游路由器 IP 地址。

与实际地址相同的地址（身份 NAT）

身份 NAT 的默认行为已启用代理 ARP，并且与其他静态 NAT 规则匹配。如果需要，可以禁用代理 ARP。如果需要，还可以为常规静态 NAT 禁用代理 ARP，在这种情况下，需要确保上游路由器上有适当的路由。

通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，Firewall Threat Defense 将代理地址的 ARP，即使数据包实际上不以 Firewall Threat Defense 为目标。（请注意，即便已设置手动 NAT 规则，也会造成此问题；虽然 NAT 规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理 ARP 决定）。如果在实际主机 ARP 响应之前收到 Firewall Threat Defense ARP 响应，则流量会错误地发送到 Firewall Threat Defense。

NAT 策略的要求和先决条件

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

NAT 准则

以下主题提供有关实施 NAT 的详细准则。

NAT 防火墙模式准则

在路由和透明防火墙模式下支持 NAT。

不过，在桥接组成员接口（属于桥接组虚拟接口 [BVI] 的接口）上配置 NAT 具有以下局限性：

- 为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。
- 在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。
- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 当源接口和目标接口是同一网桥组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。但是，您可以在不同网桥组的成员之间，或在网桥组成员（源接口）和标准路由接口（目标接口）之间执行 NAT64/46。

注释 您不能为在内联、内联分流或被动模式下工作的接口配置 NAT。

IPv6 NAT 准则

NAT 支持 IPv6，但有以下准则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个网桥组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。
- 在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。

- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 最佳实践

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践：

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。转换为 IPv6 子网（/96 或更低）时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。或者，还能够以网络对网络的方式转换地址，其中第一个 IPv4 地址映射到第一个 IPv6 地址，第二个 IPv4 地址映射到第二个 IPv6，依次类推。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

对检测到的协议的 NAT 支持

检测打开辅助连接或者在数据包中嵌入 IP 地址的一些应用层协议，以提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

下表列出了应用 NAT 重写及其 NAT 限制的检测到的协议。当编写包括这些协议的 NAT 规则时，请记住这些限制。此处未列出的协议不应用 NAT 重写。这些检测包括 GTP、HTTP、IMAP、POP、SMTP、SSH 和 SSL。

注释 仅列出的端口支持 NAT 重写。对于其中某些协议，您可以使用网络分析策略将检测扩展到其他端口，但 NAT 重写不会扩展到这些端口。这包括 DCERPC、DNS、FTP 和 Sun RPC 检测。如果在非标准端口上使用这些协议，请勿对连接使用 NAT。

表 *84: NAT* 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建了小孔
DCERPC	TCP/135	无 NAT64。	是
DNS over UDP	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	否
ESMTP	TCP/25	无 NAT64。	否
FTP	TCP/21	（集群）无静态 PAT。	是
H.323 H.225（呼叫信令） H.323 RAS	TCP/1720 UDP/1718 对于 RAS， 则为 UDP/1718-1719	（集群）无静态 PAT。 无扩展 PAT。 无 NAT64。	是
ICMP ICMP 错误	ICMP （从不会对定向到设备接口的 ICMP 流量进行检测。）	没有限制。	否
IP 选项	RSVP	无 NAT64。	否
NetBIOS Name Server over IP	UDP/137、138（源端口）	无扩展 PAT。 无 NAT64。	否
RSH	TCP/514	无 PAT。 无 NAT64。 （集群）无静态 PAT。	是
RTSP	TCP/554 （对于 HTTP 隐藏没有任何处理。）	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	是
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。 （集群）无静态 PAT。	是
Skinny (SCCP)	TCP/2000	无扩展 PAT。 无 NAT64、NAT46 或 NAT66。 （集群）无静态 PAT。	是

应用	检测到的协议、端口	NAT 限制	创建了小孔
SQL*Net （版本 1、2）	TCP/1521	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	是
Sun RPC	TCP/111 UDP/111	无扩展 PAT。 无 NAT64。	是
TFTP	UDP/69	无 NAT64。 （集群）无静态 PAT。 不转换负载 IP 地址。	是
XDMCP	UDP/177	无扩展 PAT。 无 NAT64。 （集群）无静态 PAT。	支持

FQDN 目标准则

您可以使用完全限定域名 (FQDN) 网络对象而不是 IP 地址在手动 NAT 规则中指定转换（映射）目的。例如，您可以基于发往 www.example.com Web 服务器的流量创建规则。

使用 FQDN 时，系统基于返回的地址获取 DNS 解析并编写 NAT 规则。 如果使用多个 DNS 服务器组，则系统会使用过滤器域，并根据过滤器从相应的组请求地址。如果从 DNS 服务器获取多个地址，则使用的地址基于以下条件：

- 如果某个地址与指定接口位于相同的子网上，则使用该地址。如果没有地址位于相同的子网上，则使用返回的第一个地址。
- 转换后的源和转换后的目的的 IP 类型必须匹配。例如，如果转换后的源地址为 IPv6，则 FQDN 对象必须指定 IPv6 作为地址类型。如果转换后的源为 IPv4，则 FQDN 对象可以指定 IPv4 或 IPv4 和 IPv6。在这种情况下，将选择 IPv4 地址。

不能在用于手动 NAT 目的的网络组中包含 FQDN 对象。在 NAT 中，必须单独使用 FQDN 对象，因为只有单个目的主机才适用于此类 NAT 规则。

如果 FQDN 无法解析为 IP 地址，则在获得 DNS 解析之前该规则不起作用。

NAT 的其他准则

- NAT 规则仅适用于通过设备的流量，不适用于设备发起的流量（如 RADIUS 身份验证）。
- 对于作为网桥组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。

- 您不能为站点间 VPN 中使用的虚拟隧道接口 (VTI) 编写 NAT 规则。为 VTI 的源接口编写规则不会将 NAT 应用于 VPN 隧道。要编写应用于 VTI 上通过隧道传输的 VPN 流量的 NAT 规则，您必须使用“任何”作为接口，而不能明确指定接口名称。
- （仅限于 自动 NAT。）您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。
- 如果在接口上定义了 VPN，则接口上的入站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

  如果创建应应用于现有连接（例如 VPN 隧道）的新 NAT 规则，则需要使用 **clear conn** 来终止连接。然后，尝试重新建立连接应符合 NAT 规则，且连接应正确进行 NAT。



注释 如果删除动态 NAT 或 PAT 规则，然后使用与已删除规则中地址重叠的映射地址添加新规则，则系统将不使用新规则，直至与已删除规则关联的所有连接超时，或已使用 **clear xlate** 或 **clear conn** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- NAT 中使用的网络对象不能包含超过 131838 个 IP 地址，无论是显式还是隐式包含在地址或子网范围中。将地址空间分成更小的范围，并为较小的对象编写单独的规则。
- （仅限于手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“任何”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，Firewall Threat Defense 才能对数据包执行 NAT；借助此前提条件，Firewall Threat Defense 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“任何”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则 **任何**指“任何 IPv6 流量”。如果配置从“任何”到“任何”的规则，并且将源映射至接口 IPv4 地址，则**任何**指“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
  - 映射接口的 IP 地址。如果为该规则指定“任何”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。
  - 故障转移接口 IP 地址。
  - （透明模式。）管理 IP 地址。
  - （动态 NAT。）启用 VPN 时的备用接口 IP 地址。

- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 如果在规则中指定目标接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。
- 如果对用于连接 NFS 服务器的 Sun RPC 流量使用 PAT，请注意，在通过 PAT 方式转换的端口号大于 1024 时，NFS 服务器可能会拒绝连接。NFS 服务器的默认配置是拒绝来自端口号大于 1024 的连接。错误通常为“权限被拒”。 如果不选择将保留端口 (1-1023) 包括在 PAT 池的端口范围内的选项，则系统会映射高于 1024 的端口。您可以通过将 NFS 服务器配置更改为允许所有端口号来避免此问题。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 pat-pool。
- 单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (手动 NAT) 为双 ISP 接口设置（使用路由配置中的服务级别协议的主接口和备用接口）编写 NAT 规则时，请勿在规则中指定目标条件。确保主接口的规则在备用接口的规则之前。这允许设备在主 ISP 不可用时根据当前路由状态选择正确的 NAT 目的接口。如果指定目标对象，NAT 规则将始终为其他规则选择主接口。
- 如果您收到不应与为接口定义的 NAT 规则匹配的流量的 ASP drop reason nat-no-xlate-to-pat-pool，请为受影响的流量配置身份 NAT 规则，以便流量可以不经转换地通过。
- 如果为 GRE 隧道终端配置 NAT，则您必须在终端上禁用保持连接，否则将无法建立隧道。终端将保持连接发送到原始地址。
- DHCP 和 BOOTP 共享端口 UDP/67-68。由于 BOOTP 已经过时，如果同时运行 DHCP，为 bootps 端口编写 NAT 规则可能会导致端口分配问题。请考虑使用 DHCP 中继来传输网段之间的 DHCP 请求。
- (Cisco Secure Firewall 200) 如果将 PAT 与 SIP 会话配合使用，且通过设备发送数千个 SIP 连接，请将 SIP 邀请超时时间缩短到最低 1 分钟。这可以避免与 SIP 会话相关的转换消耗空闲内存的问题。在平台设置策略的**超时**页面上配置超时。
- 极少数情况下，已有转换 (xlate) 的返回流量（服务器至客户端）可能在连接事件中被记录为新流。当客户端已关闭连接，服务器在连接关闭与 xlate 移除的短暂间隔内发来数据包时会触发此情况，通常由应用行为或 TCP 栈清理引起。设备仅在删除连接后才移除 xlate，故 xlate 仍存在时服务器数据包可能到达。若未找到有效连接条目，设备将根据匹配的访问控制策略规则记录单独的连接事件。

管理 NAT 策略

网络地址转换 (NAT) 会将传入数据包的 IP 地址转换为传出数据包中的其他地址。NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的可路由地址。NAT 会对转换进行跟踪（也称为 xlate），以确保将返回流量定向到正确的未转换主机地址。

过程

步骤 1 选择**策略** > **网络策略** > **NAT** 。

步骤 2 管理 NAT 策略：

- 创建 - 点击 **新建策略** 按钮，。请参阅创建 NAT 策略，第 1309 页。
- 复制 - 点击要复制的策略旁边的 **复制** ()。系统将提示您为副本指定唯一的新名称。该副本包含所有策略规则和配置，但不包含设备分配。
- 报告 - 点击 **报告** () 以获取策略。系统会提示您保存 PDF 报告，其中包括策略属性、设备分配、规则以及对象使用信息。
- 编辑 - 点击要编辑的策略旁边的 **编辑** ()。请参阅配置用于威胁防御的 NAT，第 1310 页。
- 删除 - 点击要删除的策略旁边的 **删除** ()，然后点击**确定**。当系统提示是否继续时，还会告知您是否有其他用户在策略中有未保存的更改。

  注意
  将NAT策略部署于托管设备后，就不能从设备删除策略。相反，如果要删除托管设备上已出现的 NAT 规则，则必须部署不带任何规则的 NAT 策略。您也不能删除上一次部署于任何目标设备的策略，即使该策略已过时。要完全删除该策略，必须向目标部署其他策略。

创建 NAT 策略

创建新的NAT策略时，必须至少为其提供一个唯一的名称。虽然在创建策略过程中不需要识别策略目标，但必须执行这个步骤后才能部署策略。如果将不带有规则的NAT策略应用于某台设备，系统会从该设备删除所有 NAT 规则。

过程

步骤 1 选择**策略** > **网络策略** > **NAT** 。

步骤 2 从下拉列表中点击 **新策略**，。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 选择要部署策略的设备：

- 从**可用设备 (Available Devices)** 列表中选择一个设备，然后点击**添加到策略 (Add to Policy)**。
- 点击**可用设备 (Available Devices)** 列表中的设备并将其拖移到**所选设备 (Selected Devices)** 列表。
- 点击设备旁边的 **删除** ()，从**所选设备 (Selected Devices)** 列表中删除设备。

步骤 6 点击**保存**。

配置 NAT 策略目标

创建或编辑策略时，可以确定要应用策略的托管设备。可以搜索一系列可用设备和高可用性对，并将其添加到所选设备列表。

过程

步骤 1 选择**策略** > **网络策略** > **NAT** 。

步骤 2 点击要修改的 NAT 策略旁边的 **编辑** () 。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**策略分配**。

步骤 4 执行以下任一操作：

- 要将设备、高可用性对或设备组分配给策略，请在**可用设备 (Available Devices)** 列表中将其选中，然后点击**添加到策略 (Add toPolicy)**。还可以进行拖放。
- 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除** ()。

步骤 5 点击**确定**。

配置用于威胁防御的 NAT

网络地址转换可能非常复杂。我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。以下程序说明了规划的基本方法。

NAT 策略为共享策略。您将策略分配给应具有类似 NAT 规则的设备。

策略中的给定规则是否适用于分配的设备由规则中使用的接口对象（安全区域或接口组）来确定。如果接口对象包括设备的一个或多个接口，则规则会部署到设备。因此，通过仔细设计接口对象，

您可以配置应用于单个共享策略内的设备子集的规则。适用于“任意”接口对象的规则会部署到所有设备。

如果将某个接口的类型更改为不适用于以具有该接口的设备为目标的NAT策略的类型，策略会将该接口标记为“已删除”。在 NAT 策略中点击**保存**会自动从策略删除接口。

如果设备组需要显著不同的规则，则可以配置多个 NAT 策略。

过程

步骤 1 选择**策略** > **网络策略** > **NAT** 。

- 点击**新建策略 (New Policy)** 以创建新策略。为策略命名，或者为其分配设备，然后点击**保存**。

  还可以在以后更改设备分配，只需编辑策略并点击**策略分配 (Policy Assignments)**。

- 点击 **编辑** (✎) 以编辑现有威胁防御 NAT 策略。

  如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 决定您需要哪些类型的规则。

可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅NAT 类型，第 1294 页。

步骤 3 决定应将哪些规则作为手动或自动 NAT 来实施。

有关这两种实施选项的比较，请参阅自动 NAT 和手动 NAT，第 1297 页。

步骤 4 决定哪些规则应该根据设备来自定义。

由于您可以将NAT策略分配给多台设备，因此可以在多台设备上配置单个规则。但是，您可能会具有一些每台设备应有不同解释的规则，或一些仅适用于设备子集的规则。

使用接口对象来控制应在哪些设备上配置规则。然后，在网络对象上使用对象覆盖以自定义每台设备使用的地址。

有关详细信息，请参阅为多个设备自定义 NAT 规则，第 1312 页。

步骤 5 遵循以下部分中的说明创建规则。

- 动态 NAT，第 1316 页
- 动态 PAT，第 1321 页
- 静态 NAT，第 1331 页
- 身份 NAT，第 1339 页

步骤 6 管理 NAT 策略和规则。

您可以执行以下操作来管理策略及其规则。

- 要编辑策略名称或说明，请在那些字段中点击，键入您的更改，然后在字段之外点击。

- 要查看那些仅适用于特定设备的规则，请点击**按设备过滤 (Filter by Device)** 并选择所需的设备。如果某个设备使用的接口对象包括该设备上的接口，则规则适用于该设备。
- 要查看策略中的任何警告或错误，请点击**显示警告 (Show Warnings)**，，然后选择**设备 (Device)**。警告和错误标记出会对流量产生不利影响或阻碍策略部署的配置。
- 要更改策略所分配到的设备，请点击**策略分配 (Policy Assignments)** 链接并根据需要修改所选设备列表。
- 要更改规则是启用还是禁用，请使用右键点击规则并通过 **State** 命令选择所需的选项。可以暂时禁用一条规则而不使用这些控制来删除规则。
- 要添加规则，请点击**添加规则**按钮。
- 要编辑规则，请点击规则的 **编辑** ()。
- 要删除规则，请点击规则的 **删除** ()。
- 要更改页面上显示的规则数量，请使用**每页行数 (Rows Per Page)** 下拉列表。
- 要选择多个规则以启用、禁用或删除，请点击规则的复选框或标题中的复选框，然后再执行操作。

步骤 7 点击**保存**。

此时，您可以转至**部署** > **部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

为多个设备自定义 NAT 规则

由于NAT策略已共享，可以将给定策略分配给多个设备。但您最多只可为某个给定对象配置一个自动NAT规则。因此，如果您要根据执行转换的特定设备为对象配置不同的转换，则需要谨慎配置接口对象（安全区域或接口组）和定义转换地址的网络对象覆盖。

接口对象确定在哪些设备上配置规则。网络对象覆盖确定给定设备为该对象使用哪些 IP 地址。

请考虑以下情景：

- FTD-A 和 FTD-B 具有连接到名为“inside”的接口的网络 192.168.1.0/24。
- 在 FTD-A 上，当转至“outside”接口时，您要将所有 192.168.1.0/24 地址转换为 10.100.10.10 - 10.100.10.200 范围内的一个 NAT 池。
- 在 FTD-B 上，当转至“outside”接口时，您要将所有 192.168.1.0/24 地址转换为 10.200.10.10 - 10.200.10.200 范围内的一个 NAT 池。

要实现上述配置，请执行以下操作。虽然此示例规则适用于动态自动 NAT，但您也可以将此方法推广到任何类型的 NAT 规则。

过程

步骤 1 为内部和外部接口创建安全区域。

a) 选择**对象**。

b) 从目录中选择**接口对象 (Interface Objects)** 并点击**添加 (Add)** > **安全区域 (Security Zone)**。（您可以使用接口组而不是区域。）

c) 配置内部区域属性。

- **名称 (Name)** - 输入名称，例如，**inside-zone**。
- **类型 (Type)** - 为路由模式设备选择**路由 (Routed)**，为透明模式选择**交换 (Switched)**。
- **所选接口 (Selected Interfaces)** - 将 FTD-A/内部和 FTD-B/内部接口添加到所选列表。

d) 点击**保存**。

e) 点击**Add (添加)** > **安全区域 (Security Zone)** 并定义外部区域属性。

- **名称 (Name)** - 输入名称，例如，**outside-zone**。
- **接口类型 (Interface Type)** - 为路由模式设备选择**路由 (Routed)**，为透明模式选择**交换 (Switched)**。
- **所选接口 (Selected Interfaces)** - 将 FTD-A/外部和 FTD-B/外部接口添加到所选列表。

f) 点击**保存**。

步骤 2 在“对象管理”(Object Management) 页面上为原始内部网络创建网络对象。

a) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 配置内部网络属性。

- **名称 (Name)** - 输入名称，例如，**inside-network**。
- **网络 (Network)** - 输入网络地址，例如，**192.168.1.0/24**。

c) 点击**保存**。

步骤 3 为已转换的 NAT 池创建网络对象并定义覆盖。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为 FTD-A 配置 NAT 池属性。

- **名称 (Name)** - 输入名称，例如，**NAT-pool**。
- **网络 (Network)** - 输入要包含在 FTD-A 池中的地址范围，例如，**10.100.10.10-10.100.10.200**。

c) 选择**允许覆盖 (Allow Overrides)**。

d) 点击**覆盖 (Overrides)** 标题以打开对象覆盖列表。

e) 点击**添加 (Add)** 以打开“添加对象覆盖”(Add Object Override) 对话框。

f) 选择 FTD-B 和**添加 (Add)** 以将其添加到“所选设备”(Selected Devices) 列表。

g) 点击**覆盖 (Override)** 并将**网络 (Network)** 更改为 **10.200.10.10-10.200.10.200**

h) 点击**添加 (Add)** 以将覆盖添加到设备。

通过定义 FTD-B 的覆盖，每当系统在 FTD-B 上配置此对象时，将使用覆盖值而不是原始对象中定义的值。

i) 点击**保存**。

步骤 4 配置 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象 (Source Interface Objects)** = 内部区域。
- **目标接口对象 (Destination Interface Objects)** = 外部区域。

注释
接口对象用于控制应在哪些设备上配置规则。由于在本例中区域仅包含 FTD-A 和 FTD-B 的接口，因此即使 NAT 策略分配给其他设备，规则也将仅部署到这两台设备。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源 (Original Source)** = 内部网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = NAT 池对象。

f) 点击**保存**。

您现在有一条对 FTD-A 和 FTD-B 有不同解释的规则，为每个防火墙保护的内部网络提供唯一转换。

搜索和过滤 NAT 规则表

您可以搜索和过滤NAT规则表，以帮助您查找需要修改或查看的规则。过滤表时，仅显示匹配的规则。请注意，尽管规则编号依次更改为1、2等，但过滤不会更改实际规则编号或规则在表中相对于隐藏规则的位置。过滤只是更改您可以看到的内容，以帮助您找到您感兴趣的规则。

编辑 NAT 策略时，可以使用表上方的字段执行以下类型的搜索/过滤：

- **按设备过滤 (Filter by Device)** - 点击 **按设备过滤 (Filter by Device)**，然后选择要查看其规则的设备，然后点击 **确定 (OK)**。规则是否适用于设备取决于规则的接口限制。如果为源接口或目标

接口指定安全区域或接口组，则当设备的至少一个接口位于该区域或组中时，该规则将应用于该设备。如果 NAT 规则适用于任何源接口和任何目标接口，则它适用于所有设备。

如果您还执行文本或多属性搜索，则结果仅限于所选设备。

要删除此过滤器，请点击**按设备过滤 (Filter by Device)** 并取消选择设备，或选择**全部 (All)**，然后点击**确定 (OK)**。

- **简单文本搜索**-在 **过滤器** 框中，键入字符串，然后按 Enter 键。该字符串将与规则中的所有值进行比较。例如，如果输入“network-object-1”（网络对象的名称），则会获得在源、目标和 PAT 池属性中使用该对象的规则。

  对于网络和端口对象，该字符串还会与规则中使用的对象的内容进行比较。例如，如果 PAT 池对象包括 10.100.10.3-10.100.10.100 范围，则在 10.100.10.3 或 10.100.10.100（或部分 10.100.10）上搜索将包括使用该 PAT 池对象的规则。但是，匹配必须精确：在 10.100.10.5 上搜索将不匹配此 PAT 池对象，即使 IP 地址在对象的 IP 地址范围内。

  要删除过滤器，请点击过滤器框右侧的 **x**。

- **多属性搜索**-如果简单文本搜索提供的结果过多，可以为搜索配置多个值。点击**过滤器 (Filter)** 框以打开属性列表，然后选择或输入要搜索的属性的字符串，然后点击**过滤器**按钮。这些属性与您在 NAT 规则中配置的属性相同。属性已进行 AND 运算，因此过滤后的结果仅包含与您配置的所有属性匹配的规则。

  - 对于二进制属性，例如规则状态（启用/禁用）、是否配置了 PAT 池（启用/禁用）、规则的方向（uni/bi）或规则类型（静态/动态），只需选中或取消选中相应的复选框。如果您不关心属性值，请选中这两个复选框。如果取消选中这两个框，则没有任何规则与过滤器匹配。
  - 对于字符串属性，请键入与该属性相关的完整或部分字符串。这些将是安全区域/接口组、网络对象或端口对象的对象名称。它也可以是网络或端口对象内容，其匹配方式与简单文本搜索相同。

  要删除过滤器，请点击“过滤器”(Filter) 框右侧的 **x**，或点击“过滤器”(Filter) 框以打开下拉列表，然后点击清除按钮。

启用、禁用或删除多个规则

您可以逐一启用或禁用手动 NAT 规则，或者删除任何 NAT 规则。您也可以选择多个规则，并将更改一次性应用于所有规则。由于启用/禁用仅适用于手动NAT，如果您选择了混合规则类型，那么就只能将其删除。

请注意，在启用或禁用规则时，选择一些已启用或禁用的规则并不重要。例如，启用已启用的规则只会让该规则保持启用状态。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT**，并编辑威胁防御 NAT 策略。

步骤 2 （可选。）过滤 NAT 规则，以便找到要更改的规则。

如果您有大型 NAT 策略，过滤特别有用。例如，您可以搜索已禁用的规则以便查找需要启用的规则。

步骤 3 选择要更改的规则。

- 点击规则左列中的复选框，以便选择（或取消选择）单个规则。
- 点击表头中的复选框，以便选择当前显示页面上的所有规则。

在翻页时，您的选择会被保留。但实际上，最好是在转到下一页之前对页面上选择的规则执行操作。

步骤 4 执行所需的操作。如果选择了多个规则，系统会要求您确认操作。

请注意，这些操作也可通过右键点击菜单来执行。

- 要启用所有规则，请点击**选择批量操作 (Select Bulk Action)** > **启用 (Enable)**。
- 要禁用所有规则，请点击**选择批量操作 (Select Bulk Action)** > **禁用 (Disable)**。
- 要删除所有规则，请点击**选择批量操作 (Select Bulk Action)** > **删除 (Delete)**。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

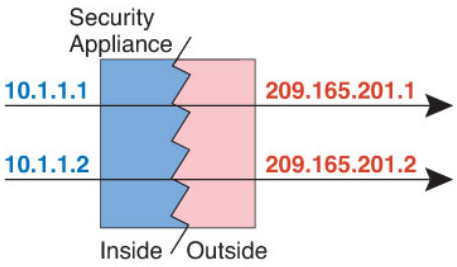
关于动态 NAT

动态NAT将一个实际地址组转换为一个可在目标网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标网络时，NAT会从映射池中为该主机分配IP地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保持同一IP地址。因此，目标网络上的用户不能向使用动态NAT的主机发起可靠连接，即使访问规则允许该连接。

注释 在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。远程主机的成功连接可重置连接的空闲计时器。

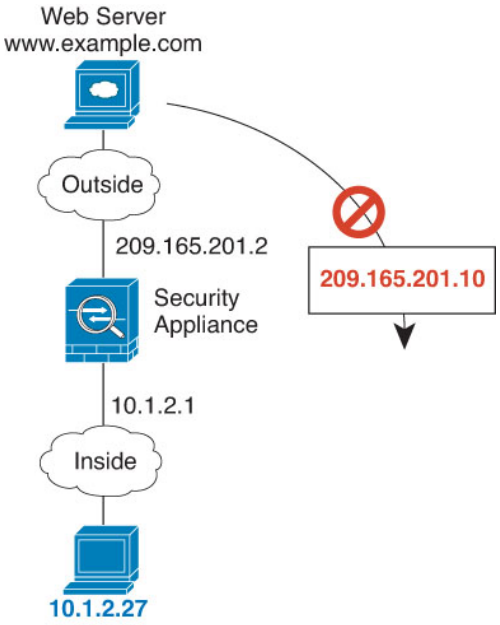
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 412: 动态 NAT



下图显示一台远程主机尝试发起到映射地址的连接。该地址当前不在转换表中；因此，会丢弃数据包。

图 413: 远程主机尝试向映射地址发起连接



动态 NAT 的不足与优势

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。

  如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。

- 不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不适用于以下项：

- 没有超载端口的 IP 协议，例如 GRE 0 版本。

- 某些多媒体应用，它们在一个端口上有数据流，在另一个端口上有控制路径，并且不是开放标准。

配置动态自动 NAT

使用动态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 此选项可以是网络对象或组，但不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。如果对象仅包含一个主机地址，则将该地址用于 PAT。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型** - 选择**动态**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **常规转换**上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 包含映射地址的网络对象或组。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于

从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 1395 页。

- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置动态手动 NAT

当自动 NAT 不能满足您的需求时，请使用动态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。动态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源 (Original Source)** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 此选项可以是网络对象或组，但不能包含在子网中。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。如果对象仅包含一个主机地址，则将该地址用于 PAT。

如果您要在规则中为 **原始目标** 和 **转换后的目标** 配置静态转换，还可以为这些地址创建网络对象或组。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

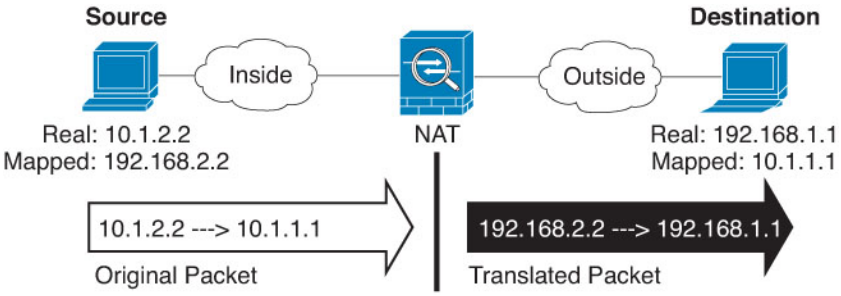
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源** - 包含将要转换的地址的网络对象或组。
- **原始目标** -（可选。）包含目的目标地址的网络对象或组。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以选择**源接口 IP (Source Interface IP)** 以使原始目的基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 包含映射地址的网络对象或组。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- （仅适用于源转换。）**转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 1395 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 9 点击**保存**以添加规则。

步骤 10 点击“NAT”页面上的**保存**以保存更改。

动态 PAT

以下主题介绍动态 PAT。

关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。

每个连接都需要单独的转换会话，因为每个连接的源端口都不同。例如，10.1.1.1:1025 需要来自 10.1.1.1:1026 的单独的转换。

下图显示一个典型的动态 PAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。映射地址对于每次转换都是相同的，但端口需要动态分配。

图 *414:* 动态 *PAT*



对于转换持续时间，如果访问规则允许，目标网络上的远程主机可以发起到转换后主机的连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

在连接过期后，端口转换也将过期。



注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 的优缺点

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 Firewall Threat Defense 接口 IP 地址用作 PAT 地址。

在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组成员或一个接口为网桥组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关详细信息，请参阅对检测到的协议的 NAT 支持，第 1304 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。可以配置一个 PAT 地址池，使用 PAT 地址轮询分配来避免出现这种情况。

PAT 池对象准则

当为 PAT 池创建网络对象时，请遵守以下准则。

对于 PAT 池

- 端口会映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

  在集群中运行时，每个地址的512个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。如果更改集群设备限制（集群大小），请确保清除转换或重新启动设备，以便将 PAT 池适当地重新分配到集群设备。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。

- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT，则另一条规则也必须指定扩展 PAT。

- 如果主机拥有现有连接，则来自该主机的后续连接会使用相同的 PAT IP 地址。如果没有可用的端口，这可能会阻止连接。使用轮询选项可避免此问题。

- 为获得最佳性能，请将 PAT 池中的 IP 地址数量限制为 10,000。

对于 PAT 池的扩展 PAT

- 许多应用检测不支持扩展 PAT。

- 如为动态 PAT 规则启用扩展 PAT，则不能在支持端口转换规则的另一静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。
- 扩展 PAT 会增加设备上的内存使用率。

对于 PAT 池的轮询

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。不过，这种“粘性”不能超越故障转移。如果该设备执行故障转移，来自主机的后续连接可能会使用初始 IP 地址。
- 如果在同一接口上混合使用 PAT 池/轮询规则和接口 PAT 规则，IP 地址"粘性"也会受到影响。对于任何给定接口，请选择 PAT 池或接口 PAT；请勿创建竞争 PAT 规则。
- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议/IP 地址/端口范围创建 NAT 池，因此，轮询会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 甚至将导致更多数量的并发 NAT 池。

配置动态自动 PAT

使用动态自动 PAT 规则可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。您可以转换为单个地址（目标接口的地址或其他地址），或者使用地址的 PAT 池来提供更多的可能转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 可通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。
  - **PAT 池** - 创建一个包含范围的网络对象，或创建一个包括主机、范围或这两者的网络对象组。不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** ( )以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型** - 选择**动态**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **常规转换**上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。跳过配置 PAT 池的步骤。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。跳过配置 PAT 池的步骤。
  - 若要使用 PAT 池，请将**转换后的源**留空。请不要选择目标接口 IP 或单个地址作为**转换后的源**。

步骤 6 如果使用的是 PAT 池，请选择 **PAT 池**页面并执行以下操作：

a) 选择**启用 PAT 池 (Enable PAT pool)**。

b) 选择包含 **PAT** > **地址**字段中的池地址的网络对象组。

或者，可以选择**目的接口 IP (Destination Interface IP)**，它是实施接口 PAT 的另一种方法。

c) （可选）根据需要选择以下选项：

- **使用轮询分配** - 以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。

- **扩展 PAT 表** - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。
- **扁平端口范围、包括保留端口** - 在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的 Firewall Threat Defense 设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。
- **块分配** - 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 7 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。 如果已配置接口 PAT 作为转换后的地址或 PAT 池，则不能选择此选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 8 点击**保存**以添加规则。

步骤 9 点击“NAT”页面上的**保存**以保存更改。

配置动态手动 PAT

当自动 PAT 不能满足您的需求时，请使用动态手动 PAT 规则。例如，如果您要根据目标进行不同的转换。动态 PAT 可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。您可以转换为单个地址（目标接口的地址或其他地址），或者使用地址的 PAT 池来提供更多的可能转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源 (Original Source)** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 可通过以下选项指定 PAT 地址：

- **目标接口** - 要使用目标接口地址，不需要网络对象。
- **单个 PAT 地址** - 创建包含单个主机的网络对象。
- **PAT 池** - 创建一个包含范围的网络对象，或创建一个包括主机、范围或这两者的网络对象组。不能包含子网。

如果您要在规则中为 **原始目标** 和 **转换后的目标** 配置静态转换，还可以为这些地址创建网络对象或组。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

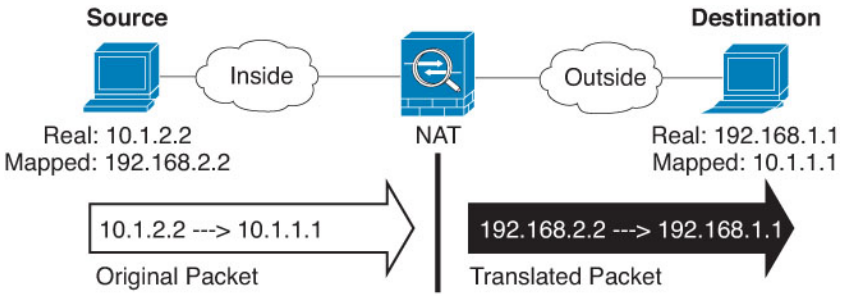
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源** - 包含将要转换的地址的网络对象或组。
- **原始目标** -（可选。）包含目的目标地址的网络对象或组。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以选择**源接口 IP (Source Interface IP)** 以使原始目的基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。跳过配置 PAT 池的步骤。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。跳过配置 PAT 池的步骤。
  - 若要使用 PAT 池，请将**转换后的源**留空。请不要选择目标接口 IP 或单个地址作为**转换后的源**。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 如果使用的是 PAT 池，请选择 **PAT 池**页面并执行以下操作：

a) 选择**启用 PAT 池 (Enable PAT pool)**。

b) 选择包含 **PAT** > **地址**字段中的池地址的网络对象组。

或者，可以选择**目的接口 IP (Destination Interface IP)**，它是实施接口 PAT 的另一种方法。

c) （可选）根据需要选择以下选项：

- **使用轮询分配** - 以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
- **扩展 PAT 表** - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。
- **扁平端口范围、包括保留端口** - 在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的 Firewall Threat Defense 设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。
- **块分配** - 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 9 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。

步骤 10 点击**保存**以添加规则。

步骤 11 点击“NAT”页面上的**保存**以保存更改。

使用端口块分配配置 PAT

对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。当使用块中端口的最后一个转换被删除时，系统将释放该块。

分配端口块的主要原因是为了减少日志记录。记录端口块分配，记录连接，但不会记录在端口块中创建的转换。另一方面，这样会使日志分析变得更加复杂。

只能在 1024-65535 范围内分配端口块。TCP、UDP 和 ICMP 连接有各自独立的块，且这些块可能重叠。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。您可以创建一个单独的 NAT 规则，对于使用低端口号的应用不应用块分配；对于两次 NAT，请确保该规则位于块分配规则之前。

开始之前

NAT 规则的使用说明：

- 您可以包含**使用轮询分配 (Use Round Robin Allocation)** 选项，但无法包含扩展 PAT 唯一性、使用宽范围、包含保留的端口或后退至接口 PAT 的选项。此外，还允许其他源/目标地址和端口信息。
- 同所有 NAT 变更一样，如果要替换现有的规则，必须清除与被替换规则相关的转换，新规则才会生效。可以显式清除它们，也可以静待它们超时。但是，在集群模式下运行时，必须重新加载集群，以便设备能正确分配块。



注释 如果要在常规 PAT 和块分配 PAT 规则之间切换，您必须先删除规则，然后再清除转换。然后，您可以创建新的对象 NAT 规则。否则，您将在 **show asp drop** 输出中看到 pat-port-block-state-mismatch 丢弃。

- 对于特定 PAT 池，必须为使用该池的所有规则指定（或不指定）块分配。不能在一个规则中分配块，而在另一个规则中不分配块。重叠的 PAT 池也不能混合块分配设置。此外，该池的静态 NAT 不能与端口转换规则重叠。

过程

步骤 1 （可选。）配置全局 PAT 端口块分配设置。

有一些可以控制端口块分配的全局设置。如果要更改这些选项的默认值，必须配置一个 FlexConfig 对象，并将其添加到 FlexConfig 策略中。

a) 选择 **对象** > **FlexConfig** > **FlexConfig 对象** 并创建新对象。

b) 配置块分配大小，即每个块中的端口数。

xlate block-allocation size *value*

范围为 32-4096。默认值为 512。使用“no”形式可恢复默认值。

如果不使用默认值，请确保 64,512 能被您所选的大小整除（1024-65535 范围中的端口数)。否则，会出现无法使用的端口。例如，如果指定 100，会有 12 个未使用端口。

使用默认的块分配大小时，单个 PAT IP 可供 126 个唯一的并发用户使用（端口数 64,512 除以 512）。

c) 配置每个主机可分配的最大块数。

xlate block-allocation maximum-per-host *number*

限制是针对每个协议，因此限制为 4 表示每个主机最多 4 个 UDP 块、4个 TCP 块和 4 个 ICMP 块。范围为 1-8，默认值为 4。使用“no”形式可恢复默认值。

d) （可选。）启用临时系统日志生成。

xlate block-allocation pba-interim-logging *seconds*

默认情况下，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志记录，系统会按您指定的时间间隔生成以下消息。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。可以指定 21600 至 604800 秒（6 小时至 7 天）的时间间隔。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

示例：

以下示例将块分配大小设置为 64，将每主机最大数设置为 8，并且每 6 小时启用一次临时日志记录。

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) 在 FlexConfig 对象中选择以下选项：

- **部署** = **每次**
- **类型** = **附加**

f) 点击**保存**以创建 FlexConfig 对象。

g) 选择 **设备** > **+ 显示更多** > **FlexConfig**，创建或编辑分配给需要调整这些设置的设备的 FlexConfig 策略。

h) 在可用对象列表中选择对象，然后点击 **>** 将其移动至所选的对象列表。

i) 点击**保存**。

您可以点击**预览配置**，选择其中一个目标设备，并验证 xlate 命令是否正确显示。

步骤 2 添加使用 PAT 池端口块分配的 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** ，添加或编辑威胁防御 NAT 策略。

b) 添加或编辑 NAT 规则，并至少配置以下选项。

- **类型** = **动态**
- 在 **转换** > **原始源**中，选择定义源地址的对象。
- 在 **PAT 池 (PAT Pool)** 中配置以下选项：
  - 选择**启用 PAT 池**
  - 在 **PAT** > **地址**中选择定义 PAT 池的网络对象或组。
  - 选择**块分配**选项。

c) 保存对规则和 NAT 策略所做的更改。

静态 NAT

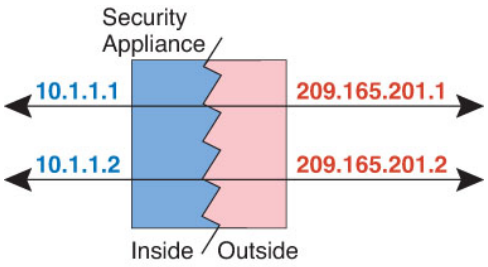
以下主题介绍静态 NAT 以及如何实施静态 NAT。

关于静态 NAT

静态NAT创建实际地址到映射地址的固定转换。因为映射地址对于每个连续连接都是相同的，所以静态NAT允许双向连接发起，即到主机发起和从主机发起（如果有允许这样做的访问规则）。另一方面，通过动态 NAT 和 PAT，每台主机为每次后续转换使用不同的地址或端口，因此，不支持双向发起。

下图显示典型的静态 NAT 场景。转换始终处于活动状态，所以，实际主机和远程主机可以发起连接。

图 *415:* 静态 *NAT*



注释 如果需要，可以禁用双向性。

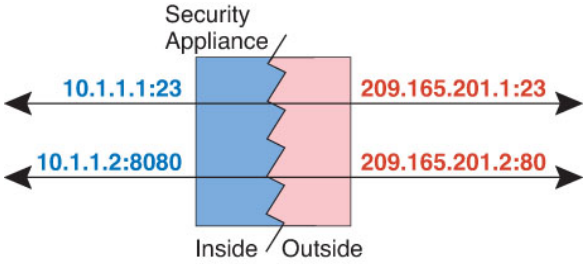
带端口转换的静态 NAT

支持端口转换的静态 NAT 让您可以指定实际和映射协议及端口。

指定带静态 NAT 的端口时，可以选择将端口和/或 IP 地址映射到同一值或不同值。

下图显示支持端口转换的典型静态NAT场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，所以，转换后主机和远程主机可以发起连接。

图 *416:* 支持端口转换的典型静态 *NAT* 场景



支持端口转换的静态 NAT 规则支持仅访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的的目标 IP 地址，连接将被阻止。此外，对于手动 NAT，如果流量与 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，您必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。例如，您可以为 IP 地址配置静态 NAT 规则（不含端口规范），并将其放置在端口转换规则后面。

注释 对于需要对辅助信道执行应用检查的应用（例如 FTP 和 VoIP），NAT 会自动转换辅助端口。

下面是使用支持端口转换的静态 NAT 的其他情况。

具有身份端口转换的静态 NAT

可以简化对内部资源的外部访问。例如，如果您有在不同端口上提供服务（例如 FTP、HTTP 和 SMTP）的三个单独的服务器，可以为外部用户提供单个 IP 地址以访问这些服务。然后，可以配置具有身份端口转换的静态NAT，从而根据尝试访问的端口将单个外部IP地址映射到实际服务器的正确 IP 地址。您无需更改端口，因为服务器使用的是标准端口（分别是 21、80 和 25)。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

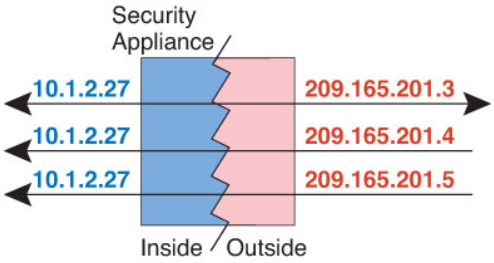
可以配置静态NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

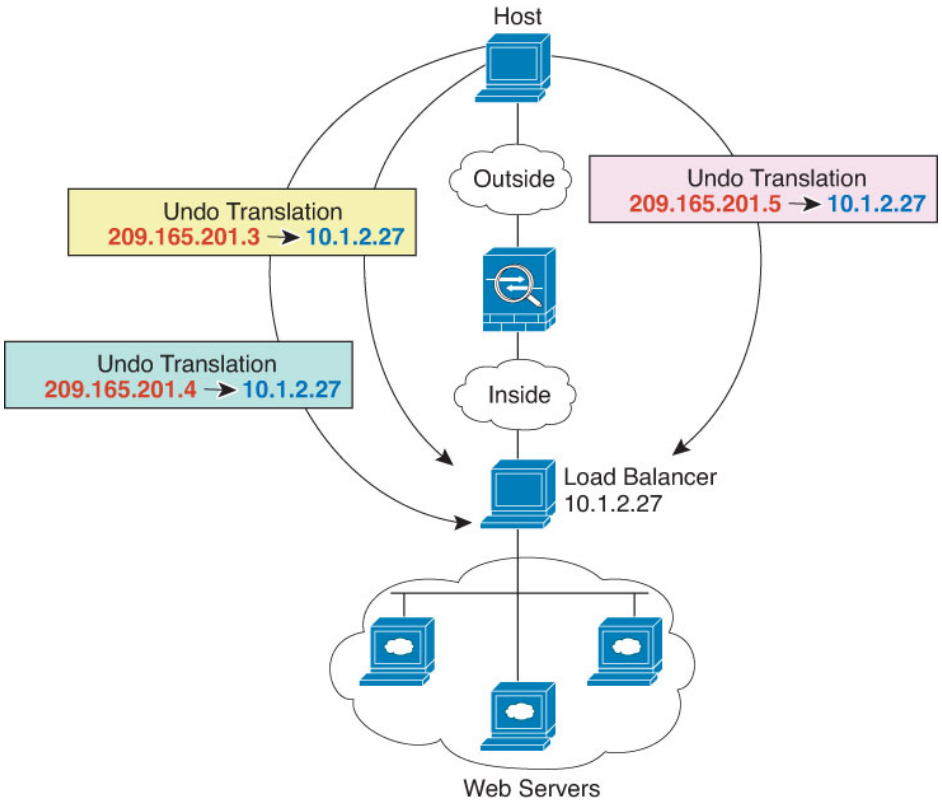
下图显示典型的一对多静态NAT场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 *417:* 一对多静态 ***NAT***



例如，在 10.1.2.27 上有一个负载均衡器。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。

图 *418:* 一对多静态 ***NAT*** 示例



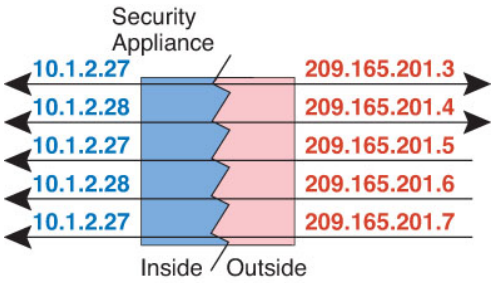
其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，依此类推，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起到实际主机，但所有从实际主机发起的流量仅将第一个映射地址用于源。

下图显示典型的少对多静态 NAT 场景。

图 *419:* 少对多静态 ***NAT***

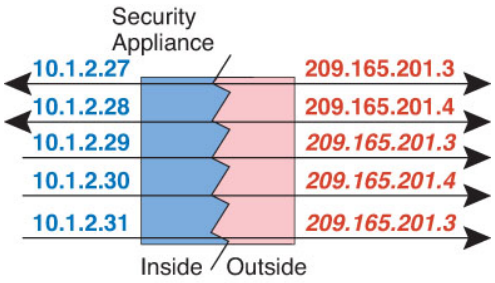


对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。

注释 多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不唯一），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 *420:* 多对少静态 ***NAT***



我们建议不要这样使用静态规则，而是为需要双向发起的流量创建一对一规则，为其他地址创建动态规则。

配置静态自动 NAT

使用静态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 可以通过以下选项指定转换后的地址：
  - **目标接口** - 要使用目标接口地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
  - **地址**-创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **常规转换**上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 以下项之一：

- 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
- （具有端口转换的静态接口NAT。）要使用目标接口的地址，请选择**目标接口IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- （可选。）**原始端口**、**转换后的端口** - 如果需要转换 TCP 或 UDP 端口，请在**原始端口**中选择协议，并输入原始和转换端口编号。例如，如有必要，可以将 TCP/80 转换为 8080。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 1395 页。如果您在进行端口转换，则此选项不可用。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **网络到网络映射** - 对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置静态手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。静态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源 (Original Source)** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 可以通过以下选项指定转换后的地址：

- **目标接口** - 要使用目标接口地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
- **地址 (Address)** - 创建包主机、范围或子网的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

如果您要在规则中为**原始目标 (Original Destination)** 和**转换后的目标 (Translated Destination)** 配置静态转换，还可以为这些地址创建网络对象或组。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

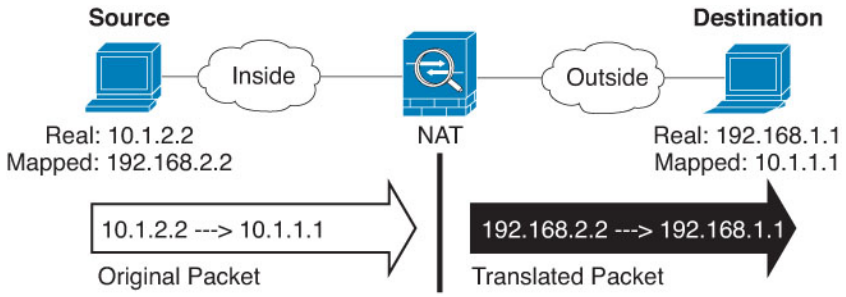
- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** - （网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 （在**转换**页面上。）确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源** - 包含将要转换的地址的网络对象或组。
- **原始目标** -（可选。）包含目的目标地址的网络对象或组。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以选择**源接口 IP (Source Interface IP)** 以使原始目的基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级 (Advanced)** 上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对

于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 1395 页。如果您在进行端口转换，则此选项不可用。

- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **网络到网络映射** - 对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **单向** - 选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。

步骤 9 点击**保存**以添加规则。

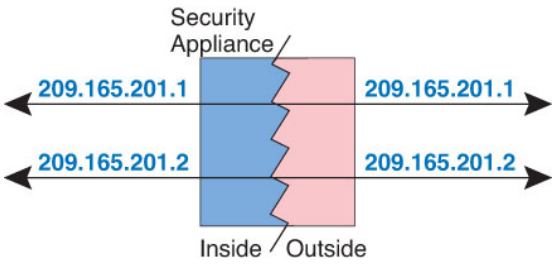
步骤 10 点击“NAT”页面上的**保存**以保存更改。

身份 NAT

可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果您创建了一条将 NAT 应用于所有网络的大范围规则，但希望豁免其中一个网络不受NAT影响，可以创建一条静态NAT规则，将该网络转换为其本身。

下图显示典型的身份 NAT 场景。

图 *421: 身份 NAT*



以下主题介绍如何配置身份 NAT。

配置身份自动 NAT

使用静态身份自动 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址**-该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的源** - 其内容与原始源对象完全相同的网络对象或组。您可以使用相同的对象。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**自动 NAT 规则**。
- **类型 (Type)** - 选择**静态 (Static)**。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 在 **常规转换**上配置以下选项：

- **原始源** - 包含您要转换的地址的网络对象。
- **转换后的源** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

不要为身份 NAT 配置**原始端口**和**转换后的端口**选项。

步骤 6 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **IPv6** - 请勿为身份 NAT 配置此选项。
- **网络到网络映射** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。

步骤 7 点击**保存**以添加规则。

步骤 8 点击“NAT”页面上的**保存**以保存更改。

配置身份手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态身份手动 NAT 规则。例如，如果您要根据目标进行不同的转换。使用静态身份 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源** - 此选项可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源** - 与原始源相同的对象或组。或者，您可以选择内容完全相同的其他对象。

如果您要在规则中为**原始目标 (Original Destination)** 和**转换后的目标 (Translated Destination)** 配置静态转换，还可以为这些地址创建网络对象或组。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。您可以为身份 NAT 使用相同的对象。

过程

步骤 1 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

步骤 2 执行以下操作之一：

- 点击**添加规则 (Add Rule)** 按钮以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

右键点击菜单还具有用于剪切、复制、粘贴、插入和删除规则的选项。

步骤 3 配置基本规则选项：

- **NAT 规则** - 选择**手动 NAT 规则**。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。
- **启用** - 您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。

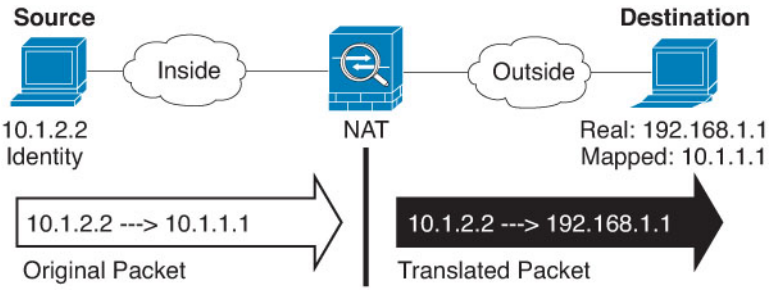
- **插入** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后）或指定规则的上方或下方。

步骤 4 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象**、**目标接口对象** -（网桥组成员接口的必选项。）用于识别此 NAT 规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



- **原始源** - 包含要转换的地址的网络对象或组。
- **原始目标** -（可选。）包含目的目标地址的网络对象或组。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以依次选择**接口对象**，以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源** - 与原始源相同的对象或组。或者，您可以选择内容完全相同的其他对象。
- **转换后的目标** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）在**高级 (Advanced)** 上选择所需选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **IPv6** - 是否为接口 PAT 使用目的地接口的 IPv6 地址。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。
- **单向** - 选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。

步骤 9 点击**保存**以添加规则。

步骤 10 点击“NAT”页面上的**保存**以保存更改。

Firewall Threat Defense 的 NAT 规则属性

使用网络地址转换 (NAT) 规则将 IP 地址转换为其他 IP 地址。通常使用 NAT 规则将私有地址转换为可公开路由的地址。可以将一个地址转换成另一个地址，或可以使用端口地址转换 (PAT) 将多个地址转换为一个或几个地址，并使用端口号区分源地址。

NAT 规则包括以下基本属性。自动 NAT 和手动 NAT 规则的属性相同，除非另行指明。

NAT 类型

是否要配置**手动 NAT 规则**或**自动 NAT 规则**。自动 NAT 仅转换源地址，不能根据目标地址进行不同的转换。因为自动 NAT 更易于配置，因此除非需要手动 NAT 的附加功能，可以使用自动 NAT。有关两者区别的详细信息，请参阅自动 NAT 和手动 NAT，第 1297 页。

类型

转换规则是**动态**还是**静态**。在实施PAT时，动态转换会自动从地址池中选择映射的地址或地址/端口组合。如果要精确定义映射的地址/端口，请使用静态转换。

启用（仅限手动 NAT。）

您是否希望规则处于活动状态。可以随后使用“规则”(Rules) 页面上的右键点击菜单激活或停用该规则。不能禁用自动 NAT 规则。

插入（仅限手动 NAT。）

要添加规则的位置。可以将其插入类别中（在自动NAT规则之前或之后）或指定规则的上方或下方。

说明（可选。仅手动 NAT。)

规则的用途说明。

以下主题介绍 NAT 规则属性的选项卡。

接口对象 NAT 属性

接口对象（安全区或接口组）定义适用NAT规则的接口。在路由模式下，可将默认值“任何”同时用于源和目标，以适用于所有已分配设备的所有接口。但您通常希望选择特定的源和目标接口。

注意

- “任何”接口的概念并不适用于桥接组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，必须指定成员接口。您不能为桥接虚拟接口 (BVI) 本身配置 NAT，只能为成员接口配置 NAT。

  如果选择多个接口对象，则仅当某一已分配的设备上具有包括在所有选定对象中的接口时，才会在该设备上配置NAT规则。例如，如果同时选择了源安全区和目标安全区，则这两个区域必须同时包含一个或多个用于指定设备的接口。

- 如果给定设备上存在多个接口对象，则会为每个接口创建相同的规则。这可能会成为包含目标转换的静态 NAT 规则的问题。由于 NAT 规则基于首次命中规则应用，因此只有为对象配置的第一个接口创建的规则与流量匹配。使用目标转换配置静态NAT时，请使用每个设备最多包含一个接口的接口对象（分配给 NAT 策略），以确保获得所需的结果。

源接口对象、目标接口对象

（网桥组成员接口的必选项。）用于识别此NAT规则应用的接口的接口对象（安全区域或接口组）。**源**是包含实际接口的对象，流量通过该接口进入设备。**目标**是包含映射接口的对象，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

自动 NAT 的转换属性

使用 **转换** 选项定义源地址和映射的转换后地址。以下属性仅适用于自动 NAT。

原始源（始终为必填项）。

包含您要转换的地址的网络对象。该地址必须是网络对象（而非组），而且可以是主机、范围或子网。

您不能为系统定义的 any-ipv4 或 any-ipv6 对象创建自动 NAT 规则。

转换后的源（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。如果对象仅包含一个主机地址，则将该地址用于 PAT。
- **动态 PAT** - 以下项之一：

- （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的IPv6地址，还必须在**高级 (Advanced)**上选择 **IPv6** 选项。请勿配置 PAT 池。
- 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。请勿配置 PAT 池。
- 要使用 PAT 池，请将**转换后的源**保留为空。在 **PAT 池 (PAT Pool)** 上选择 PAT 池对象。

- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级**选项卡上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始端口、转换后的端口（仅静态 NAT）。

如果需要转换 TCP 或 UDP 端口，请在**原始端口**中选择协议，并输入原始和转换端口编号。例如，如有必要，可以将 TCP/80 转换为 8080。不要为身份 NAT 配置这些选项。

手动 NAT 的转换属性

使用 **转换** 选项定义源地址和映射的转换后地址。以下属性仅适用于手动NAT。所有选项均为可选，除非另行指明。

原始源（始终为必填项）。

包含您要转换的地址的网络对象或组。该地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以在规则中指定**任何**。

转换后的源（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。如果对象仅包含一个主机地址，则将该地址用于 PAT。

- **动态 PAT** - 以下项之一：
  - （接口 PAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的IPv6地址，还必须在**高级 (Advanced)**上选择 **IPv6** 选项。请勿配置 PAT 池。

- 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。请勿配置 PAT 池。
- 要使用 PAT 池，请将**转换后的源**保留为空。在 **PAT 池 (PAT Pool)** 上选择 PAT 池对象。

- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择**地址**和包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**目标接口 IP (Destination Interface IP)**。您还必须选择特定目标接口。要使用接口的 IPv6 地址，还必须在**高级**选项卡上选择 **IPv6** 选项。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始目标

包含目的目标地址的网络对象或组。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以选择**源接口 IP (Source Interface IP)** 以使原始目的基于源接口（不能为“任意”[Any]）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

转换目标

包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

您可以使用指定完全限定域名作为转换目的的网络对象；有关更多信息，请参阅FQDN 目标准则，第 1306 页。

原始源端口、转换后的源端口、原始目标端口、转换后的目标端口

为原始和转换后的数据包定义源和目标服务的端口对象。您可以转换端口，或者选择同一对象以便在没有转换端口的情况下使规则敏感察觉到该服务。在配置服务时请记住以下规则：

- （动态 NAT 或 PAT。）不能对**原始源端口**和**转换后的源端口**进行转换。您可以仅对目标端口进行转换。
- NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

PAT 池 NAT 属性

在配置动态 NAT 时，可以定义一个地址池，以用于使用 **PAT 池**选项卡上的属性的“端口地址转换”。

启用 PAT 池

选择此选项可为 PAT 配置一个地址池。

PAT

用于以下 PAT 池之一的地址：

- **地址** - 定义 PAT 池地址的对象，或者是包括某一范围的网络对象，或者是包含主机、范围或二者的网络对象组。不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- **目标接口 IP**-指示您希望将目标接口用作 PAT 地址。对于此选项，必须选择某一特定 **目标接口对象**；不能将 **任何** 用作目标接口。这是实施接口 PAT 的另一种方法。

循环法

以轮询方式分配地址/端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的一个地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。

扩展 PAT 表

使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。不能将此选项用于接口 PAT 或接口 PAT 回退。

不分段端口范围；包括保留端口

在分配 TCP/UDP 端口时使用 1024 到 65535 的端口范围作为单个扁平范围。（6.7 以下版本）为转换选择映射端口号时，PAT 使用实际源端口号（若可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的整个范围，另请勾选**包括保留端口 (Include Reserved Ports)** 选项。对于运行版本 6.7 或更高版本的 Firewall Threat Defense 设备，无论是否选择该选项，始终配置扁平端口范围。您仍可以为这些系统选择**包括保留端口 (Include Reserved Ports)** 选项，并且系统将采用该设置。

阻止分配

启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

高级 NAT 属性

在配置 NAT 时，可以在**高级**选项中配置提供专业化服务的属性。所有这些属性都是可选的：仅当需要服务时才对其进行配置。

转换与此规则匹配的 DNS 回复

是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 1395 页。 如果在静态 NAT 规则中进行端口转换，则此选项不可用。

贯穿到接口 PAT（目标接口）（仅动态 NAT。）

当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。要使用接口的 IPv6 地址，另请勾选 **IPv6** 选项。如果已配置了接口 PAT 配置作为转换的地址，则不能选择此选项。另外，配置 PAT 池时也不能选择此选项。

IPv6

是否为接口 PAT 使用目的地接口的 IPv6 地址。

网络到网络映射（仅静态 NAT）。

对于 NAT 46，请选择此选项以将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此选项。

不在目标接口上使用代理 ARP（仅静态 NAT。）

为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

对目标接口执行路由查找（仅静态身份 NAT。仅路由模式。）

如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

单向（仅手动 NAT，仅静态 NAT。）

选择此选项以阻止目标地址发起流向源地址的流量。单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。

转换 IPv6 网络

当需要在仅 IPv6 网络和仅 IPv4 网络之间传递流量时，需要使用 NAT 在地址类型之间进行转换。即使两个都是 IPv6 网络，您也可能需要对外部网络隐藏内部地址。

对于 IPv6 网络，您可以使用以下转换类型：

- NAT64、NAT46 - 将 IPv6 数据包转换成 IPv4 数据包，反之亦然。您需要定义两个策略，一个用于 IPv6 向 IPv4 的转换，另一个用于 IPv4 向 IPv6 的转换。虽然您可以使用单一 手动 NAT 规

则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和网桥组成员接口上使用。

NAT64/46：将 IPv6 地址转换为 IPv4 地址

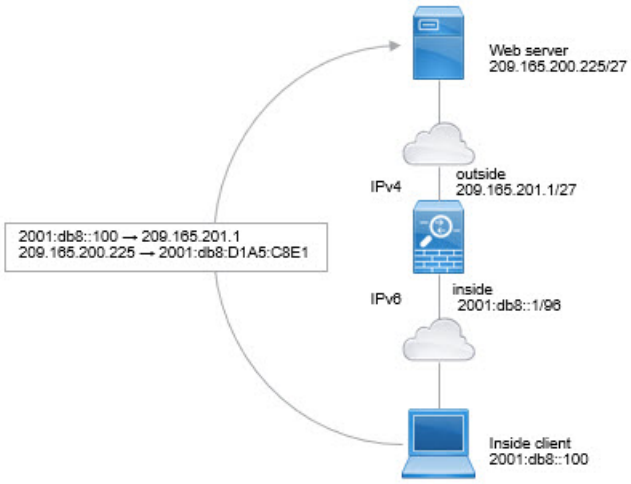
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 Ipv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目标 IPv4 网络。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网

以下是一个非常简单的示例，假设您具有仅包含 IPv6 的内部网络，且您希望将发送到互联网的流量转换为 IPv4。此示例假定您无需 DNS 转换，以便可以在单个手动 NAT 规则中执行 NAT64 和 NAT46 转换。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。

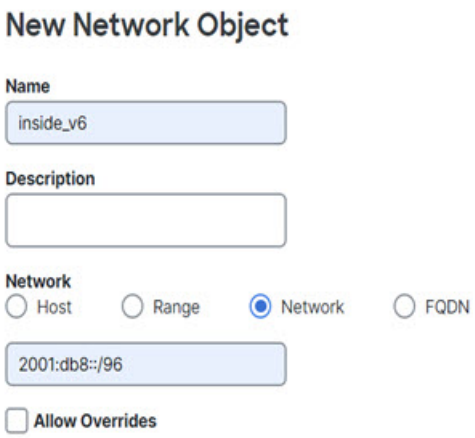
过程

步骤 1 创建定义内部 IPv6 网络的网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8::/96。



c) 点击**保存**。

步骤 2 创建手动 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

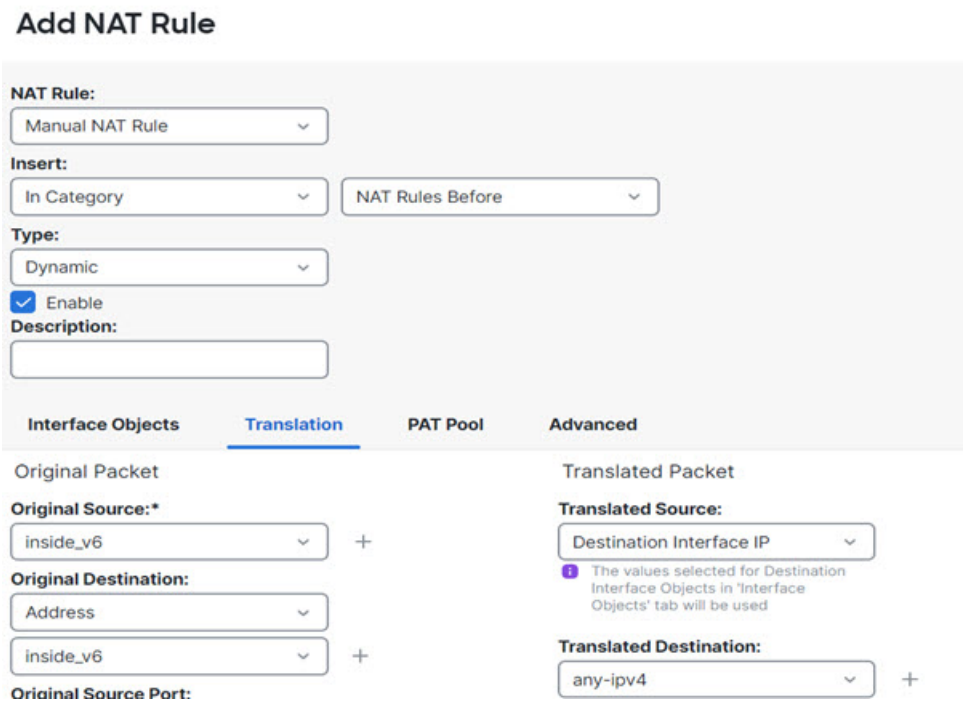
- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **已转换的源** = **目标接口 IP**。
- **原始目标 (Original Destination)** = inside_v6 网络对象。
- **转换后的目标 (Translated Destination)** = any-ipv4 网络对象。



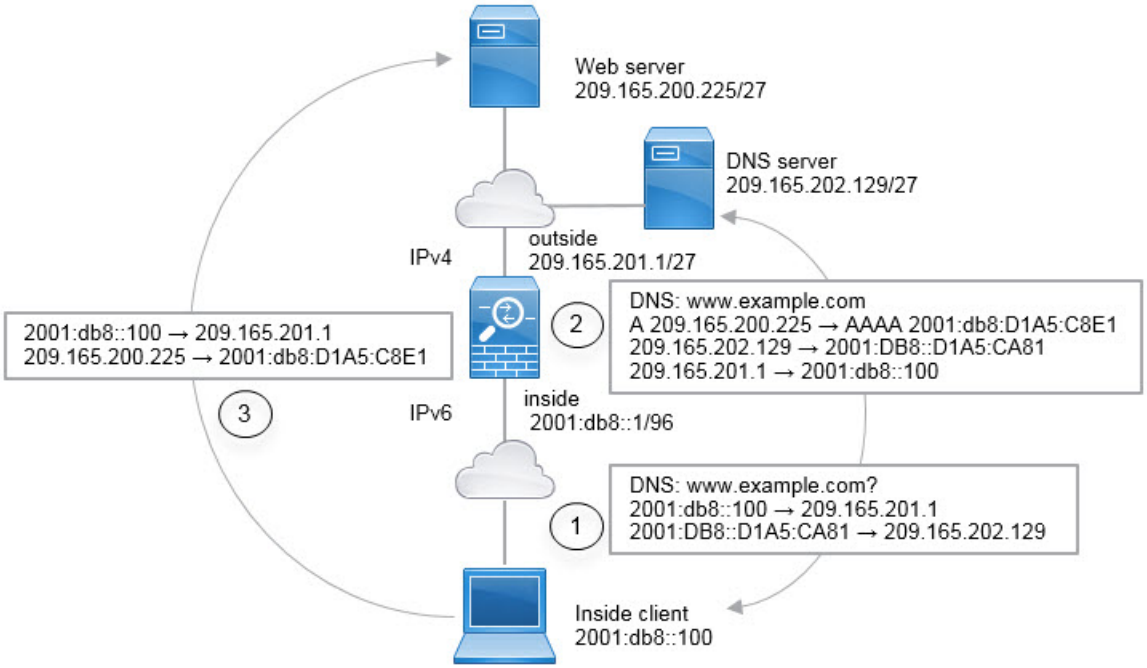
f) 点击**确定**。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。相反，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。

g) 点击 NAT 规则页面上的**保存**。

NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络

下面是一个典型的示例：内部网络只支持 IPv6，但外部互联网上有一些内部用户所需的服务只支持 IPv4。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。对 NAT46 规则启用 DNS 重写，使外部 DNS 服务器的回复可以从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，地址也能从 IPv4 地址转换为 IPv6 地址。

当内部 IPv6 网络中地址为 2001:DB8::100 的客户端尝试打开 www.example.com 时，此 Web 请求的典型顺序如下。

1. 客户端的计算机向地址为 2001:DB8::D1A5:CA81 的 DNS 服务器发送 DNS 请求。NAT 规则对 DNS 请求中的源和目的进行以下转换：
   - 2001:DB8::100 转换为 209.165.201.1 上的唯一端口（NAT64 接口 PAT 规则。）
   - 2001:DB8::D1A5:CA81 转换为 209.165.202.129（NAT46 规则。）D1A5:CA81 是 209.165.202.129 的 IPv6 对应物。）
2. DNS 服务器以 A 记录进行响应，指出 www.example.com 位于 209.165.200.225。NAT46 规则（已启用 DNS 重写）将 A 记录转换为 IPv6 对应物 AAAA 记录，并在 AAAA 记录中将 209.165.200.225 转换为 2001:db8:D1A5:C8E1。此外，DNS 响应中的源地址和目标地址未转换：
   - 209.165.202.129 转换为 2001:DB8::D1A5:CA81
   - 209.165.201.1 转换为 2001:db8::100

3. IPv6 客户端现在有 Web 服务器的 IP 地址，于是向位于 2001:db8:D1A5:C8E1 的 www.example.com 发出 HTTP 请求。（D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物。）HTTP 请求中的源和目的进行转换：
   - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）
   - 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

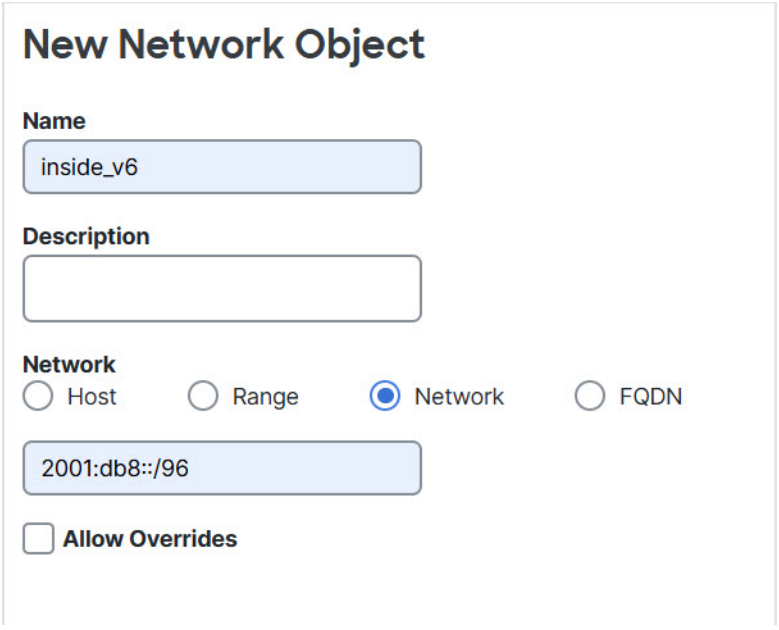
过程

步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义内部 IPv6 网络。

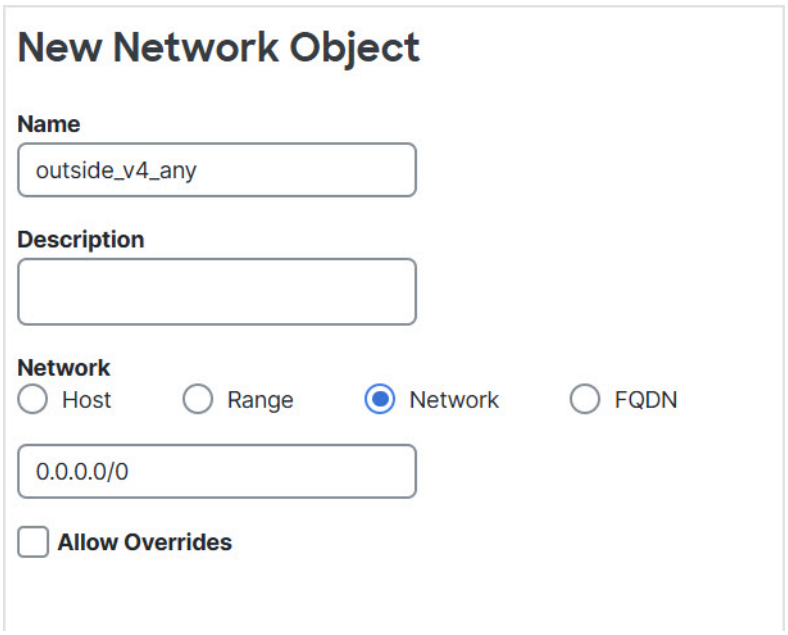
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8::/96。



c) 点击**保存**。

d) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**并定义外部 IPv4 网络。

为网络对象命名（例如，outside_v4_any），然后输入网络地址 0.0.0.0/0。



e) 点击**保存**。

步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

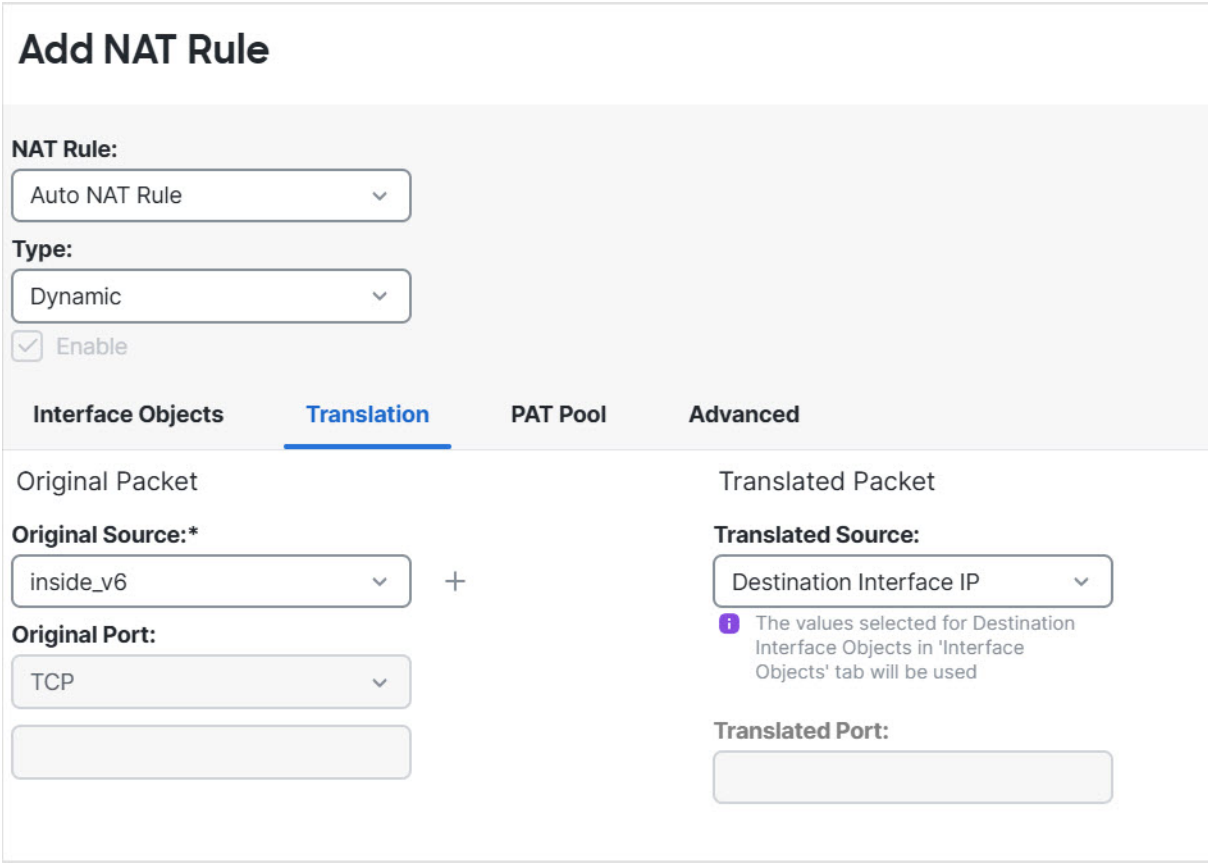
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = outside_v4_any 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = inside_v6 网络对象。

e) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。



f) 点击**确定**。

使用此规则时，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。此外，DNS 响应从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，其地址也从 IPv4 地址转换为 IPv6 地址。

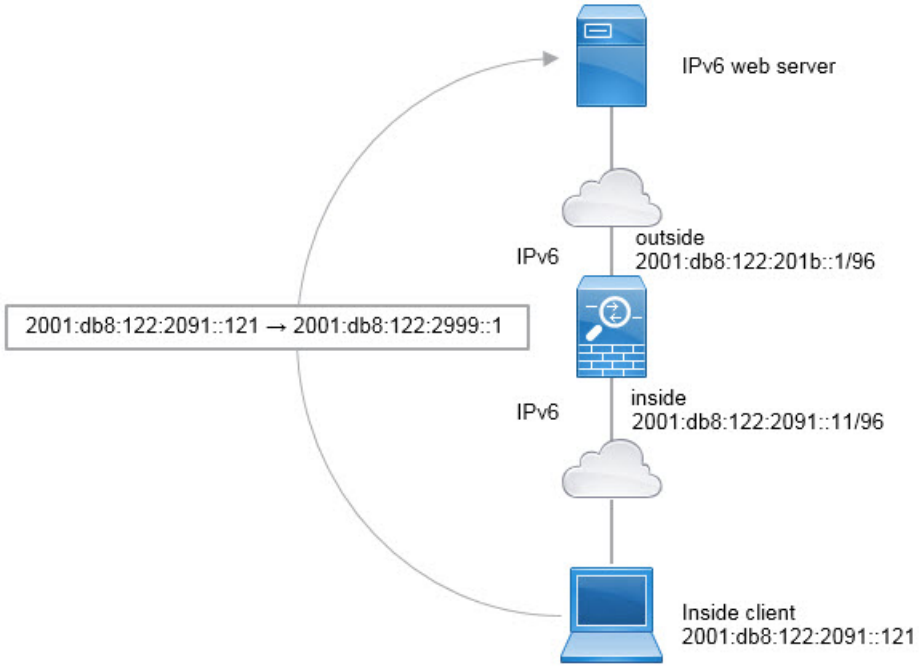
NAT66：将 IPv6 地址转换为其他 IPv6 地址

当从一个 IPv6 网络进入另一个 IPv6 网络时，您可以将地址转换为外部网络上的不同 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

因为您不是在不同的地址类型之间转换，所以您需要一个单一的 NAT66 转换规则。使用自动 NAT 可轻松地为这些规则建模。但是，如果不想允许返回流量，您可以仅使用手动 NAT 将静态 NAT 规则设为单向。

NAT66 示例，网络之间的静态转换

您可以使用自动NAT在IPv6地址池之间配置静态转换。以下示例说明如何将2001:db8:122:2091::/96网络中的内部地址转换为 2001:db8:122:2999::/96 网络中的外部地址。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

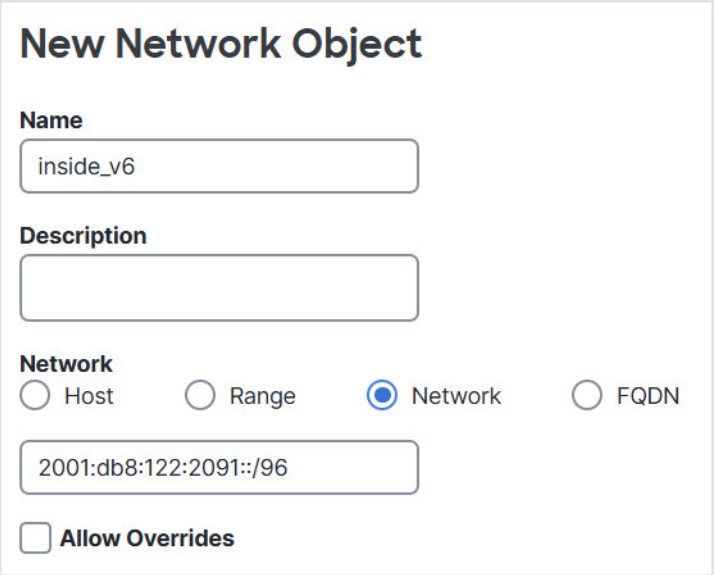
过程

步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义内部 IPv6 网络。

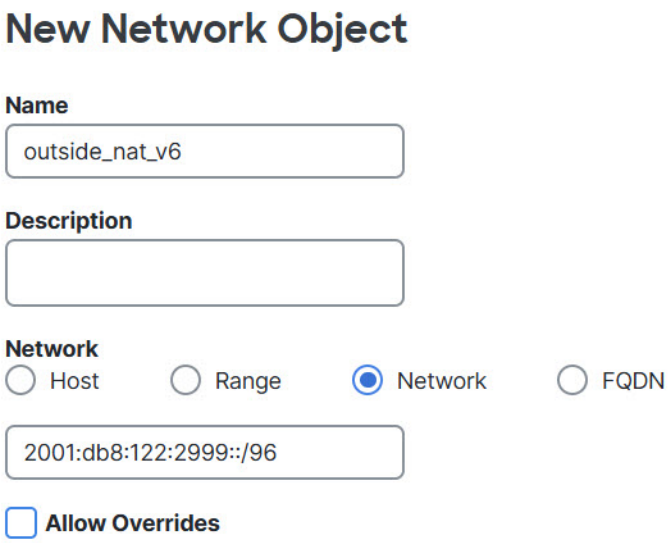
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8:122:2091::/96。



c) 点击保存。

d) 点击添加网络 **(Add Network)** > 添加对象 **(Add Object)** 并定义外部 IPv6 NAT 网络。

为网络对象命名（例如，outside_nat_v6），然后输入网络地址 2001:db8:122:2999::/96。



e) 点击保存。

步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击添加规则。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。

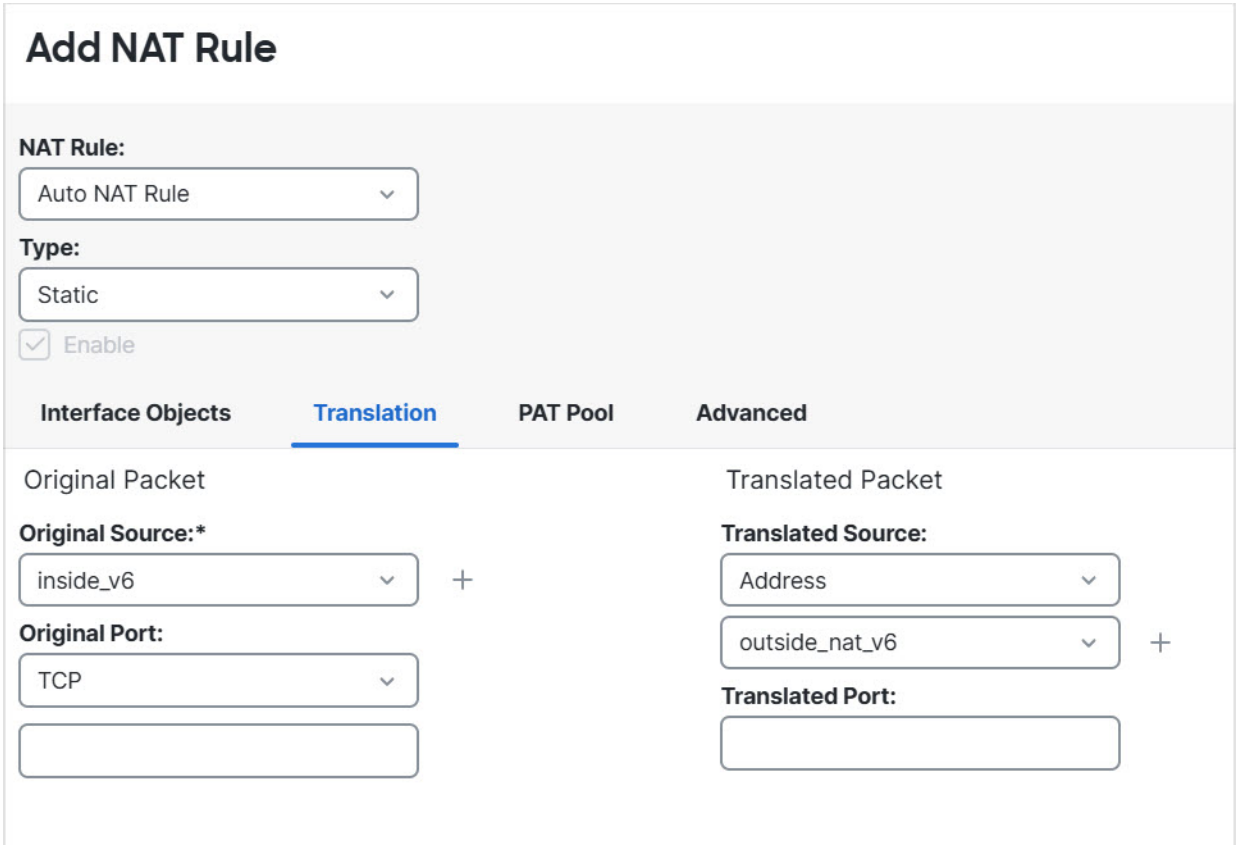
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = outside_nat_v6 网络对象。



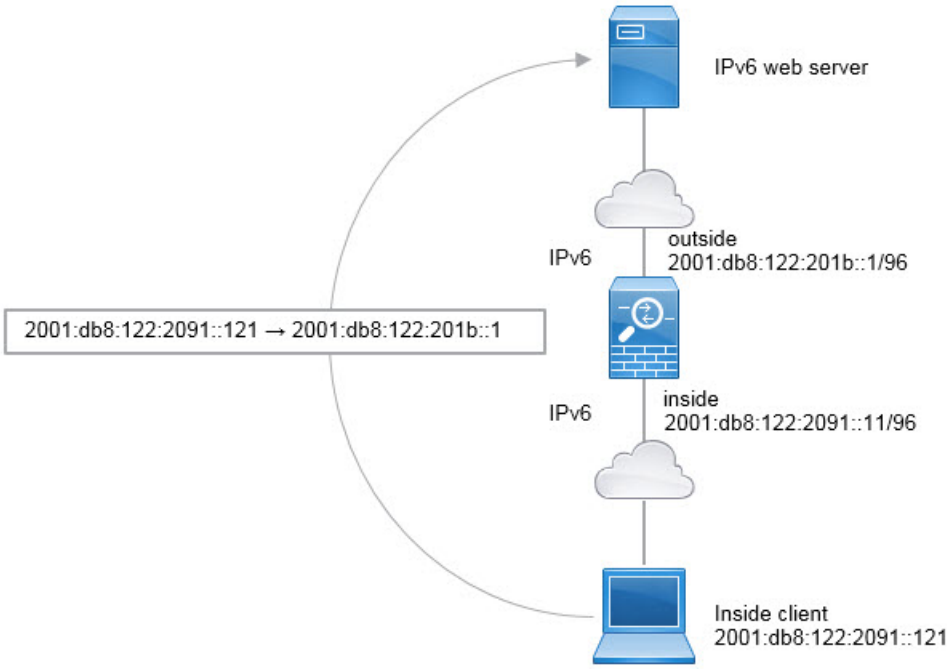
f) 点击**确定**。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

为 NAT66 配置接口 PAT 规则时，该接口上配置的所有全局地址均用于 PAT 映射。该接口的链路本地地址或站点本地地址不用于 PAT。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

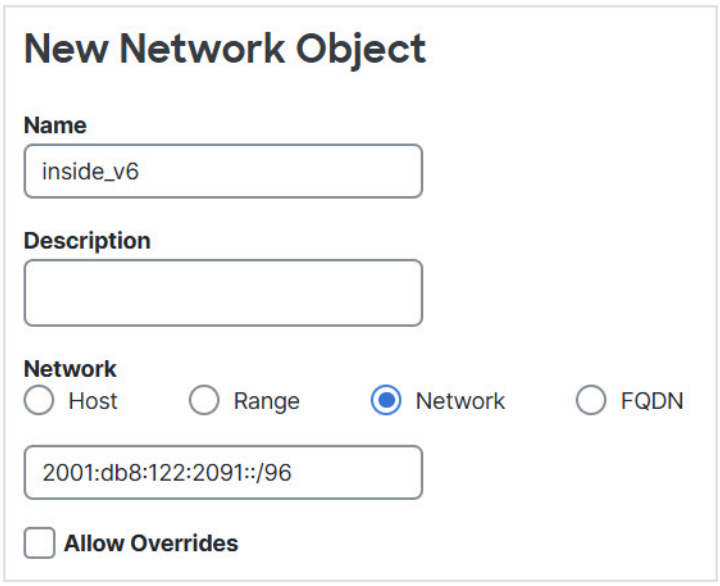
过程

步骤 1 创建定义内部 IPv6 网络的网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），然后输入网络地址 2001:db8:122:2091::/96。



c) 点击**保存**。

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

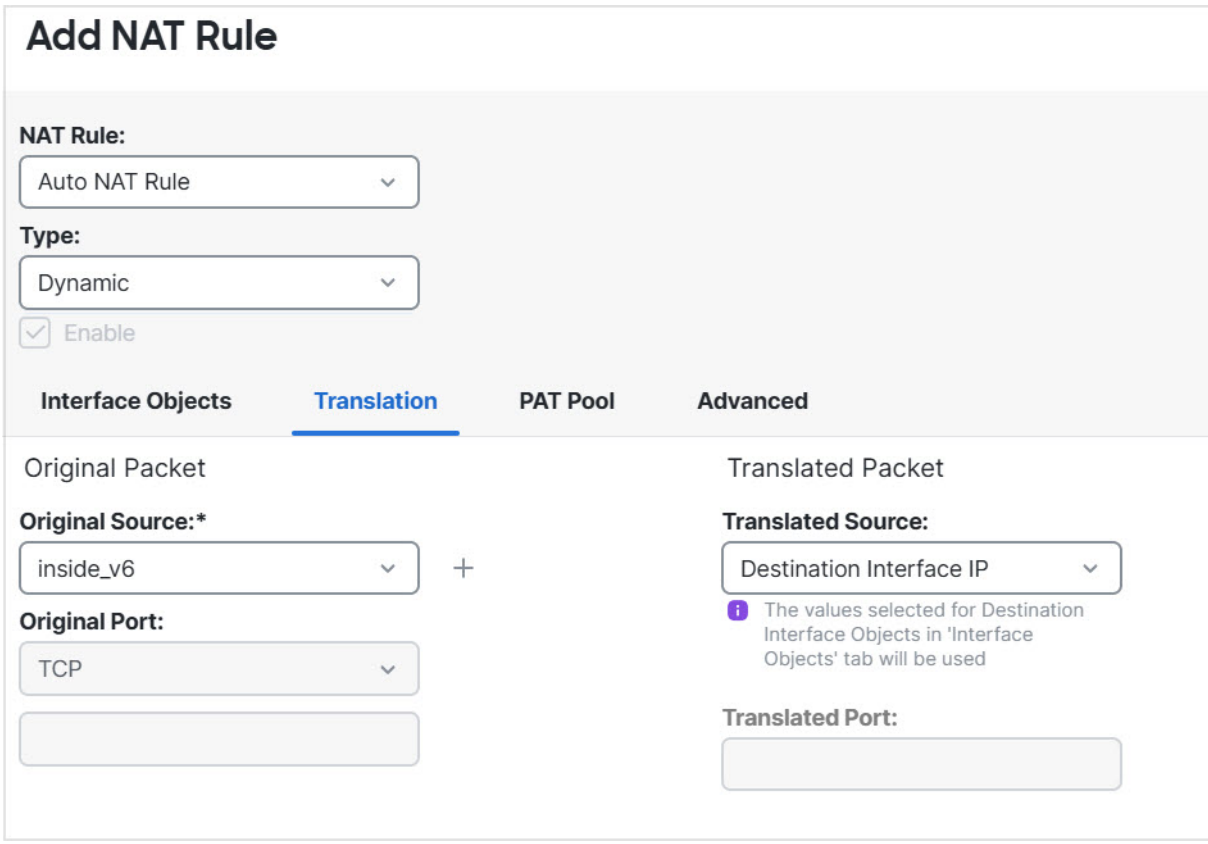
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = inside_v6 网络对象。
- **已转换的源** = **目标接口 IP**。

f) 在 **高级**上，选择 **IPv6**，指示应使用的目标接口 IPv6 地址。



g) 点击**确定**。

使用此规则，从内部接口的 2001:db8:122:2091::/96 子网到外部接口的任何流量均会通过 NAT66 PAT 转换为为外部接口配置的 IPv6 全局地址之一。

监控 NAT

要对 NAT 连接进行监控和故障排除，请登录设备 CLI 并使用以下命令。

- **show nat** 显示 NAT 规则和每个规则的命中计数。还有其他关键字可用于显示 NAT 的其他方面信息。
- **show xlate** 显示当前处于活动状态的实际 NAT 转换。
- **clear xlate** 允许删除处于活动状态的 NAT 转换。如果更改 NAT 规则，您可能需要删除活动的转换，因为现有连接继续使用旧的转换槽，直到连接结束。清除转换允许系统根据您的新规则，在客户端的下一次连接尝试中为客户端构建新的转换。

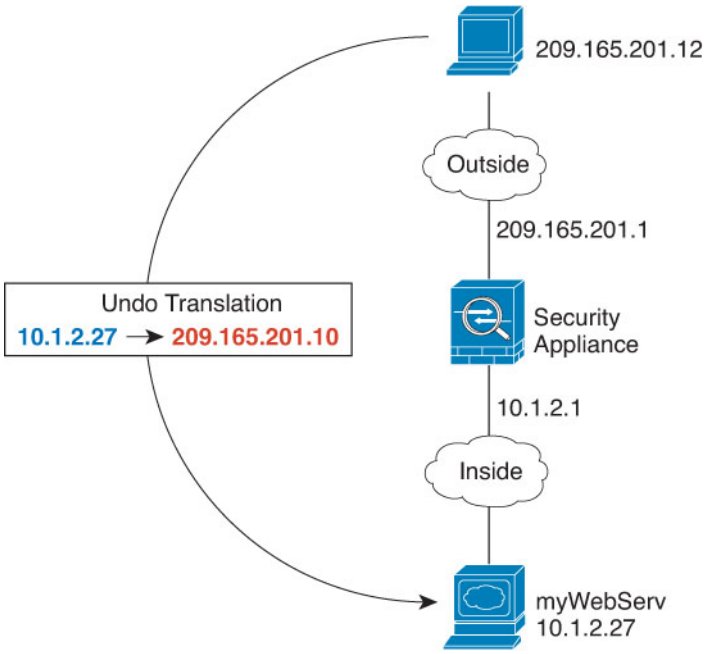
NAT 示例

以下主题提供了配置 NAT 的示例。

提供对内部 Web 服务器的访问权限（静态自动 NAT）

以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。

图 *422:* 面向内部 *Web* 服务器的静态 *NAT*



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

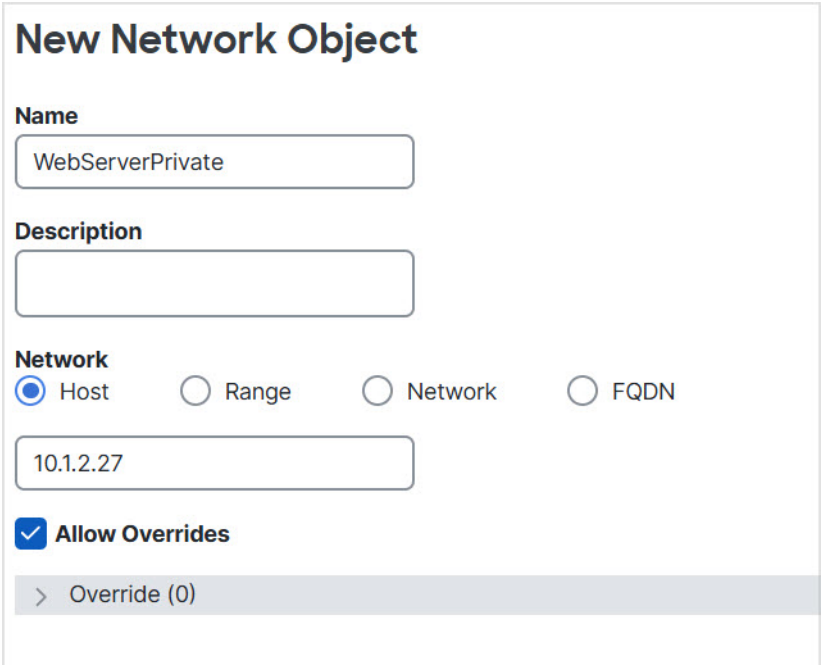
过程

步骤 1 创建定义服务器私有和公共主机地址的网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义 Web 服务器的私有地址。

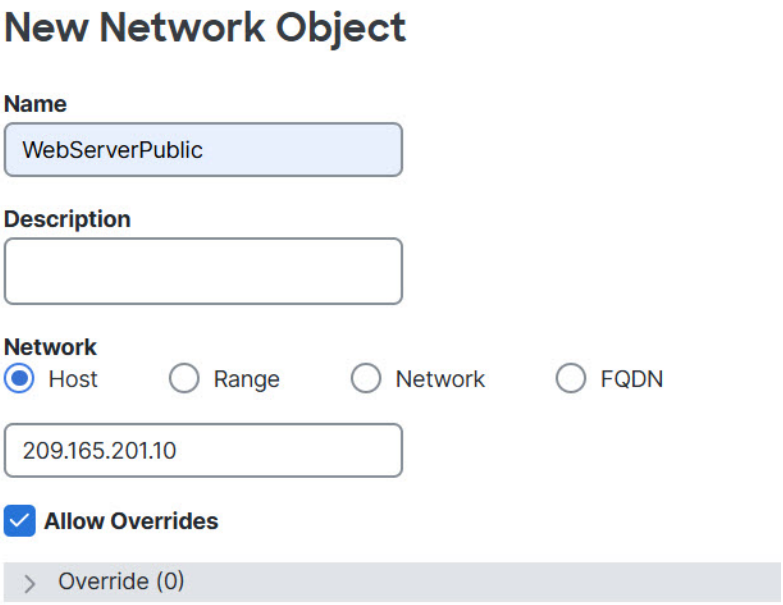
为网络对象命名（例如，WebServerPrivate），然后输入实际主机 IP 地址 10.1.2.27。



c) 点击保存。

d) 点击添加网络 **(Add Network)** > 添加对象 **(Add Object)** 并定义公共地址。

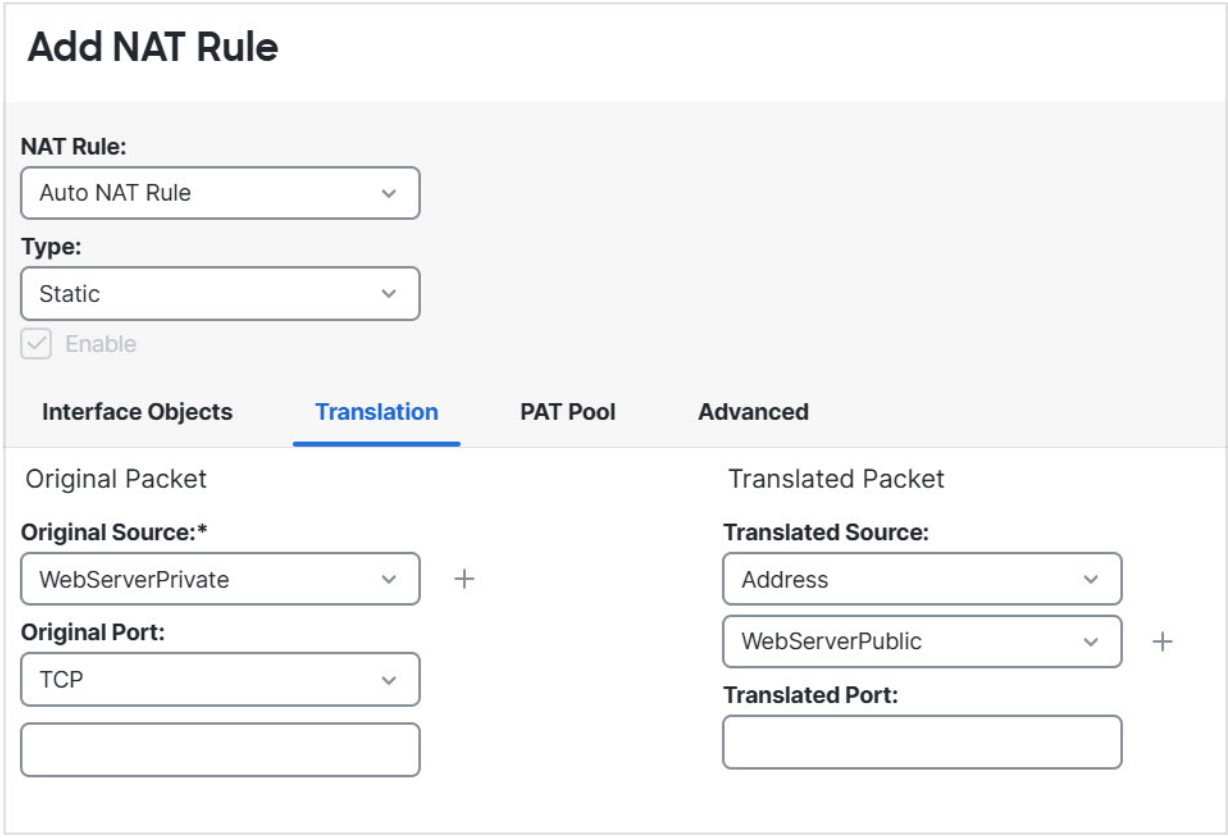
为网络对象命名（例如，WebServerPublic），并输入主机地址 209.165.201.10。



e) 点击保存。

步骤 2 配置对象的静态 NAT。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。
b) 点击**添加规则**。
c) 配置以下属性：
   - **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
   - **类型** = 静态。
d) 在**接口对象 (Interface Objects)** 上配置以下选项：
   - **源接口对象** = 内部。
   - **目标接口对象** = 外部。
e) 在**转换 (Translation)** 上配置以下选项：
   - **原始源** = WebServerPrivate 网络对象。
   - **转换后的源** > **地址** = WebServerPublic 网络对象。



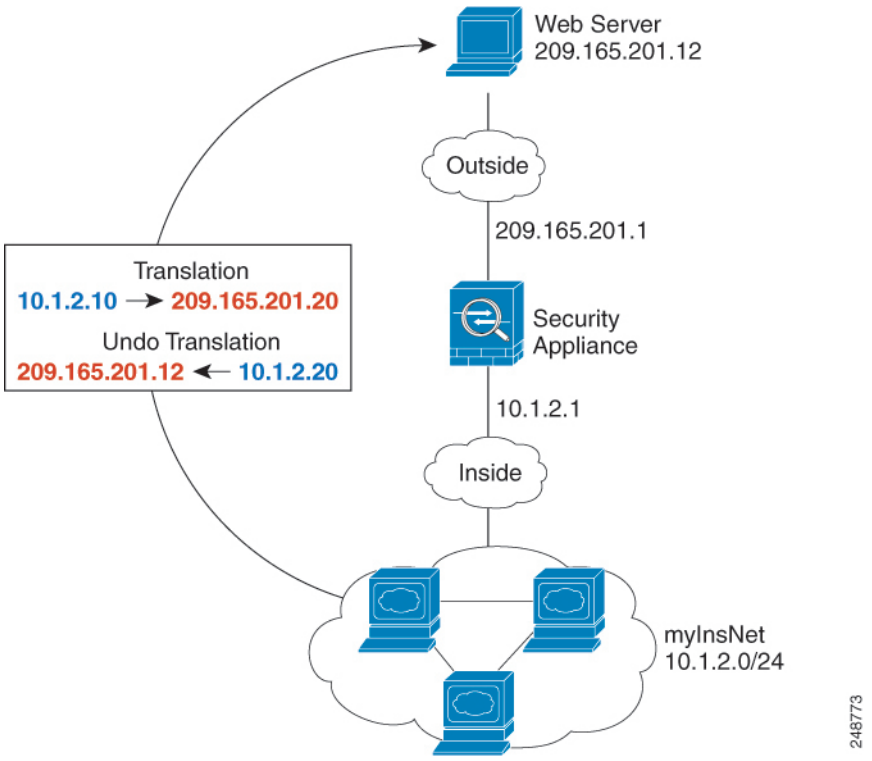
f) 点击**保存**。

步骤 3 点击 NAT 规则页面上的**保存**。

面向内部主机的动态自动 NAT 和面向外部 Web 服务器的静态 NAT

当专用网络上的内部用户访问外部 Web 服务器时，以下示例为这些用户配置动态 NAT。此外，当内部用户连接到外部 Web 服务器时，该 Web 服务器地址被转换为显示在内部网络上的地址。

图 *423:* 面向内部 ***Web*** 服务器的动态 ***NAT***，面向外部 ***Web*** 服务器的静态 ***NAT***



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择并点击**添加网络** > **添加对象对象** > **接口**。

过程

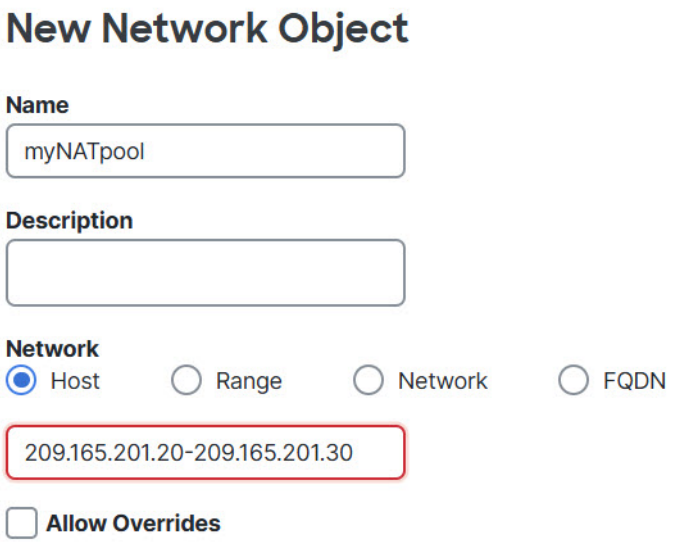
步骤 1 为要向其转换内部地址的动态 NAT 池创建一个网络对象。

a) 选择**对象**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义动态 NAT 池。

为网络对象命名（例如，myNATpool），并输入网络地址范围 209.165.201.20-209.165.201.30。

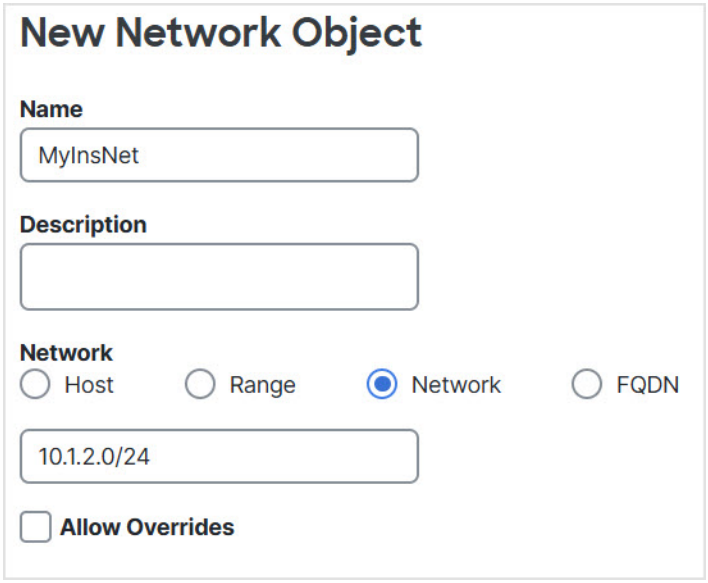


d) 点击保存。

步骤 2 为内部网络创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，MyInsNet），并输入网络地址 10.1.2.0/24。

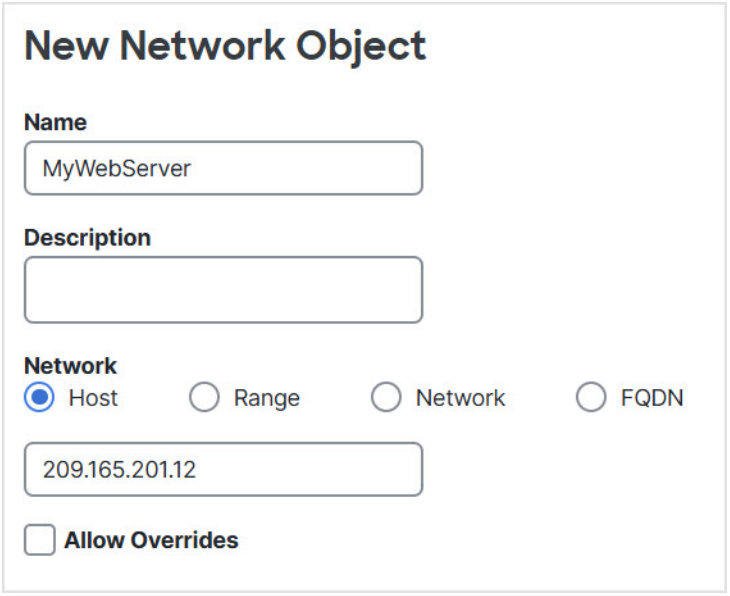


c) 点击保存。

步骤 3 为外部 Web 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，MyWebServer），并输入主机地址 209.165.201.12。

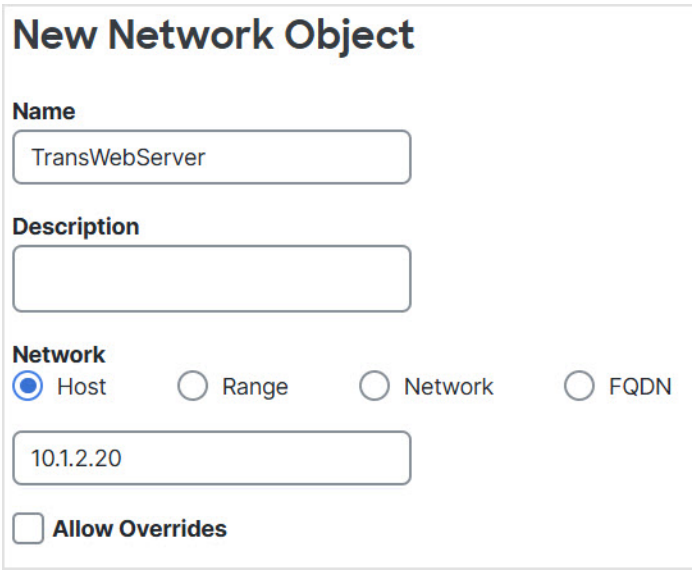


c) 点击**保存**。

步骤 4 为转换的 Web 服务器地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，TransWebServer），并输入主机地址 10.1.2.20。



c) 点击**保存**。

步骤 5 使用动态 NAT 池对象为内部网络配置动态 NAT。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

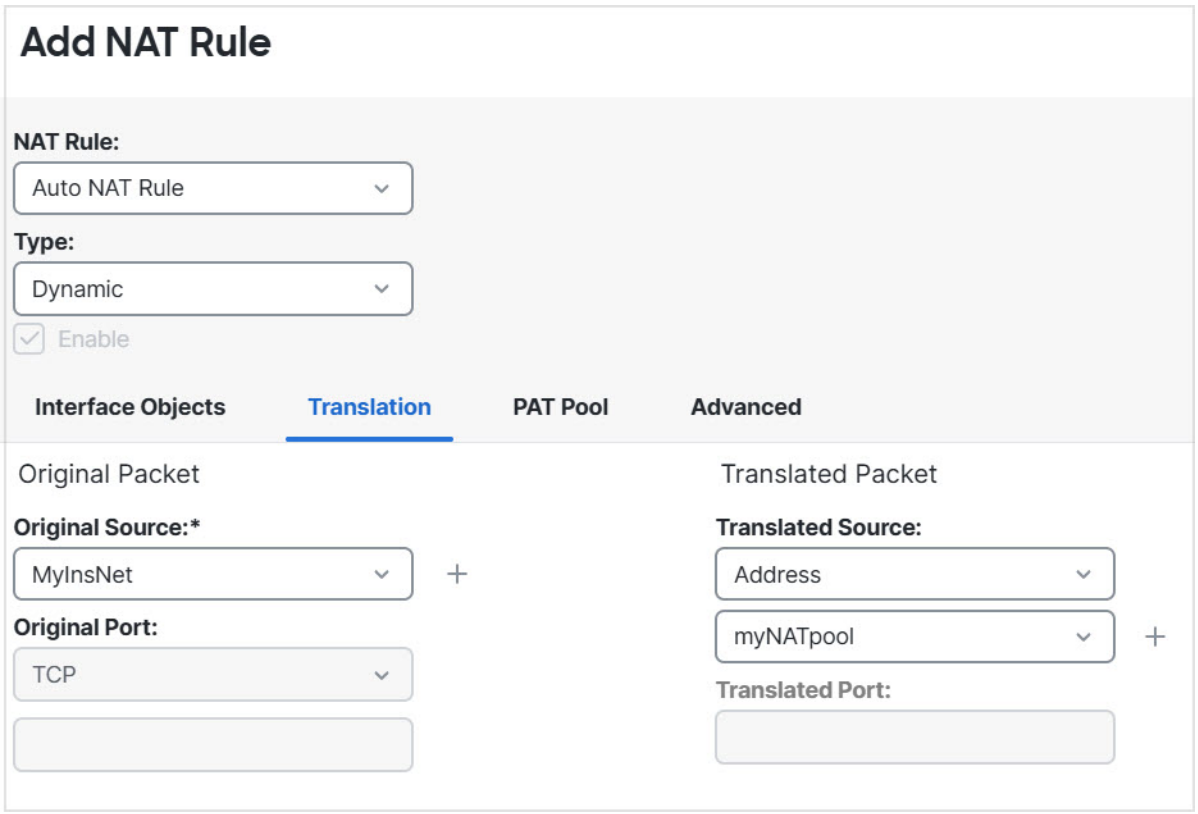
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsNet 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = myNATpool 网络组。



f) 点击**保存**。

步骤 6 为 Web 服务器配置静态 NAT。

a) 点击**添加规则**。

b) 配置以下属性：

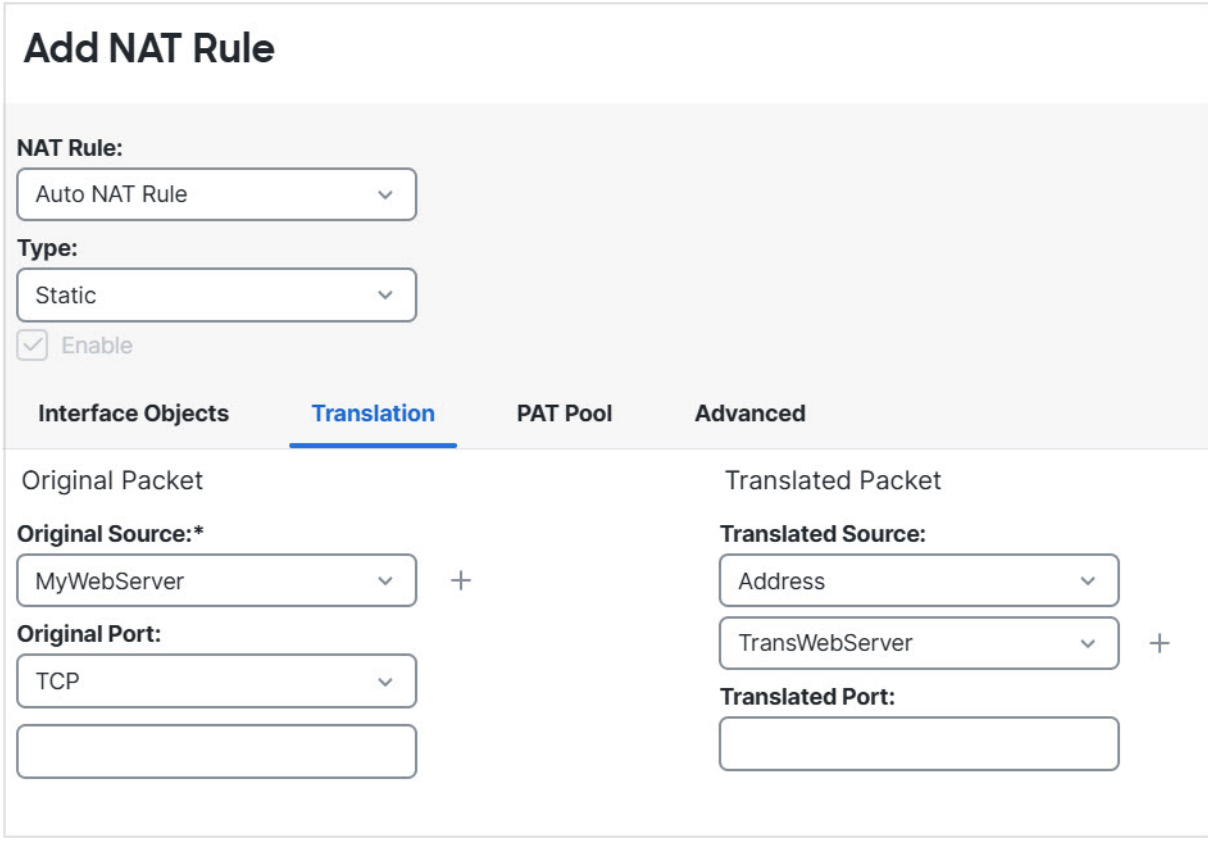
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myWebServer 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = TransWebServer 网络对象。



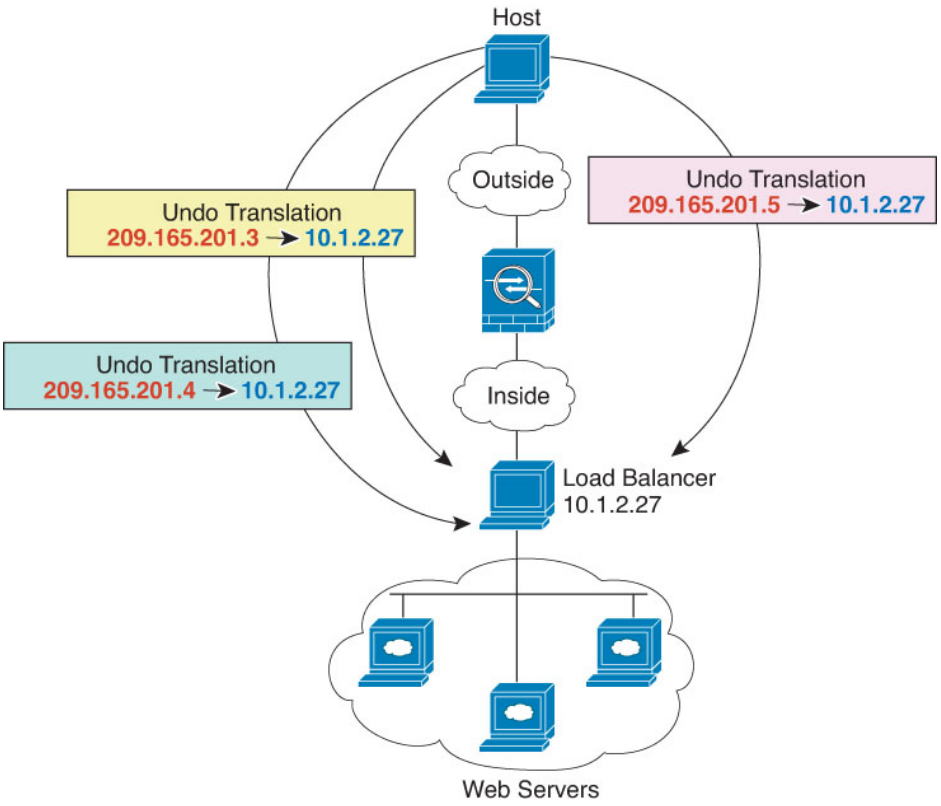
e) 点击**保存**。

步骤 7 点击 NAT 规则页面上的**保存**。

具有多个映射地址的内部负载均衡器（静态自动 NAT，一对多）

以下示例显示转换为多个 IP 地址的内部负载均衡器。当外部主机访问其中一个映射 IP 地址时，将该地址反向转换为单一负载均衡器地址。根据请求的URL，它会将流量重新定向到正确的Web服务器。

图 *424:* 内部负载均衡器的一对多静态 *NAT*



开始之前

确保存在包含保护 Web 服务器的设备接口的接口对象（安全区域或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

过程

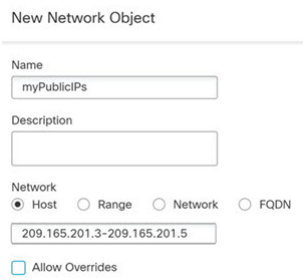
步骤 1 为要向其映射负载均衡器的地址创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络 (Network)** 并点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

c) 定义地址。

为网络对象命名（例如，myPublicIPs）并输入网络范围 209.165.201.3-209.165.201.5。

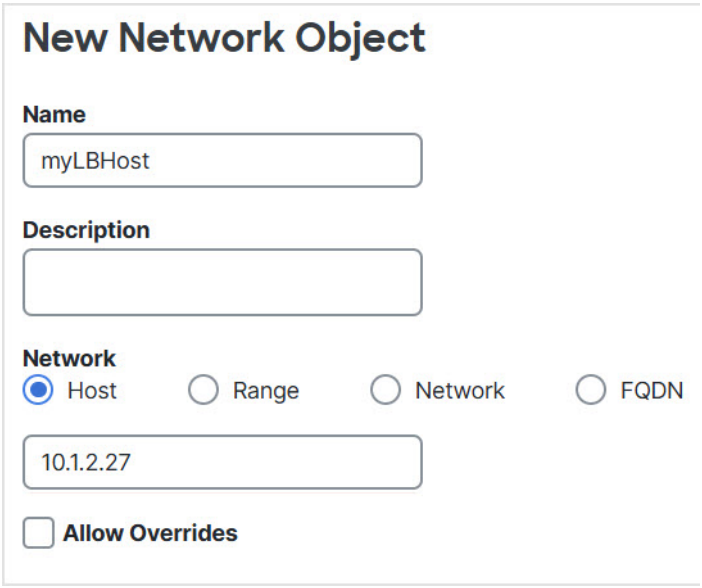


d) 点击保存。

步骤 2 为负载均衡器创建网络对象。

a) 点击添加网络 **(Add Network)** > 添加对象 **(Add Object)**。

b) 为网络对象命名（例如，myLBHost)，然后输入主机地址 10.1.2.27。



c) 点击保存。

步骤 3 为负载均衡器配置静态 NAT。

a) 选择 策略 > 网络策略 > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击添加规则。

c) 配置以下属性：

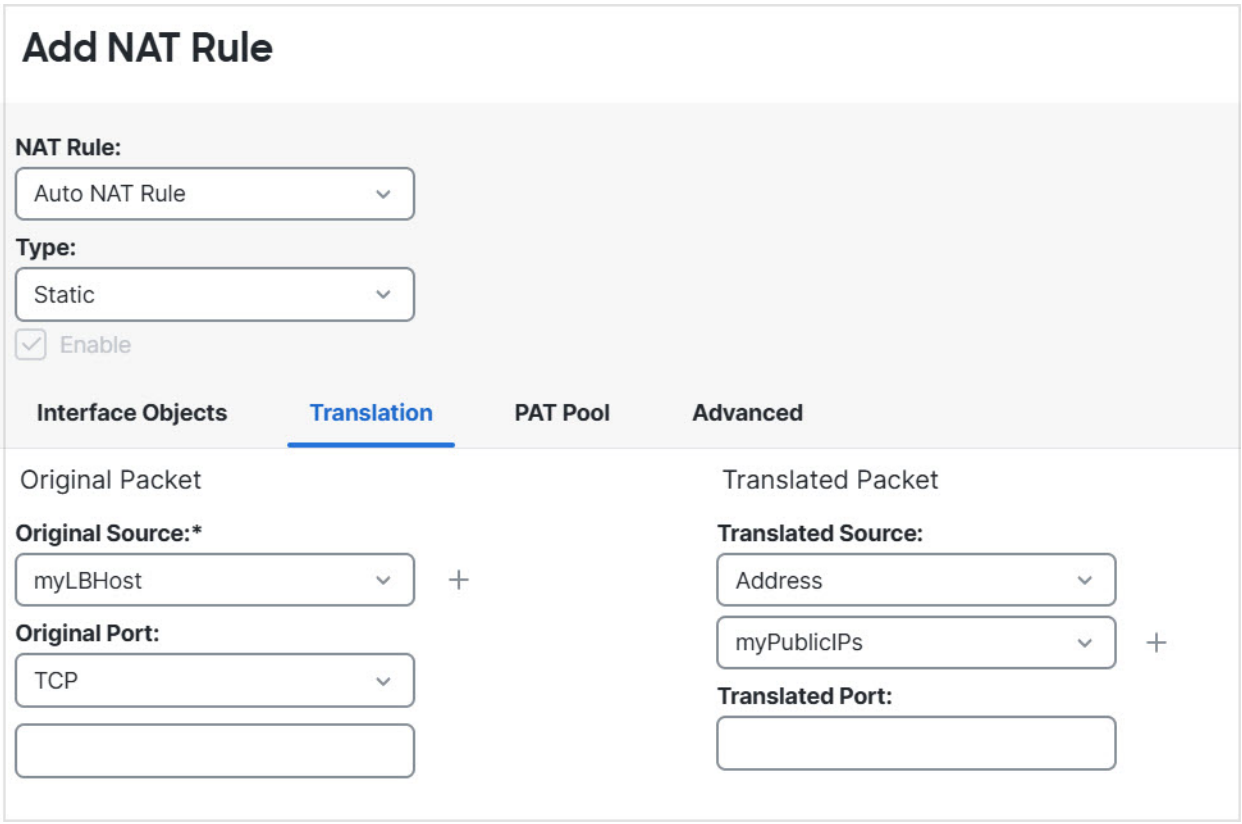
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- 类型 = 静态。

d) 在接口对象 **(Interface Objects)** 上配置以下选项：

- 源接口对象 = 内部。
- 目标接口对象 = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myLBHost 网络对象。
- **转换后的源** > **地址 (Translated Source Address)** = myPublicIPs 网络组。



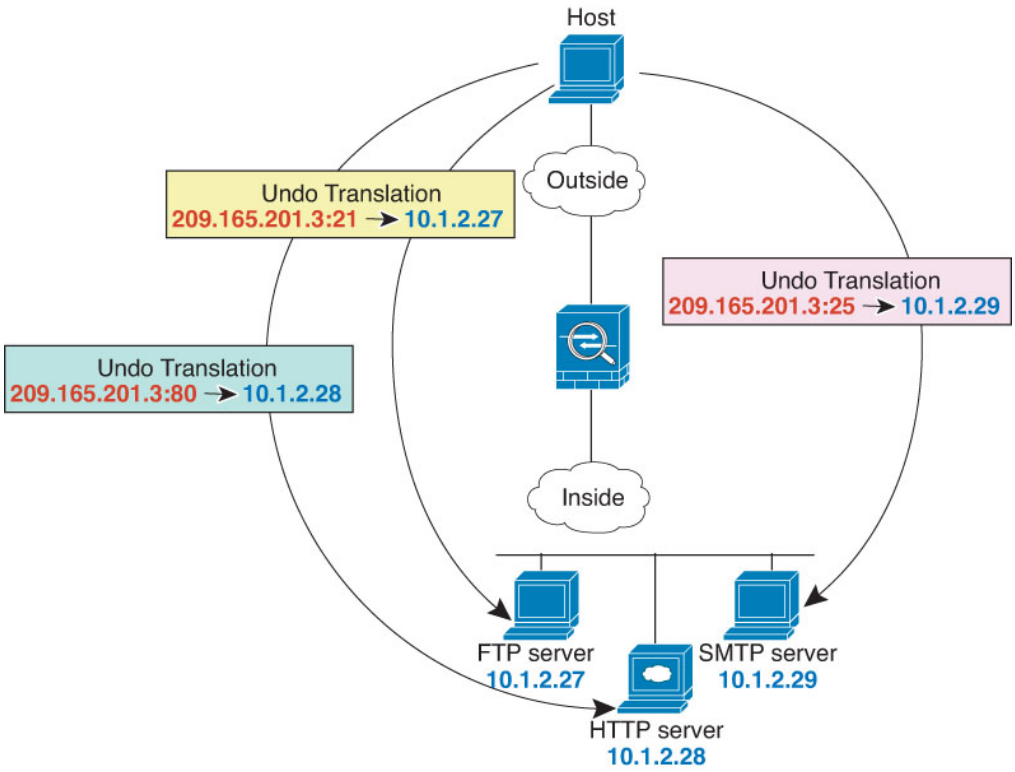
f) 点击**保存**。

步骤 4 点击 NAT 规则页面上的**保存**。

FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）

以下支持端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态NAT，这些规则使用同一映射 IP 地址和不同端口。

图 *425:* 支持端口转换的静态 *NAT*



开始之前

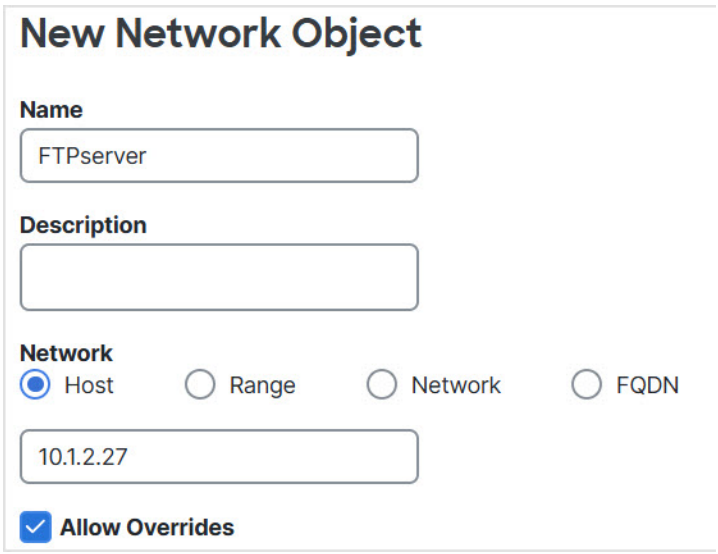
确保您的接口对象（安全区域或接口组）包含保护服务器的设备的接口。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择并点击**添加网络** > **添加组对象** > **接口**。

过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 为网络对象命名（例如，FTPserver），然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。

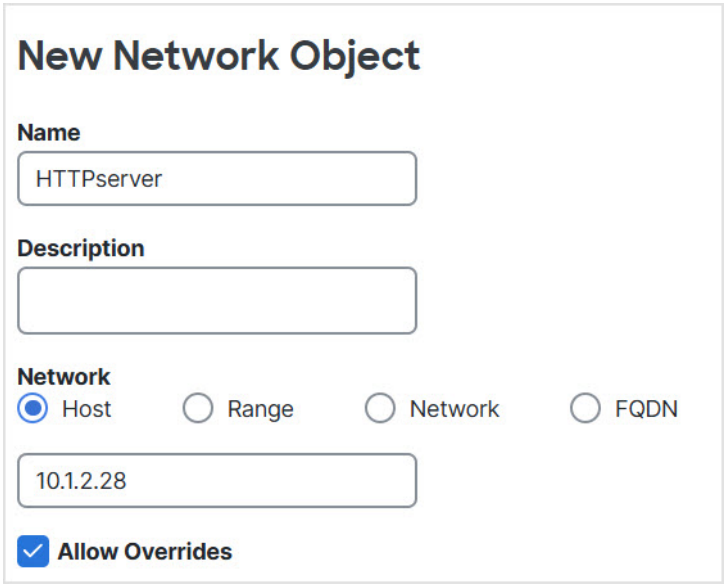


c) 点击保存。

步骤 2 为 HTTP 服务器创建网络对象。

a) 点击添加网络 **(Add Network)** > 添加对象 **(Add Object)**。

b) 为网络对象命名（例如，HTTPserver），然后输入主机地址 10.1.2.28。

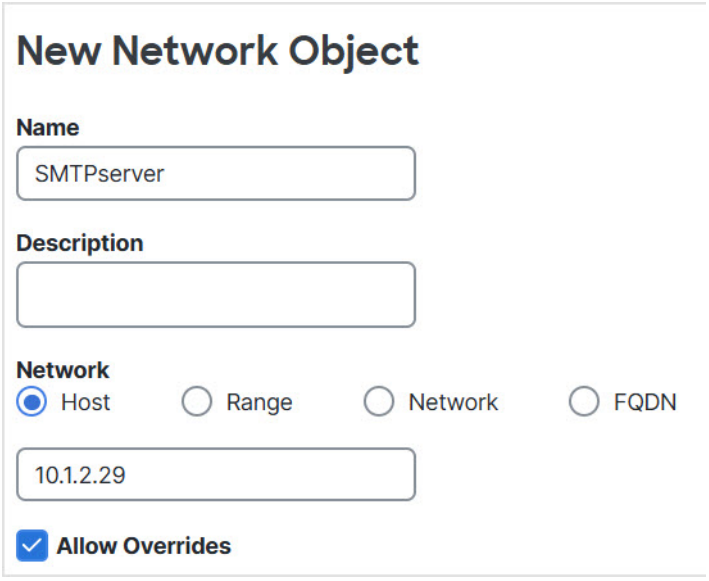


c) 点击保存。

步骤 3 为 SMTP 服务器创建网络对象。

a) 点击添加网络 **(Add Network)** > 添加对象 **(Add Object)**。

b) 为网络对象命名（例如，SMTPserver），然后输入主机地址 10.1.2.29。

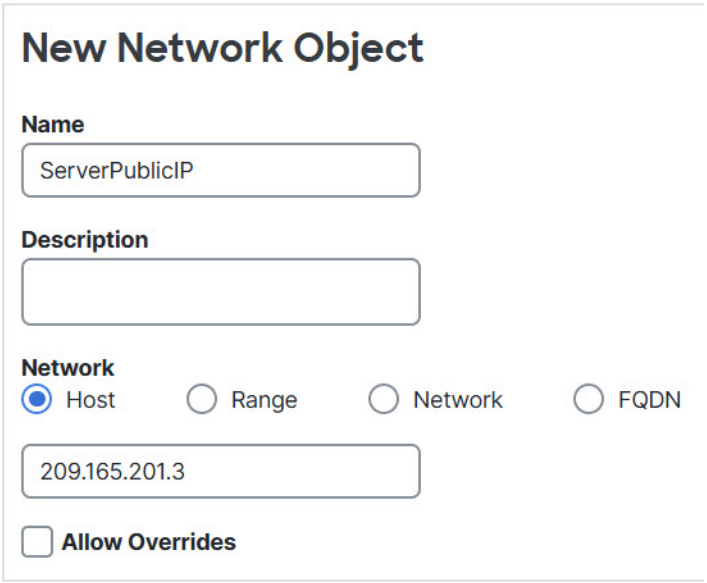


c) 点击**保存**。

步骤 4 为用于三台服务器的公共 IP 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，ServerPublicIP），然后输入主机地址 209.165.201.3。



c) 点击**保存**。

步骤 5 为 FTP 服务器配置具有端口转换的静态 NAT，并将 FTP 端口映射到其自身。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

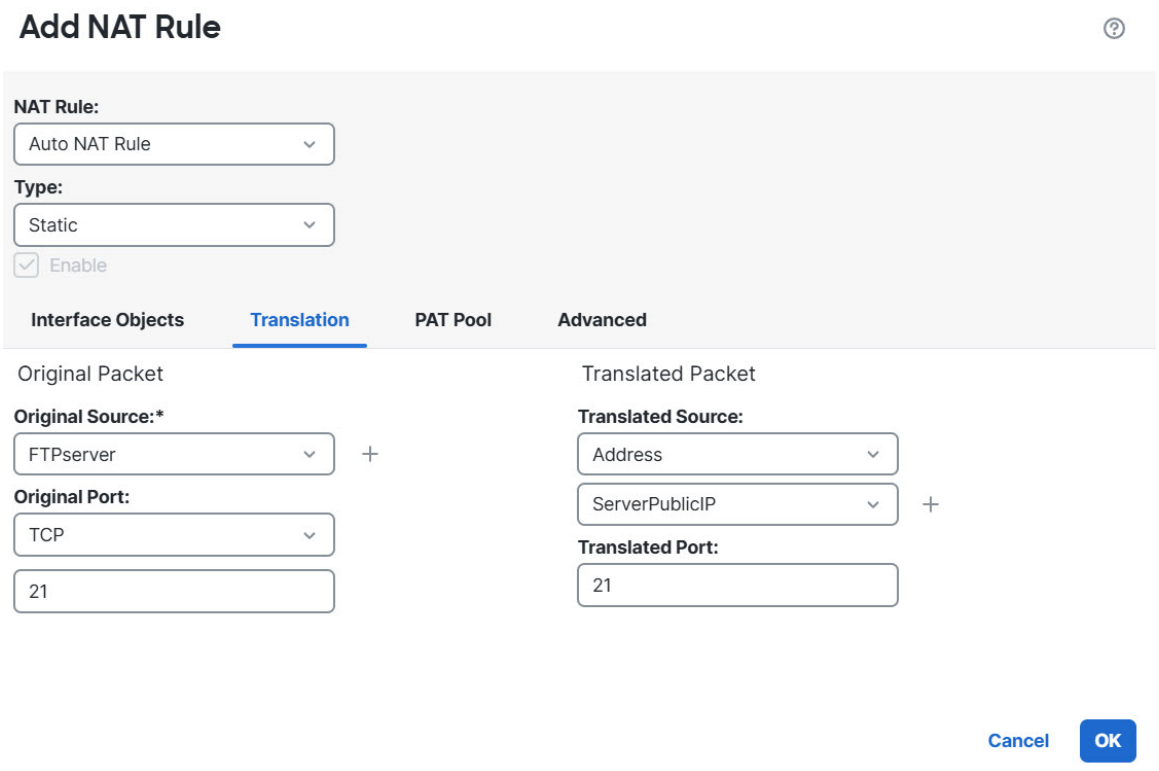
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = FTPserver 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ServerPublicIP 网络对象。
- **原始端口 (Original Port)** > **TCP** = 21。
- **转换后的端口** = 21。



f) 点击**保存**。

步骤 6 为 HTTP 服务器配置具有端口转换的静态 NAT，并将 HTTP 端口映射到其自身。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。

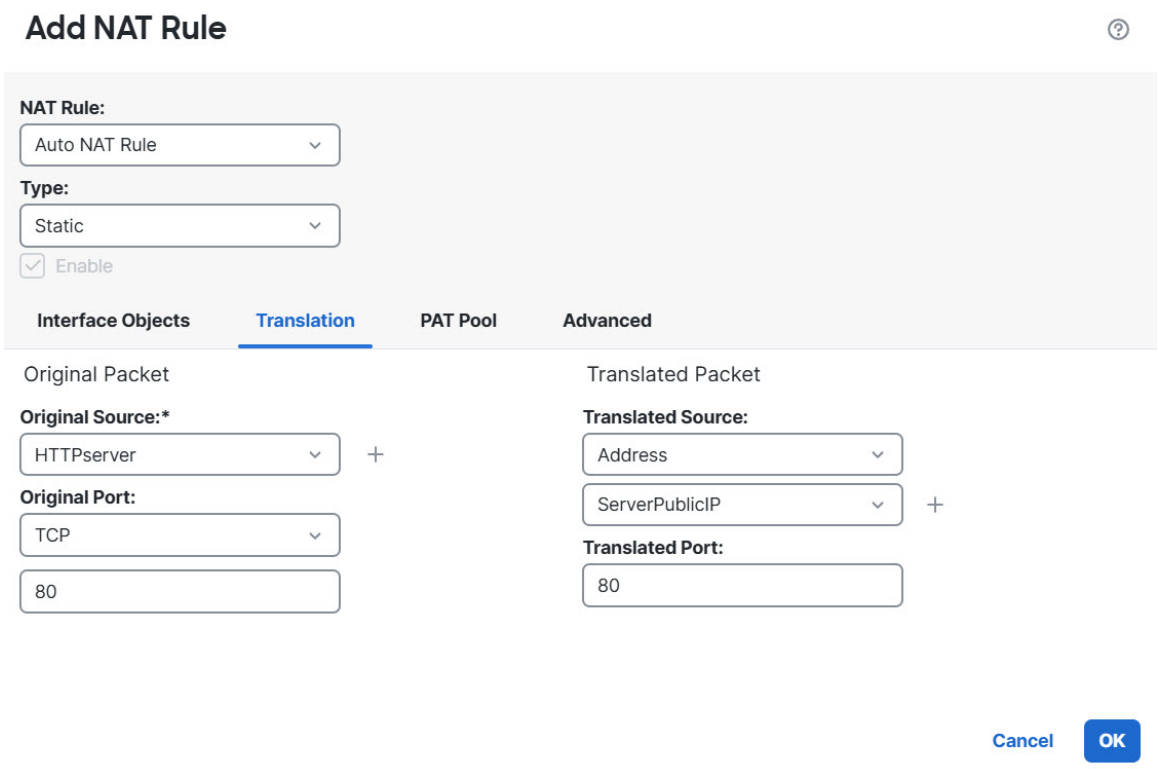
- **类型** = 静态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = HTTPserver 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ServerPublicIP 网络对象。
- **原始端口 (Original Port)** > **TCP** = 80。
- **转换后的端口** = 80。



e) 点击**保存**。

步骤 7 为 SMTP 服务器配置具有端口转换的静态 NAT，并将 SMTP 端口映射到其自身。

a) 点击**添加规则**。

b) 配置以下属性：

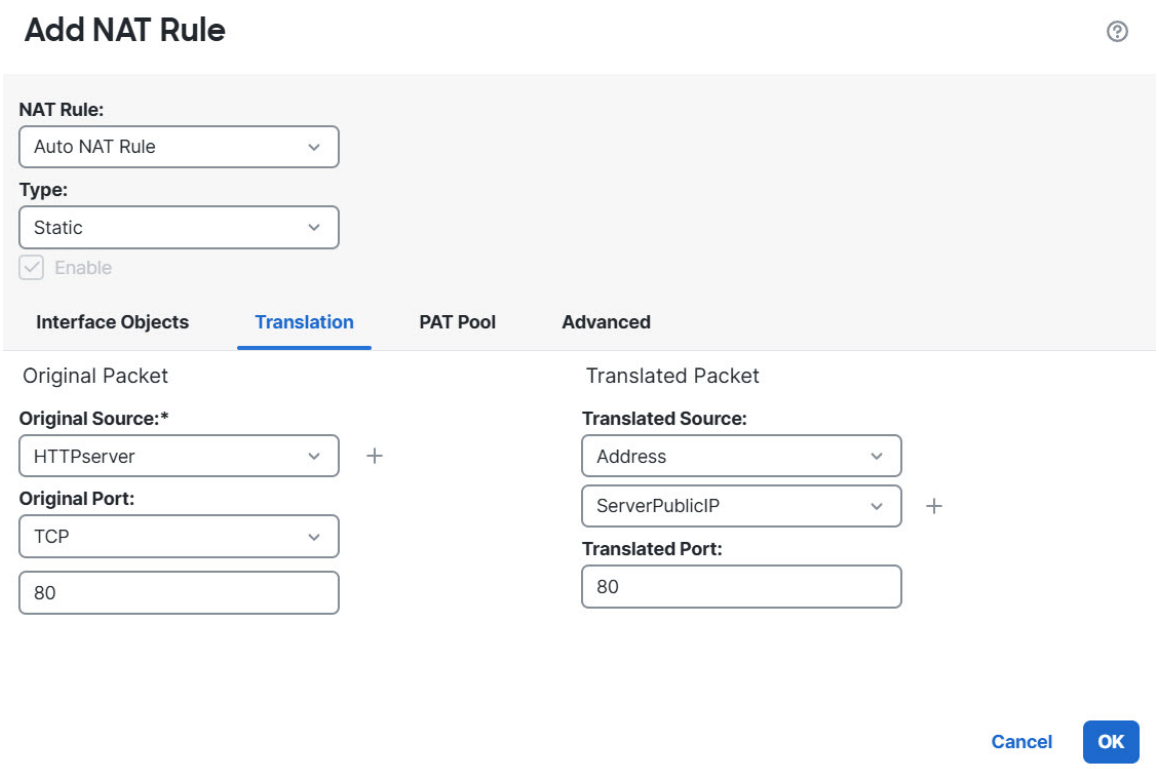
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = SMTPserver 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ServerPublicIP 网络对象。
- **原始端口 (Original Port)** > **TCP** = 25。
- **转换后的端口** = 25。



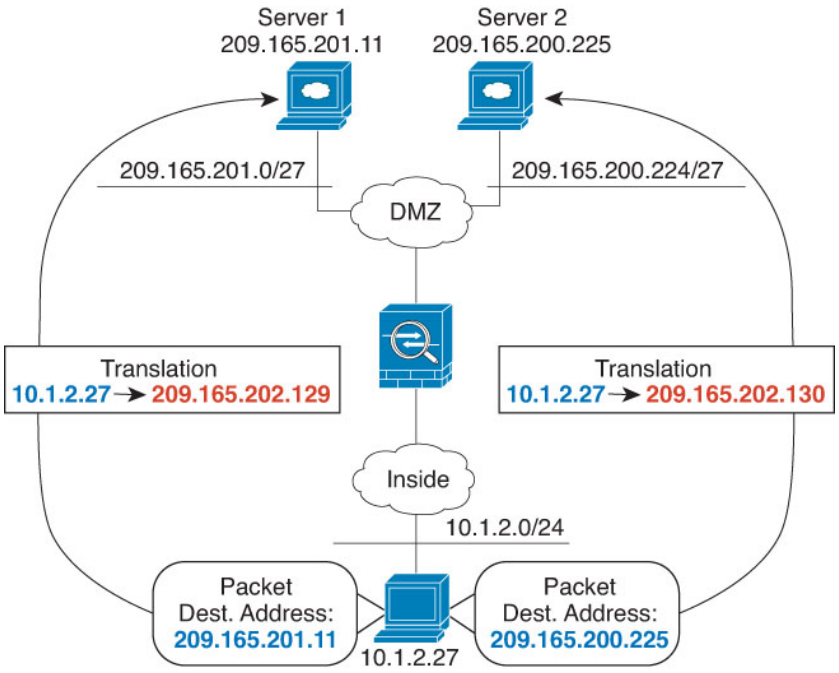
e) 点击**保存**。

步骤 8 点击 NAT 规则页面上的**保存**。

转换因目标而异（动态手动 PAT）

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:*port*。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:*port*。

图 *426:* 具有不同目标地址的手动 *NAT*



开始之前

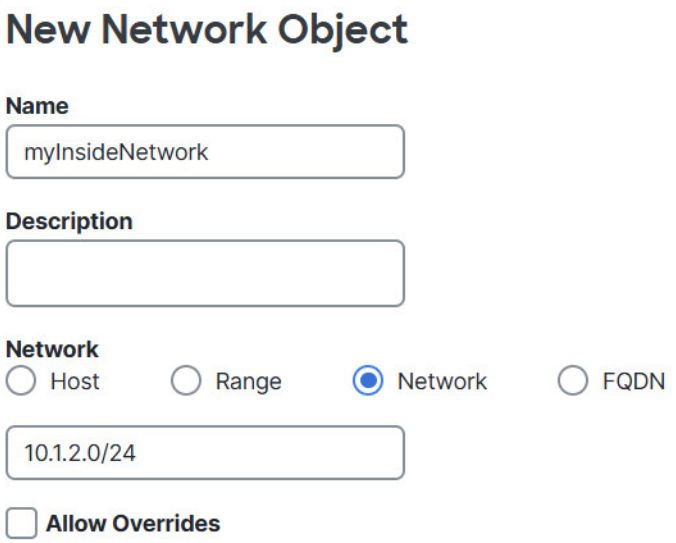
确保具有接口对象（安全区域或接口组），其包含保护服务器的设备的接口。在本例中，我们将假定接口对象是名为**内部**和 **dmz** 的安全区域。要配置接口对象，请选择 **对象** > **接口**。

过程

步骤 1 为内部网络创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 为网络对象命名（例如，myInsideNetwork），然后输入实际网络地址 10.1.2.0/24。

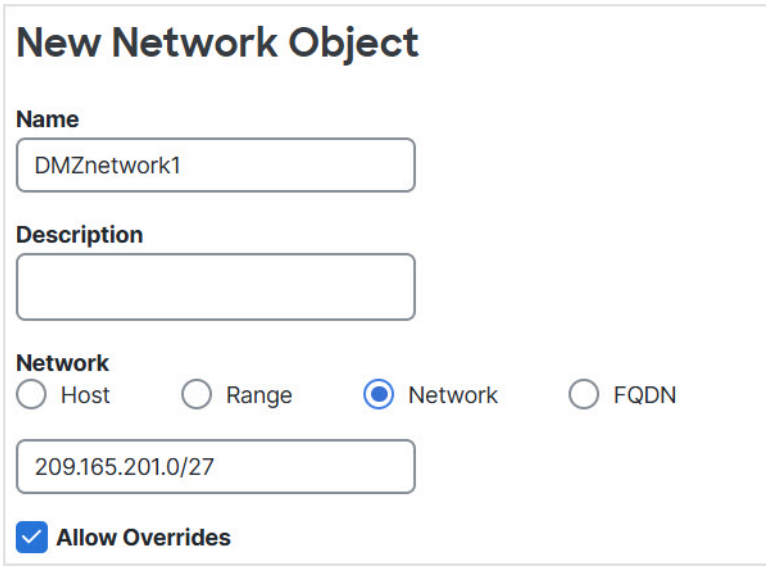


c) 点击**保存**。

步骤 2 为 DMZ 网络 1 创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，DMZnetwork1），然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。

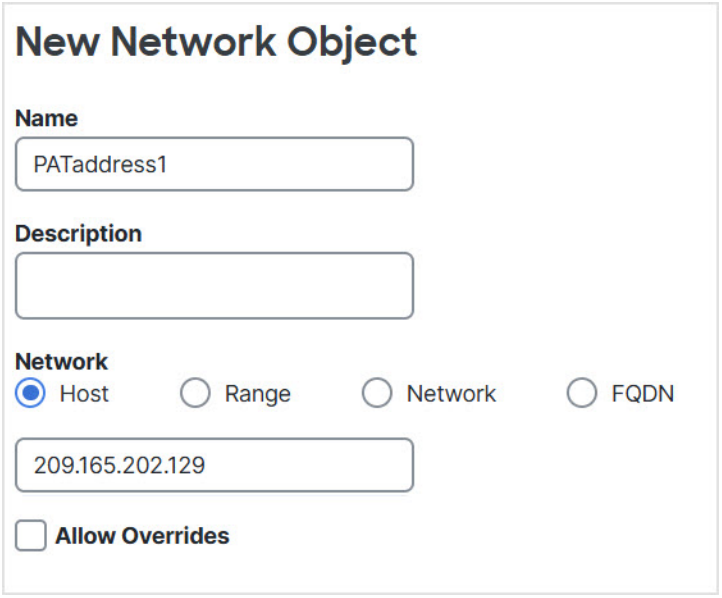


c) 点击**保存**。

步骤 3 为 DMZ 网络 1 的 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress1），然后输入主机地址 209.165.202.129。

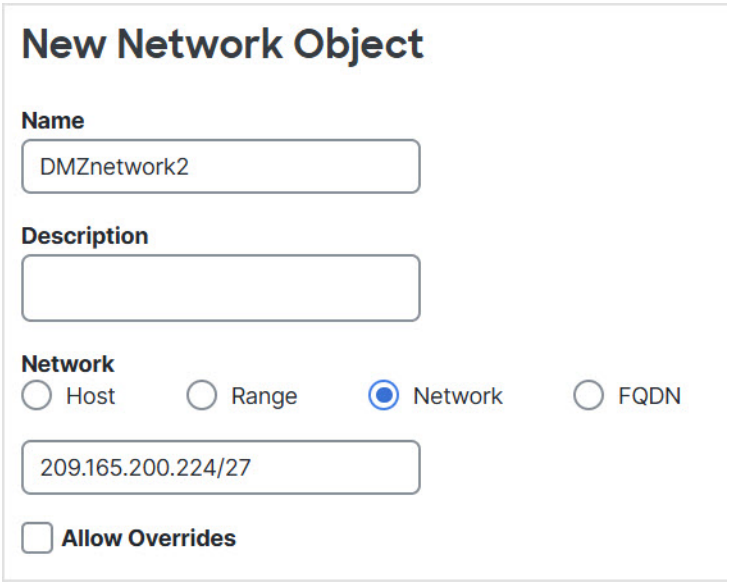


c) 点击**保存**。

步骤 4 为 DMZ 网络 2 创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，DMZnetwork2），然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。

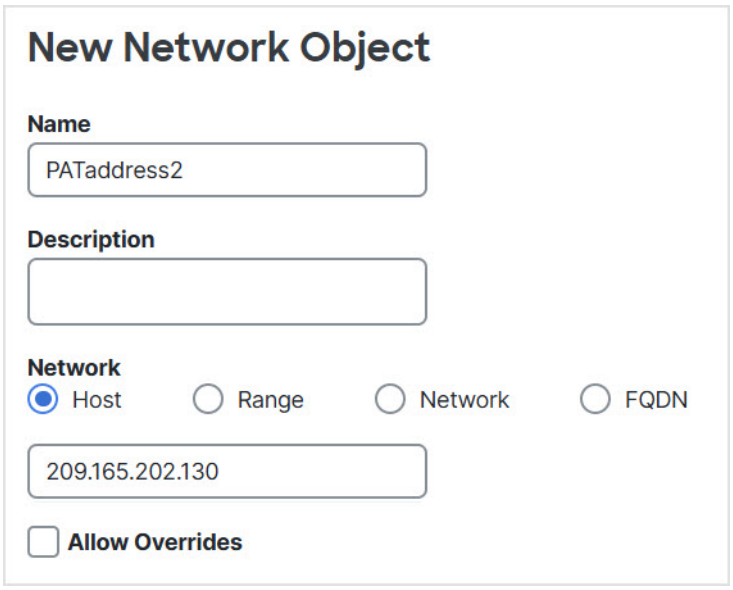


c) 点击**保存**。

步骤 5 为 DMZ 网络 2 的 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress2），然后输入主机地址 209.165.202.130。



c) 点击**保存**。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

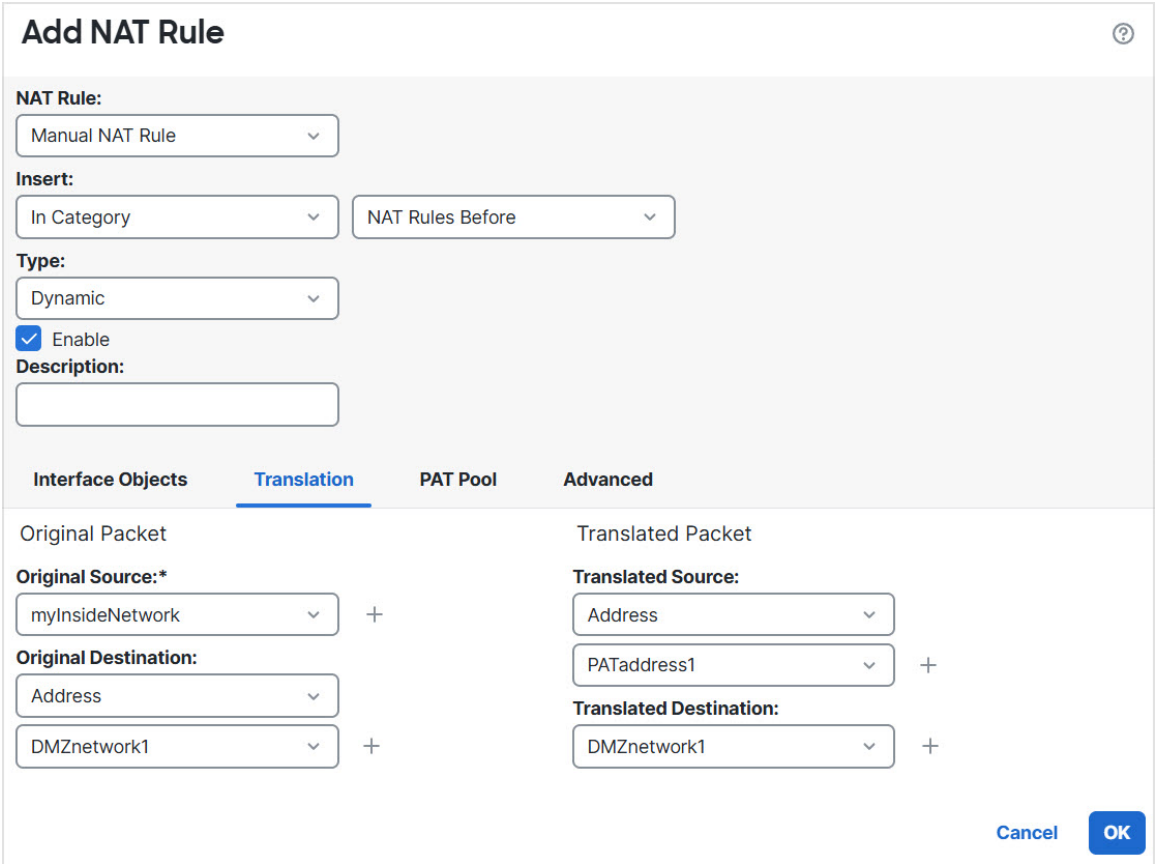
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress1 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = DMZnetwork1 网络对象。
- **转换后的目标** = DMZnetwork1 网络对象。

  注释
  由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。



f) 点击**保存**。

步骤 7 为 DMZ 网络 2 配置动态手动 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

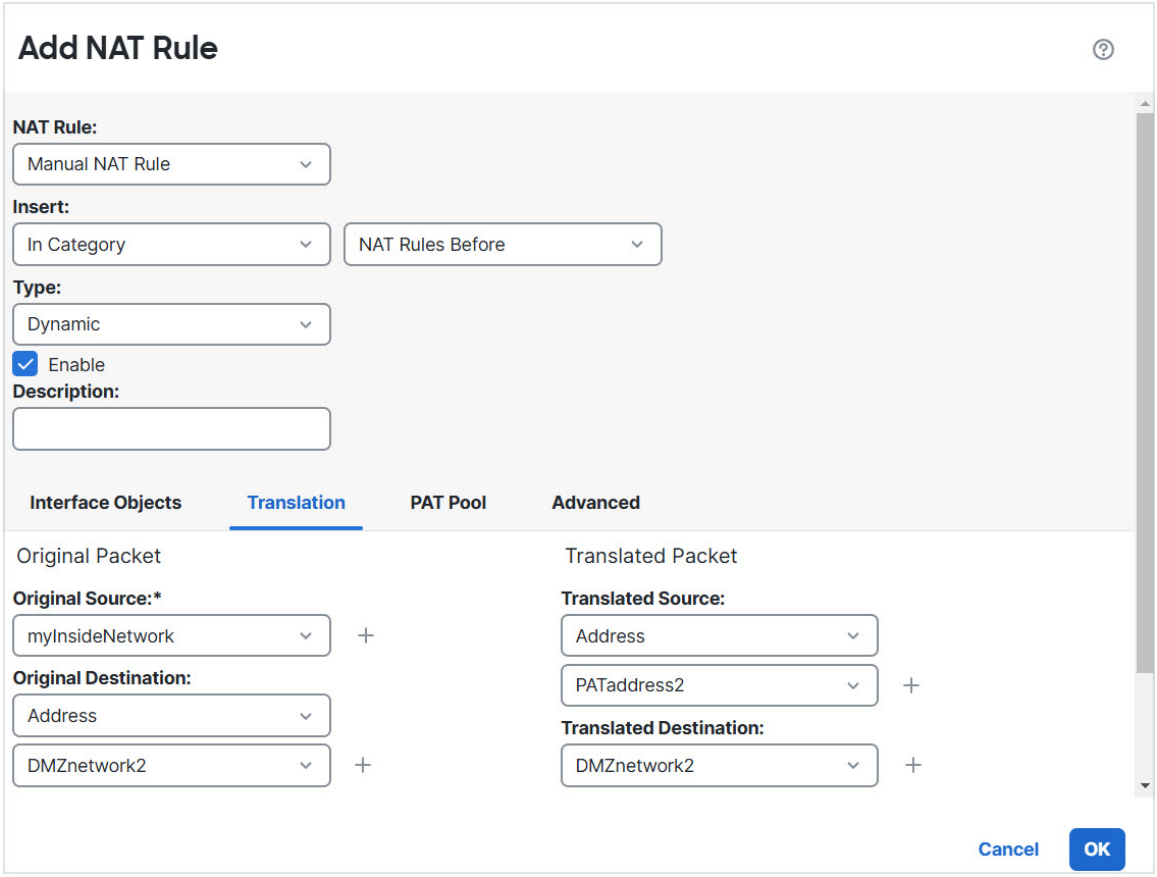
- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress2 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = DMZnetwork2 网络对象。
- **转换后的目标** = DMZnetwork2 网络对象。



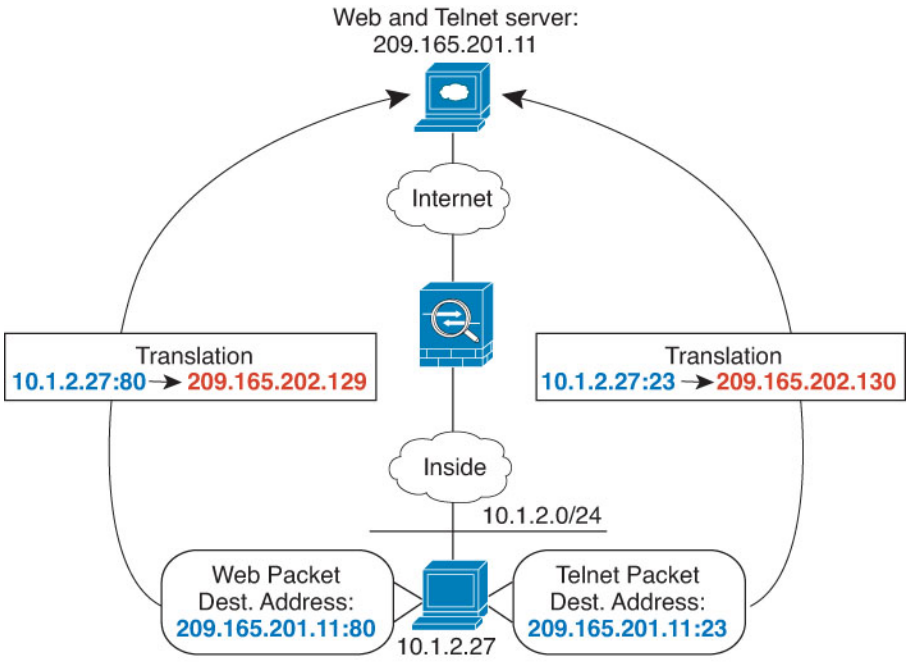
e) 点击**保存**。

步骤 8 点击 NAT 规则页面上的**保存**。

转换因目标地址和端口而异（动态手动 PAT）

下图显示源端口和目标端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:*port*。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:*port*。

图 *427:* 具有不同目标端口的手动 *NAT*



开始之前

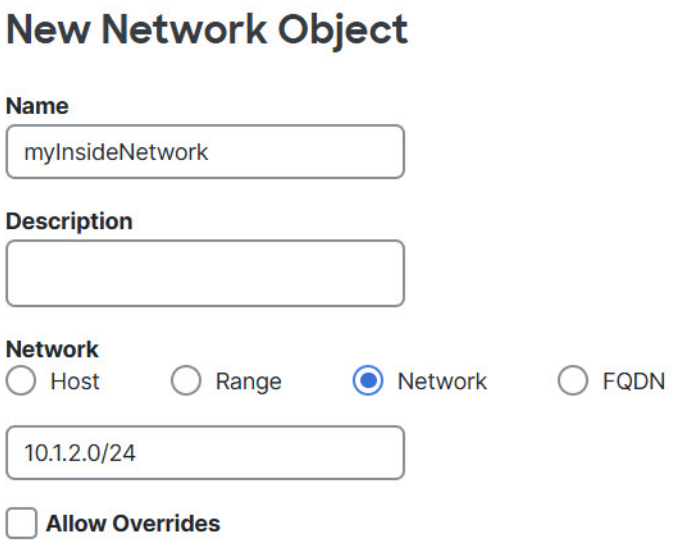
确保具有接口对象（安全区域或接口组），其包含保护服务器的设备的接口。在本例中，我们将假定接口对象是名为**内部**和 **dmz** 的安全区域。要配置接口对象，请选择 **对象** > **接口**。

过程

步骤 1 为内部网络创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 为网络对象命名（例如，myInsideNetwork），然后输入实际网络地址 10.1.2.0/24。

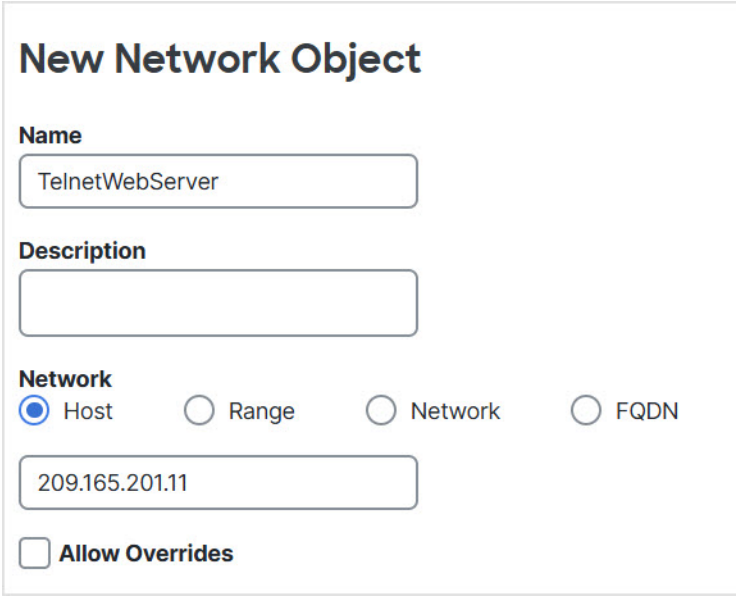


c) 点击**保存**。

步骤 2 为 Telnet/Web 服务器创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，TelnetWebServer），然后输入主机地址 209.165.201.11。

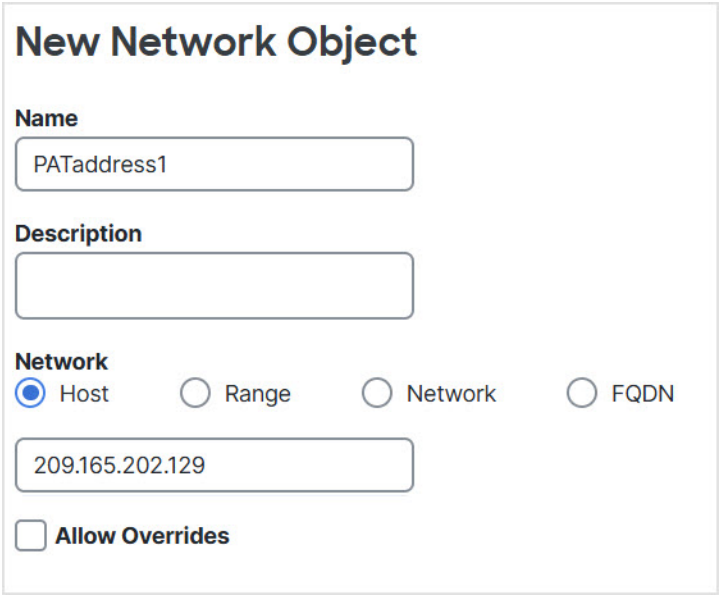


c) 点击**保存**。

步骤 3 使用 Telnet 时为 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress1），然后输入主机地址 209.165.202.129。

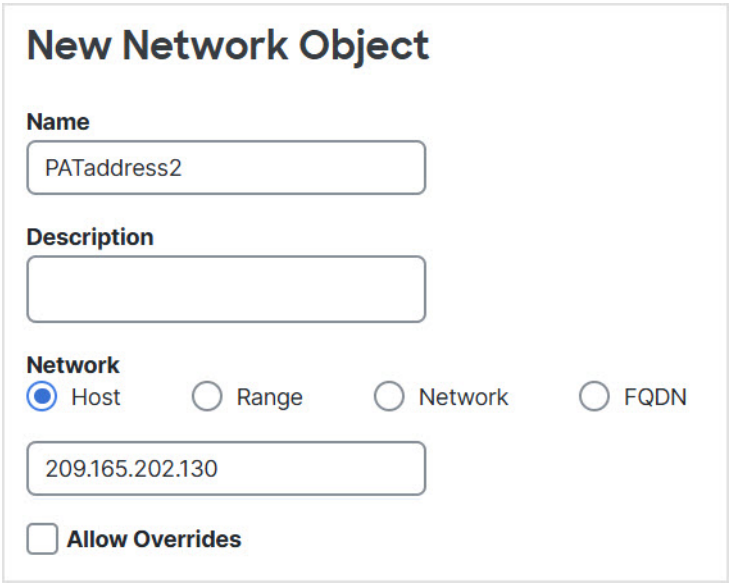


c) 点击**保存**。

步骤 4 使用 HTTP 时为 PAT 地址创建网络对象。

a) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**。

b) 为网络对象命名（例如，PATaddress2），然后输入主机地址 209.165.202.130。



c) 点击**保存**。

步骤 5 为 Telnet 访问创建动态手动 PAT。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

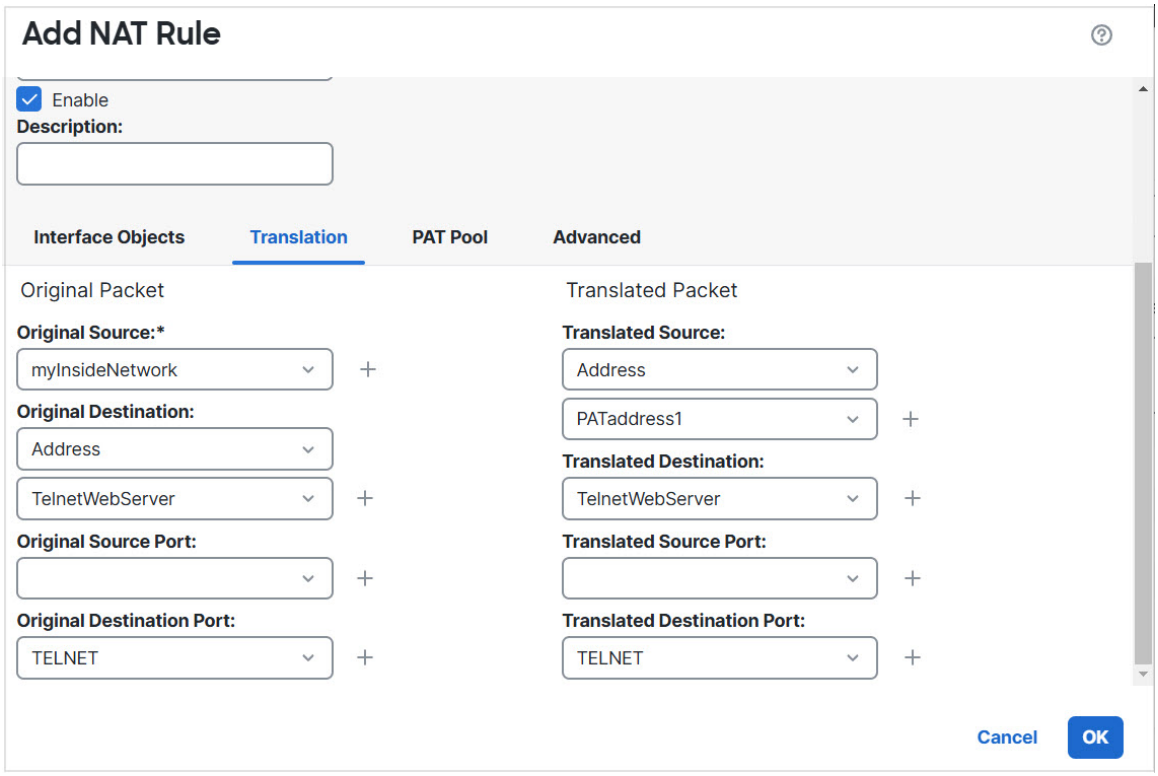
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress1 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = TelnetWebServer 网络对象。
- **转换后的目标** = TelnetWebServer 网络对象。
- **原始目标端口** = TELNET 端口对象（系统定义）。
- **转换后的目标端口** = TELNET 端口对象（系统定义）。

注释
由于您不需要转换目标地址或端口，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，以及为原始端口和转换后的端口指定相同的端口，从而为它们配置身份NAT。



f) 点击**保存**。

步骤 6 为 Web 访问创建动态手动 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

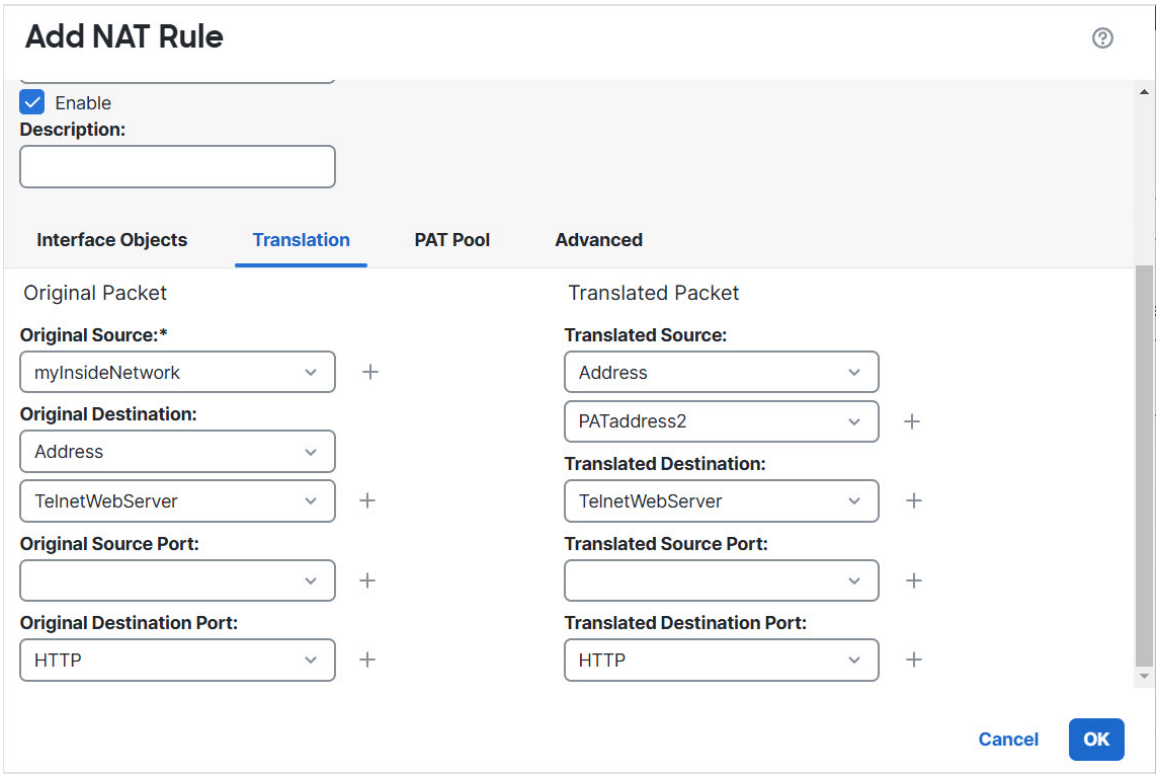
- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。

c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目的接口对象** = dmz。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = myInsideNetwork 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = PATaddress2 网络对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = TelnetWebServer 网络对象。
- **转换后的目标** = TelnetWebServer 网络对象。
- **原始目标端口** = HTTP 端口对象（系统定义）。
- **转换后的目标端口** = HTTP 端口对象（系统定义）。



e) 点击**保存**。

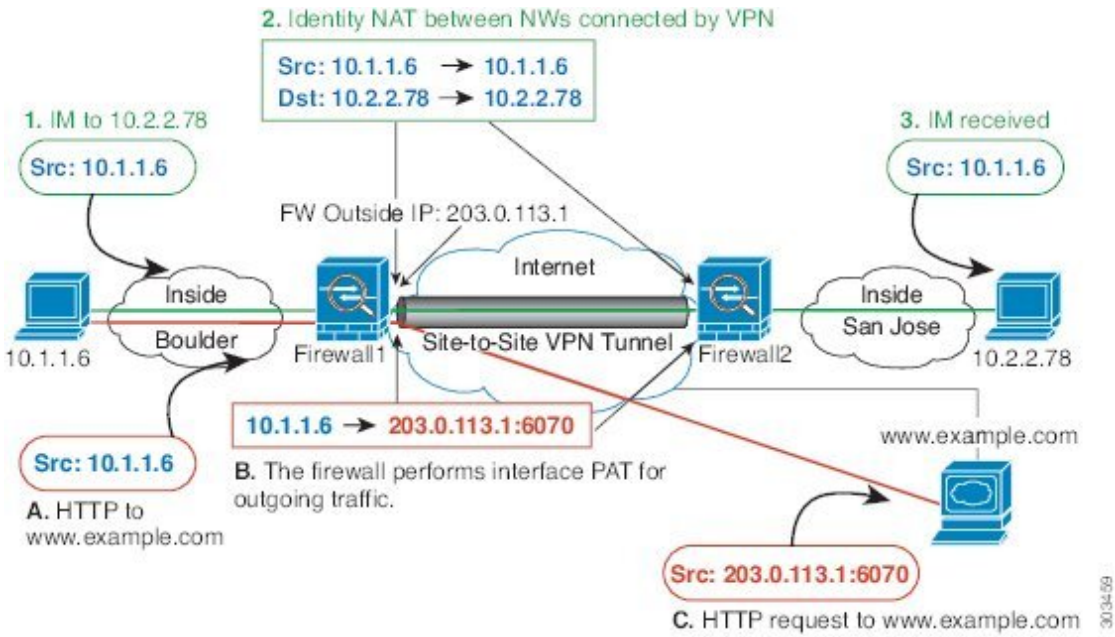
步骤 7 点击 NAT 规则页面上的**保存**。

NAT 和站点间 VPN

使用管理中心 VPN 向导（**设备 > 站点间**）创建基于策略的站点间 VPN 时，可以选择 NAT 免除选项以自动创建规则。您可以在 NAT 策略页面（**设备 > NAT > NAT 免除**）中查看设备的 NAT 免除。如果不想在 VPN 向导中配置 NAT 免除，可以使用以下程序进行 NAT 免除。

下图显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 *428:* 用于站点间 *VPN* 的接口 *PAT* 和身份 *NAT*



以下示例说明 Firewall1（博尔德办公室）的配置。

开始之前

确保您有包含VPN中设备接口的接口对象（安全区域或接口组）。在本例中，我们假定接口对象为针对 Firewall1（博尔德办公室）接口的名为 **inside-boulder** 和 **outside-boulder** 的安全区域。要配置接口对象，请选择 **对象** > **接口**。

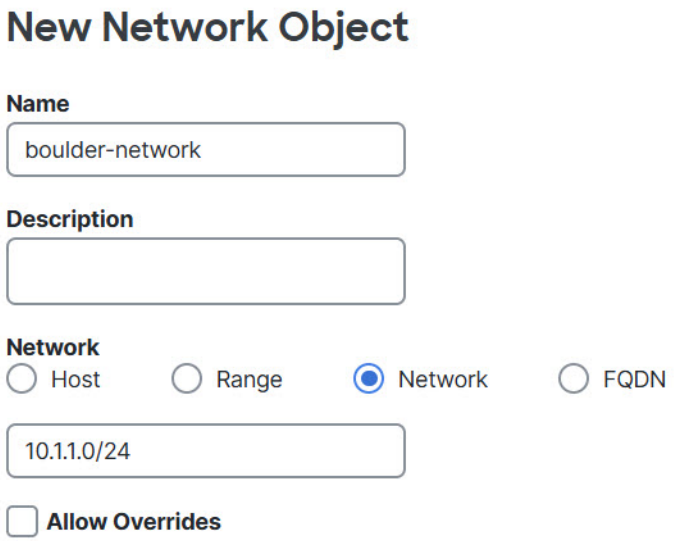
过程

步骤 1 创建对象来定义各种网络。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 找到博尔德办公室内部网络。

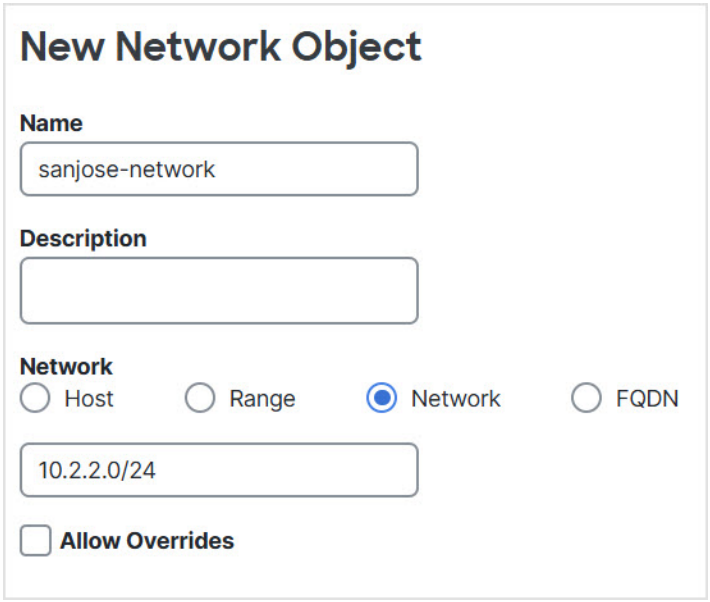
为网络对象命名（例如，boulder-network），然后输入网络地址 10.1.1.0/24。



c) 点击**保存**。

d) 点击**添加网络** > **添加对象**，并定义内部圣荷西网络。

为网络对象命名（例如，sanjose-network），然后输入网络地址 10.2.2.0/24。



e) 点击**保存**。

步骤 2 在Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过VPN连接到圣荷西办公室时的手动身份 NAT。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

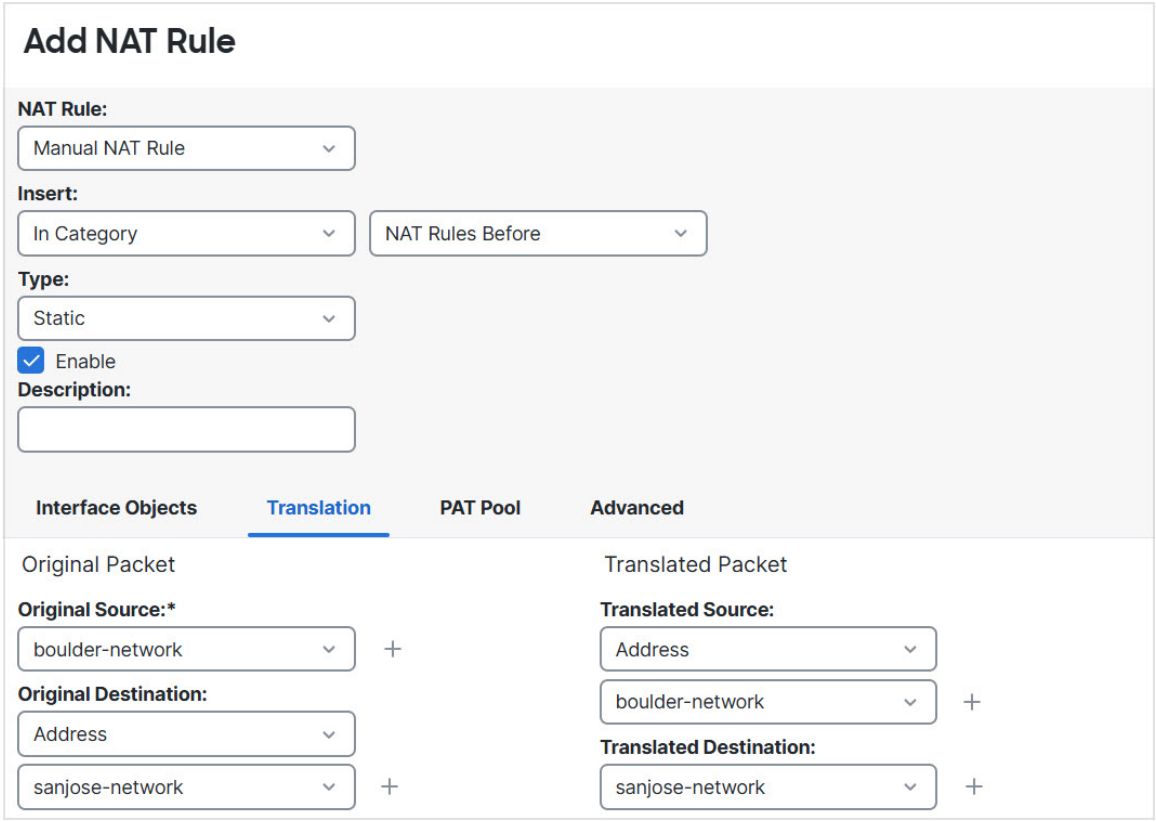
- **源接口对象** = inside-boulder。
- **目标接口对象** = outside-boulder。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = boulder-network 对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = boulder-network 对象。
- **原始目标 (Original Destination)** > **地址 (Address)** = sanjose-network 对象。
- **转换后的目标** = sanjose-network 对象。

  注释
  由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。

f) 在**高级 (Advanced)** 选项卡中，选择**不在目标接口上使用代理 ARP (Do not proxy ARP on Destination interface)**。



g) 点击**保存**。

步骤 3 在Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则** = 手动 NAT 规则。
- **类型 (Type)**= 动态。
- **插入规则** = 在第一个规则之后的任何位置。由于此规则将应用于所有目的地址，使用 sanjose-network 作为目的的规则必须在此规则之前，否则永远也不会匹配 sanjose-network 规则。默认设置是将新的手动 NAT 规则放到“NAT 规则在自动 NAT 之前”部分的末尾。

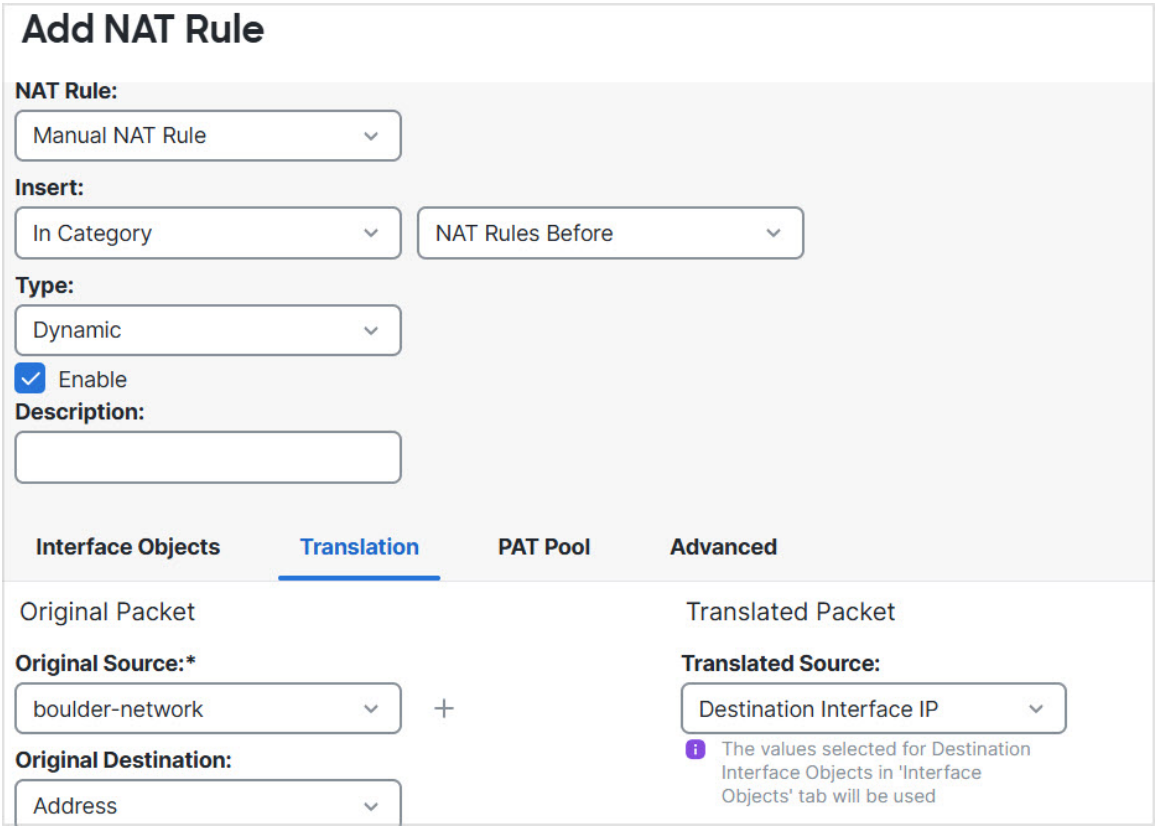
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = inside-boulder。
- **目标接口对象** = outside-boulder。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = boulder-network 对象。
- **转换后的源 = 目标接口 IP**。此选项使用目标接口对象中包含的接口来配置接口 PAT。

- 原始目标 **(Original Destination)** > 地址 **(Address)** = 任意（留空）。
- 转换后的目标 = 任意（留空）。



e) 点击**保存**。

步骤 4 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 sanjose-network。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 sanjose-network。

使用 NAT 重写 DNS 查询和响应

可能需要配置 Firewall Threat Defense 以修改 DNS 应答，方法是用匹配 NAT 配置的地址替换应答中的地址。配置每条转换规则时，可以配置 DNS 修改。DNS 修改也称为“DNS Doctoring”。

此功能可以重写匹配 NAT 规则的 DNS 查询和应答中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的DNS应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的DNS应答，记录会从实际值被重写为映射值。此功能适用于 NAT44、NAT 66、NAT46 和 NAT64。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。
- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS 服务器在内部并以专用 IP 地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

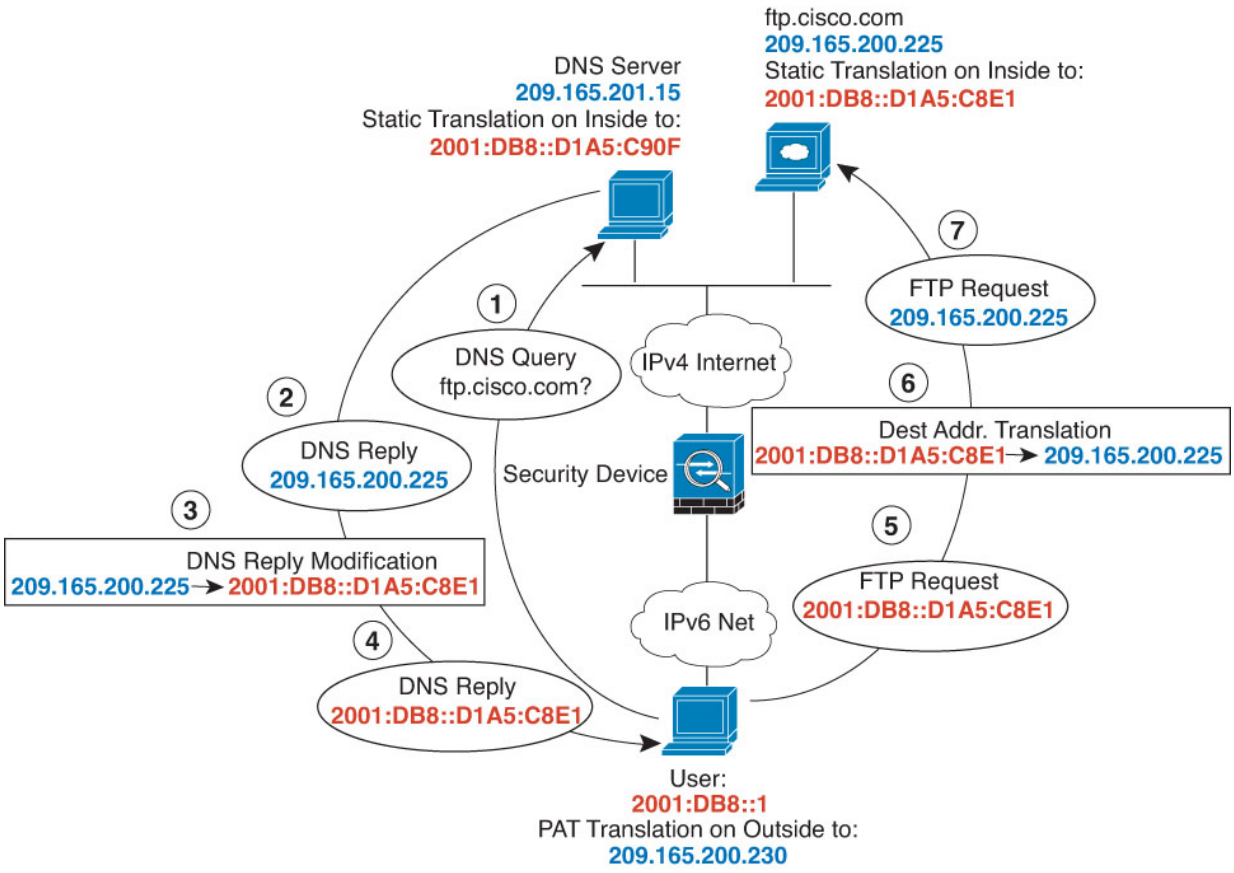
- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 要重写 DNS 查询和响应，您必须启用针对 NAT 规则启用了 DNS NAT 重写的 DNS 应用检查。默认情况下，启用了 DNS NAT 重写的 DNS 检查会全局应用，因此可能无需更改检查配置。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。
- DNS 重写不会重写 DNS 动态更新消息（操作码为 5）。

以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS64 回复修改

下图显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。

由于您希望内部用户使用 ftp.cisco.com 的映射地址（2001:DB8::D1A5:C8E1，其中 D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物），因此需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

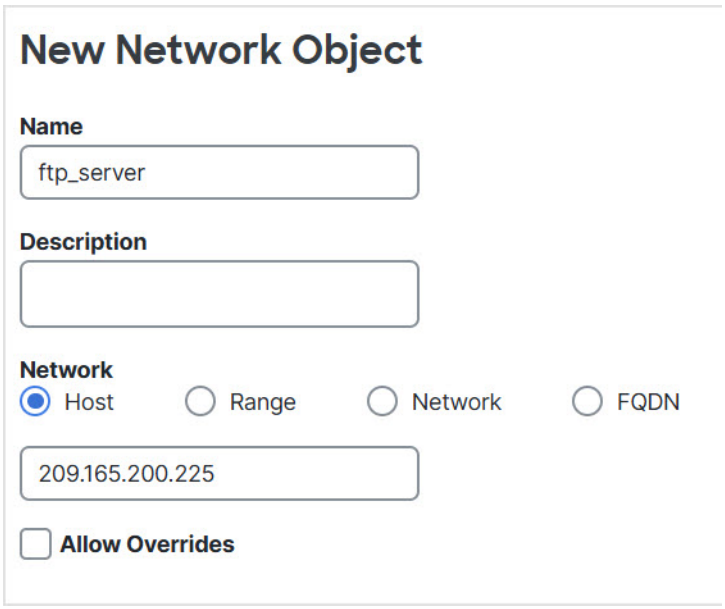
过程

步骤 1 为 FTP 服务器、DNS 服务器、内部网络和 PAT 池创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义实际 FTP 服务器地址。

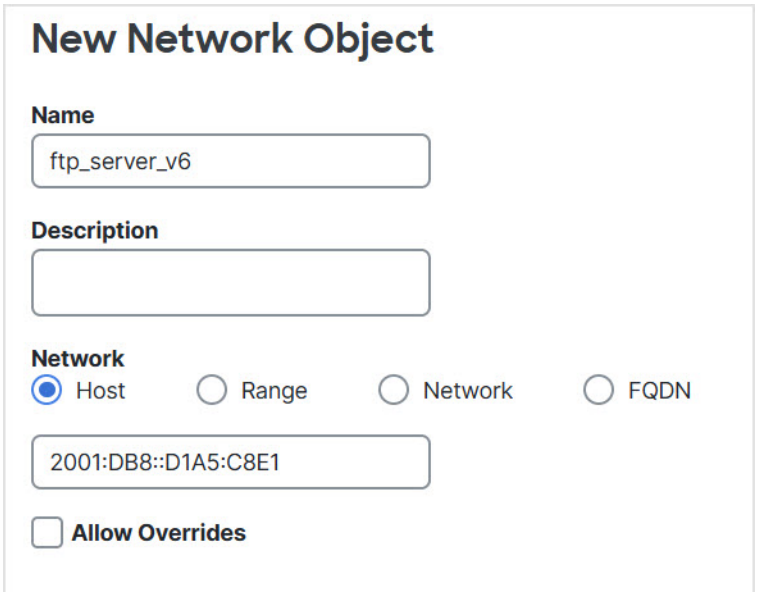
为网络对象命名（例如，ftp_server），然后输入主机地址 209.165.200.225。



c) 点击**保存**。

d) 点击**添加网络** > **添加对象**并定义 FTP 服务器的转换后 IPv6 地址。

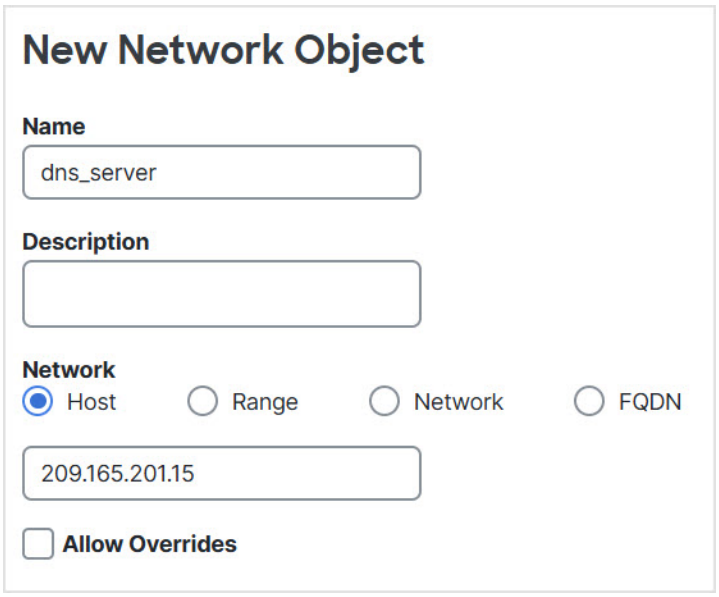
为网络对象命名（例如，ftp_server_v6），然后输入主机地址 2001:DB8::D1A5:C8E1。



e) 点击**保存**。

f) 点击**添加网络** > **添加对象**并定义 DNS 服务器的实际地址。

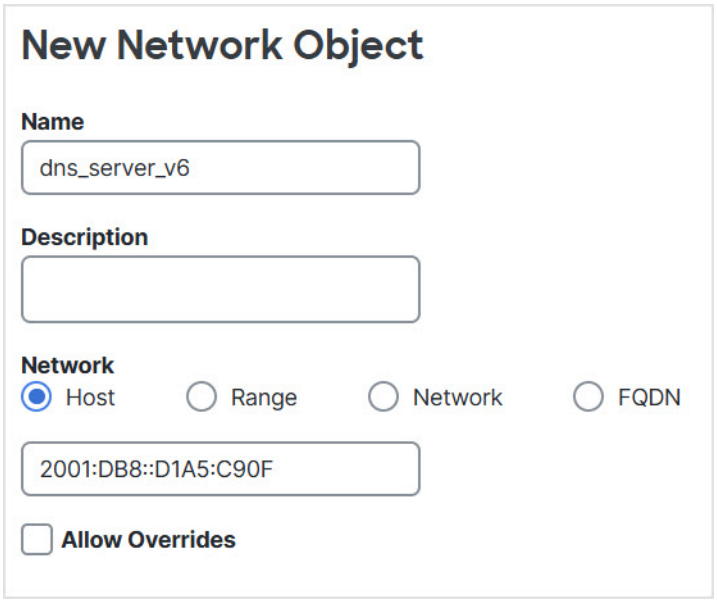
为网络对象命名（例如，dns_server），然后输入主机地址 209.165.201.15。



g) 点击**保存**。

h) 点击**添加网络** > **添加对象**并定义 DNS 服务器的转换后 IPv6 地址。

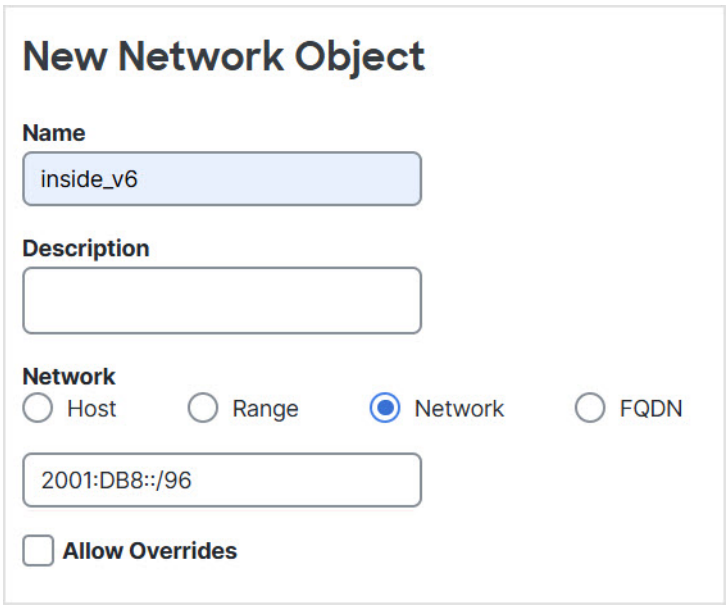
为网络对象命名（例如，dns_server_v6）并输入主机地址 2001:DB8::D1A5:C90F（其中 D1A5:C90F 是 209.165.201.15 的 IPv6 对应项）。



i) 点击**保存**。

j) 点击**添加网络** > **添加对象**并定义内部 IPv6 网络。

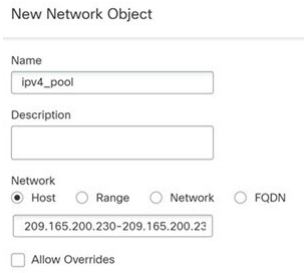
为网络对象命名（例如，inside_v6），然后输入网络地址 2001:DB8::/96。



k) 点击**保存**。

l) 点击**添加网络** > **添加对象**并定义内部 IPv6 网络的 IPv4 PAT 池。

为网络对象命名（例如，ipv4_pool），然后输入范围 209.165.200.230-209.165.200.235。



m) 点击**保存**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

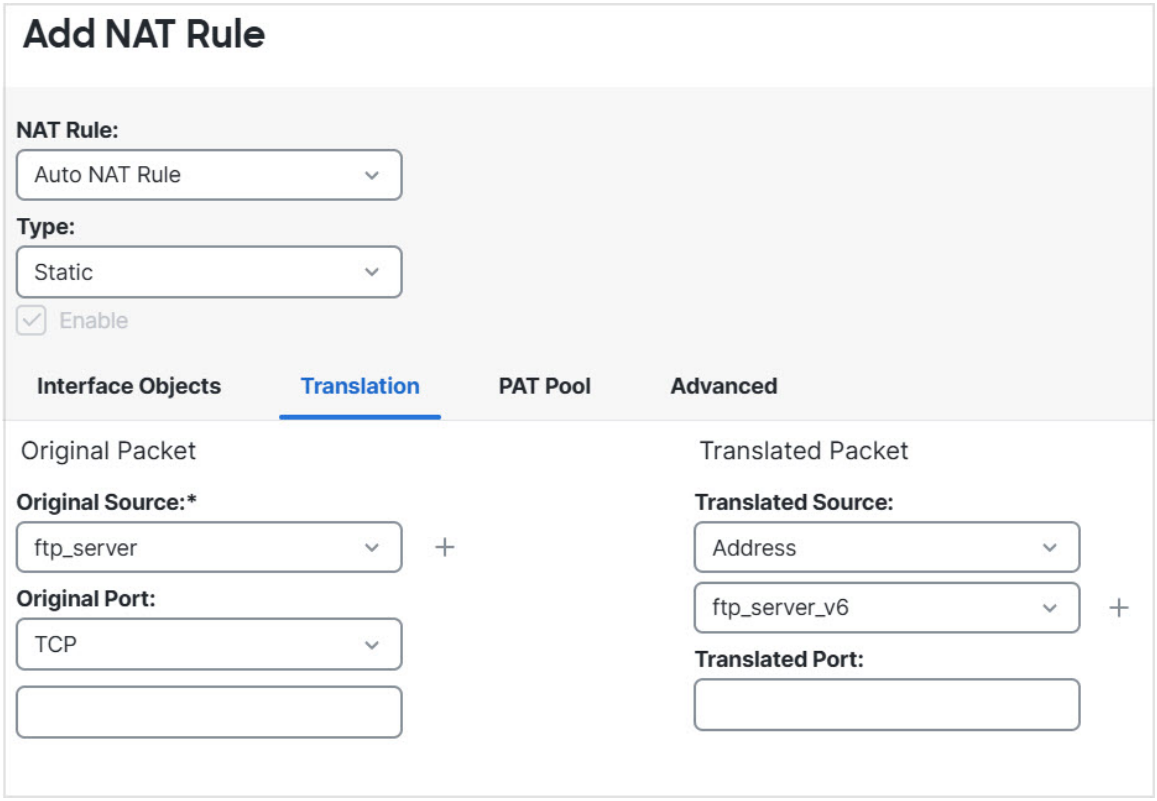
- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = ftp_server 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = ftp_server_v6 网络对象。



f) 在**高级 (Advanced)** 上，选择以下选项：

- **转换匹配该规则的 DNS 回复**。
- **网到网映射**，因为这是一对一 NAT46 转换。

g) 点击**确定**。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

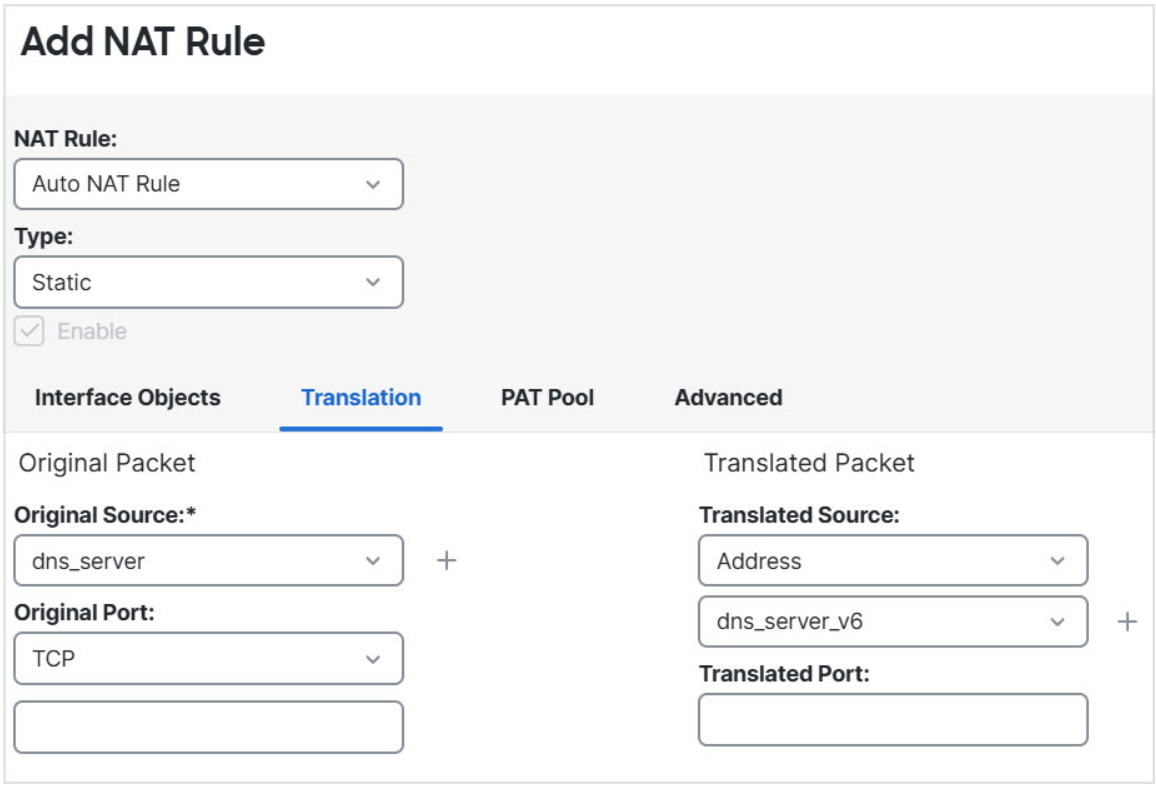
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

d) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = dns_server 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = dns_server_v6 网络对象。

e) 在**高级 (Advanced)** 上，选择**网到网映射 (Net to Net Mapping)**，因为这是一对一 NAT46 转换。



f) 点击**确定**。

步骤 4 为内部 IPv6 网络配置具有 PAT 池规则的动态 NAT。

a) 点击**添加规则**。

b) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型 (Type)**= 动态。

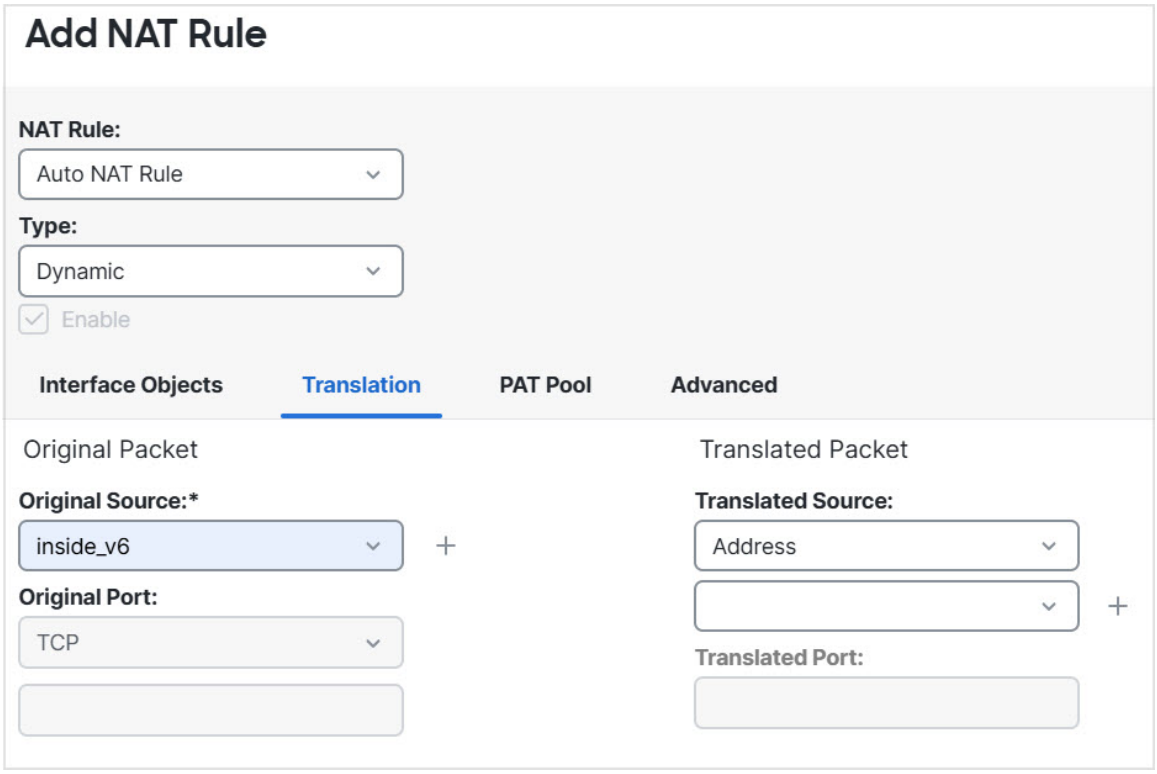
c) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

d) 在**转换 (Translation)** 上配置以下选项：

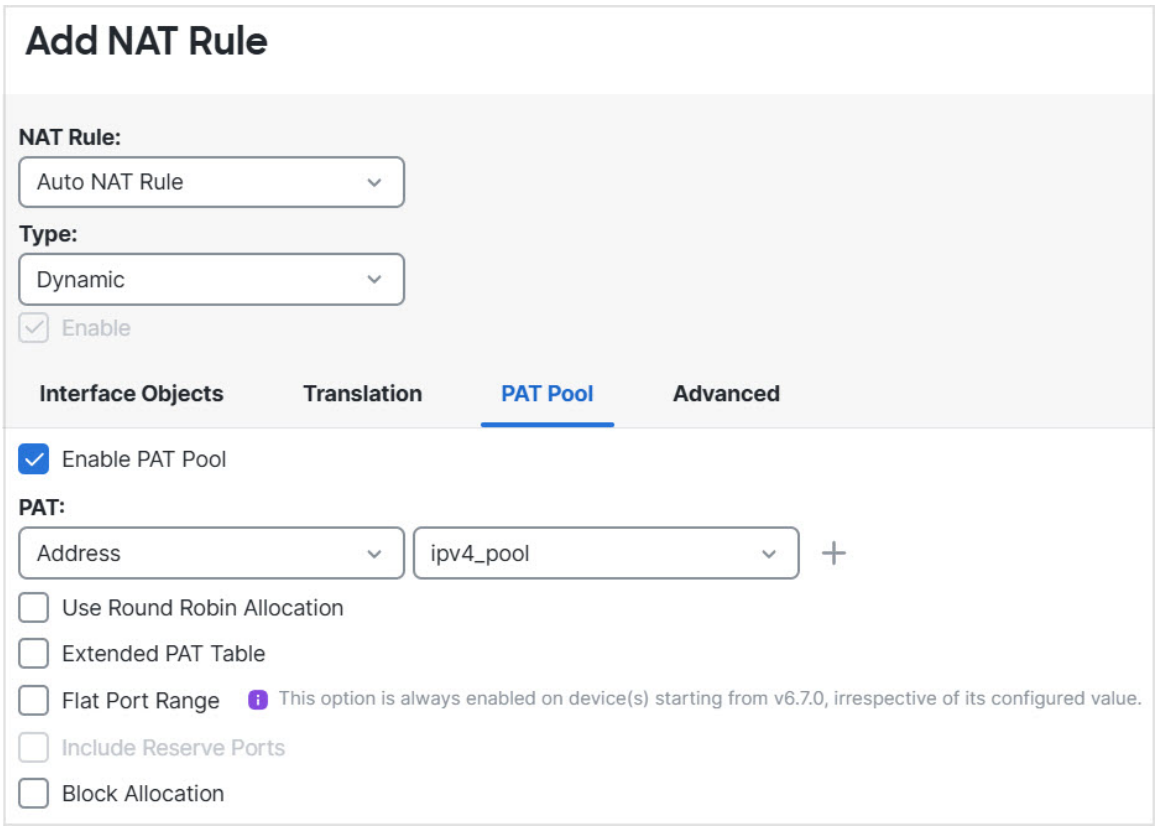
- **原始源** = inside_v6 网络对象。

- 转换后的源 > 地址 **(Translated Source Address)** = 将此字段留空。



e) 在 **PAT 池 (PAT Pool)** 中配置以下选项：

- 启用 **PAT 池** = 选择此选项。
- 转换后的源 > 地址 **(Translated Source Address)** = ipv4_pool 网络对象。



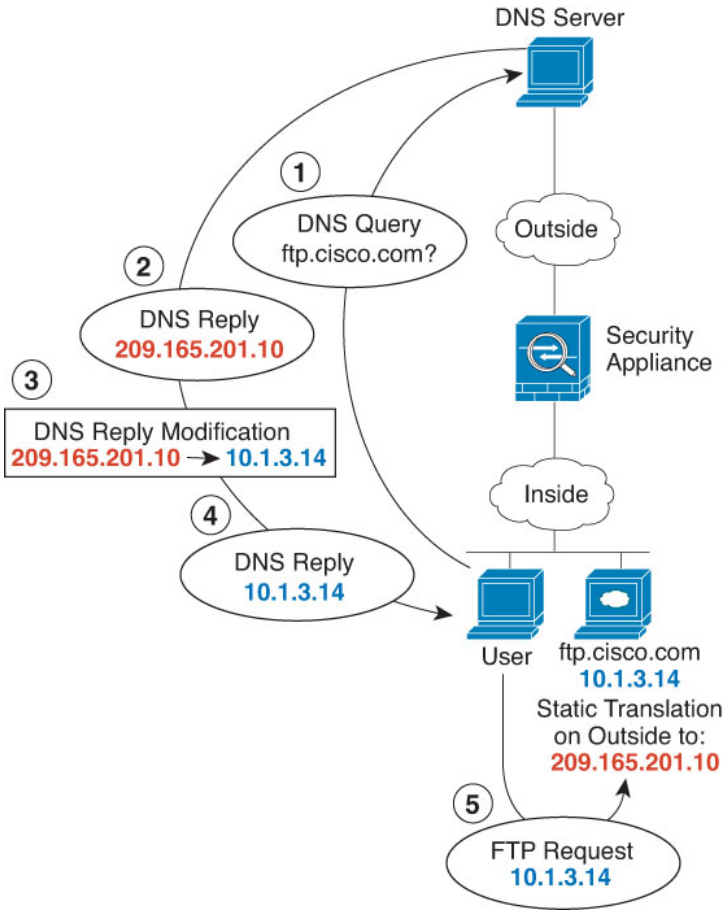
f) 点击**确定**。

DNS 应答修改，外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 NAT 配置为将 ftp.cisco.com 实际地址 (10.1.3.14) 静态转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。系统引用内部服务器的静态规则，并将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 回复修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

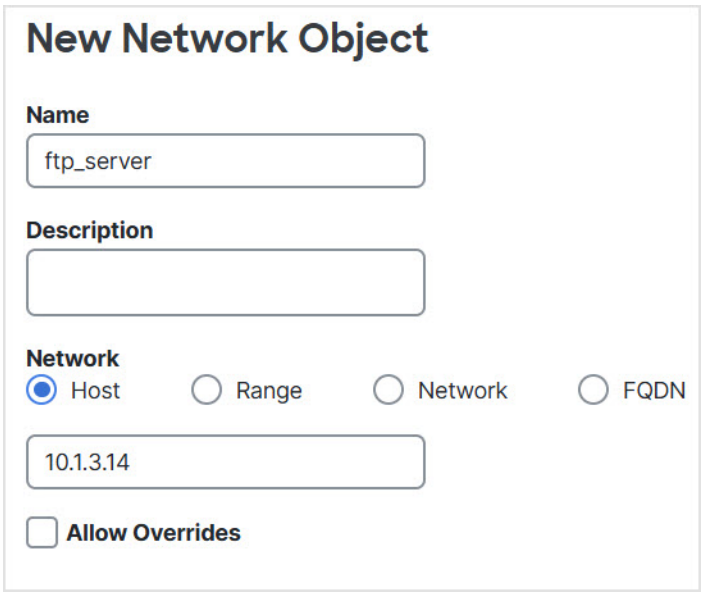
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义实际 FTP 服务器地址。

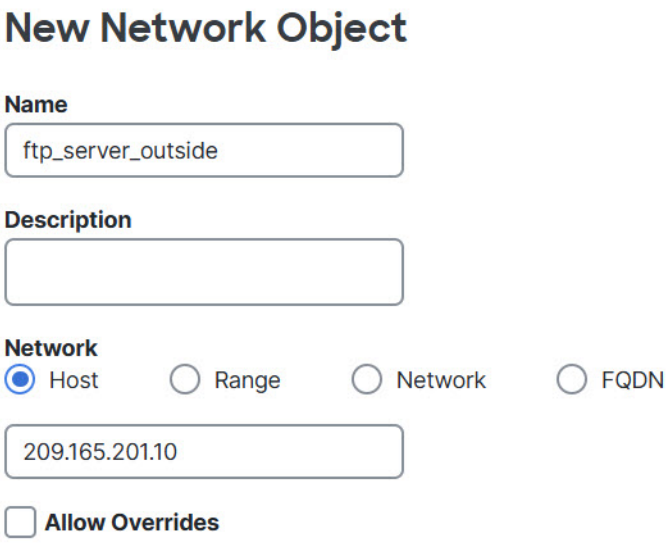
为网络对象命名（例如，ftp_server），然后输入主机地址 10.1.3.14。



c) 点击**保存**。

d) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**，然后定义 FTP 服务器的转换后地址。

为网络对象命名（例如，ftp_server_outside），然后输入主机地址 209.165.201.10。



e) 点击**保存**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。

- **类型** = 静态。

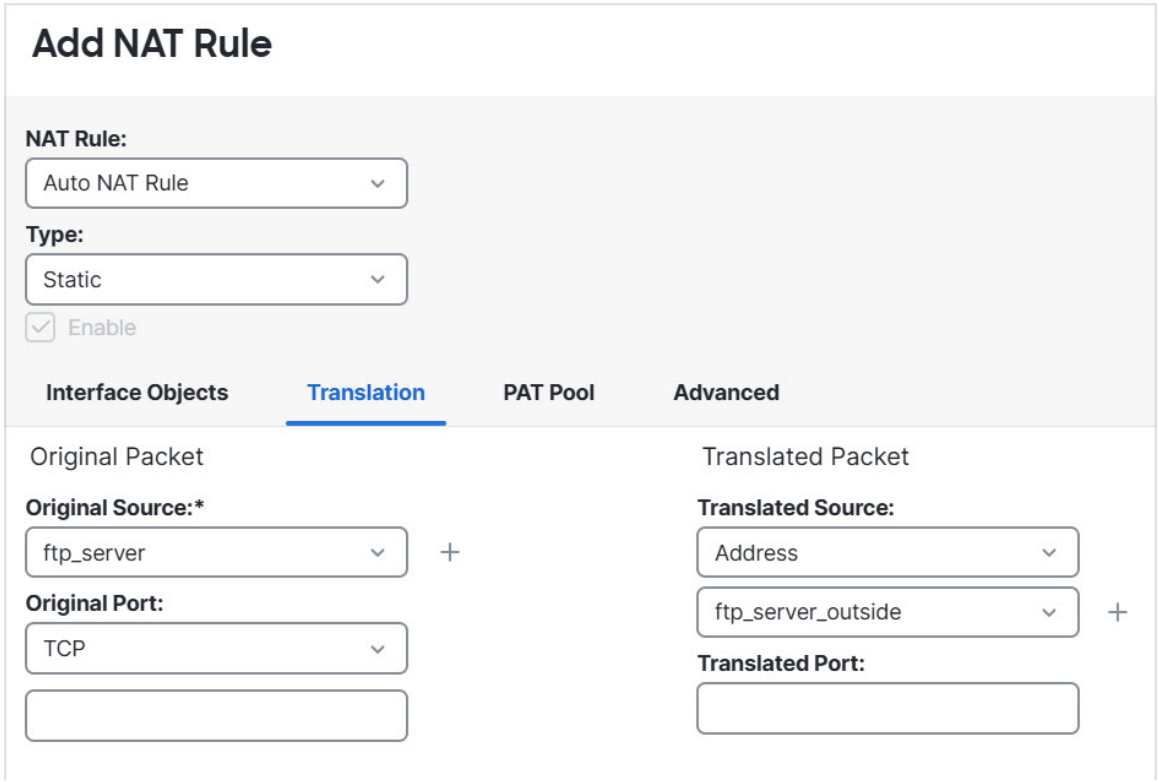
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 内部。
- **目标接口对象** = 外部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = ftp_server 网络对象。
- **转换后的源 (Translated Source)** > **地址 (Address)** = ftp_server_outside 网络对象。

f) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。

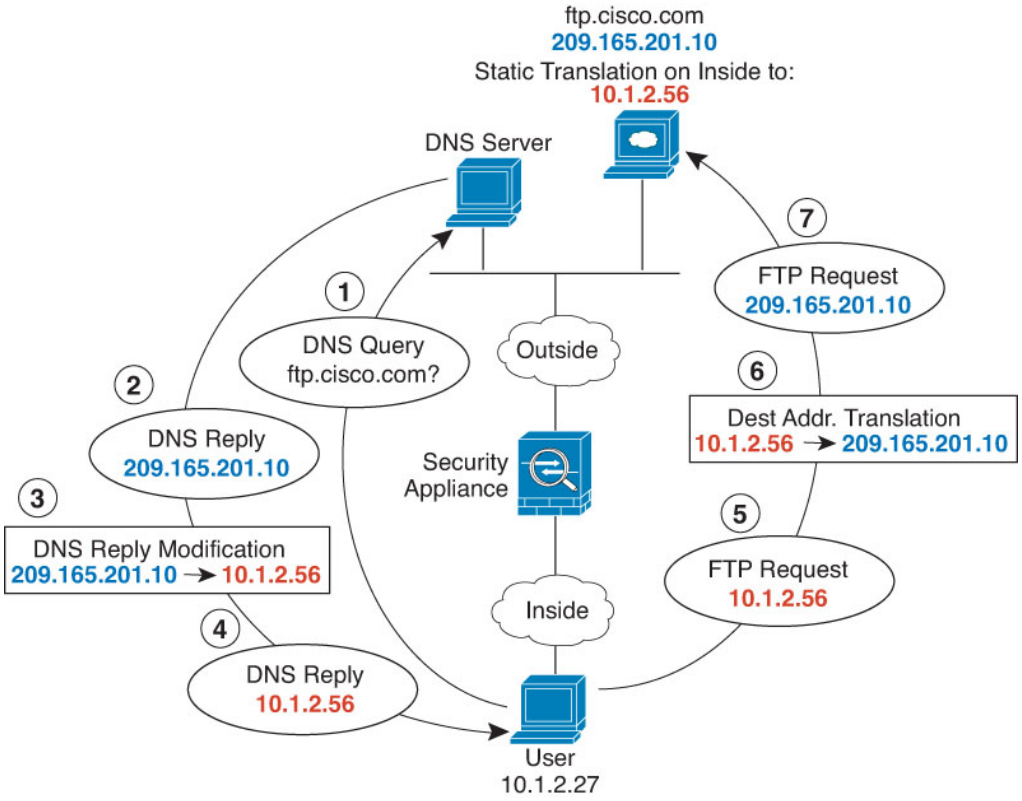


g) 点击**确定**。

DNS 应答修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10

作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。



开始之前

确保具有包含用于设备的接口的接口对象（安全区或接口组）。在本示例中，我们假定接口对象是名为**内部**和**外部**的安全区。要配置接口对象，请选择 **对象** > **接口**。

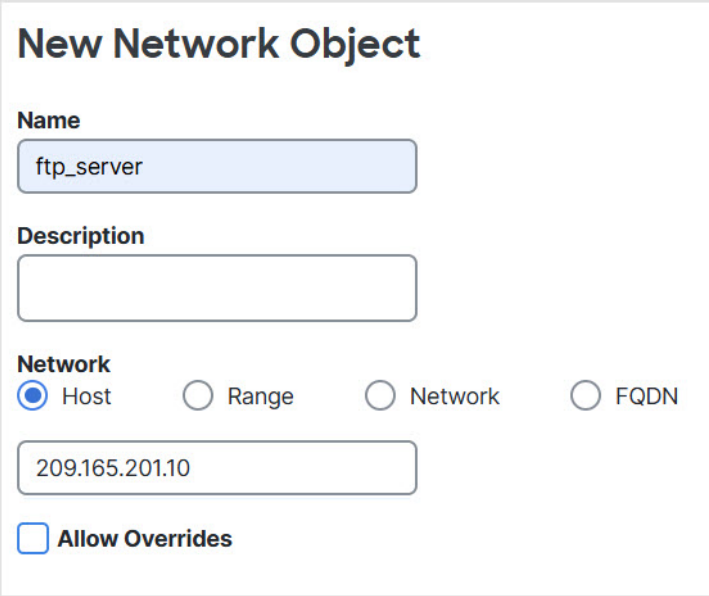
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择 **对象** > **网络** 并点击**添加网络** > **添加对象**。

b) 定义实际 FTP 服务器地址。

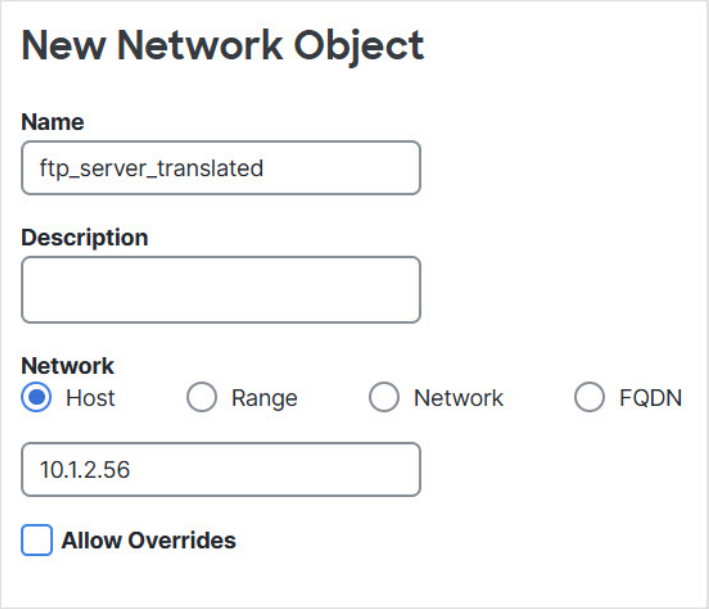
命名网络对象（例如，ftp_server），然后输入主机地址 209.165.201.10。



c) 点击**保存**。

d) 点击**添加网络 (Add Network)** > **添加对象 (Add Object)**，然后定义 FTP 服务器的转换后地址。

命名网络对象（例如，ftp_server_translated），然后输入主机地址 10.1.2.56。



e) 点击**保存**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

a) 选择 **策略** > **网络策略** > **NAT** 并创建或编辑 Firewall Threat Defense NAT 策略。

b) 点击**添加规则**。

c) 配置以下属性：

- **NAT 规则 (NAT Rule)** = 自动 NAT 规则。
- **类型** = 静态。

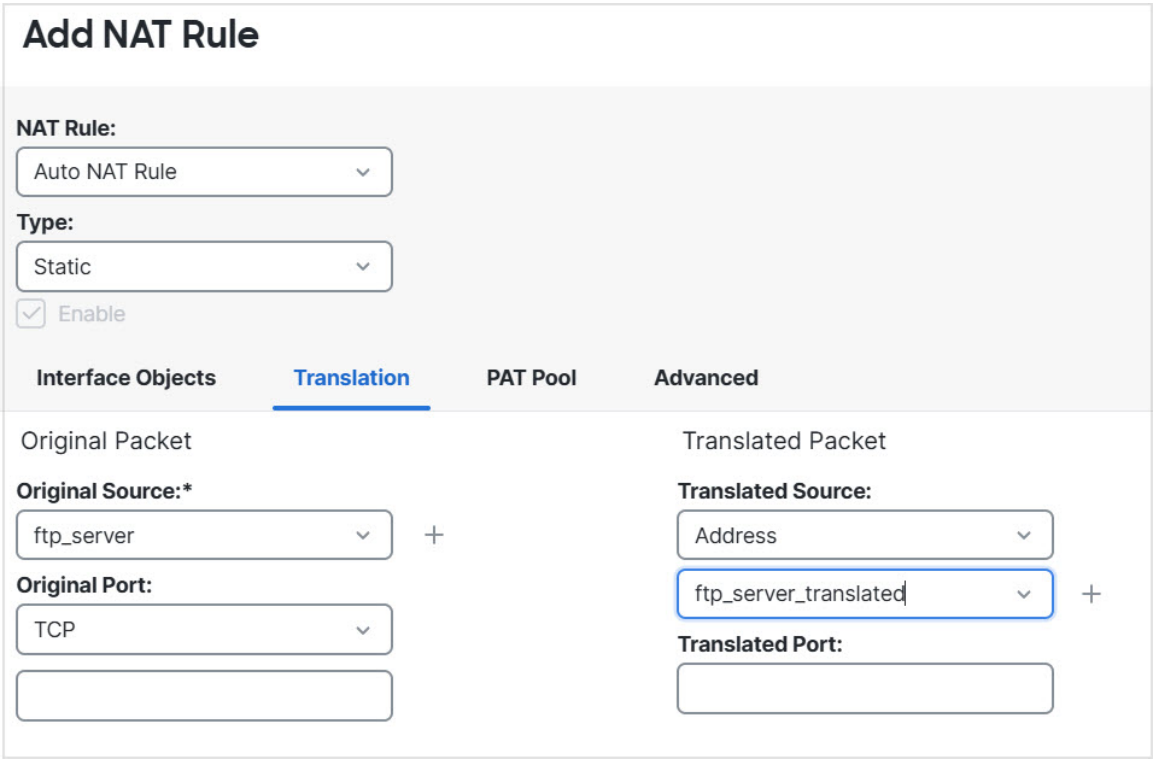
d) 在**接口对象 (Interface Objects)** 上配置以下选项：

- **源接口对象** = 外部。
- **目标接口对象** = 内部。

e) 在**转换 (Translation)** 上配置以下选项：

- **原始源** = ftp_server 网络对象。
- **转换后的源 > 地址 (Translated Source Address)** = ftp_server_translated 网络对象。

f) 在**高级 (Advanced)** 选项卡上，选择**转换与此规则匹配的 DNS 回复 (Translate DNS replies that match this rule)**。

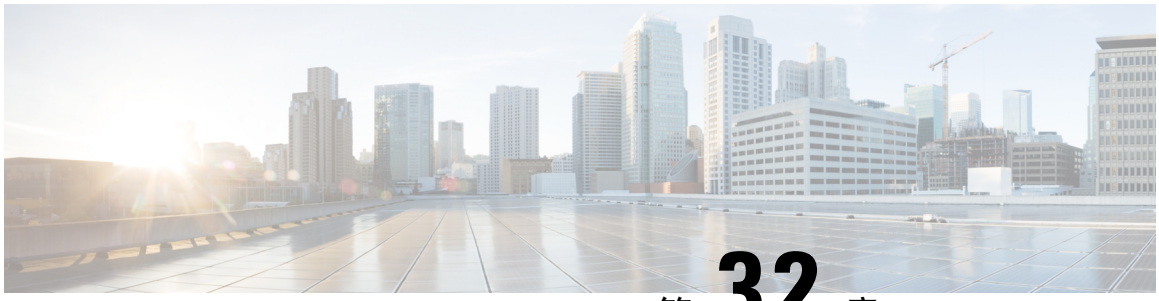


g) 点击**确定**。

Firewall Threat Defense NAT 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
编辑 NAT 规则时创建网络组。	7.2.6 7.4.1	任意	编辑 NAT 规则时，除网络对象外，还可以创建网络组。 版本 7.3.x 或7.4.0 不支持此功能。
能够一次启用、禁用或删除多个 NAT 规则。	7.2	任意	您可以选择多个 NAT 规则，并同时启用、禁用或删除它们。启用和禁用仅适用于手动 NAT 规则，而删除适用于任何 NAT 规则。
手动 NAT 支持完全限定域名 (FQDN) 对象作为转换目的。	7.1	任意	您可以使用 FQDN 网络对象（例如指定 www.example.com 的网络对象）作为手动 NAT 规则中的转换目标地址。系统根据 DNS 服务器返回的 IP 地址配置规则。
集群中对PAT地址分配的更改。PAT 池 **平面端口范围** 选项现在已默认启用，并且不可配置。	6.7	任意	更改PAT地址分配给集群成员的方式。以前，地址是分配给集群成员的，因此您的PAT池每个集群成员至少需要一个地址。现在，控制设备改为将每个PAT池地址划分为大小相等的端口块，并在集群成员之间分配它们。每个成员都有相同 PAT 地址的端口块。因此，您可以根据通常需要 PAT 的连接数量，将 PAT 池的大小减小到一个 IP 地址。能在 1024-65535 范围内，在 512 端口块中分配端口块。配置 PAT 池规则时，可以选择在此块分配中包含保留端口 1-1023。例如，在4节点集群中，每个节点获得32个数据块，与每个PAT池IP地址处理65535个连接的单个节点相比，它能够处理每个PAT池IP地址16384个连接。 作为此更改的一部分，所有系统的PAT池（无论是独立系统还是在集群中运行）现在都使用1023-65535的平面端口范围。以前，您可以通过在 PAT 池规则中包含**不分段端口范围 (Flat Port Range)** 选项来选择性地使用不分段范围。 **不分段端口范围 (Flat Port Range)** 选项现已被忽略：PAT池现在始终是不分段的。您可以选择 **包括保留端口 (Include Reserved Ports)** 选项，以在 PAT 池中包括 1-1023 端口范围。 请注意，如果配置端口块分配（ **块分配 (Block Allocation)** PAT 池选项），则会使用块分配大小，而不是默认的 512 端口块。此外，不能为集群中的系统的PAT池配置扩展PAT。
能够搜索和过滤 Firewall Threat Defense NAT 规则表。	6.7	任意	现在，您可以在 Firewall Threat Defense NAT 策略中搜索规则，以帮助您根据 IP 地址、端口、对象名称等查找规则。搜索结果包括部分匹配项。搜索条件会过滤规则表，以便仅显示匹配的规则。 当您编辑 Firewall Threat Defense NAT 策略时，我们在规则表上方添加了一个搜索字段。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
对服务提供商级 NAT 的改进。	6.5	任意	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。 新增/修改的屏幕：已将**块分配 (Block Allocation)** 选项添加到 Firewall Threat Defense NAT 规则的“NAT PAT 池”(NAT PAT Pool) 选项卡中。
支持 Firewall Threat Defense的 NAT 中的网络范围对象。	6.1.0	任意	您现在可以在适当时在 Firewall Threat Defense NAT 规则中使用网络范围对象。
Firewall Threat Defense 的网络地址转换 (NAT)。	6.0.1	任意	已添加 Firewall Threat Defense的 NAT 策略。 新增/修改的屏幕：威胁防御已作为一种 NAT 策略添加到**设备 (Devices)** > **NAT** 页面中。



第 32 章

服务质量

以下主题介绍如何将服务质量 (QoS) 功能用于采用 Firewall Threat Defense设备的策略网络流量：

- QoS 简介，第 1413 页
- 关于 QoS 策略，第 1413 页
- QoS 的要求和前提条件，第 1414 页
- QoS 策略准则和限制，第 1414 页
- 使用 QoS 策略的速率限制，第 1415 页
- QoS 的历史记录，第 1424 页

QoS 简介

访问控制允许或信任的服务质量（也称 QoS）、速率限制（策略）网络通信。系统不对快速路径的流量进行速率限制。

虽然 QoS 仅在 Firewall Threat Defense 设备的路由接口上支持，但在站点间 VPN 和 VTI 接口上并不支持。

日志记录速率限制连接

没有用于 QoS 的日志记录配置。可以在不记录的情况下对连接限制速率，但不能仅因为连接被限制速率而不记录连接。要查看连接事件中的 QoS 信息，必须单独将相应连接的两端记录到 防火墙管理中心数据库。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的您可以登录的其他连接。

速率限制连接的连接事件包含流量被丢弃的数量信息，以及有关限制流量的 QoS 配置的信息。您可以在事件视图（工作流）、仪表板和报表中查看此信息。

关于 QoS 策略

部署到托管设备上的 QoS 策略用于监管速率闲置。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

系统按照您指定的顺序将流量与 QoS 规则相匹配。系统根据第一条规则（其中所有规则的条件都与流量匹配）对流量进行速率限制。与任何规则都不匹配的流量不受速率限制。

注释 设备上的规则总数（包括 QoS 规则）不能超过 255。达到此阈值时，系统将显示部署警告消息。您需要减少成功部署的规则数量。

必须按源接口或目标（路由）接口来限制 QoS 规则。系统将对其中每个接口单独强制实施速率限制；不能为一组接口指定一个汇聚速率限制。

QoS规则还可以按其他网络特性以及情景信息（如应用、URL、用户身份和自定义安全组标记(SGT)）对流量实施速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

注释 QoS 不从属于主访问控制配置；您将单独配置 QoS。不过，部署到同一设备上的访问控制和 QoS 策略将共享身份配置；请参阅将其他策略与访问控制相关联，第 1719 页。

QoS 的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

QoS 策略准则和限制

- QoS 规则和服务策略规则（在访问控制策略中）将转换为防火墙上的命令。这包括创建策略映射。每个接口只能有一个策略映射。系统会自动将 QoS 和服务策略配置合并到每个接口的单个策略映射中。

  但是，您也可以使用 FlexConfig 手动创建策略映射。对于低端防火墙（例如 Cisco Secure Firewall 3100），您可以在配置中创建多达 64 个策略映射。对于功能更强大的防火墙（例如 Firepower

4100），您最多可以创建 128 个策略映射。请注意不要超过此限制，否则部署将失败。您可以从 CLI 查看设备配置，也可以使用部署脚本查看如何将规则转换为命令。

使用 QoS 策略的速率限制

要执行基于策略的速率限制，请配置 QoS 策略并将它们部署到托管设备。每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略** > **网络策略** > **QoS**。

步骤 2 点击**新建策略 (New Policy)** 创建新的 QoS 策略，并且可以选择分配目标设备；请参阅创建 QoS 策略，第 1416 页。

您也可以 **复制** () 或 **编辑** () 现有策略。

步骤 3 配置 QoS 规则；请参阅配置 QoS 规则，第 1417 页和QoS 规则条件，第 1419 页。

QoS 策略编辑器中的规则将按评估顺序列出每条规则，并显示规则条件和速率限制配置的摘要。右键点击菜单提供规则管理选项，包括移动、启用和禁用。

为有助于较大规模的部署，可以**按设备过滤**，以仅显示影响特定设备或设备组的规则。可以搜索规则，也可以在规则内部进行搜索；系统会将您在**搜索规则**字段中输入的文本匹配与规则名称和条件值相匹配，包括对象和对象组。

注释
正确创建规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果不认真规划，这些规则会抢占其他规则、需要额外的许可证或包含无效配置。图标代表注释、警告和错误。如果存在问题，请点击**显示警告**显示列表。有关详细信息，请参阅访问控制规则的最佳实践，第 1758 页。

步骤 4 点击**策略分配**识别策略针对的托管设备；请参阅为 QoS 策略设置目标设备，第 1416 页。

如果在创建策略过程中识别出了目标设备，请验证您的选择。

步骤 5 保存 QoS 策略。

步骤 6 由于此功能必须允许某些数据包通过，因此必须将系统配置为检查这些数据包。。

步骤 7 部署配置更改；请参阅 部署配置更改，第 180 页。

创建 QoS 策略

没有规则的新 QoS 策略不会执行速率限制。

过程

步骤 1 选择**策略** > **网络策略** > **QoS**。

步骤 2 点击**新建策略 (New Policy)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 （可选）选择要部署策略的**可用设备**，然后点击**添加到策略**或拖放**所选设备**。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。

在部署策略之前必须分配设备。

步骤 5 点击**保存**。

下一步做什么

- 配置和部署 QoS 策略；请参阅使用 QoS 策略的速率限制，第 1415 页。

为 QoS 策略设置目标设备

每项 QoS 策略可以多台设备为目标；每天设备每次只能部署一项 QoS 策略。

过程

步骤 1 在 QoS 策略编辑器中，点击**策略分配**。

步骤 2 制定目标联系人列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。
- 删除 - 点击单个设备旁边 **删除** ()，或选择多个设备，点击鼠标右键，然后选择 **删除所选项**。
- 搜索 - 在搜索字段中输入搜索字符串。点击 **清除** () 以清除搜索。

步骤 3 点击**确定** 以保存策略分配。

步骤 4 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

按设备过滤 QoS 规则

您可以根据规则适用的设备过滤 QoS 策略规则列表。系统使用规则的接口限制来确定该规则是否影响设备。

提示 将指针悬停在规则标准上方可查看其值。如果标准代表具有设备特定覆盖的对象，则系统会在您仅按该设备过滤规则列表时显示覆盖值。如果标准代表具有域特定覆盖的对象，则系统会在您按该域中的设备过滤规则列表时显示覆盖值。

过程

步骤 1 在策略编辑器中，点击**规则 (Rules)**，然后点击**按设备过滤 (Filter by Device)**。
系统将会显示目标设备和设备组列表。

步骤 2 选中一个或多个复选框，以仅显示应用于这些设备或组的规则。或者，选中**全部 (All)** 复选框，以重置和显示所有的规则。

步骤 3 点击**确定**。

按钮旁边会出现一条消息，指定正在使用的过滤器。要移除过滤器，请点击消息中的 X，或者返回并在“按设备过滤”对话框中选择**所有**。

配置 QoS 规则

创建或编辑规则时，请使用规则编辑器的上半部分配置常规规则属性。使用规则编辑器的下半部分来配置规则条件和注释。

过程

步骤 1 在 QoS 策略编辑器的“规则”上：

- 添加规则 - 点击**添加规则 (Add Rule)**。
- 编辑规则-点击 **编辑** ( )。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分。

- **已启用** -指定规则是否为已启用。
- QoS 应用位置 - 选择要进行速率限制的接口：**目标接口对象中的接口 (Interfaces in Destination Interface Objects)** 或**源接口对象中的接口 (Interfaces in Source Interface Objects)**。您的选择必须与填入的接口限制相对应（不为**任意 [any]**）。

- 每个接口的流量限制 - 以兆位/秒为单位输入**下载限制**和**上传限制**。默认值**无限制**可防止在该方向上对匹配流量进行速率限制。
- 条件 - 点击要添加的相应的条件。必须配置源或目标接口条件，与您选择的 **QoS 应用位置**相对应。
- 注释-点击 **注释**。要添加注释，请点击**新建注释 (New Comment)**，输入注释，然后点击**确定**。您可以在保存规则之前编辑或删除此注释。

如需有关规则组成部分的详细信息，请参阅QoS 规则组成部分 ，第 1418 页。

步骤 4 保存规则。

步骤 5 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。

规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 6 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改 ，第 180 页。

相关主题

访问控制规则的最佳实践 ，第 1758 页

QoS 规则组成部分

状态（启用/禁用）

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

接口（QoS 应用位置）

您不能保存对所有流量都进行速率限制的 QoS 规则。对于每个 QoS 规则，必须将 QoS 应用于以下两个选项之一：

- 源接口对象中的接口 - 对通过规则源接口的流量进行速率限制。如果选择此选项，必须至少添加一个源接口限制（不能为**任何 [any]**）。
- 目标接口对象中的接口 - 对通过规则目标接口的流量进行速率限制。如果选择此选项，必须至少添加一个目标接口限制（不能为**任何 [any]**）。

每个接口的流量限制

QoS 规则对您使用“QoS 应用位置”(Apply QoS On) 选项指定的每个接口单独实施速率限制。不能为一组接口指定汇聚速率限制。

您可以按兆位/秒对流量进行速率限制。默认值**无限制 (Unlimited)** 可防止对匹配流量进行速率限制。

您可以单独对下载流量和上传流量进行速率限制。系统根据连接发起方确定下载和上传方向。

如果指定限制大于接口的最大吞吐量高，系统不会对匹配的流量进行速率限制。最大吞吐量可能受接口的硬件配置影响，可在每台设备的属性中指定硬件配置（**设备** > **设备管理**）。

条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。有关详细信息，请参阅QoS 规则条件，第 1419 页。

备注

每次保存对规则所做的更改时，都可以添加备注。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。

在策略编辑器中，系统会显示规则具有的注释数量。在规则编辑器中，请使用“注释”(Comments) 选项卡查看现有注释和新注释。

QoS 规则条件

条件指定规则处理的特定流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。每种条件类型在规则编辑器中都有自己的选项卡。您可以使用以下方式对流量进行速率限制：

有关详细信息，请参阅以下各节之一：

相关主题

接口规则条件，第 1419 页
网络规则条件，第 1420 页
用户规则条件，第 1420 页
应用规则条件，第 1420 页
端口规则条件，第 1421 页
URL 规则条件，第 1423 页
自定义 SGT 规则条件，第 1423 页

接口规则条件

接口规则条件按流量的源接口和目标接口控制流量。

根据规则类型和部署中的设备，您可以使用名为 安全区域 或 接口组 的预定义 接口对象 构建接口条件。接口对象对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量；请参阅接口，第 2655 页。QoS 规则只能应用于路由接口。

提示 按接口限制规则是提高系统性能的一种最佳方式。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

网络规则条件

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

用户规则条件

根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

您只能为 Microsoft Active Directory 领域中的用户配置用户规则条件。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1719 页中所述。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅应用检测器基础知识，第 2564 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *85:* 应用特征

特征	说明	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

对于会动态打开独立通道以区分控制流和数据流的应用（如 Firewall Threat Defense），也建议使用应用过滤。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标记。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 Firewall Threat Defense设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- 解密 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅关于使用类别和信誉进行 URL 过滤，第 1786 页。

自定义 SGT 规则条件

如果未将 ISE/ISE-PIC 配置为身份源，可以使用**非** ISE 分配的安全组标记 (SGT) 来控制流量。SGT 会指定可信网络内的流量源的权限。

自定义 SGT 规则条件使用手动创建的 SGT 对象来过滤流量，而不是使用从系统与 ISE 服务器的连接中获取的 ISE SGT 进行过滤。这些手动创建的 SGT 对象与要控制的流量的 SGT 属性相对应。使用自定义 SGT 控制流量不属于用户控制。

ISE SGT 与自定义 SGT 规则条件

某些规则允许您根据分配的 SGT 来控制流量。根据规则类型和您的身份源配置，您可以使用 ISE 分配的 SGT 或自定义 SGT 将流量与分配的 SGT 属性进行匹配。

注释 如果您使用 ISE SGT 匹配流量，即使一个数据包没有分配的 SGT 属性，当与该数据包的源 IP 地址关联的 SGT 在 ISE 中已知时，该数据包仍会匹配 ISE SGT 规则。

条件类型	要求在目录	规则编辑器中列出的 SGT
ISE SGT	ISE 身份源	通过查询 ISE 服务器获得的 SGT，包含自动更新的元数据
自定义 SGT	无 ISE/ISE-PIC 身份源	您创建的静态 SGT 对象

从自定义 SGT 自动过渡到 ISE SGT

如果您创建与自定义 SGT 匹配的规则，然后将 ISE/ISE-PIC 配置为身份源，则系统：

- 禁用对象管理器中的**安全组标记**选项。尽管系统会保留现有 SGT 对象，但您不能修改它们或添加新的 SGT 对象。
- 保留使用自定义 SGT 条件的现有规则。但是，这些规则与流量不匹配。您也不能为现有规则添加其他自定义 SGT 条件，或创建具有自定义 SGT 条件的新规则。

如果您配置了 ISE，则思科建议您删除或禁用具有自定义 SGT 条件的现有规则。相反，使用 ISE 属性条件将流量与 SGT 属性相匹配。

QoS 的历史记录

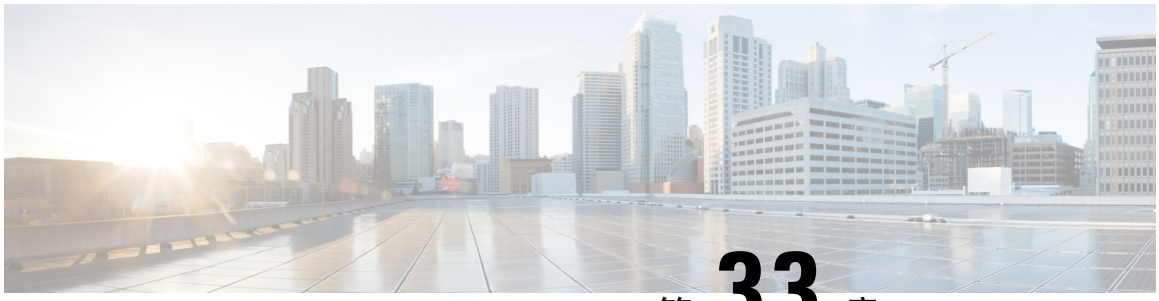
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
已弃用：具有 FlexConfig 的优先级队列。	7.2.5	7.2.5	FlexConfig 用于在威胁防御中配置优先级队列。此命令行已删除。
能够指定具有未知信誉的 URL 的处理方式。	6.7.0	任意	有关详细信息，请参阅URL 过滤的历史记录，第 1810 页。 新增/修改的屏幕：QoS 规则编辑器
增加了速率限制。	6.2.1	任意	将最大速率限制从 1000 Mbps 增加到 100,000 Mbps。 新增/修改的屏幕：QoS 规则编辑器
自定义 SGT 和原始客户端网络过滤。	6.2.1	任意	可以使用自定义安全组标记 (SGT) 和原始客户端网络信息（XFF、真实客户端 IP 或自定义的 HTTP 报头）来限制流量的速率。 新增/修改的屏幕：QoS 规则编辑器
引入了 QoS（速率限制）。	6.1.0	任意	FTD 会对访问控制允许或信任的网络流量进行速率限制（策略）。 新增/修改的屏幕：**设备 (Devices)** > **QoS**



第 VI 部分

安全连接

- 安全连接概览， 第 1427 页
- 站点间 VPN， 第 1443 页
- SD-WAN， 第 1507 页
- 远程访问 VPN， 第 1531 页
- 动态访问策略 ， 第 1649 页



第 33 章

安全连接概览

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本章适用于 Cisco Secure Firewall Threat Defense 设备上的 远程访问和 站点间 VPN。它描述了互联网协议安全 (IPsec)、互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及用于构建站点间 和远程访问 VPN 的 SSL 标准。

- VPN 类型， 第 1427 页
- VPN 基础知识， 第 1428 页
- VPN 数据包流， 第 1431 页
- IPsec 流分流， 第 1431 页
- VPN 许可， 第 1432 页
- VPN 加密与性能， 第 1432 页
- 已弃用的哈希算法、加密算法和 Diffie-Hellman 模数组， 第 1437 页
- VPN 拓扑， 第 1438 页

VPN 类型

VPN 类型是一种网络连接类别，

- 在远程位置和专用网络之间提供安全、加密的连接
- 支持部署模式，包括远程访问和站点到站点配置，以及
- 使用各种协议（包括 SSL 和 IPsec）建立安全隧道。

支持的 VPN 连接类型

防火墙管理中心 支持这些类型的 VPN 配置：

- Firewall Threat Defense 设备上的远程接入 VPN。

  远程接入VPN提供远程用户和您公司的专用网络之间的安全、加密连接或隧道。这些连接使用两种设备：一种是 VPN 终端设备，它具有 VPN 客户端功能的工作站或移动设备；一种是位于企业专用网络边缘的 VPN 前端设备或安全网关。

Cisco Secure Firewall Threat Defense设备可以配置为通过 防火墙管理中心支持 SSL 或 IPsec IKEv2 上的远程接入 VPN。这些设备作为安全网关，可以验证远程用户身份、授权访问并加密数据，从而为您的网络提供安全连接。仅这些设备支持由 防火墙管理中心 管理的远程访问 VPN 连接。

Cisco Secure Firewall Threat Defense安全网关支持 安全客户端完整隧道客户端。为远程用户提供安全的 SSL IPsec IKEv2 连接需要此客户端。在建立连接后，系统会自动安装此客户端，因此网络管理员无需在远程计算机上手动安装或配置此客户端。它是终端设备上唯一受支持的客户端。

- Firewall Threat Defense 设备上的站点间 VPN。

  站点间VPN可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他思科或第三方对等体之间创建站点间的 IPsec 连接。这些对等体可以使用 IPv4 和 IPv6 地址。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件和 IKEv1 或 IKEv2 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

VPN 基础知识

VPN 是一种安全的网络技术，

- 利用隧道技术在公共TCP/IP网络（如互联网）上建立远程用户与企业专用网络之间的安全连接
- 采用基于 IPsec 的技术（符合 ISAKMP [IKE] 和 IPsec 隧道标准）来构建和管理隧道，并
- 通过封装和解封装数据包的隧道端点实现双向数据传输。

VPN 隧道管理功能

ISAKMP 和 IPsec 实现以下隧道管理功能：

- 协商隧道参数。
- 建立隧道。
- 验证用户和数据。
- 管理安全密钥。
- 加密和解密数据。
- 管理隧道中的数据传输。
- 作为隧道终端或路由器管理入站和出站数据传输。

VPN 中的设备可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目标。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

建立站点间 VPN 连接之后，本地网关后的主机可通过安全 VPN 隧道连接至远程网关后的主机。一个连接由以下部分组成：这两个网关的IP地址和主机名、这两个网关后的子网，以及这两个网关用来进行相互身份验证的方法。

VPN 部署使用两种主要设备类型：

- 中心：实现与一个或多个远程分支设备或分支之间的安全VPN连接的设备。中心还充当分支相互通信的网关。
- 分支：通过VPN连接到中心设备，以安全访问中心设备背后的企业资源的设备。分支通过中心相互通信。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是一种关键管理协议，可以

- 对 IPsec 对等体进行身份验证
- 协商并分发 IPsec 加密密钥，并且
- 自动建立 IPsec 安全关联 (SA)。

IKE 协商阶段和政策

IKE 协商包括两个阶段：

- 第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。
- 在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。

每个阶段都使用提议来协商连接。

IKE 策略是一组算法，供两个对等体用于保护它们之间的 IKE 协商。当每个对等体同意一个共同的 IKE 策略时，IKE 协商开始。此策略定义了保护后续 IKE 协商的安全参数。IKEv1 策略包含一组算法和一个模数组。在 IKEv2 策略中，您可以选择多个算法和模数组供对等体在第一阶段协商期间选择。您可以创建单个 IKE 策略，或创建多个策略以优先考虑首选选项。对于站点间 VPN，您可以创建 IKE 策略。IKEv1 和 IKEv2 最多分别支持 20 个 IKE 策略，每个都有不同的值集。为您创建的每个策略分别分配一个唯一的优先级。较低的优先级数字表示较高的策略优先级。

要定义 IKE 策略，请指定：

- 唯一的优先级（1 到 65,543，1 为最高优先级）。
- 一种 IKE 协商加密方法，用于保护数据并确保隐私。
- 一种散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于验证发送方的身份，并确认消息在传输过程中未被更改。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。这些选项与用于散列算法的选项相同。
- Diffie-Hellman组，用于确定加密密钥确定算法的强度。设备使用此算法派生加密密钥和散列密钥。
- 身份验证方法，用于确保对等体的身份。

- 在更换加密密钥前，设备可使用该加密密钥的时间限制。

当 IKE 协商开始时，发起对等体将其所有策略发送到远程对等体。远程对等体按优先级顺序搜索与其自身策略的匹配项。如果两个对等体使用相同的加密、散列（IKEv2 中的完整性和 PRF）、身份验证和 Diffie-Hellman 值，则 IKE 策略匹配。SA 生存期必须小于或等于发送的策略中的生存期。如果生存期不完全相同，则采用远程对等体策略中的较短值。默认情况下，为确保所有VPN终端协商成功，Secure Firewall Management Center 会为所有 VPN 终端部署具有最低优先级的 IKEv1 策略。

IPSec

IPsec 是一种用于设置 VPN 的安全方法：

- 提供 IP 数据包级别的数据加密，
- 通过隧道在公共网络上传输数据，隧道是两个对等体之间安全的逻辑通信路径，并且
- 通过安全协议和算法的组合来保护进入 IPsec 隧道的流量。

使用 IPsec，数据通过隧道在公共网络上传输。

IPsec 提议策略组件

IPsec 提议策略定义了 IPsec 隧道的设置。IPsec 提议包含一个或多个加密映射，这些映射应用于设备中的 VPN 接口。加密映射整合了设置 IPsec 安全关联所需的所有元素，包括：

- 提议（或转换集）结合了安全协议和算法，以保护 IPsec 隧道中的流量。在 IPsec 安全关联 (SA) 协商过程中，对等方会寻找匹配的提议。应用所选的提议以创建安全关联 (SA)，保护加密映射访问列表中的数据流并确保 VPN 流量的安全。IKEv1 和 IKEv2 有单独的 Ipsec 提议。在 IKEv1 提议（或转换集）中，每个参数都需要设置一个值。在 IKEv2 提议中，您可以为单个提议配置多个加密和集成算法。
- 加密映射整合了设置 Ipsec 安全关联 (SA) 所需的所有元素，包括 IPsec 规则、提议、远程对等体以及定义 IPsec SA 所需的其他参数。当两个对等体尝试建立 SA 时，必须至少有一个兼容的加密映射项。

  当未知的远程对等体尝试启动与本地中心的 IPsec 安全关联时，站点间 VPN 中将使用动态加密映射策略。中心不会发起安全关联协商。动态加密策略允许远程对等体与本地中心交换 Ipsec 流量，即使中心不知道远程对等体的身份。动态加密映射策略会在配置所有参数之前创建加密映射条目。IPsec 协商随后动态配置缺失的参数，以满足远程对等方的要求。

  动态加密映射策略适用于中心辐射型以及点对点VPN拓扑。要应用动态加密映射策略，请为拓扑中的一个对等体指定动态 IP 地址，同时确保在此拓扑上启用动态加密映射。在全网格 VPN 拓扑中，只能应用静态加密映射策略。



注释 对于 Firewall Threat Defense 设备上的远程访问和站点间 VPN，同一接口不支持同时使用 IKEv2 动态加密映射。

VPN 数据包流

VPN 数据包流是一个安全过程，

- 在允许流量通过之前，需要通过访问控制获得明确的权限，
- 在将传入的隧道数据包发送到 Snort 进程之前对其进行解密。
- 在加密之前，通过 Snort 处理传出的数据包，并且
- 隧道关闭时，阻断通往公共水源的隧道交通。

访问控制要求

访问控制识别 VPN 隧道中每个终端节点的受保护网络，并确定哪些流量允许通过 Firewall Threat Defense 设备并到达终端。对于远程接入 VPN 流量，必须将组策略过滤器或访问控制规则配置为允许 VPN 流量。

IPsec 流分流

IPsec 流卸载是一项性能优化功能：

- 初始建立后，将 IPsec 连接卸载至现场可编程门阵列 (FPGA) 或专用硬件组件
- 通过在硬件中处理预解密、解密、预加密和加密来提升设备性能，并且
- 在支持的设备型号上默认启用，系统软件仍处理内层流安全策略。

IPsec 流卸载特性

初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)。此过程可提高设备性能。在 Cisco Secure Firewall 1200 系列上，IPsec 连接被分流到Marvell 加密加速器 (CPT)，以提高设备性能。Cisco Secure Firewall 6100 系列中，IPsec 连接卸载至 Kintex 7 (KC400) FPGA。该 FPGA 内置加密引擎，支持 AES-GCM-128 和 AES-GCM-256 加解密。

卸载操作包括入向和出向的预解密及解密处理。系统软件对内层流应用安全策略。

IPsec 流卸载适用于以下设备类型：

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

启用设备的 VTI 环回接口时，也会使用 IPsec 数据流分流。

对于集群分布式站点间 VPN 模式中的不对称流量，IPsec 流分流可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，且在启用 IPsec 流卸载时始终可用。

默认情况下，系统在支持的設備型号上启用 IPsec 流卸载。要更改配置，请使用 FlexConfig 实施 **flow-offload-ipsec** 命令。有关详细信息，请参阅 ASA 命令参考。

VPN 许可

您不需要特定的许可证即可在 Firewall Threat Defense 设备上启用 VPN，该功能默认可用。

防火墙管理中心会根据设备中的出口管制功能来决定允许还是阻止在 Firewall Threat Defense 设备中使用强加密。在注册思科智能软件管理器时，可启用此功能。如果您使用的是评估许可证，或者您没有启用出口控制功能，则无法使用强加密。选择 **管理** > **许可证** > **智能许可证** 以便在 防火墙管理中心 中验证此功能。

如果您使用评估许可证创建了VPN配置，后来将许可证升级为具有出口管制功能的智能许可证，请检查并更新您的加密算法以使用更强的加密，确保 VPN 正常运行。请勿使用基于 DES 的加密，因为它不受支持。

VPN 加密与性能

配置 VPN 隧道加密时，请提供充分的保护，并通过平衡安全性和性能来维持效率。

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。您可以通过 IKE 策略和 IPsec 提议来定义加密及其他安全技术。使用更强的隧道加密可能会降低系统性能。

如果您的设备许可证允许使用强加密，您可以从丰富的加密算法、散列算法和Diffie-Hellman组中进行选择。本文档不提供关于具体选项选择的指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

符合安全认证要求

查看您的认证要求和可用选项以规划 VPN 配置。许多 VPN 设置都有允许您遵守各种安全认证标准的选项。

为 VPN 策略决定加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

- 对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。
- 对于 IKEv1，仅可以选择一个选项。

- 对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀。

如果设备许可证符合强加密要求，可以从可用的加密算法中选择。如果不符合强加密要求，则只能选择 DES。

强加密许可证注意事项



注释 如果符合强加密要求，在从评估许可证升级到智能许可证之前，请检查并更新加密算法以实现更强的加密，从而使 VPN 配置正常工作。选择基于 AES 的算法。如果您使用支持强加密的帐户注册，则不支持 DES。注册后，在删除对 DES 的所有使用之前，您无法部署更改。

可用的加密算法：

- AES-GCM — （仅限 IKEv2）Galois/计数器模式下的高级加密标准是一种分组密码模式，提供机密性和数据源身份验证。它比 AES 提供更高的安全性。

  AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。较长的密钥可提高安全性，但会降低性能。NSA Suite B 是一组加密算法，设备必须支持该算法集以满足联邦密码强度标准，其要求使用 GCM。

- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。较长的密钥可提高安全性，但会降低性能。

- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证帐户不符合导出控制要求，这将是您唯一的选择。

- Null、ESP-Null - 空加密算法提供无加密的身份验证。此方法不安全，请自行决定是否使用。

决定使用哪些散列算法

在 IKE 政策中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，您可以选择一个散列算法用于完整性，另一个用于伪随机函数 (PRF)。

在 IPsec 提议中，封装安全协议 (ESP) 使用散列算法进行身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称包含 ESP- 前缀和 -HMAC 后缀。

系统将按安全性从高到低的顺序排列您的设置，并按此顺序与对等体进行协商。对于 IKEv1，请仅选择一个选项。

选择满足安全和性能需求的散列算法：

- SHA（安全散列算法）— 生成 160 位摘要的标准 SHA (SHA1)。

  这些 SHA-2 选项提供更高的安全性，且可用于 IKEv2 配置。如果需要 NSA Suite B 密码学合规，请选择其中之一。

  - SHA256 - 指定具有 256 位摘要的安全散列算法 SHA 2。

- SHA384 - 指定具有 384 位摘要的安全散列算法 SHA 2。
- SHA512 - 指定具有 512 位摘要的安全散列算法 SHA 2。

- 空或无（NULL、ESP-NONE）—（仅限 IPsec 提议）仅将空散列算法用于测试目的。如果您选择其中一个 AES-GCM 选项作为加密算法，则应选择空完整性算法。对于这些加密标准，即使您选择非空选项，完整性散列也会被忽略。

决定要使用的 Diffie-Hellman 模数组

您可使用 Diffie-Hellman 密钥推导算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大安全性越高，但所需处理时间也越长。两个对等体上必须具有一个匹配的模数组。

若使用 AES 加密，应选用 Diffie-Hellman (DH) 组 5 或更高以支持 AES 所需的大密钥长度。IKEv1 策略不支持所有的组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较不易受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，然后使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 15 - Diffie-Hellman 组 15：3072 位 MODP 组。
- 16 - Diffie-hellman 组 16：4096 位 MODP 组。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 31 - Diffie-Hellman 组 31：椭圆曲线 25519 256 位 EC 组。

决定 VPN 身份验证方法

VPN 身份验证方法是一种安全机制，它会

- 验证 VPN 连接中对等体的身份
- 实现网络设备之间的安全通信，并且
- 确保只有授权的设备才能建立 VPN 连接。

可用的身份验证方法

VPN 支持两种主要的身份验证方法：

- **预共享密钥**：在对等体之间共享的密钥，由 IKE 在身份验证阶段使用。必须在每个对等体上配置相同的共享密钥，否则无法建立 IKE SA。
- **数字证书**：使用 RSA 密钥对为 IKE 密钥管理消息进行签名和加密。证书提供两个对等体之间通信的证明。

VPN 类型支持因身份验证方法而异。

表 *86: VPN* 身份验证方法支持

VPN 类型	**预共享密钥**	**数字证书**
站点到站点 IKEv1 和 IKEv2	支持	支持
远程访问（SSL 和 IPsec IKEv2）	不支持	支持

使用数字证书身份验证时，您需要为对等体定义公钥基础设施 (PKI)，以便从证书颁发机构 (CA) 获取数字证书。CA 管理证书请求并向参与的网络设备颁发证书，从而为所有参与设备提供集中式密钥管理。

预共享密钥难以在大型网络中管理。CA 使管理和扩展 IPsec 网络更加容易。使用 CA，不需要在所有加密设备之间配置密钥。向 CA 注册每个设备以请求其证书。拥有自己的证书和 CA 公钥的设备可以验证 CA 域内其他设备。

预共享密钥

预共享密钥是一种密钥，

- 使您可以在两个对等体之间共享身份验证凭证
- 由 IKE 在身份验证阶段使用，以及
- 必须在每个对等体上进行完全相同的配置，否则无法建立 IKE SA。

密钥配置选项

要配置预共享密钥，请选择手动密钥或自动生成的密钥。在 IKEv1 或 IKEv2 选项中指定此密钥。在部署配置时，将在拓扑中的所有设备上配置该密钥。

PKI 基础设施与数字证书

PKI 基础设施是一种集中式密钥管理系统，

- 提供已定义的策略、流程和角色，以支持公钥密码学
- 生成、验证和撤销公钥证书（通常称为数字证书），以及
- 管理由 VPN 端点公钥和私钥组成的密钥对，用于对消息进行签名和加密。

公钥密码学与证书组件

在公钥加密中，连接的每个终端均具有包含公钥和私钥的密钥对。密钥对被VPN终端用于消息签名和加密。这对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密，保证了连接上数据流的安全性。

生成通用的RSA、ECDSA或EDDSA密钥对，用于签名和加密。或者，为每种用途分别生成独立的密钥对。独立的签名密钥和加密密钥有助于降低密钥泄露风险。SSL 使用密钥进行加密，而 IKE 使用密钥进行签名。每种用途使用独立的密钥可最大限度地减少暴露风险。

证书还能通过提供两个对等体之间发生过通信的证明来确保不可否认性。

您可以通过以下方式获取 CA 证书：

- 使用简单证书注册协议 (SCEP) 或安全传输注册 (EST) 从 CA 服务器检索 CA 的证书
- 从另一个参与的设备手动复制 CA 证书

信任点是CA及其关联证书的对象表示。信任点包含 CA 的身份、CA 特定的参数，以及与一个已注册身份证书的关联。

PKCS#12或PFX文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。这种类型的文件可以直接导入到设备中以创建信任点。

CA 还可以为不再参与网络的对等体撤销证书。撤销的证书由联机证书状态协议 (OCSP) 服务器管理，或在存储于 LDAP 服务器上的证书撤销列表 (CRL) 中列出。对等体可以在从其他对等体接受证书之前对证书进行检查。

数字证书或身份证书

当将数字证书用作 VPN 连接的身份验证方法时，系统将对等体配置为从证书颁发机构 (CA) 获取数字证书。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。

数字证书包含以下组件：

- 所有者用于身份验证的数字识别信息，例如名称、序列号、公司、部门或 IP 地址。
- 向证书所有者发送和从证书所有者接收加密数据所需要的公钥。
- CA 的安全数字签名。

证书注册流程包括以下步骤：

1. 作为 PKI 的一部分，CA 服务器管理公共 CA 证书请求，并为参与的网络设备颁发证书。
2. 每个参与设备需使用 CA 服务器单独注册，该服务器负责验证身份并创建设备的身份证书。
3. 每个参与的对等体将其身份证书发送给另一个对等体，以使用证书中包含的公钥验证身份并建立加密会话。

证书注册

使用PKI可提高VPN的可管理性和可扩展性，因为您无需配置所有加密设备之间的预共享密钥。您只需使用 CA 服务器注册每个参与设备，该服务器负责验证身份并创建设备的身份证书。注册完成

后，每个参与的对等体将其身份证书发送给对方，以使用证书中包含的公钥验证身份并建立加密会话。有关注册 Firewall Threat Defense 设备证书的详细信息，请参阅证书注册对象，第 2669 页。

证书颁发机构证书

为了验证对等体的证书，每个参与设备都必须从服务器检索 CA 证书。CA 证书用于签署其他证书。它是自签名证书，也称为根证书。此证书包含 CA 的公钥，用于解密和验证收到的对等体证书的 CA 数字签名及其内容。

要获取 CA 证书，请执行以下操作：

- 使用简单证书注册协议 (SCEP) 或安全传输注册 (EST) 从 CA 服务器检索 CA 的证书
- 从另一个参与的设备手动复制 CA 证书

信任点

完成注册后，会在托管设备上创建信任点。它是 CA 及关联证书的对象代表。信任点包含 CA 的身份、CA 特定参数以及一个已注册的身份证书。

PKCS#12 文件

PKCS#12 文件或 PFX 文件将服务器证书、中间证书和私钥保存在一个加密文件中。这种类型的文件可以直接导入到设备中以创建信任点。

撤销检查

CA 还可以为不再参与网络的对等体撤销证书。撤销的证书由联机证书状态协议 (OCSP) 服务器管理，或在存储于 LDAP 服务器上的证书撤销列表 (CRL) 中列出。对等体可以在从其他对等体接受证书之前对证书进行检查。

已弃用的哈希算法、加密算法和 Diffie-Hellman 模数组

请先更新您的 VPN 配置，以使用受支持的 DH 和加密算法，然后再升级到 Firewall Threat Defense 6.70 或更高版本。

- 更新您的 IKE 提议和 IPSec 策略，使其与 Firewall Threat Defense 6.70 或更高版本支持的策略相匹配。
- 请在更新为支持的算法后部署配置更改。

从 Firewall Threat Defense 6.70 版本开始，已移除对这些安全性较低的加密算法的支持：

- 已弃用 IKEv1 和 IKEv2 的 **Diffie-Hellman GROUP 5** 。
- Diffie-Hellman 组 2 和 24 已被删除。
- **加密算法**：3DES、AES-GMAC、AES-GMAC-192 和 AES-GMAC-256 已被删除。

注释 在评估模式下或对不满足强加密导出控制要求的用户继续支持 **DES**。

NULL 在 IKEv2 策略中已已删除，但在 IKEv1 和 IKEv2 IPsec 转换集中仍支持。

VPN 拓扑

在创建新的VPN拓扑时，您必须为其提供唯一名称，指定拓扑类型，然后选择IKE版本。您可以从三种拓扑类型中进行选择，每种类型都包括一组 VPN 隧道。

- 点到点 (PTP) 拓扑会在两个终端之间建立 VPN 隧道。
- 中心辐射型拓扑会建立一组 VPN 隧道，将中心终端连接到一组分支终端。
- 全网状拓扑会在一组终端之间建立一组 VPN 隧道。

VPN 身份验证没有默认的预共享密钥。您必须手动定义预共享密钥或让系统自动生成该密钥。如果选择自动，Secure Firewall Management Center会生成预共享密钥并将其分配给拓扑中的所有节点。

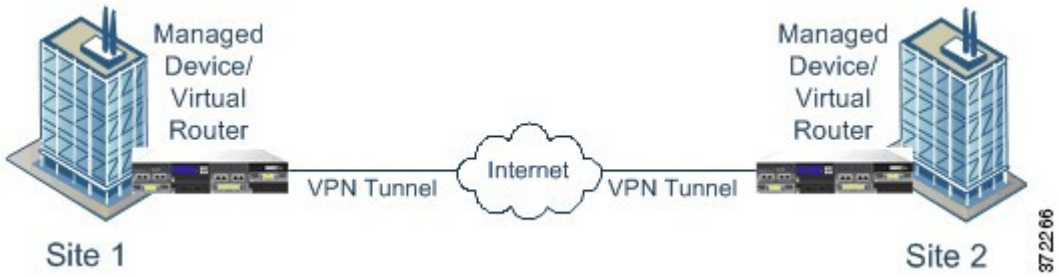
点对点 VPN 拓扑

点对点 VPN 拓扑是一种网络配置，

- 使两个终端能够直接相互通信
- 允许您将两个终端配置为对等设备，并且
- 允许任一设备启动安全连接。

此图显示了典型的点对点 VPN 拓扑。

图 *429:* 点对点 *VPN* 拓扑



中心辐射型 VPN 拓扑

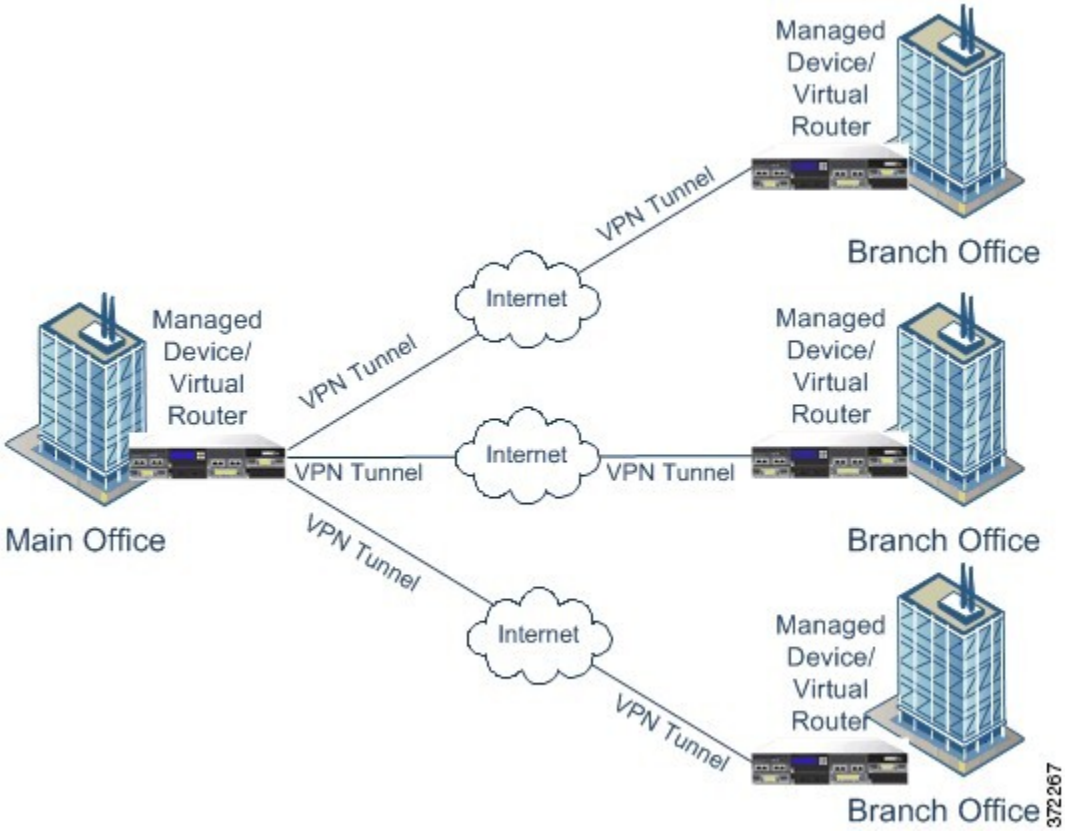
中心辐射型 VPN 拓扑是一种网络架构，

- 将中心终端（中心节点）与多个远程终端（分支节点）连接起来
- 将中心节点与各个分支节点之间的每个连接都建立为一个独立的 VPN 隧道，并且
- 使任何分支节点后面的主机都能通过中心节点相互通信。

中心辐射型拓扑结构通常代表 VPN，它使用互联网或其他第三方网络上的安全连接将组织的总部和分支机构连接起来。这些部署为所有员工提供对公司网络的受控访问权。通常，集线器节点位于总部。辐射节点位于分支机构并启动大部分流量。

此图展示了一种典型的中心辐射型 VPN 拓扑结构。

图 *430:* 中心辐射型 *VPN* 拓扑图



全网状 VPN 拓扑

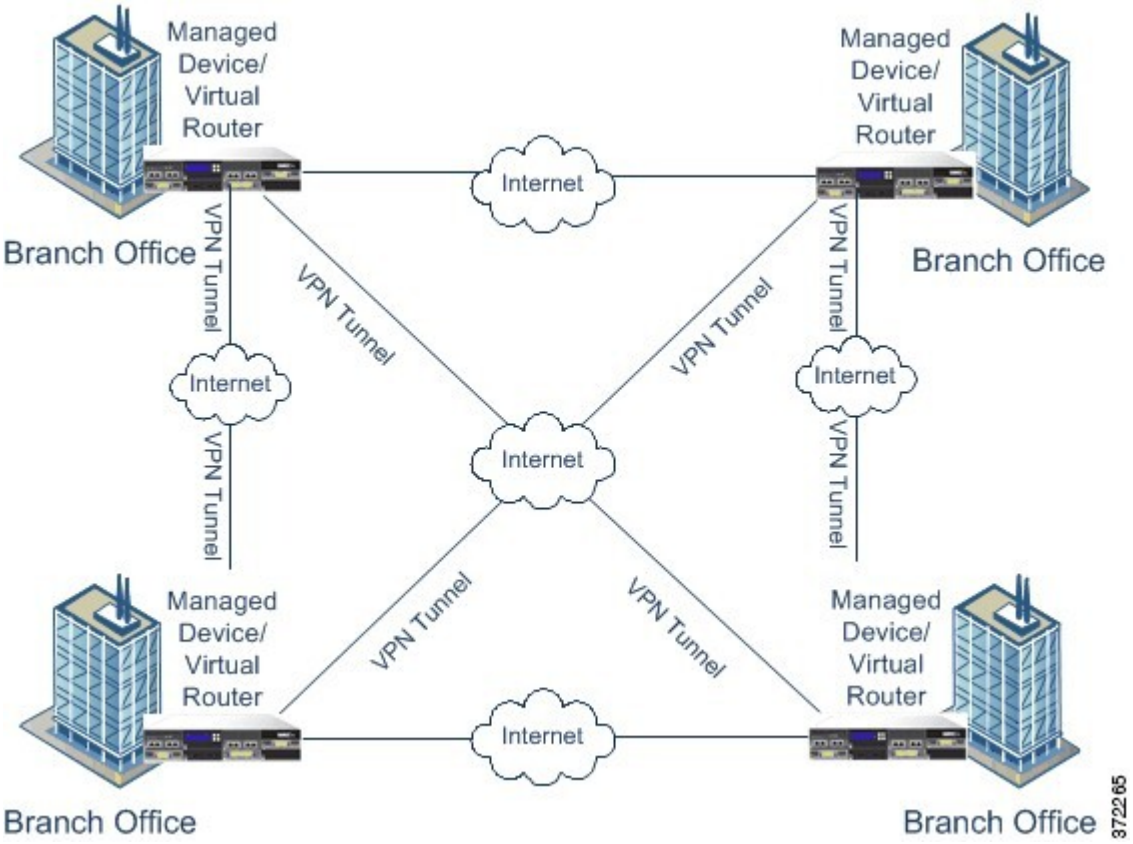
全网状 VPN 拓扑是一种网络配置，

- 允许所有终端通过独立的 VPN 隧道与其他所有终端通信。
- 提供冗余，以便在某个终端出现故障时，其他终端仍然能够相互通信，以及
- 通常代表连接一组分散式分公司地点的 VPN。

在此配置中，所部署的支持 VPN 的托管设备数量取决于所需的冗余级别。

此图展示了一个典型的全网状 VPN 拓扑结构。

图 *431:* 全网状 *VPN* 拓扑



隐式拓扑

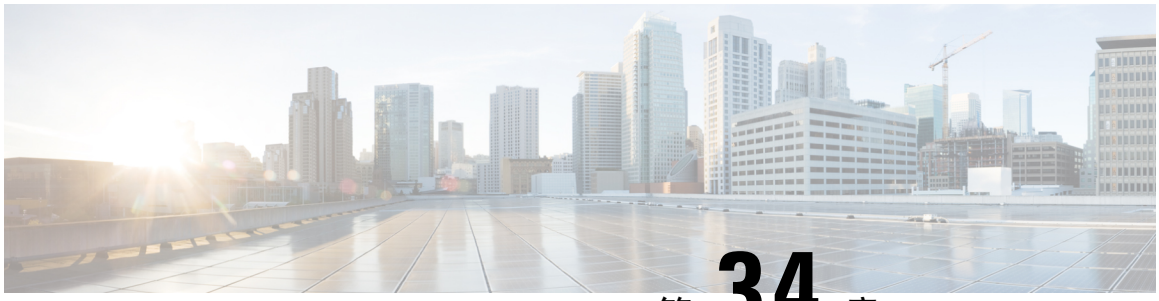
隐式拓扑是一种复杂的 VPN 网络配置，

- 结合了三种主要 VPN 拓扑（全网状、中心辐射型和点对点）的元素
- 创建比单个拓扑类型更高级的网络架构，以及
- 提供满足特定网络要求的定制连接解决方案。

隐式拓扑类型

- **部分网状结构**：一种网络，其中部分设备采用全网状拓扑结构，而其他设备则与部分全网状设备形成中心辐射型拓扑或点对点连接。部分网状不提供全网状结构的冗余，但实施成本较低。外围网络采用部分网状拓扑结构连接到全网状骨干网。
- **分层中心辐射型结构**：一种中心辐射型拓扑网络，其中设备在某些拓扑结构中充当中心设备，而在另一些拓扑结构中充当分支设备。分支组可以将流量发送到最近的中心。

- **联合中心辐射型结构：** 两种连接起来形成点对点隧道的拓扑的组合（中心辐射型、点对点或全网状）。例如，联合中心辐射型拓扑可能包含两种中心辐射型拓扑，它们的中心充当点对点拓扑中的对等设备。



第 34 章

站点间 VPN

- 关于站点间 VPN， 第 1443 页
- 站点间 VPN 拓扑的类型， 第 1446 页
- 站点间 VPN 的许可证要求， 第 1446 页
- 站点间 VPN 的要求和前提条件， 第 1447 页
- 管理站点间 VPN， 第 1447 页
- 配置策略型站点间 VPN， 第 1449 页
- 配置 Virtual Tunnel Interfaces， 第 1462 页
- 在 Umbrella 上部署 SASE 隧道， 第 1488 页
- 监控站点间拓扑， 第 1495 页
- 站点间 VPN 的历史记录， 第 1503 页

关于站点间 VPN

Cisco Secure Firewall Threat Defense站点间 VPN 支持以下功能：

- IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的证书和自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持 防火墙管理中心和 Firewall Threat Defense HA 环境。
- 当隧道关闭时，VPN 会发出警报。
- 可使用 Firewall Threat Defense统一 CLI 获得的隧道统计信息。
- 点对点外联网和中心辐射型 VPN 的 IKEv1 和 IKEv2 备份对等体配置。
- “中心辐射型”部署中作为中心的外联网设备。
- 与“点对点”部署中外联网设备配对的托管终端的动态 IP 地址。

- 作为终端的外联网设备的动态 IP 地址。
- “中心辐射型”部署中作为外联网设备的中心。

VPN 拓扑

要创建一个新的站点间 VPN 拓扑，必须为其指定一个唯一名称，指定拓扑类型，选择用于 IPsec IKEv1 和/或 IKEv2 的 IKE 版本。此外， 确定您的身份验证方法。配置完毕后，可以将拓扑部署到 Firewall Threat Defense设备。Secure Firewall Management Center仅在 Firewall Threat Defense设备上配置站点间 VPN。

您可以从三种拓扑类型中进行选择，包括一个或多个 VPN 隧道：

- 点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。
- 中心辐射型部署会建立一组 VPN 隧道，将中心终端连接到一组分支节点。
- 全网状部署会在一组终端之间建立一组 VPN 隧道。

IPsec 和 IKE

在 Secure Firewall Management Center中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点间 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

身份验证

要对VPN连接进行身份验证，请在拓扑中配置预共享密钥，或在每个设备上配置信任点。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。信任点包含 CA 的身份、CA 特定的参数，以及与一个已注册身份证书的关联。

外部网设备

每种拓扑类型都可以包括外部网设备，即不在 防火墙管理中心中管理的设备。其中包括：

- Secure Firewall Management Center 支持但您的组织不负责的思科设备。例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。
- 非思科设备。不能使用 Secure Firewall Management Center 创建配置以及将配置部署到非思科设备。

将非思科设备或未由 Secure Firewall Management Center管理的思科设备作为“外联网”设备添加到 VPN 拓扑。此外，还指定每个远程设备的 IP 地址。

Cisco Secure Firewall Threat Defense站点间 VPN 准则和限制

- 站点间 VPN 支持 ECMP 区域接口。
- 必须为拓扑中的所有节点配置加密 ACL 或受保护的网络。不可在一个节点上为拓扑配置加密 ACL，而在另一个节点上配置受保护的网络。

- 您可以通过对不在当前域中的终端使用外联网对等体，在域之间建立 VPN 连接。
- 您可以使用 防火墙管理中心 备份来备份 Firewall Threat Defense VPN。
- IKEv1 不支持 CC/UCAPL 兼容设备。我们建议您对这些设备使用 IKEv2。
- 不能在域之间移动 VPN 拓扑。
- VPN 中不支持具有 “range” 选项的网络对象。
- Firewall Threat Defense VPN 当前不支持 PDF 导出和策略比较。
- 对于 Firewall Threat Defense VPN，没有按隧道或按设备的编辑选项，只能编辑整个拓扑。
- 选择加密 ACL 时， 防火墙管理中心 不会验证传输模式的设备接口地址。
- 不支持自动镜像 ACE 生成。在任一端，对等设备的镜像 ACE 生成都是手动过程。
- 使用加密 ACL 时， 防火墙管理中心 仅支持点对点 VPN，不支持隧道运行状况事件。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 隧道状态不会实时更新，但是在 防火墙管理中心中以五分钟为间隔进行更新。
- 您无法使用字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保更改该字符。
- 在具有由同一 防火墙管理中心 管理的两台设备的站点间 VPN 配置中，无法将设备配置为备份对等体。您必须将拓扑中的一台对等设备配置为外网设备。
- 为所有 VPN 拓扑中的所有隧道配置唯一的本地 IKE 身份。
- 在具有高可用性的远程分支机构部署 (RBD) 中，当您中断一个高可用性对时：
  - 对于中心辐射型 VPN：
    - 如果 Firewall Threat Defense HA 是一个中心，则 VPN 配置将在主用设备中可用，并在备用设备中删除。
    - 如果 Firewall Threat Defense HA 是一个分支，则 VPN 配置将在主用设备和备用设备中均可用。
  - 对于点对点 VPN，如果终端具有 RBD Firewall Threat Defense HA WAN 接口，则 VPN 配置将从备用设备中删除。

站点间 VPN 拓扑的类型

站点间 VPN 拓扑	说明	更多信息
SD-WAN 拓扑	使用 SD-WAN 向导配置安全的分支机构网络。此向导简化并自动执行网络中心辐射型拓扑中的 VPN 和路由配置，从而启用 SD-WAN 功能。	使用 SD-WAN 向导进行安全分支机构网络部署，第 1510 页
基于路由的 VPN	配置根据虚拟隧道接口 (VTI) 上的路由动态保护对等体之间的流量。	创建基于路由的站点间 VPN，第 1471 页
基于策略的 VPN	配置使用受保护网络根据静态策略保护对等体之间的流量。	配置策略型站点间 VPN，第 1449 页
SASE 拓扑	配置从 Firewall Threat Defense 设备到 Umbrella 安全互联网网关 (SIG) 的 IPsec IKEv2 隧道。该隧道会将所有互联网绑定流量转发到 Umbrella SIG 进行检查和过滤。	为 Umbrella 配置 SASE 隧道，第 1493 页

站点间 VPN 的许可证要求

策略型和路由型 VPN 许可证要求

借助 基础版 许可证，您可以在 Firewall Threat Defense 设备上设置策略型和路由型的 VPN。

根据您的智能软件许可账户中是否启用了出口控制功能，防火墙管理中心 将确定是允许还是阻止在设备上使用强加密。要验证是否为您的智能许可证账户启用了出口控制功能，请选择 **管理** > **许可证** > **智能许可证**。

注释 如果您使用的是评估许可证，或者尚未启用出口管制功能，则无法对 VPN 连接使用强加密。

在 Umbrella 上部署 SASE 隧道的许可证要求

要从 防火墙管理中心 在 Umbrella 上部署 SASE 隧道，您必须启用智能许可证账户的出口控制功能。如果未启用此功能，则只能创建 SASE 拓扑，无法在 Umbrella 上部署隧道。

站点间 VPN 的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

枝叶

用户角色

管理员

支持的接口

拓扑类型	接口类型

基于策略的 SD-WAN	• 物理接口
	  • 非管理
	  • 接口模式必须为“路由”或“无”
	• 子接口接口
	• 冗余接口
	• Etherchannel 接口
	• VLAN 接口

基于路由	静态虚拟隧道接口

注释 支持的最大安全关联 (SA) 数量取决于您平台的最大 VPN 对等体数量。有关最大 VPN 对等体的详细信息，请参阅 Cisco Secure Firewall Threat Defense 设备的数据手册。

管理站点间 VPN

“站点间 VPN”(Site-to-Site VPN) 页面提供了站点间 VPN 隧道的快照。您可以查看隧道的状态，并根据设备、拓扑或隧道类型来过滤隧道。该页面每页列出20个拓扑，您可以在页面之间导航，以便查看更多拓扑详细信息。您可以点击单个 VPN 拓扑，以便展开并查看终端的详细信息。

开始之前

对于站点间 VPN 的证书身份验证，您必须通过按照证书，第 2743 页中的说明分配信任点来准备设备。

过程

选择 **安全连接** > **站点间 VPN 和 SD-WAN** 以管理您的 Firewall Threat Defense 站点间 VPN 配置和部署。

该页面列出了站点间 VPN 拓扑，并使用颜色代码来指示隧道的状态：

- 活动（绿色）-存在活动的 IPsec 隧道。
- 未知（琥珀色）-未从设备收到隧道建立事件。
- 关闭（红色）-不存在活动的 IPsec 隧道。
- 待部署 - 设备上尚未部署拓扑。

从以下选项中选择：

- **刷新**-查看 VPN 的更新状态。
- **添加**-创建新的策略型或路由型站点间 VPN。
- **编辑**-修改现有 VPN 拓扑的设置。

  注释
  在最初保存拓扑类型之后，不能对其进行编辑。要更改拓扑类型，应删除该拓扑并新建一个拓扑。

  两个用户不应 同时编辑同一拓扑；然而，Web 界面不会阻止同时编辑。

- **删除 (Delete)** - 要删除 VPN 部署，请点击 **删除** ()。
- 部署 - 选择 **部署** > **部署**；请参阅部署配置更改，第 180 页。

  注释
  一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

配置策略型站点间 VPN

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在**拓扑名称 (Topology Name)** 字段中输入拓扑的名称。

步骤 3 点击**基于策略的 VPN (Policy-Based VPN)** 单选按钮。

步骤 4 选择 VPN 拓扑并点击**创建 (Create)**。

步骤 5 选择要在 IKE 协商期间使用的 IKE 版本。选中 **IKEv1** 或 **IKEv2** 复选框。

默认值是 IKEv2。根据需要选择一个或两个选项；如果拓扑中的任何设备不支持 IKEv2，请选择 IKEv1。

您也可以为点对点外联网 VPN 配置备份对等体。有关详细信息，请参阅Firewall Threat Defense VPN 终端选项，第 1450 页。

步骤 6 必需： 通过点击拓扑中每个节点的 **添加** (+)，为该 VPN 部署添加终端。

按照Firewall Threat Defense VPN 终端选项，第 1450 页中的描述配置每个终端字段。

- 对于“点到点”，配置**节点 A** 和**节点 B**。
- 对于“中心辐射型”，配置 **中心节点**和**分支节点**
- 对于“全网格”，配置多个**节点**

步骤 7 （可选） 按照描述为该部署指定非默认 IKE 选项 Firewall Threat Defense VPN IKE 选项，第 1454 页

步骤 8 （可选） 按照描述为该部署指定非默认 IPsec 选项 Firewall Threat Defense VPN IPSec 选项，第 1456 页

步骤 9 （可选） 按照Firewall Threat Defense高级站点间 VPN 部署选项，第 1458 页中的描述为该部署指定非默认高级选项。

步骤 10 点击**保存**。
终端将添加到您的配置中。

下一步做什么

部署配置更改；请参阅 部署配置更改，第 180 页。

注释 一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

如果您收到 VPN 隧道处于非活动状态的警报，即使 VPN 会话已启动，请按照 VPN 故障排除说明来验证并确保 VPN 处于活动状态。

Firewall Threat Defense VPN 终端选项

导航路径

在基于路由的VPN中配置点对点拓扑的基本参数，如为点对点拓扑配置终端中所述，然后点击**终端 (Endpoints)** 选项卡。

字段

设备

为您的部署选择一个终端节点：

- 由此 防火墙管理中心管理的 Firewall Threat Defense设备
- 由此 防火墙管理中心管理的 Firewall Threat Defense高可用性容器
- **外部网**设备，并非由此 防火墙管理中心 管理的任意设备（思科或第三方设备）。

设备名称

仅对于外部网设备，为该设备提供一个名称。我们建议其命名可将其识别为非托管设备。

接口

如果选择托管设备作为其终端，请在该托管设备上选择一个接口。

对于“点对点”部署，您还可以配置具有动态接口的终端。具有动态接口的终端只能与外联网设备配对，无法与具有托管设备的终端配对。

您可以在 **设备** > **设备管理** 配置设备接口：**添加/编辑设备** > **接口**。

IP 地址

- 如果选择外联网设备（**不**由 防火墙管理中心管理的设备），请为终端指定一个 IP 地址。

  对于外联网设备，选择**静态**并指定一个 IP 地址，或选择**动态**以允许动态外联网设备。

- 如果选择托管设备作为终端，则从下拉列表中选择一个 IPv4 地址或多个 IPv6 地址。这些 IP 地址已分配给托管设备上的此接口。
- 拓扑中的所有终端都必须具有相同的 IP 寻址方案。IPv4 隧道可以传输 IPv6 流量，反之亦然。受保护的网络定义隧道流量将使用的寻址方案。
- 如果托管设备是高可用性容器，请从接口列表中进行选择。

此 IP 为私有 IP

如果终端驻留在带网络地址转换 (NAT) 的防火墙后面，请选中此复选框。



注释 仅当对等体由同一个防火墙管理中心管理时才使用此选项，如果对等体是外联网设备，则不要使用此选项。

公有 IP 地址

如果选中了**此 IP 为私有 IP** 复选框，请为防火墙指定公共 IP 地址。如果终端为响应方，则必须指定此值。

连接类型

将允许的协商指定为双向、只应答或只发起。受支持的连接类型组合有：

表 *87:* 受支持的连接类型组合

远程节点	中心节点
只发起	只应答
双向	只应答
双向	双向

证书映射

选择预配置的证书映射对象，或点击**添加**(+)以添加证书映射对象。证书地图定义在接收的客户端证书中需要哪些信息才能使其对 VPN 连接有效。有关详细信息，请参阅证书映射对象，第 2721 页。

受保护网络

⚠

注意 中心辐射型拓扑 - 为避免动态加密映射的流量丢弃，请确保不要为两个终端选择 任何 受保护的网络。

如果受保护的网络配置为 任何，则不会在两个终端上生成适用于隧道的加密 ACL。

定义受此 VPN 终端保护的网络。通过选择定义这些网络（受此终端保护的网络）的子网/IP 地址列表来选择网络。点击**添加**(+)可选择可用的网络对象，或添加新的网络对象。请参阅创建网络对象，第 2660 页。访问控制列表会由此处所做的选择生成。

- **子网/IP 地址（网络）** - VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络包含 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不会与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

注释 防火墙管理中心中默认 **启用反向路由注入** 。

子网/IP 地址（**网络**） 将保持默认选择。

如果已为“受保护的网络”选择 任何 并观察到默认路由流量被丢弃，请禁用反向路由注入。选择 **VPN** > **站点间**。编辑 VPN，然后点击 **IPsec** > **启用反向路由注入**。部署配置更改，以便从加密映射配置中删除 set reverse-route（反向路由注入），并删除导致反向隧道流量被丢弃的 VPN 通告反向路由。

- **访问列表（扩展）(Access List [Extended])** - 扩展访问列表提供控制此终端可接受的流量类型（例如 GRE 或 OSPF 流量）的功能。流量可通过地址或端口加以限制。点击 **添加** (+) 可添加访问控制列表对象。

注释 访问控制列表仅适用于点对点拓扑。

启用 NAT 遍历

选中此复选框可允许对等 Firewall Threat Defense 设备之间存在 NAT 设备时的无缝通信。对于中心辐射型拓扑，此选项仅可用于分支。您可以取消选中此复选框，从而为终端禁用此功能。此参数是拓扑内终端的每个对等体设置。

要查看或配置全局 NAT 遍历 (NAT-T) 设置，请在**添加/编辑 VPN 拓扑 (Add/Edit VPN Topology)** 对话框中执行以下操作：

1. 点击 **Advanced** 选项卡。
2. 在左侧导航窗格中，点击**隧道 (Tunnel)**。
3. 在 **NAT 设置 (NAT Settings)** 下，**保持连接消息遍历 (Keepalive Messages Traversal)** 是为拓扑内的所有终端启用 NAT-T 的全局设置。

豁免 VPN 流量执行网络地址转换

选中此复选框可使 VPN 流量免于执行网络地址转换 (NAT) 规则。

如果不从 NAT 规则中豁免 VPN 流量，流量将被丢弃或不会通过 VPN 隧道路由到远程设备。启用此选项后，您可以在 NAT 策略页面（**策略** > **网络策略** > **NAT** ，然后点击 **NAT 豁免**）中查看设备的 NAT 豁免。

直接连接到内部网络的内部接口

为受保护网络所在的内部接口指定安全区域或接口组。默认情况下，内部接口为任何。

点击 **+** 配置安全区域或接口组中可映射到一个或多个内部接口的一个或多个接口。确保安全区域或接口组的接口类型为“路由”。

高级设置

启用动态反向路由注入 (Enable Dynamic Reverse Route Injection) - 反向路由注入 (RRI) 可让路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。仅在成功建立 IPsec 安全关联 (SA) 后才会创建动态 RRI 路由。



注释

- 动态 RRI 仅在 IKEv2 上支持，在 IKEv1 或 IKEv1 + IKEv2 上不支持。
- 只发起对等体、全网状拓扑和外联网对等体不支持动态 RRI。
- 在点对点中，只有一个对等体可以启用动态 RRI。
- 在中心和分支之间，只有一个终端可以启用动态 RRI。
- 动态 RRI 不能与动态加密映射配合使用。

将本地身份发送到对等体 (Send Local Identity to Peers) - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 Firewall Threat Defense 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

VPN 过滤器 (VPN Filter) - 从列表中选择扩展访问列表，或点击**添加 (Add)** 以创建新的扩展访问列表对象，以过滤站点间 VPN 流量。

VPN 过滤器使用扩展访问列表来提供额外的安全性并过滤站点间 VPN 数据。通过为 VPN 过滤器选择的扩展访问列表对象，您可以在进入 VPN 隧道之前过滤预加密流量和离开 VPN 隧道的已解密流量。如果启用了 **sysopt permit-vpn** 选项，将对来自 VPN 隧道的流量绕过访问控制策略规则。如果启用了 **sysopt permit-vpn** 选项，VPN 过滤器有助于识别和过滤站点间 VPN 流量。



注释 只有点对点和中心辐射型拓扑支持 VPN 过滤器。它在网状拓扑上不支持。

对于中心辐射型拓扑，您可以选择覆盖分支终端上的中心 VPN 过滤器，以免需要在特定隧道上启用不同的 VPN 过滤器。

选择**覆盖中心上的 VPN 过滤器 (Override VPN Filter on the Hub)** 选项以覆盖辐射点上的集线器 VPN 过滤器。选择**远程 VPN 过滤器 (Remote VPN Filter)** 扩展访问列表对象或创建要覆盖的访问列表。



注释 对于作为分支的外联网设备，只有 **覆盖中心上的 VPN 过滤器** 选项可用。

有关 sysopt permit-VPN 的详细信息，请参阅Firewall Threat Defense 高级站点间 VPN 隧道选项，第 1460 页。

Firewall Threat Defense VPN IKE 选项

对于您为此拓扑选择的 IKE 版本，请指定 **IKEv1/IKEv2 设置 (IKEv1/IKEv2 Settings)**。



注释 此对话框中的设置适用于整个拓扑、所有隧道和所有托管设备。

导航路径

在基于路由的VPN中配置点对点拓扑的基本参数，如为点对点拓扑配置终端中所述，然后点击**IKE**选项卡。

字段

策略

从预定义列表中选择 IKEv1 或 IKEv2 策略对象，或者创建新的对象以供使用。您可以选择多个 IKEv1 和 IKEv2 策略。IKEv1 和 IKEv2 最多支持 20 个 IKE 策略，每个都有不同的值集。为您创建的每个策略分别分配一个唯一的优先级。优先级数值越低，优先级就越高。
建议不要使用 10、20 等值，因为远程访问 VPN 的默认 IKEv2 策略可以将这些值作为优先级值。在部署前，请确认 IKE 策略（站点间和远程访问 VPN）的优先级值不冲突。



注释 从版本 7.4.x 或更低版本（IKEv2 策略优先级字段为可选项）升级到版本 7.6.x 或更高版本（此版本为必填字段）时，将优先级字段留空可能会导致 IKEv2 策略配置问题并影响网络流量。为避免这些问题，请确保在升级前后为所有 IKEv2 策略设置一个优先级值。

有关详细信息，请参阅 IKE 策略，第 2733 页

身份验证类型

站点间VPN支持两种身份验证方法：预共享密钥和证书。有关这两种方法的说明，请参阅决定 VPN 身份验证方法，第 1434 页。

注释 在支持 IKEv1 的 VPN 拓扑中，所选 IKEv1 策略对象中指定的**身份验证方法**会成为 IKEv1 **身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

- **预共享自动密钥** - 防火墙管理中心 会自动定义此 VPN 的预共享密钥。指定**预共享密钥长度 (Pre-shared Key Length)**，即密钥中的字符数（1-27 个）。

  不支持将字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保在升级到 Cisco Secure Firewall Threat Defense 6.30 或更高版本后更改该字符。

- **预共享手动密钥** - 手动分配此 VPN 的预共享密钥。指定 **密钥**，然后重新输入以 **确认密钥**。

  在为 IKEv2 选择此选项后，将显示 **仅执行基于十六进制的预共享密钥** 复选框，如果需要则将其选中。如果已经执行，则必须使用数字 0-9 或 A-F，为该密钥输入一个有效的十六进制值（它是一个 2-256 个字符的偶数）。

- **证书 (Certificate)** - 当您将证书用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

  在 **证书** 字段中，选择预配置的证书注册对象。此注册对象可在托管设备上生成同名的信任点。证书注册对象应与设备关联并安装在设备上，之后注册过程完成，然后会创建一个信任点。

  信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

  在选择此选项之前，请注意以下事项：

  - 确保你已经在拓扑结构中的所有端点上注册了一个证书注册对象 - 证书登记对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。证书注册对象用于将托管设备注册到 PKI 基础设施中，并在支持 VPN 连接的设备上创建信任点（CA 对象）。有关创建证书注册对象的说明，请参阅添加证书注册对象，第 2671 页；有关在终端上注册对象的说明，请参阅以下适用内容之一：
    - 使用自签注册安装证书 ，第 2747 页
    - 使用 EST 注册安装证书，第 2748 页
    - 使用 SCEP 注册安装证书，第 2749 页
    - 使用手动注册安装证书，第 2750 页
    - 使用 PKCS12 文件安装证书，第 2751 页

注释 对于站点间 VPN 拓扑，请确保在拓扑中的所有终端中注册相同的证书注册对象。有关详细信息，请参阅下表。

- 请参阅下表，了解不同场景的注册要求。某些场景会要求您覆盖特定设备的证书注册对象。请参阅管理对象覆盖，第 2618 页以了解如何覆盖对象。

证书注册类型	所有终端的设备身份证书均来自同一 CA		所有终端的设备身份证书均来自不同 CA
	未在证书注册对象中指定设备特定参数	在证书注册对象中指定了设备特定的参数	
手动	无需覆盖	需要覆盖	需要覆盖
EST	无需覆盖	需要覆盖	需要覆盖
SCEP	无需覆盖	需要覆盖	需要覆盖
PKCS	需要覆盖	需要覆盖	需要覆盖
自签名	不适用	不适用	不适用

- 了解Cisco Secure Firewall Threat Defense VPN 证书准则和限制，第 2743 页中提到的 VPN 证书限制。

注释 如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须在 **PKI 证书注册** 对话框的 **密钥** 选项卡的“高级设置”部分中为所选对象选择 **忽略 IPsec 密钥使用** 选项。否则，终端无法完成站点间 VPN 连接。

Firewall Threat Defense VPN IPSec 选项

注释 此对话框中的设置适用于整个拓扑、所有隧道和所有托管设备。

在基于路由的VPN中配置点对点拓扑的基本参数，如为点对点拓扑配置终端中所述，然后点击**IPsec**选项卡。

加密映射类型

加密映射整合了设置 IPsec 安全关联 (SA) 所需的所有组件。当两个对等体尝试建立 SA 时，每个对等体均必须至少有一个兼容的加密映射项。IPsec 安全协商使用加密映射条目中定义的提议来保护该加密映射的 IPsec 规则所指定的数据流。为此部署的加密映射选择静态或动态模式：

- **静态** - 在点对点或全网状 VPN 拓扑中使用静态加密映射。
- **动态** - 动态加密映射实质上创建了一个不配置所有参数的加密映射项。稍后将动态配置缺少的参数（作为 IPsec 协商的结果）以满足远程对等体的要求。

动态加密映射策略适用于中心辐射型以及点对点VPN拓扑。要应用这些策略，请为拓扑中的一个对等体指定动态 IP 地址，同时确保在此拓扑上启用动态加密映射。在全网格 VPN 拓扑中，只能应用静态加密映射策略。

IKEv2 模式

仅限于 IPsec IKEv2，请指定将 ESP 加密和身份验证应用于隧道的封装模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。

- **隧道模式** -（默认）封装模式设置为隧道模式。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），隐藏最终的源主机和目标地址，并成为新 IP 数据包中的负载。

  隧道模式的主要优势是不需要修改终端系统即可获得IPsec的优势。此模式允许路由器等网络设备用作IPsec代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

- **传输首选**-封装模式设置为传输模式，且可选择在对等体不支持时回退到隧道模式。在传输模式下，仅加密 IP 负载，原始 IP 报头保持不变。因此，管理员必须选择与 VPN 接口 IP 地址相匹配的受保护网络。

  此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。

- **传输必要**-封装模式设置为仅传输模式，允许回退到隧道模式。如果因一个端点不支持，端点无法成功协商传输模式，将不进行 VPN 连接。

计划书

点击 **编辑** ()，以便为所选 IKEv1 或 IKEv2 方法指定提议。从可用的 **IKEv1 Ipsec 提议** 或 **IKEv2 Ipsec 提议** 对象中进行选择，或创建一个新的对象并选择该对象。请阅参配置 IKEv1 IPsec 方案对象，第 2732 页和配置 IKEv2 IPsec 方案对象，第 2732 页了解详细信息。

启用安全关联 (SA) 强度实施

启用此选项可确保子 IPsec SA 使用的加密算法不比父 IKE SA 更强 (根据密钥中的位数)。

启用反向路由注入

启用反向路由注入 (RRI) 支持静态路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。

启用完全向前保密

是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享或私有密钥。如果选择此选项，也请选择在模数组列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。

模块组

用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。 有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组 ， 第 1434 页。

生命周期持续时间

安全关联在过期之前存在的秒数。默认值为 28,800 秒。

寿命大小

使用特定安全关联的Ipsec对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。默认值为 4,608,000 千字节。不允许使用无限数据。

ESPv3 设置

验证传入 ICMP 错误消息

选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。

启用“不分段”策略

定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位。

策略

- Copy DF bit - 保持 DF 位。
- Clear DF bit - 忽略 DF 位。
- Set DF bit - 设置并使用 DF 位。

启用数据流机密性 (TFC) 数据包

启用虚拟TFC数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用**Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

注释 您可以按照任意长度和间隔对 IPsec 安全关联 (SA) 启用虚拟流量机密性 (TFC) 数据包。您必须在启用 TFC 之前设置 IKEv2 IPsec 提议。

启用 TFC 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。

Firewall Threat Defense高级站点间 VPN 部署选项

以下部分介绍在站点间VPN部署中可以指定的高级选项。这些设置适用于整个拓扑、所有隧道和所有托管设备。

Firewall Threat Defense VPN 高级 IKE 选项

高级 > IKE > ISAKAMP 设置

IKE 保持连接

启用或禁用 IKE 保持连接。您可以将此选项设置为 EnableInfinite，以便设备从不会启动保持连接来监控自身。

阈值

指定 IKE 保持连接置信间隔。该间隔是允许对等体在开始保持连接监控之前空闲的秒数。最小间隔值为 10 秒（默认值）；最大间隔值为 3600 秒。

重试间隔

指定在 IKE 保持连接重试之间等待的秒数。默认值为 2 秒；最大值为 10 秒。

发送至对等体的身份：

选择对等体将在 IKE 协商期间用于标识自身的身份：

- **autoOrDN**（默认值）- 按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
- **ipAddress** - 使用交换 ISAKMP 身份信息的主机的 IP 地址。
- **hostname** - 使用交换 ISAKMP 身份信息的主机的完全限定域名。此名称包含主机名和域名。



注释 为所有 VPN 连接启用或禁用此选项。

对等身份验证

在 IKE 隧道建立过程中，对等体提供其身份：IP 地址、完全限定域名 (FQDN) 或可分辨名称 (DN)。它还会提供一个证书，其中不包含、包含部分或全部这些字段。

如果启用了 IKE 对等体身份验证，Firewall Threat Defense 会将对等体的身份与证书中的相应字段进行比较以查看信息是否匹配。如果信息匹配，则对等体的身份通过验证，并且 Firewall Threat Defense 会建立隧道。如果信息不匹配，则不建立隧道。

- **不检查 (Do not check)** - Firewall Threat Defense 不验证对等体身份。
- **必需 (Required)** - Firewall Threat Defense 验证对等体身份。
- **如果证书支持 (If supported by cert)** - Firewall Threat Defense 仅在对等体提供证书时才验证对等体身份。

启用激进模式

如果 IP 地址未知，并且 DNS 解析在设备上可能不可用，请选择此协商方法来交换密钥信息。协商基于主机名和域名。

在隧道断开连接时启用通知

当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。

高级 > IKE > IVEv2 安全关联 (SA) 设置

IKE v2 可使用其他会话控制，限制打开的 SA 的数量。默认情况下，打开的 SA 的数量没有限制。

Cookie 质询
是否向对等体设备发送 Cookie 质询，以响应 SA 发起数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：

- 自定义
- 从不（默认）
- 始终

质询传入 Cookie 的阈值
正在协商的允许的 SA 总数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。

协商中允许的 SA 数
限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。

允许的最大 SA 数
限制允许的 IKEv2 连接数。默认值为不受限制。

在隧道断开连接时启用通知
当SA上接收的入站数据包与该SA的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下禁用发送此通知。

Firewall Threat Defense VPN高级 IPsec 选项

高级 > IPsec > IPsec 设置

加密前启用分段
此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。

路径最大传输单元老化
选中以启用“路径最大传输单元 (PMTU) 时效”，即重置安全关联 (SA) 的 PMTU 的间隔时间。

值重置间隔
输入SA的PMTU值重置为其原始值的分钟数。有效范围是10到30分钟，默认值为不受限制。

Firewall Threat Defense 高级站点间 VPN 隧道选项

导航路径

隧道选项

仅可用于中心辐射型拓扑和全网状拓扑。对于点对点配置，不会显示此部分。

- **使辐射间连接通过中心** - 默认情况下将被禁用。选择此字段将使辐射每一端上的设备将其连接通过中心节点扩展到另一台设备。

NAT 设置

- **保持连接消息遍历 (Keepalive Messages Traversal)** - 已默认启用。此参数是一个全局设置，用于为拓扑中的所有终端启用 NAT-T。选中此复选框可为 NAT 遍历启用保持连接消息。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。

  NAT 遍历可允许对等 Firewall Threat Defense 设备之间存在 NAT 设备时的无缝通信。对于中心辐射型拓扑，此选项仅可用于分支。

  如果选择此选项，请配置在辐射与中间设备之间发送两次保持连接信号（以指示会话处于活动状态）之间的**间隔**（以秒为单位）。此值可以介于 5 到 3600 秒之间。默认值为 20 秒。当使用 VPN 向导添加终端时（**添加终端 (Add Endpoint)** 对话框中的**启用 NAT 遍历 (Enable NAT Traversal)** 复选框），可以在拓扑中禁用此功能。

会话设置

- **启用 VPN 空闲超时** - 已默认启用。此超时是 VPN 连接在隧道内没有任何活动的情况下，在断开连接之前的空闲时间。默认超时是 30 分钟。

双向转发检测 (BFD) 设置

- **启用双向转发检测路由** - BFD 是用于检测转发路径故障的故障检测协议。此选项可在 SVTI 和 DVTI 上启用 BFD 路由协议。当 BFD 检测到路径故障时，流量会通过新识别的路径重新路由。

  1. 从**间隔**下拉列表中，选择发送 BFD 控制数据包的时间单位（微秒或毫秒）。
  2. 在**乘数**字段中，输入宣布对等体不可用之前允许连续丢失的 BFD 控制数据包数量。范围为 3 到 50 个数据包。
  3. 在**最小发送和接收间隔**字段中，输入 BFD 控制数据包的最小发送和接收间隔。范围介于 50 到 999 毫秒或 50000 到 999000 毫秒之间。



注释 VTI 上的 BFD 仅支持 Firewall Threat Defense 或 ASA 设备，因为它要求对等体使用 IKEv2 CFG_SET 负载通告其隧道 IP 地址。

TrustSec (SGT) 设置

- **启用通过虚拟隧道接口进行 SGT 传播** - Cisco TrustSec 使用安全组标记 (SGT) 控制网络访问并实施流量策略。此选项在 VPN 拓扑的 SVTI 和 DVTI 上启用 SGT 传播。 要启用通过特定 SVTI 或 DVTI 进行 SGT 传播，请在各个设备中进行配置。请注意，Firewall Threat Defense 设备必须为 10.0.0 及更高版本。

VPN 流量访问控制

为已解密的流量绕过访问控制策略 (sysopt permit-vpn) - 默认情况下，Firewall Threat Defense 会在解密的流量上应用访问控制策略检查。启用此选项可绕过 ACL 检查。Firewall Threat Defense 仍会将从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 应用于 VPN 流量。

启用或禁用所有 VPN 连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。



注释 对于基于路由的VPN， **sysopt permit-vpn** 不起作用。您必须创建访问控制规则允许基于路由的VPN流量通过。

证书映射设置

- **使用在终端中配置的证书映射来确定隧道**- 如果启用（选中）此选项，则将通过匹配已收到证书的内容与在终端节点中配置的证书对象的内容，来确定隧道。
- **使用证书 OU 字段来确定隧道**- 如果选择此选项，将指示如果无法根据已配置的映射确定节点（上面的选项），则将使用已收到证书的使用者可分辨名称 (DN) 中组织单位 (OU) 的值来确定隧道。
- **使用 IKE 身份来确定隧道**- 如果选择此选项，将指示如果无法根据规则匹配确定或通过 OU 获取节点（上面的选项），则会根据 phase1 IKE ID 的内容，将基于证书的 IKE 会话映射到隧道。
- **使用对等体IP地址来确定隧道**- 如果选择此选项，将指示如果无法根据规则匹配确定或通过OU或 IKE ID 方法获取节点（上面的选项），则将使用已建立的对等体 IP 地址。

配置 Virtual Tunnel Interfaces

防火墙管理中心 支持称为虚拟隧道接口 (VTI) 的可路由逻辑接口。

关于 Virtual Tunnel Interface

防火墙管理中心 支持称为虚拟隧道接口 (VTI) 的可路由逻辑接口。VTI 不需要将 IPsec 会话静态映射到物理接口。IPsec 隧道终端与虚拟接口关联。您可以像使用其他接口一样使用这些接口，并应用静态和动态路由策略。

作为策略型 VPN 的替代方案，您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。VTI 会使用静态或动态路由。设备加密或解密来自或到达隧道接口的流量，并根据路由表将其转发。这可以简化部署，而且 VTI 通过动态路由协议支持路由型VPN，还能满足虚拟私有云的诸多要求。防火墙管理中心 让您能够从基于密码图的 VPN 配置轻松迁移到基于 VTI 的 VPN。

您可以使用站点间 VPN 向导为静态 或动态 VTI 配置基于路由的 VPN。使用静态路由、BGP、OSPFv2/v3 或 EIGRP 加密流量。

您可以创建路由安全区，向其添加 VTI 接口，然后为通过 VTI 隧道为解密的流量控制定义访问控制规则。

您可以在以下对象之间创建基于 VTI 的 VPN：

- 两台 Firewall Threat Defense 设备。
- 一个Firewall Threat Defense和公共云。
- 一个Firewall Threat Defense和另一个具有运营商冗余的Firewall Threat Defense。
- 一个Firewall Threat Defense以及任何其他带有 VTI 接口的设备。
- 一个 Firewall Threat Defense 和另一个具有基于策略的 VPN 配置的设备。

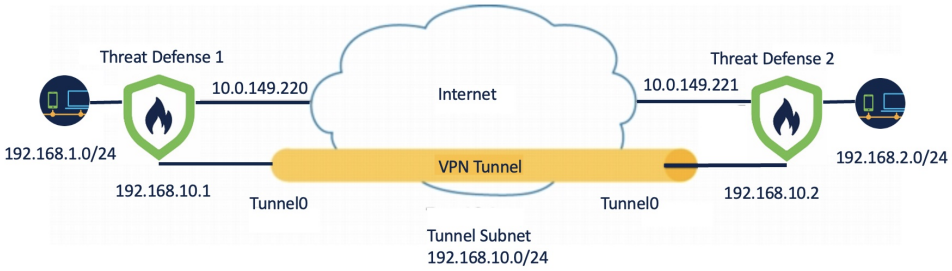
VTI 接口分为两种类型：静态 VTI 和动态 VTI。

有关详细信息，请参阅 静态 VTI，第 1463 页 和 动态 VTI，第 1464 页。

静态 VTI

静态 VTI 使用隧道接口在两个站点之间创建始终在线的隧道。对于静态 VTI，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要在管理中心创建静态 VTI 接口，请参阅添加 VTI 接口，第 1470 页。

下图显示了使用静态 VTI 的 VPN 拓扑。



关于威胁防御 1：

- 静态 VTI IP 地址为 192.168.10.1
- 隧道源为 10.0.149.220
- 隧道目的地为 10.0.149.221

关于威胁防御 2：

- 静态 VTI IP 地址为 192.168.10.2
- 隧道源为 10.0.149.221
- 隧道目的地为 10.0.149.220

优势

- 最大限度地减少和简化配置。

  您不必跟踪加密映射访问列表的所有远程子网，也不必配置复杂的访问列表或加密映射。

- 提供可路由接口。

  支持 BGP、 EIGRP 和 OSPFv2/v3 等 IP 路由协议和静态路由。

- 支持备份 VPN 隧道
- 支持使用 ECMP 进行负载均衡。
- 支持虚拟路由器。
- 为 VPN 流量提供差分访问控制。

  您可以为 VTI 配置安全区域，并将其用于 AC 策略。该配置：

  - 允许您对 VPN 流量与明文流量进行分类和区分，并选择性地允许 VPN 流量。
  - 为跨不同 VPN 隧道的 VPN 流量提供差分访问控制。

动态 VTI

动态 VTI 会使用虚拟模板来进行 IPsec 接口的动态实例化和管理。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。动态 VTI 支持多个 IPsec 安全关联，并接受分支提议的多个 IPsec 选择器。

优势

- 最大限度地减少和简化配置。

  您不必配置复杂的访问列表或加密映射。

- 简化管理。

  - 简化管理大型企业中心辐射型部署的对等体配置。
  - 仅对多个分支使用一个动态 VTI，而不是为每个分支配置一个静态 VTI。

- 提供可路由接口。

  支持 IP 路由协议，如 BGP、EIGRP 和 OSPFv2/v3。

- 简化扩展

  添加新的分支不需要在集线器上进行任何其他 VPN 配置。您可能需要根据设置更新 NAT 和路由配置。

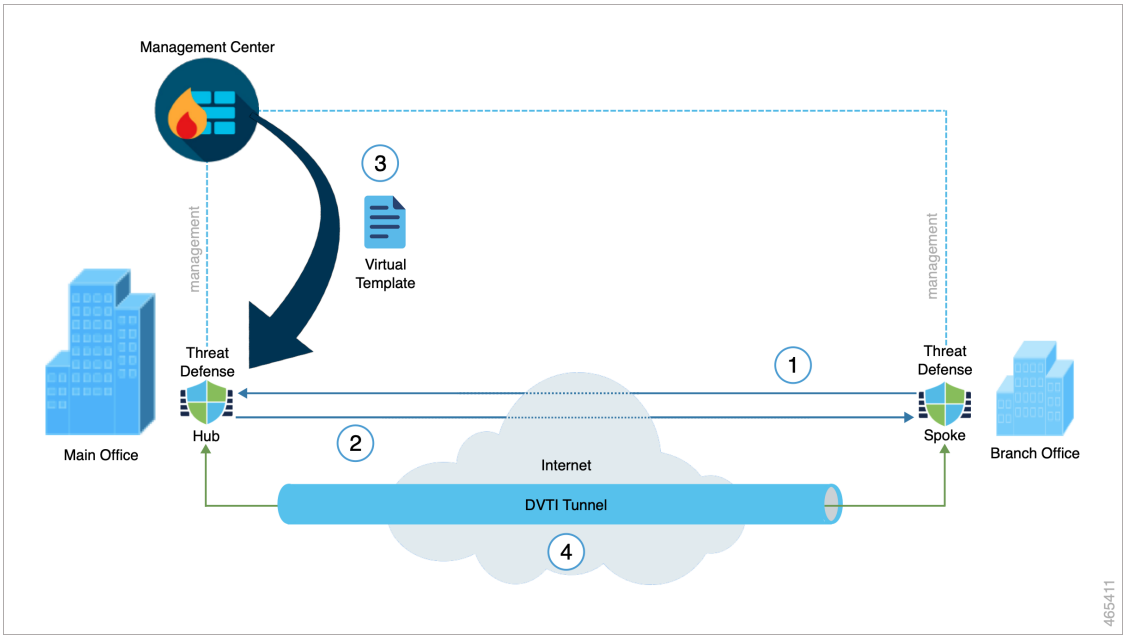
- 支持备份 VPN 隧道。
- 支持动态分支。

  您不必为分支的 DHCP IP 地址更改更新中心配置。

- 节省 IP 地址。
  - 使用 IP 未编号接口功能从另一个物理接口或环回接口借用 IP 地址。
  - 与动态 VTI 关联的所有虚拟接入接口都使用相同的 IP 地址。
- 支持虚拟路由器。
- 为 VPN 流量提供差分访问控制。

  您可以为 VTI 配置安全区域，并将其用于 AC 策略。该配置：
  - 允许您对 VPN 流量与明文流量进行分类和区分，并选择性地允许 VPN 流量。
  - 为跨不同 VPN 隧道的 VPN 流量提供差分访问控制。

防火墙管理中心 如何为 VPN 会话创建动态 VTI 隧道



当分支向中心发起隧道请求时：

1. 分支发起与中心的 IKE 交换，以建立 VPN 连接。
2. 集线器对分支进行身份验证。
3. 防火墙管理中心 会在中心辐射点上分配动态虚拟模板。

   虚拟模板会为与分支的 VPN 会话动态生成虚拟接入接口。此接口对于与分支的 VPN 会话是唯一的。
4. 中心会使用虚拟接入接口与分支建立动态 VTI 隧道。
   1. 中心和辐射点使用以下命令通过隧道交换流量：

- 分支通过 IKE 交换建议的特定流量。
- IPsec 隧道上的 BGP/OSPF/EIRGP 协议。

2. 在 VPN 会话结束后，隧道将断开连接，中心将删除相应的虚拟接入接口。

要在 防火墙管理中心创建动态 VTI 接口，请参阅 添加 VTI 接口，第 1470 页。

要使用动态 VTI 配置基于路由的站点间 VPN，请参阅 为路由型站点间 VPN 配置动态 VTI，第 1484 页。

虚拟路由器和动态 VTI

您可以创建虚拟路由器，将动态 VTI 与这些虚拟路由器关联，并在网络中扩展动态 VTI 的功能。可以将动态 VTI 与全局或用户定义的虚拟路由器关联。您可以只能将一个动态 VTI 分配给一个虚拟路由器。

与以下项关联的虚拟路由器：

- 动态 VTI 称为室内 VRF (IVRF)。
- 隧道源接口称为 Front Door VRF (FVRF)。

动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。隧道源接口可以是多个虚拟路由器的一部分。

要使用动态 VTI 为基于路由的站点间 VPN 配置虚拟路由器，请参阅 如何使用动态 VTI 配置虚拟路由器，第 1104 页。

有关配置示例的详细信息，请参阅 如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量，第 1136 页

Virtual Tunnel Interfaces 准则和限制

IPv6 支持

- VTI 支持 IPv6。
- 隧道源接口可以有一个 IPv6 地址，并且同样的地址可以用作隧道终端。
- 防火墙管理中心 支持以下 VTI IP（或内部网络 IP 版本）与公共 IP 版本的组合：
  - IPv6 over IPv6
  - 基于 IPv6 的 IPv4
  - IPv4 over IPv4
  - 基于 IPv4 的 IPv6
- VTI 支持将静态和动态 IPv6 地址作为隧道源和目的地址。

- 隧道源接口可以有一个 IPv6 地址，并且您可以将隧道终端地址。如果不指定地址， Firewall Threat Defense 使用列表中的第一个 IPv6 全局地址会被默认为隧道终端。

BGP IPv6 支持

VTI 支持 IPv6 BGP。

EIGRP IPv4 支持

VTI 支持 IPv4 EIGRP。

OSPFv2 和 OSPFv3 IPv6/IPv4 支持

VTI 支持 IPv4 和 IPv6 OSPF。

ECMP 支持

- 在 ECMP 区域中配置分支设备的静态 VTI，以均衡应用流量负载。如果不配置 ECMP 区域，当主路径发生故障时，其余路径将用作备用路径。
- VPN 向导允许您在与中心动态 VTI 关联的虚拟访问接口上启用 ECMP。中心威胁防御设备要支持 ECMP，必须为 10.0 及更高版本。

多实例和群集

- 多实例中支持 VTI。
- VTI 不支持群集。

防火墙模式

仅在路由模式中支持 VTI。

静态 VTI 的限制

- 仅支持 20 个唯一的 IPSec 配置文件。
- 在策略型路由中，您只能将 VTI 配置为出口接口。
- 您不能将 VTI 接口配置为远程访问 VPN 策略的网络接口。

动态 VTI 的限制

- 动态 VTI 不支持：
  - ECMP
  - 多实例中 VRF
  - 集群

- IKEv1
- QoS

- 如果分支具有动态 IP 地址，而集线器在 NAT 后面具有动态 VTI，则隧道状态为未知。
- 对于动态外联网，当多个分支建立连接时，站点间监控控制面板不会显示各个隧道。
- 如果使用动态分支在 NAT 后面配置具有动态 VTI 的集线器，则 VPN 监控数据将不准确。
- 您不能将 VTI 接口配置为远程访问 VPN 策略的网络接口。

静态和动态 VTI 的一般配置准则

- 如果在站点间 VPN 中使用动态加密映射和动态 VTI，则仅会出现动态 VTI 隧道。出现此问题的原因是，加密映射和动态 VTI 都尝试使用默认隧道组。

  我们的建议操作如下动作之一：

  - 将站点间 VPN 迁移到动态 VTI。
  - 使用静态加密映射及其自己的隧道组。

- VTI 只有在 IPsec 模式下才可配置。
- 动态 VTI 仅支持管理中心的中心辐射型拓扑。
- 动态 VTI 仅支持威胁防御版本 7.3 设备。
- 我们建议您仅为基于路由的中心辐射型拓扑配置一个中心。要为一组辐射点配置具有多个中心的拓扑，并将一个中心作为备份中心，请使用单个中心和同一组辐射点配置多个拓扑。有关详细信息，请参阅在基于路由的 VPN 中配置多个集线器，第 1478 页。
- 您可以将静态、BGP、EIGRP IPv4、OSPFv2/v3 路由用于使用这种隧道接口的流量。
- 在具有动态路由的 HA 配置中，备用设备无法通过 VTI 隧道访问已知子网，因为这些隧道是使用活动 IP 地址创建的。
- 您最多可以在一台设备上配置 1024 个静态和动态 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。
  - 平台上的 VTI 计数限于该平台上可配置的 VLAN 数量。例如，Firepower 1120 支持 512 个 VLAN，隧道计数为 512 减去 配置的物理接口数。
- 如果要在高可用性设置中的设备上配置超过 400 个 VTI，您必须将 45 秒配置为 Firewall Threat Defense HA 的设备保持时间。
- VTI 的 MTU 将根据底层物理接口自动设置。

- 对于动态 VTI，虚拟接入接口会从配置的隧道源接口继承 MTU。如果不指定隧道源接口，虚拟接入接口将从源接口继承 MTU，而威胁防御会从该接口接受 VPN 会话请求。
- 静态 VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目标地址之间收发数据。
- 动态 VTI 仅支持 IKE 版本 v2，并使用 IPsec 在隧道的源地址与目标地址之间收发数据。
- 对于静态和动态 VTI，请确保不将借用 IP 接口用作任何 VTI 接口的隧道源 IP 地址。
- 使用静态或动态 VTI 接口配置基于路由的站点间 VPN 时，如果使用 BGP，请确保 TTL 跳的值大于 1。
- 如果必须应用 NAT，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，所有通过 VTI 发送的流量都会被加密。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- 您可以将 VTI 接口与 ECMP 区域关联，同时配置 ECMP 静态路由以实现以下目的：
  - 负载均衡（主用/主用 VTI）- 连接可以通过任何并行 VTI 隧道进行传输。
  - 无缝连接迁移 - 当 VTI 隧道无法访问时，流会被无缝迁移到同一区域中配置的另一个 VTI 接口。
  - 非对称路由 - 通过一个 VTI 接口转发流量，并通过另一个 VTI 接口配置反向流量。

  有关配置 ECMP 的信息，请参阅ECMP 路由方法，第 1159 页。
- 对于基于路由的 VPN，用于已解密流量的绕过访问控制策略 (**sysopt connection permit-vpn**) 不起作用。您必须创建访问控制规则允许基于路由的 VPN 流量通过。
- 确保从基于路由的 IKE VPN 配置中删除未使用的转换集。如果有未使用的转换集，则 VPN 隧道可能无法建立，并且不会发生封装和解封。使用 `show run crypto` 和 `show vpn-sessiondb detail l2l` 命令查看转换集。

备份 VTI 的准则和限制

- 不支持跨隧道故障转移的流恢复能力。例如，明文 TCP 连接在隧道故障切换后丢失，而您需要重新启动故障转移期间发生的任何 FTP 传输。
- 备份 VTI 中不支持证书身份验证。

动态 VTI 和虚拟路由器准则

- 动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。
- 必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。
- 用户定义的虚拟路由器仅支持 BGPv4/v6 和 OSPFv2 路由协议。
- 隧道源接口可以位于与动态 VTI 关联的虚拟路由器之外的用户定义的虚拟路由器中。

相关主题

环回接口的准则和限制，第 766 页
创建基于路由的站点间 VPN，第 1471 页

添加 VTI 接口

要配置基于路由的站点间 VPN，您必须在 VTI 隧道的两个节点上的设备上创建 VTI 接口。

将隧道类型指定为动态并配置相关参数时，防火墙管理中心会生成动态虚拟模板。虚拟模板会为每个 VPN 会话动态生成独一无二的虚拟访问接口。

开始之前

配置环回接口以实现静态和动态 VTI VPN 隧道的冗余。有关详细信息，请参阅配置环回接口，第 766 页。

对于 Cisco Secure Firewall 1200/3100/4200/6100 设备，当设备的 VTI 环回接口已启用时，也会使用 IPsec 数据流分流。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要创建 VTI 接口的设备旁边的**编辑**图标。

步骤 3 选择 **添加接口** > **虚拟隧道接口**。

步骤 4 选择**静态 (Static)** 或**动态 (Dynamic)** 作为**隧道类型 (Tunnel Type)**。

步骤 5 输入接口的名称和说明。默认情况下，接口处于启用状态。

确保指定的名称不超过 28 个字符。

步骤 6 （可选）从 **安全区域** 下拉列表中选择一个安全区域，以便以将静态 VTI 或动态 VTI 接口添加到该区域。

如果要在安全区域的基础上执行流量检查，请将 VTI 接口添加到安全区域并配置访问控制 (AC) 规则。要允许 VPN 流量通过隧道，您需要添加一条将此安全区域作为源区域的 AC 规则。

步骤 7 在**优先级**字段中，输入在多个 VTI 间负载均衡流量的优先级。

范围是从 0 到 65535。最小的数字具有最高优先级。此选项不适用于动态 VTI。

步骤 8 选中**传播安全组标记**复选框以启用通过 VTI 的安全组标记 (SGT) 传播。

TrustSec 使用 SGT 来控制网络上的访问并实施流量管理。要在 VPN 拓扑的 SVTI 和 DVTI 上启用 SGT 传播，请在 VPN 向导的**高级 > 隧道**选项卡中选中**在虚拟隧道接口上启用 SGT 传播**复选框。

步骤 9 根据隧道类型，执行以下操作之一：

- 对于动态 VTI，请在 **模板 ID** 字段中输入 1 到 10413 范围内的唯一 ID。
- 对于静态 VTI，请在 **隧道 ID** 字段中输入 0 到 10413 范围内的唯一隧道 ID。

步骤 10 （对于动态 VTI 为可选）从 **隧道源** 下拉列表中选择隧道源接口。

VPN 隧道在此接口（物理 或环回 接口）处终止。从下拉列表中选择接口的 IP 地址。无论 IPsec 隧道模式如何，您都可以选择 IP 地址。如果有多个 IPv6 地址，请选择要用作隧道终端的地址。

步骤 11 在 **IPSec 隧道模式**下，点击 **IPv4** 或 **IPv6** 单选按钮以指定通过 IPsec 隧道的流量类型。

步骤 12 在 **IP 地址 (IP Address)** 下：

- **配置 IP**：为静态 VTI 接口输入 IPv4 或 IPV6 地址。您不能为动态 VTI 接口配置 IP 地址。将**借用 IP** 字段用于动态 VTI 接口。
- **借用 IP**：从下拉列表中选择物理或环回接口，VTI 接口将继承此 IP 地址。

  确保使用不同于隧道源 IP 地址的 IP 地址。您可以将此选项用于静态或动态 VTI 接口。

  点击 添加＋以配置环回接口。环回接口有助于克服路径故障。如果接口发生故障，您可以通过分配给环回接口的 IP 地址来访问所有接口。

步骤 13 点击**确定**。

步骤 14 点击**保存**。

创建基于路由的站点间 VPN

您可以为以下两种拓扑配置基于路由的站点间 VPN：

- **点对点**：在隧道的两个节点上配置 VTI，并使用向导配置 VPN。
- **中心辐射型**：在中心和分支上配置 VTI。配置带有动态 VTI 的中心，以及带有静态 VTI 的分支。

您可以将外联网设备配置为集线器，并将托管设备配置为分支。您可以配置多个中心和分支，也可以配置备份中心和分支。

- 对于外联网中心和分支，您可以将多个 IP 配置为备份。
- 对于托管分支，您可以配置备份静态 VTI 接口以及主 VTI 接口。

有关 VTI 的详细信息，请参阅关于 Virtual Tunnel Interface，第 1462 页。

注释 除非提及，否则所有对 VTI 的引用都代表静态 VTI 和动态 VTI。

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在 **拓扑名称** 字段中，输入 VPN 拓扑的名称。

步骤 3 选择 **基于路由 (VTI)** 并执行以下操作之一：

- 选择 **点对点** 作为网络拓扑。要为路由型 **点对点** 拓扑配置终端，请参阅 为点对点拓扑配置终端，第 1472 页。
- 选择 **中心辐射型** 作为网络拓扑。要为路由型**中心辐射型**拓扑配置终端，请参阅 为中心辐射型拓扑配置终端，第 1475 页。

步骤 4 点击**创建 (Create)**。

步骤 5 （可选） 为部署指定 **IKE** 选项，如 Firewall Threat Defense VPN IKE 选项，第 1454 页中所述。

步骤 6 （可选） 为部署指定 **IPsec** 选项，如Firewall Threat Defense VPN IPSec 选项，第 1456 页中所述。

步骤 7 （可选） 为部署指定 **高级** 选项，如 Firewall Threat Defense高级站点间 VPN 部署选项，第 1458 页中所述。

步骤 8 点击**保存**。

下一步做什么

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由策略。有关详细信息，请参阅为 VTI 配置路由和 AC 策略，第 1485 页。
- 用于允许已加密的流量的访问控制规则。选择 **策略** > **访问控制**。

为点对点拓扑配置终端

配置以下参数，为 **点对点** 拓扑节点为路由型站点间 VPN 配置终端：

开始之前

在基于路由的 VPN 中配置点对点拓扑的基本参数，如 创建基于路由的站点间 VPN，第 1471 页 中所述，然后点击 **终端** 选项卡。

过程

步骤 1 在 **节点 A** 下，从 **设备** 下拉菜单中选择要用作 VTI 隧道第一个终端的已注册设备 (Firewall Threat Defense) 或外联网的名称。

对于外联网对等体，请指定以下参数：

1. 指定设备的名称。
2. 在 **终端 IP 地址** 中输入主 IP 地址。如果配置备份 VTI，请添加一个逗号，然后指定备份 IP 地址。
3. 点击**确定**。

为外联网集线器配置上述参数后，请在 **IKE** 选项卡中指定外联网的预共享密钥。

注释
AWS VPC 会将 **AES-GCM-NULL-SHA-LATEST** 作为默认策略。如果远程对等体连接到 AWS VPC，请从 **策略** 下拉列表中选择 **AES-GCM-NULL-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

步骤 2 对于已注册的设备，您可以从 **虚拟隧道接口** 下拉列表中指定节点 A 的 VTI 接口。

所选隧道接口是节点 A 的源接口，并且它将成为节点 B 的隧道目的接口。

如果要在节点 A 上创建一个新接口，请点击 添加 ＋ 图标并配置字段，如添加 VTI 接口，第 1470 页中所述。

如果要编辑现有 VTI 的配置，请在**虚拟隧道接口 (Virtual Tunnel Interface)** 下拉字段中选择 VTI，然后点击**编辑 VTI (Edit VTI)**。

步骤 3 如果您的节点 A 设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 4 **将本地身份发送到对等体 (Send Local Identity to Peers)** - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 Firewall Threat Defense 在 NAT 后面有多个 IPsec 隧道，以便连接到思科 Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

步骤 5 （可选）点击 **添加备份 VTI** 以指定其他 VTI 接口作为备份接口。

注释
确保两个拓扑对等体的备份 VTI 具有不同的隧道源。一台设备不能有两个具有相同隧道源和隧道目标的 VTI；因此，请配置唯一的隧道源和隧道目标组合。

虽然虚拟隧道接口是在备用VTI下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

步骤 6 在**其他配置 (Additional Configuration)** 下，执行以下操作：

- 要将流量路由到 VTI，请点击**路由策略 (Routing Policy)**。防火墙管理中心 会显示**设备 (Devices)** > **路由 (Routing)** 页面。

  您可以为 VPN 流量配置静态、BGP、OSPF v2/v3 或 EIGRP 路由。

- 要允许 VPN 流量，请点击 **AC 策略 (AC Policy)**。防火墙管理中心 会显示设备的访问控制策略页面。继续添加用于指定 VTI 安全区域的允许/阻止规则。配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

步骤 7 展开 **高级设置**，为设备配置其他配置。有关详细信息，请参阅基于路由的 VPN 中点对点拓扑的高级配置，第 1474 页。

步骤 8 对节点 B 重复上述程序。

步骤 9 点击**确定**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如 Firewall Threat Defense VPN IKE 选项，第 1454 页中所述。
- （可选）为部署指定 **IPsec** 选项，如 Firewall Threat Defense VPN IPSec 选项，第 1456 页中所述。
- （可选）为部署指定 **高级** 选项，如 Firewall Threat Defense高级站点间 VPN 部署选项，第 1458 页中所述。
- 点击**保存**。
- 要将流量路由到VTI，请依次选择**设备**>**设备管理**，编辑威胁防御设备，然后点击**路由**选项卡。

  您可以为 VPN 流量配置静态，或者使用 BGP、OSPF v2/v3 或 EIGRP 来路由 VPN 流量。
- 要允许 VPN 流量，请选择**策略** > **安全策略** > **访问控制**。添加用于指定 VTI 安全区域的规则。对于备份 VTI，请确保包含与主 VTI 相同的安全区域的备份 VTI。

基于路由的 VPN 中点对点拓扑的高级配置

为基于路由的 VPN 中的点对点拓扑配置以下高级配置：

开始之前

在基于路由的VPN中配置点对点拓扑的基本参数，如中所述，并展开高级设置。为点对点拓扑配置终端，第 1472 页

过程

步骤 1 选中 **将虚拟隧道接口 IP 发送到对等体** 复选框，以将 VTI IP 地址发送到对等体设备。

步骤 2 选中 **允许来自对等体的传入 IKEv2 路由** 复选框以允许来自分支和对等体的传入 IKEv2 路由。

步骤 3 从 **连接类型** 下拉列表中选择以下选项之一：

仅应答：设备只能在对等设备发起连接时做出响应，不能发起任何连接。

双向：设备可以发起或响应连接。这是默认选项。

为中心辐射型拓扑配置终端

您可以使用动态 VTI 仅为中心辐射型拓扑创建路由型站点间 VPN。集线器只能使用动态 VTI，辐射点只能使用静态 VTI 接口。您还可以将外联网设备配置为集线器。

配置以下参数，为 **中心辐射型** 拓扑节点配置路由型站点间 VPN 终端：

开始之前

在基于路由的 VPN 中配置中心辐射型拓扑的基本参数，如 创建基于路由的站点间 VPN，第 1471 页中所述，然后点击 **终端** 选项卡。

过程

步骤 1 在 **集线器节点**下：

a) 点击 添加 ＋ 以在**添加终端 (Add Endpoint)** 对话框中配置中心节点。

b) 从 **设备** 下拉列表中选择中心 。

对于外联网中心，请指定以下参数：

1. 输入设备的名称。
2. 输入主 IP 地址。如果配置备份 VTI，请添加一个逗号，然后指定备份 IP 地址。
3. 点击**确定**。

为外联网集线器配置上述参数后，请在 **IKE** 选项卡中指定外联网的预共享密钥。

注释
AWS VPC 会将 **AES-GCM-NULL-SHA-LATEST** 作为默认策略。如果远程对等体连接到 AWS VPC，请从 **策略** 下拉列表中选择 **AES-GCM-NULL-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

c) 从 **动态虚拟隧道接口** 下拉列表中选择动态 VTI。

DVTI 接口的隧道源配置是强制性的，因为管理中心需要此信息来确定分支的隧道目标。

点击 添加 ＋ 以添加新的动态 VTI。我们建议您从环回接口为动态接口配置借用 IP。

如果要编辑现有的动态 VTI，请选择接口，然后点击 **编辑 VTI**。

d) （可选）如果终端设备位于 NAT 设备后面，请选中 **隧道源 IP 为私有** 复选框，并在 **隧道源公共 IP 地址** 字段中配置隧道源 IP 地址。
e) 点击 **路由策略**，为中枢配置路由策略。
f) 点击 **AC 策略** 以配置访问控制策略。
g) 展开 **高级设置** 以在集线器上配置其他配置。有关详细信息，请参阅基于路由的 VPN 中集线器和分支的高级配置，第 1477 页。
h) 点击**确定**。
i) 选中 **ECMP** 复选框，以在 10.0 及更高版本的中心设备的动态 VTI 上启用 ECMP。中心上所有连接至同一分支的虚拟访问接口均被归入一个 ECMP 区域。

请注意，此选项不会在分支 SVTI 上启用 ECMP。您必须在分支 SVTI 上手动启用 ECMP。

步骤 2 在 **分支节点**下：

a) 点击 添加 ＋ 以在**添加终端 (Add Endpoint)** 对话框中配置分支。
b) 从 **设备** 下拉列表中选择辐射。

对于外联网分支，请指定以下参数：

1. 输入设备的名称。
2. 在 **终端 IP 地址**下，选择以下选项之一：
   - **静态**：输入设备的 IP 地址和备用 IP 地址（如果需要）。
   - **动态**：选择此选项可为外联网分支动态分配 IP 地址。
3. 点击**确定**。

c) 从 **静态虚拟隧道接口** 下拉列表中选择静态 VTI。

点击 添加 ＋ 添加新的静态 VTI。静态 VTI 的隧道 IP 会自动填充，请确保此 IP 地址对于分支是唯一的。

如果要编辑现有静态 VTI，请选择接口，然后点击 **编辑 VTI**。

d) （可选）如果您的终端设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。管理中心需要使用隧道源接口地址来在分支上配置隧道目标 IP 地址。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。
e) （可循啊）**将本地身份发送到对等体 (Send Local Identity to Peers)** - 选中此复选框可将本地身份信息发送到对等设备。从**本地身份配置 (Local Identity Configuration)** 下拉列表中选择以下参数之一并配置本地身份：
   - **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
   - **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。

- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 Firewall Threat Defense 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的详细信息，请参阅《*Cisco Umbrella SIG* 用户指南》。

f) （可选）点击**添加备份 VTI** 以指定其他 VTI 接口作为备份接口。

注释
确保两个拓扑对等体均未在同一隧道源上配置备份 VTI。例如，如果对等体 A 的两个 VTI（主和备份）配置了一个隧道源接口，例如 10.10.10.1/30，则对等体 B 的 2 个 VTI 也不能使用一个隧道源 IP，例如 20.20 .20.1/30。

虽然虚拟隧道接口是在备用 VTI 下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

g) 点击 **路由策略**，为分支配置路由策略。
h) 点击 **AC 策略** 以配置访问控制策略。
i) 展开 **高级设置** 以在分支上配置其他配置。有关详细信息，请参阅基于路由的 VPN 中集线器和分支的高级配置，第 1477 页。
j) 点击**确定**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如 Firewall Threat Defense VPN IKE 选项，第 1454 页中所述。
- （可选）为部署指定 **IPsec** 选项，如 Firewall Threat Defense VPN IPSec 选项，第 1456 页中所述。
- （可选）为部署指定 **高级** 选项，如 Firewall Threat Defense高级站点间 VPN 部署选项，第 1458 页中所述。
- 点击**保存**。

基于路由的 VPN 中集线器和分支的高级配置

为基于路由的 VPN 中的中心辐射点配置以下高级配置：

开始之前

在基于路由的 VPN 中配置中心辐射点的基本参数，如 为中心辐射型拓扑配置终端，第 1475 页 中所述，并展开 **高级设置**。

过程

步骤 1 选中 **将虚拟隧道接口 IP 发送到对等体** 复选框，以将 VTI IP 地址发送到对等体设备。

对于集线器，如果使用 BGP 作为路由协议，则必须选中此复选框。此配置可确保在 BGP 路由表中共享环回 IP 地址。

对于分支，此选项会默认启用。

步骤 2 添加 **受保护的网络** 以定义受该 VPN 终端保护的网络。请点击 添加 ＋ 以选择受保护网络。

对于集线器，配置集线器后面的受保护网络。这些信息和分支的受保护网络会生成分支访问列表。

不能使用动态 VTI 为集线器上的虚拟接入接口创建静态路由。集线器在隧道建立和终止期间动态创建和删除这些接口。

对于分支，请配置分支的受保护网络。

要为分支启用静态路由，请在为拓扑配置终端后，点击 IPsec 选项卡并选中启用反向路由注入复选框。

如果使用 BGP、OSPF 或 EIGRP，则不需要此选项。

步骤 3 选中 **允许来自对等体的传入 IKEv2 路由** 复选框以允许来自分支和对等体的传入 IKEv2 路由。

对于枢纽：在 IKE 交换期间，集线器会将动态创建的虚拟接入接口通告给分支，然后分支会将其 VTI IP 地址通告给集线器。

对于分支：此选项会默认启用。

步骤 4 在 **连接类型** 下拉列表中，选择以下选项之一：

仅应答：设备只能在对等设备发起连接时做出响应，不能发起任何连接。

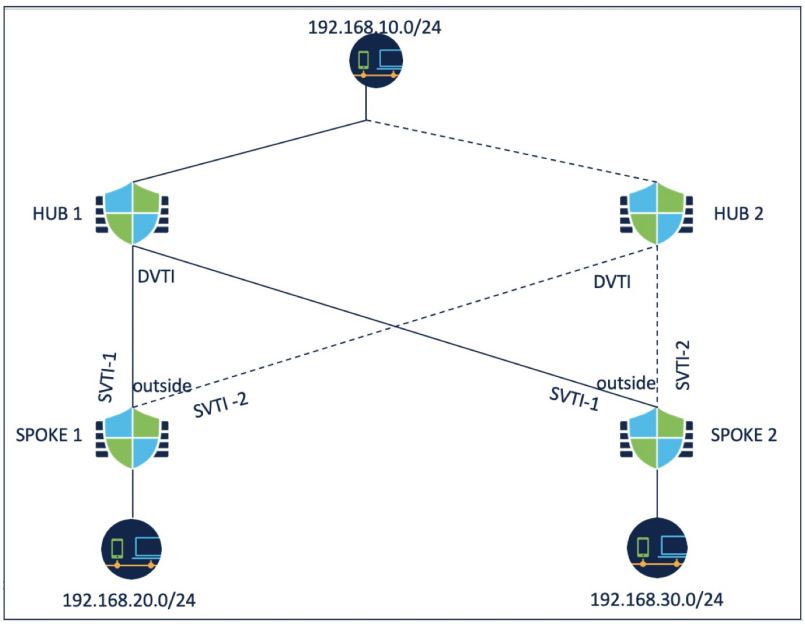
双向：设备可以发起或响应连接。这是默认选项。

在基于路由的 VPN 中配置多个集线器

您可以为一组分支配置具有多个中心的拓扑。将一个集线器用作备份集线器，您可以使用单个集线器和同一组辐射点配置多个拓扑。

在下面的示例中，有两个集线器连接到同一组辐射点。集线器 1 是主集线器，集线器 2 是辅助集线器。要在 防火墙管理中心中配置此网络，必须配置两种基于路由的中心辐射型拓扑：

- 拓扑 1：集线器 1 连接到分支 1 和分支 2。
- 拓扑 2：集线器 2 连接到分支 1 和分支 2。



要配置拓扑 1：

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在 **拓扑名称** 字段中，输入 VPN 拓扑的名称。

步骤 3 选择 **基于路由 (VTI)** 并执行以下操作之一：

- 选择 **点对点** 作为网络拓扑。要为路由型 **点对点** 拓扑配置终端，请参阅 为点对点拓扑配置终端，第 1472 页。
- 选择 **中心辐射型** 作为网络拓扑。要为路由型**中心辐射型**拓扑配置终端，请参阅 为中心辐射型拓扑配置终端，第 1475 页。

步骤 4 点击**创建 (Create)**。

步骤 5 配置 IKE 版本。

步骤 6 点击 **终端** 选项卡。

步骤 7 在 **集线器节点**下：

a) 点击 添加 ＋ 添加集线器。

b) 从 **设备** 下拉列表中选择中心 1。

c) 从**动态虚拟隧道接口 (Dynamic Virtual Tunnel Interface)** 下拉列表中选择动态 VTI，或点击 添加 ＋ 添加新的动态 VTI。

我们建议您从环回接口为动态接口配置借用 IP。

d) （可选）如果终端设备位于 NAT 设备后面，请选中 **隧道源 IP 为私有** 复选框，并在 **隧道源公共 IP 地址** 字段中配置隧道源 IP 地址。

e) 点击 **路由策略** ，为中枢配置路由策略。您可以使用 BGP 配置动态路由。

f) 展开 **高级设置**。您可以为集线器配置以下高级设置，以启用 IKEv2 路由，如果不使用动态路由，则可以使用这些设置。

- （可选）选中 **将虚拟隧道接口 IP 发送到对等体** 复选框。
- 选中 **允许来自对等体的传入 IKEv2 路由** 复选框以允许中心接受来自辐射的路由，并更新的路由表。
- 从下拉列表中选择 **连接类型** 为“双向”。

g) 点击**确定**。

步骤 8 在 **分支节点**下：

a) 点击 添加 ＋ 添加分支。

b) 从 **设备** 下拉列表中选择辐射 1。

c) 从**静态虚拟隧道接口 (Static Virtual Tunnel Interface)** 下拉列表中选择 SVTI-1 作为分支的静态 VTI，或者点击 添加 ＋ 添加新的静态 VTI。

选择外部接口作为 SVTI-1 的隧道源。SVTI-1 的隧道 IP 是自动填充的，请确保此 IP 地址对于两个拓扑中的分支 1 在对等体之间是唯一的。

d) 展开 **高级设置**。如果不使用动态路由，则可以配置这些设置来为分支启用 IKEv2 路由。

- 选中 **将虚拟隧道接口 IP 发送到对等体** 复选框，以将 VTI IP 地址发送到对等体设备。
- 选中 **允许来自对等体的传入 IKEv2 路由** 复选框以允许来自对等体的传入 IKEv2 路由。
- 从下拉列表中选择 **连接类型** 为“双向”。

e) 点击**确定**。

f) 重复步骤 5a 至 5e以添加分支 2。将 SVTI-1 配置为分支 2 的静态 VTI。

步骤 9 根据需要配置 IKE 和 IPSec 参数，或使用默认值。

下一步做什么

1. 为拓扑 2 配置中心 2、分支 1 和分支 2。

   将 SVTI-2 配置为分支 1 的静态 VTI，将 SVTI-2 配置为分支 2 的静态 VTI（请参阅上图）。SVTI-2 的隧道源应为同一外部接口。

2. 对于每个分支，配置路由策略。有关详细信息，请参阅为基于路由的 VPN 中的多个集线器配置路由 ，第 1481 页。

3. 验证配置和隧道状态。有关详细信息，请参阅验证基于路由的VPN中的多中心配置，第1482页。

为基于路由的 VPN 中的多个集线器配置路由

以下程序介绍如何在中心辐射点上配置动态路由，以及如何在辐射点上配置策略型路由。

开始之前

配置拓扑 1 和 2，如 在基于路由的 VPN 中配置多个集线器，第 1478 页中所述。

过程

步骤 1 使用 BGP 为集线器配置动态路由。

a) 选择 **设备** > **设备管理**，然后点击 **编辑** (✎) 并点击**路由**选项卡。
b) 在左侧窗格中，选择 **常规设置** > **BGP**。
c) 选中 **启用 BGP** 复选框并输入 **AS 编号**。

您可以根据需要配置其他字段。

d) 点击**保存**。
e) 在左侧窗格中，选择 **BGP** > **IPv4**。
f) 选中 **Enable IPv4** 复选框。
g) 点击 **邻居** 选项卡，点击 **添加** 并配置参数。

1. **IP 地址**：输入分支 1 的隧道接口 IP 地址。
2. **远程 AS**：分支 1 的 AS 编号。
3. 选中 **已启用的地址** 复选框。
4. 点击**确定**。

重复上述步骤，将 Spoke 2 添加为邻居。

h) 点击**保存**。
i) 点击 **网络** 选项卡，然后点击 **添加** ，将集线器背后的网络通告给对等体。

步骤 2 使用 BGP 为分支配置动态路由。

除以下差异外，分支的 BGP 配置与集线器的 BGP 配置类似：

- 将集线器 1 和集线器 2 配置为两个分支的邻居，并使用集线器的隧道接口 IP 地址。
- 配置网络时，请使用每个分支背后的网络。

步骤 3 在辐射上配置策略型路由。

a) 在左侧窗格中，选择 **策略型路由** ，然后点击 **添加**。
b) 从下拉列表中选择 **入口接口** 。
c) 点击 **添加** 以配置匹配 ACL。

例如，对于分支 1，源网络为 192.168.20.0/24，目的网络为 192.168.10.0/24。

d) 在 **发送到** 下拉列表中，选择“出口接口”。
e) 从 **接口排序** 下拉列表中选择“顺序”。
f) 选择 SVTI-1 和 SVTI-2 接口作为出口接口。
g) 点击**保存**。

如果要将集线器用作负载均衡对，则必须配置 ECMP。

步骤 4 在中心和辐射点上部署配置。

下一步做什么

验证配置和隧道状态。有关详细信息，请参阅验证基于路由的 VPN 中的多中心配置，第 1482 页。

验证基于路由的 VPN 中的多中心配置

要验证多中心配置和隧道状态，请执行以下操作：

- 部署后，在控制面板 中检查隧道状态。
- 从站点间监控控制面板使用数据包跟踪器验证流量的选定路径（集线器 1 或集线器 2）。
- 对每个终端使用以下 show 命令验证配置：
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

通过备用 VTI 隧道路由流量

Cisco Secure Firewall Threat Defense 支持为基于路由的 (VTI) VPN 配置备份隧道。当主 VTI 无法路由流量时，VPN 中的流量会通过备用 VTI 传送。

您可以在以下场景中部署备份 VTI 隧道：

- 两个对等体都有服务提供商冗余备份。

  在这种情况下有两个物理接口，可充当对等体的两个 VTI 的隧道源。

- 只有一个对等体具有服务提供商冗余备份。

  在这种情况下，只有对等体的一端有一个接口备份，而另一端只有一个隧道源接口。

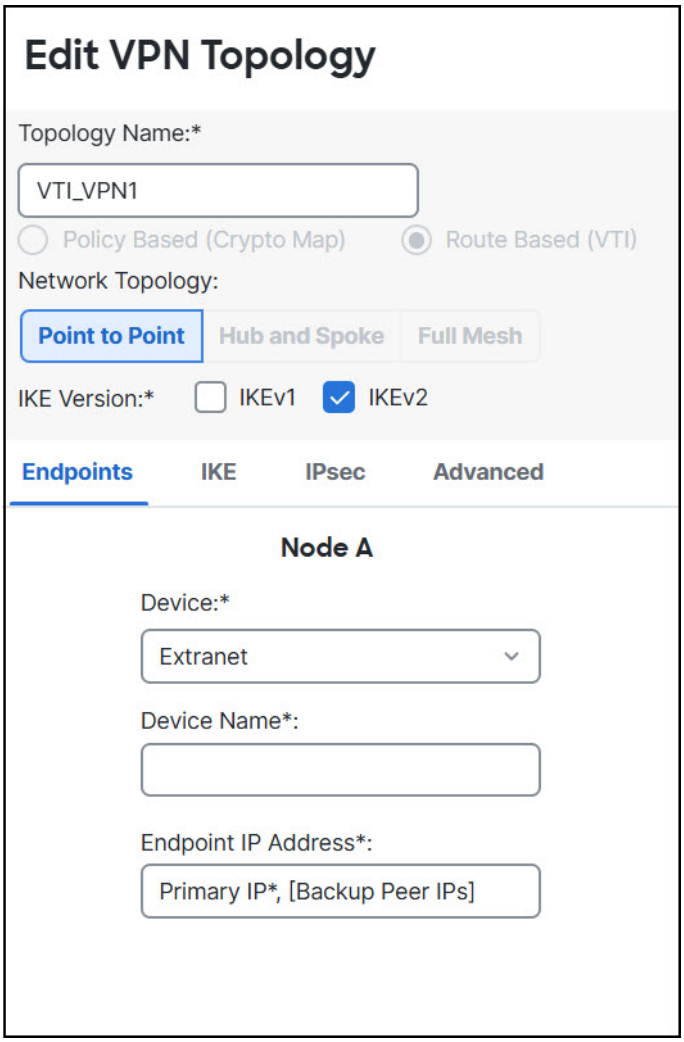
步骤	相应操作	更多信息
1	查看准则和限制。	Virtual Tunnel Interfaces 准则和限制，第 1466 页
2	创建 VTI 接口。	添加 VTI 接口，第 1470 页

步骤	相应操作	更多信息
3	在 **创建新 VPN 拓扑向导** 的 **添加终端** 对话框中，点击 **添加备份 VTI**，为每个对等体配置相应的备份接口。	• 为点对点拓扑配置终端，第 1472 页 • 为中心辐射型拓扑配置终端，第 1475 页
4	配置路由策略。	• 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。 • 点击**路由**。
5	配置访问控制策略。	• 选择 **策略 > 访问控制**。

配置备份 VTI 隧道的准则

- 对于外联网对等体，您可以在托管的对等体上指定备用接口的隧道源 IP 地址并配置隧道目标 IP。

  您可以在 **创建新的 VPN 拓扑** 向导的 **终端 IP 地址** 字段中指定备份对等体 IP 地址。



- 在配置备份接口后，请为路由流量配置路由策略和访问控制策略。

  虽然主 VTI 和备用 VTI 始终可用，但流量只会通过路由策略中配置的隧道来传输。有关详细信息，请参阅为 VTI 配置路由和 AC 策略，第 1485 页。

- 配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

- 当为 VPN 配置了备用隧道，请配置具有不同指标的静态路由，以便处理通过备用隧道的流量的故障转移。

为路由型站点间 VPN 配置动态 VTI

要在管理中心为路由型站点间 VPN 配置动态 VTI，请执行以下操作：

步骤	相应操作	更多信息
1	在集线器上创建动态 VTI 接口。	添加 VTI 接口，第 1470 页
2	在分支上创建静态 VTI 接口。	添加 VTI 接口，第 1470 页
3	创建路由型站点间 VPN。	创建基于路由的站点间 VPN，第 1471 页
4	配置路由策略和访问控制策略。	为中心辐射型拓扑配置终端，第 1475 页

如何使用动态 VTI 配置虚拟路由器

要在管理中心为路由型站点间 VPN 配置具有动态 VTI 的虚拟路由器，请执行以下操作：

步骤	相应操作	更多信息
1	使用中枢上的动态VTI接口和分支上的静态 VTI 创建基于路由的站点间 VPN。	创建基于路由的站点间 VPN，第 1471 页
2	创建虚拟路由器。	创建虚拟路由器，第 1114 页
3	将接口分配给虚拟路由器。	配置虚拟路由器，第 1114 页
4	为中心辐射点配置路由策略。	为中心辐射型拓扑配置终端，第 1475 页
5	为中心辐射型配置访问控制策略。	为中心辐射型拓扑配置终端，第 1475 页

为 VTI 配置路由和 AC 策略

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由策略。
- 用于允许已加密的流量的访问控制规则。

VTI 的路由配置

对于 VTI 接口，可以配置静态路由或路由协议，例如 BGP、EIGRP、OSPF/OSPFv3。

1. 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。
2. 点击**路由 (Routing)**。
3. 配置静态路由或 BGP、EIGRP、OSPF/OSPFv3。

路由	参数	更多信息
Static Route	• **接口**-选择 VTI 接口。对于备份隧道，请选择备份 VTI 接口。 • **所选网络**-远程对等体的受保护网络。 • **网关**-远程对等体的隧道接口 IP 地址。对于备用隧道，请选择远程对等体的备用隧道接口 IP 地址。 • **指标**-对于备用隧道，请配置不同指标，以便处理通过备用隧道的流量的故障转移。 **注释** DVTI 不支持静态路由。	添加静态路由，第 1090 页

BGP	• 在 **常规设置** > **BGP** 下启用 BGP，提供本地设备的 AS 编号，并添加路由器 ID（如果您选择手动）。
	• 在 **BGP**下，启用 IPv4/IPv6 并点击 **邻居** 选项卡以配置邻居。
	  • **IP 地址**-远程对等体的 VTI 接口 IP 地址。对于备用隧道，则还要添加具有远程对等体的备用 VTI 接口 IP 地址的邻居。
	  • **远程 AS**-远程对等体的 AS 编号。
	• 点击 **重新分发** 选项卡，将 **源协议** 选择为“已连接”，以便启用连接的路由重新分发。
		配置 BGP，第 1217 页

路由	参数	更多信息
EIGRP	• 启用 EIGRP，提供本地设备的 AS 编号，并选择参与 EIGRP 路由过程的网络或主机。 • 点击 **邻居** 选项卡并定义 EIGRP 进程的静态邻居。 • 要从 VTI 接口通告汇总地址，请在 **汇总地址** 选项卡上从 **接口** 下拉列表中选择 VTI 接口。从 **网络** 下拉列表中，选择要汇总的网络。 • 点击 **接口** 选项卡中为 VTI 接口配置接口特定的 EIGRP 路由属性。 要在接口上启用 EIGRP 水平分割，请选中**水平分割 (Split Horizon)** 复选框。您还可以配置设备在 EIGRP Hello 数据包中通告的 **保持时间** 。	配置 EIGRP，第 1206 页
OSPF	• 选中**进程 1 (Process 1)** 复选框，然后选择 OSPF 角色。 • 点击 **接口** 选项卡，然后选择 VTI 接口。	配置 OSPFv2，第 1180 页
OSPFv3	• 选中 **进程 1** 和**启用进程 1** 复选框，然后选择 OSPFv3 角色。 • 点击 **接口** 选项卡，然后选择 VTI 接口。	配置 OSPFv3，第 1192 页

AC 策略规则

将访问控制规则添加到设备上的访问控制策略，以便允许使用以下设置在 VTI 隧道之间加密流量：

1. 通过“允许”操作来创建规则。
2. 选择本地设备的 VTI 安全区域作为源区域，然后选择远程对等体的 VTI 安全区域作为目标区域。
3. 选择远程对等体的 VTI 安全区域作为源区域，然后选择本地设备的 VTI 安全区域作为目标区域。

有关配置访问控制规则的详细信息，请参阅创建和编辑访问控制规则，第 1764 页。

查看虚拟隧道信息

您可以在设备上查看基于路由的 VPN 的动态和静态 VTI 的详细信息。对于每个 VPN 拓扑，您还可以查看与每个动态 VTI 相关联的所有动态生成的虚拟访问接口的详细信息。

开始之前

- 对于静态 VTI：Firewall Threat Defense 版本 7.0 及更高版本
- 对于动态 VTI：Firewall Threat Defense 版本 7.3 及更高版本

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 点击**虚拟隧道 (Virtual Tunnels)** 选项卡。

您可以查看每个 VTI 的详细信息，如名称、IP 地址、IPsec 模式、隧道源接口详细信息、拓扑结构和远程对等 IP。

您还可以查看接口的 ECMP 区域。

在 Umbrella 上部署 SASE 隧道

Cisco Umbrella 是思科基于云的安全互联网网关 (SIG) 平台，可针对基于互联网的威胁提供多个级别的防御。Umbrella 集成了安全的 Web 网关、DNS 层安全和云访问安全代理 (CASB) 功能，以保护系统抵御威胁。

您可以使用管理中心建立从威胁防御设备到 Umbrella 的 IPsec IKEv2 隧道。该隧道会将所有互联网绑定流量转发到 Umbrella SIG 进行检查和过滤。该解决方案提供集中式安全管理，因此网络管理员不必单独管理每个分支机构的安全设置。

要直接从威胁防御设备配置和部署Umbrella隧道，您可以使用简单的向导来创建SASE拓扑。SASE拓扑是一种新型的站点间 VPN 拓扑，并且它支持：

- 基于静态 VTI 的站点间 VPN。
- 中心辐射型拓扑，其中 Umbrella 是中心，而托管威胁防御设备是分支。
- 基于预共享密钥的身份验证
- Firewall Threat Defense 在 HA 模式下部署。
- 多实例：在多实例部署中，您只能集成一个 Umbrella 账户。

为了实现高可用性，您可以从威胁防御设备配置两个隧道，并将第二个隧道用作备用隧道。确保为每个隧道配置不同的本地隧道 ID。

为了简化配置，管理中心配置默认 IPsec 和 IKEv2 策略。

默认 IKEv2 策略配置：

- 完整性算法：NULL
- 加密算法：AES-GCM-256
- PRF 算法：SHA-256
- DH 组：19、20

默认 IKEv2 IPsec 策略配置：

- ESP 散列：SHA-256
- ESP 加密：AES-GCM-256

相关主题

如何在 Umbrella 上部署 SASE 隧道，第 1490 页

为 Umbrella 配置 SASE 隧道的准则和限制

SASE 拓扑支持：

- 仅基于 PSK 的身份验证
- IKEv2
- 高可用性

常规配置准则

- 防火墙管理中心 不会发现直接在 Umbrella 上创建的隧道或由其他应用创建的隧道。
- 您只能将 防火墙管理中心 管理的设备添加为 SASE 拓扑的终端。您无法添加外联网设备。

  对于高可用性对，高可用性对名称会显示在终端列表中。
- 在从 防火墙管理中心 删除隧道时，如果从 Umberlla 无法删除隧道，则您必须通过登录 Umbrella 手动将其删除。
- 如果正在进行部署到 Umbrella，则您无法编辑或删除 SASE 拓扑。您可以在 Umbrella 上查看隧道的部署状态：
  - 向导的 Cisco Umbrella 配置对话框
  - 部署 和任务选项卡下的通知页面
  - 站点间 VPN 监控控制面板

- 如果选中向导中的 **在威胁防御节点** 上部署配置复选框，则仅在在 Umbrella 上部署隧道后，才会在 Firewall Threat Defense上部署 Umbrella SASE 拓扑配置。

  防火墙管理中心 需要本地隧道 ID 才能在 Firewall Threat Defense上部署 Umbrella 配置。 防火墙管理中心 在 Umbrella 上部署隧道后，Umbrella 会生成完整的隧道 ID (<*prefix*>@<*umbrella generated ID*>-umbrella.com)。

- 防火墙管理中心 不会将在版本 7.3 之前创建的 Umbrella 数据中心拓扑识别为 SASE 拓扑。您必须在版本 7.3 中创建新的 SASE 拓扑并删除现有的拓扑。
- Firewall Threat Defense 高可用性切换后，SASE 拓扑将不会显示在站点间监控/VPN 摘要控制面板中。我们建议您使用 **vpn-sessiondb logoff index** 命令关闭隧道，然后使用数据包跟踪器将其打开。

限制

SASE 拓扑不支持：

- 集群
- 基于证书的身份验证
- IKEv1

如何在 Umbrella 上部署 SASE 隧道

本部分提供使用 防火墙管理中心从 Firewall Threat Defense 设备在 Umbrella 上部署 SASE 隧道的说明。

步骤	相应操作	更多信息
1	查看准则和限制。	为 Umbrella 配置 SASE 隧道的准则和限制，第 1489 页
2	确保您已满足前提条件。	配置 Umbrella SASE 隧道的前提条件，第 1490 页
3	配置 Cisco Umbrella 连接设置。	• 配置 Cisco Umbrella 连接设置 • 映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥，第 1491 页
4	在 Umbrella 上配置 SASE 隧道。	为 Umbrella 配置 SASE 隧道，第 1493 页
5	查看 SASE 隧道的状态。	查看 SASE 隧道状态，第 1494 页

配置 Umbrella SASE 隧道的前提条件

- 您必须拥有 Cisco Umbrella 安全互联网网关 (SIG) 基础版订用。

- 您必须启用具有出口控制功能的智能许可证帐户，才能从 防火墙管理中心在Umbrella上部署隧道。如果未启用此许可证，则您只能创建 SASE 拓扑。您无法在 Umbrella 上部署隧道。
- 您必须在 https://umbrella.cisco.com 上使用 Cisco Umbrella 创建一个帐户，然后通过 http://login.umbrella.com 登录 Umbrella，获取与 Cisco Umbrella 建立连接所需的信息。
- 您必须向 防火墙管理中心 注册 Cisco Umbrella，并在 Cisco Umbrella 连接设置中配置管理密钥和管理密码。管理中心需要管理密钥和管理密码才能从思科 Umbrella 云获取数据中心详细信息。您还必须在思科Umbrella连接设置中配置组织ID、网络设备密钥、网络设备密钥和旧版网络设备令牌。

  有关详细信息，请参阅：

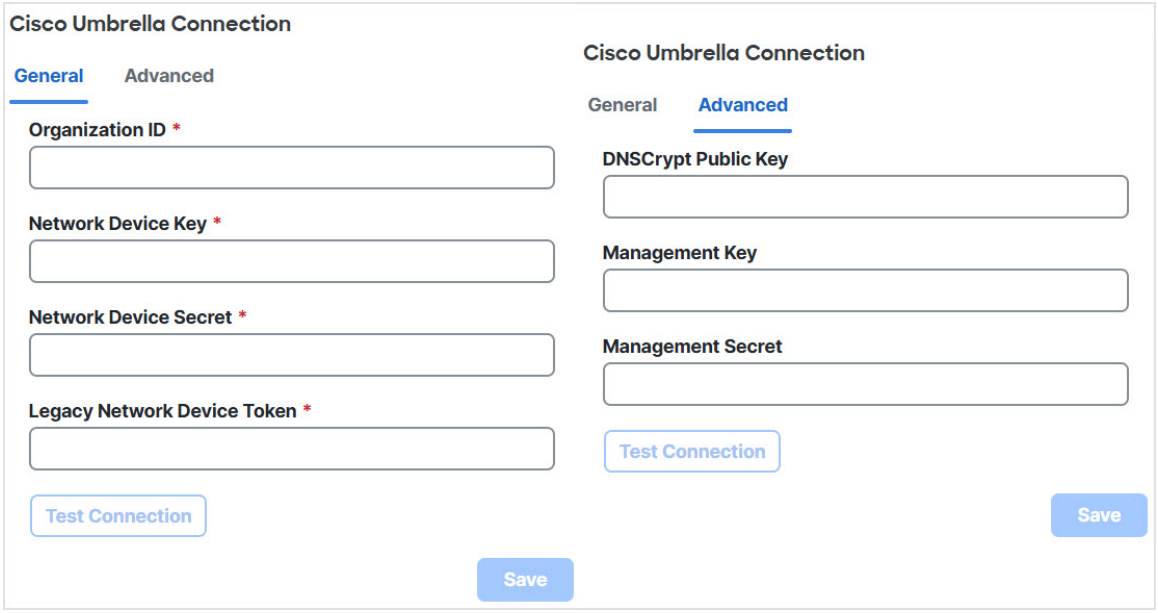
  - 配置 Cisco Umbrella 连接设置
  - 映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥 ， 第 1491 页
- 确保可从 Firewall Threat Defense访问 Umbrella 数据中心。
- 您只能在 Cisco Umbrella 和 Firewall Threat Defense 版本 7.1.0 及更高版本之间部署隧道。

映射管理中心 Umbrella 参数和 Cisco Umbrella API 密钥

要向 防火墙管理中心 注册 Cisco Umbrella 并在 防火墙管理中心配置 Umbrella 参数，您必须：

1. 登录 Cisco Umbrella。
2. 选择 **管理 > API 密钥 > 旧版密钥**。
3. 生成并复制所需的 API 密钥。
4. 使用 API 密钥在 防火墙管理中心中配置 Cisco Umbrella 连接参数。

下图显示了您必须在 防火墙管理中心的 Cisco Umbrella 连接中配置的参数。DNScrypt 公共密钥是可选参数。



下图显示了向 防火墙管理中心注册 Cisco Umbrella 时必须使用的 Cisco Umbrella 中的 API 密钥。

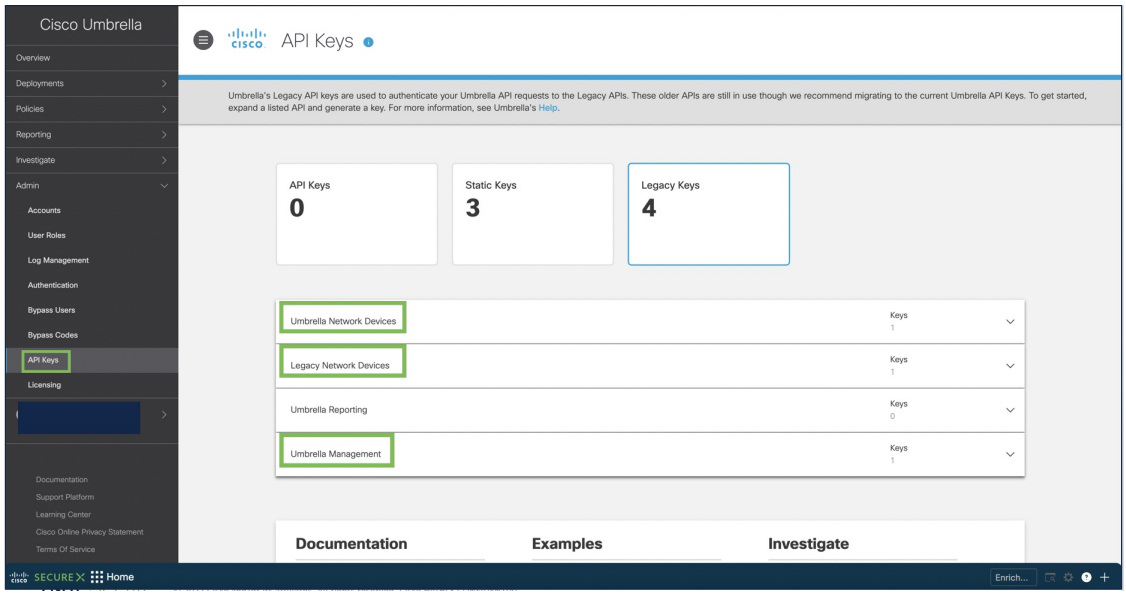


表 *88:* 映射 防火墙管理中心 ***Umbrella*** 参数和 ***Cisco Umbrella API*** 密钥

管理中心参数	**Cisco Umbrella API** 密钥
网络设备密钥 网络设备密钥	Umbrella 网络设备
旧版网络设备令牌	旧版网络设备

管理中心参数	Cisco Umbrella API 密钥
管理密钥 管理密钥	Umbrella 管理

为 Umbrella 配置 SASE 隧道

开始之前

确保查看 配置 Umbrella SASE 隧道的前提条件，第 1490 页 和 为 Umbrella 配置 SASE 隧道的准则和限制，第 1489 页 中的前提条件和准则。

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在**拓扑名称 (Topology Name)** 字段中输入拓扑的名称。

步骤 3 点击**SASE 拓扑 (SASE Topology)** 单选按钮，然后点击**创建 (Create)**。

步骤 4 **预共享密钥 (Pre-shared Key)**：此密钥会根据 Umbrella PSK 要求自动生成。对于单个拓扑，预共享密钥对所有威胁防御分支和 Umbrella 均通用。

设备和 Cisco Umbrella 分享此密钥，IKEv2 将其用于身份验证。如果配置此密钥，长度必须介于 16 到 64 个字符之间，至少包含一个大写字母、一个小写字母和一个数字，并且不包含特殊字符。每个拓扑都必须具有唯一的预共享密钥。如果拓扑有多个隧道，则所有隧道都具有相同的预共享密钥。

步骤 5 从 **Umbrella 数据中心 (Umbrella Data center)** 下拉列表中选择数据中心。（在 Firewall Threat Defense 上配置路由，以确保从 Firewall Threat Defense可访问 Umbrella DC。）

步骤 6 点击 **添加** 以添加 Firewall Threat Defense 节点。

a) 从 **设备** 下拉列表中选择 Firewall Threat Defense 。

列表中只会显示由 防火墙管理中心 管理的设备。对于高可用性对，高可用性对名称会显示在终端列表中。

b) 从 **VPN 接口 (VPN Interface)** 下拉列表选择静态 VTI 接口。

要创建新的静态 VTI 接口，请点击 添加 +。系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

- 隧道类型为静态。
- 名称为 *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>*. 例如，outside_static_vti_2。
- 隧道 ID 会自动填充一个唯一 ID。
- 隧道源接口会自动填充一个带有“外部”前缀的接口。
- IPsec 隧道模式为 IPv4。

- IP 地址在 169.254.xx/30 专用 IP 地址范围内。

c) 在**本地隧道 ID (Local Tunnel ID)** 字段中输入本地隧道 ID 的前缀。

前缀最少包含 8 个字符，最多包含 100 个字符。管理中心在 Umbrella 上部署隧道后，Umbrella 会生成完整的隧道 ID (<*prefix*>@<*umbrella generated ID*>-umbrella.com)。然后，管理中心会检索并更新完整的隧道 ID，并将其部署在威胁防御设备上。每个隧道都有唯一的本地隧道 ID。

d) 点击**保存**以将终端设备添加到拓扑。

您可以在 SASE 拓扑中添加多个终端。

步骤 7 点击 **下一步** 以查看 Umbrella SASE 隧道配置摘要。

- **终端 (Endpoints)** 窗格：显示已配置终端的摘要。
- **加密设置** 窗格：显示拓扑的默认 IKEv2 策略和 IKEv2 IPsec 转换集。

步骤 8 选中**在威胁防御节点上部署配置 (Deploy configuration on threat defense nodes)** 复选框，以触发将网络隧道部署到威胁防御。此部署会在将隧道部署到 Umbrella 之后进行。威胁防御部署需要本地隧道 ID。

步骤 9 点击**保存**。

此操作：

1. 在管理中心保存拓扑。
2. 触发将网络隧道部署到 Umbrella。
3. 如果启用此选项，则会触发将网络隧道部署到威胁防御设备。此操作会提交并部署自上次在设备上部署以来更新的所有配置和策略，包括非 VPN 策略。
4. 打开 **Cisco Umbrella 配置 (Cisco Umbrella Configuration)** 窗口并显示 Umbrella 上的隧道部署状态。有关详细信息，请参阅查看 SASE 隧道状态，第 1494 页。

下一步做什么

对于要通过 SASE 隧道的需要关注的流量，请使用特定匹配条件配置 PBR 策略，以通过 VTI 接口发送流量。

确保为 SASE 拓扑的每个终端配置 PBR 策略。

查看 SASE 隧道状态

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在**拓扑名称 (Topology Name)** 字段中输入拓扑的名称。

步骤 3 点击**SASE 拓扑 (SASE Topology)** 单选按钮，然后点击**创建 (Create)**。

步骤 4 输入唯一的 和**预共享密钥 (Pre-shared Key)**，选择数据中心，添加设备，然后点击**下一步 (Next)**。

步骤 5 查看 Umbrella SASE 隧道配置的摘要，然后点击**保存**。系统将显示 **Cisco Umbrella 配置 (Cisco Umbrella Configuration)** 窗口。

您可以查看拓扑详细信息，例如隧道部署的名称、数据中心、数据中心 IP 地址、开始时间和结束时间。

您可以在 Umbrella 上查看隧道的部署状态。不同的隧道部署状态如下：

- 待处理：管理中心尚未将配置推送到 Umbrella。
- 成功 (Success)：管理中心已成功在 Umbrella 上配置隧道。
- 进行中 (In Progress)：管理中心正在 Umbrella 上部署隧道。
- 失败：管理中心无法在 Umbrella 上配置隧道。

如果状态显示为待处理或失败，请使用脚本对隧道创建进行故障排除。点击**脚本 (Transcript)** 按钮以查看脚本详细信息，例如 API、请求的负载以及从 Umbrella 收到的响应。

步骤 6 点击 **Umbrella 控制面板** ， 查看 Cisco Umbrella 中的网络隧道。

步骤 7 通过以下位置查看 Umbrella 隧道部署状态：

- **部署 (Deployments)** 和**任务 (Tasks)** 选项卡下的**通知 (Notifications)** 页面。
- **站点间** VPN 控制面板 (**洞察和报告** > **VPN 控制面板** > **站点间 VPN**)。

  控制面板提供站点间 VPN 拓扑的摘要，包括 Umbella SASE 拓扑。您可以查看对等设备之间的隧道以及每个隧道的状态。您还可以使用 CLI 命令和数据包跟踪器来对隧道部署的任何问题进行故障排除。

监控站点间拓扑

使用站点间 VPN 摘要页面监控站点间 VPN

您可以在**站点间 VPN 摘要**页面查看站点间 VPN 拓扑的摘要。对于每个拓扑，您可以查看详细信息，例如 VPN 类型、网络拓扑、VPN 接口、VPN 设备和隧道状态。

您可以通过编辑和删除按钮来编辑或删除拓扑。对于 SASE 拓扑 VPN，您可以选择部署、编辑和删除任何拓扑。

使用站点间 VPN 控制面板监控站点间 VPN

选择 **洞察和报告** > **VPN 控制面板** > **站点间 VPN** 以打开站点间控制面板。

Secure Firewall Management Center 提供站点间 VPN 隧道的快照，包括 SASE 拓扑隧道， 以便确定站点间VPN隧道的状态。您可以查看对等设备之间的隧道列表以及每个隧道的状态：活动、非活动或无活动数据。您可以根据拓扑结构、设备和状态来过滤表中的数据。监控控制面板中的表格会显示实时数据，您可以配置为按指定的时间间隔来刷新数据。该表显示了基于加密映射的VPN的点对点、中心辐射型以及全网状拓扑。隧道信息还包含路由型 VPN 或虚拟隧道接口 (VTI) 的数据。

您可以使用此数据：

- 确定有问题的 VPN 隧道并进行故障排除。
- 验证站点间 VPN 对等设备之间的连接。
- 监控 VPN 隧道的运行状况，以便在站点间提供不间断的 VPN 连接。

站点间 VPN 控制面板显示站点间 VPN 隧道的以下构件：

- **隧道状态**- 列出使用 防火墙管理中心配置的站点间 VPN （包括 Umbrella 的 SASE 隧道） 的隧道状态
- **隧道汇总 (Tunnel Summary)** - 以环状图来显示隧道的聚合状态。
- **拓扑 (Topology)** - 按拓扑来汇总的隧道状态。

准则和限制

- 该表会显示已部署的站点间，包括 SASE 拓扑，VPN 的列表。它不会显示已创建但未部署的隧道。
- 该表不会显示有关基于策略的 VPN 和备份 VTI 的备份隧道的信息。
- 对于集群部署，该表不会显示实时数据中的导向器更改。它只会显示部署VPN时存在的导向器信息。只有在更改后重新部署了隧道 AM，导向器更改才会在表中体现出来。

VPN 隧道的状态

站点间监控控制面板会列出以下状态的 VPN 隧道：

- **非活动 (Inactive)** - 如果所有 IPSec 隧道都关闭，则策略型（基于加密映射）的 VPN 隧道将处于非活动状态。如果 VTI 或和 SASE 拓扑 VPN 隧道遇到任何配置或连接问题，则该隧道将关闭。
- **活动 (Active)** - 在 防火墙管理中心 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议来配置的。如果 防火墙管理中心 在部署后通过隧道识别出需要关注的流量，则策略型 VPN 隧道将处于活动状态。只有当至少有一个 IPsec 隧道正常运行时，IKE 隧道才会正常运行。

  路由型 VPN (VTI) 和 SASE 拓扑 VPN 隧道不需要所关注的流量处于活动状态。如果它们的配置和部署没有错误，则它们将处于活动状态。
- **无活动数据 (No Active Data)** - 策略型 VPN 和 SASE 拓扑 VPN 隧道会保持“无活动数据”(No Active Data) 状态，直到第一次有流量事件通过隧道。“无活动数据”(No Active Data) 状态还会列出已部署但出错的策略型和路由型 VPN。

有关隧道状态的重要说明 防火墙管理中心

- 防火墙管理中心 中的 VPN 状态基于事件。 防火墙管理中心 不启动状态更新。因此，控制面板和 Firewall Threat Defense中的隧道状态可能不匹配。您可以在 **隧道状态** 构件的 **CLI 详细信息** 选项卡中查看正确的状态。
- 当 Firewall Threat Defense 切换到辅助 Firewall Threat Defense时， 防火墙管理中心 和 Firewall Threat Defense中的 VPN 隧道状态不匹配。当设备切换回主设备时，会显示正确的隧道状态。
- 设备重新启动后， 防火墙管理中心 不会更新早于 7.3 版本的 Firewall Threat Defense 设备的隧道状态。我们建议您使用命令 **vpn-sessiondb logoff index** 关闭隧道，然后使用数据包跟踪器将其打开。

隧道状态

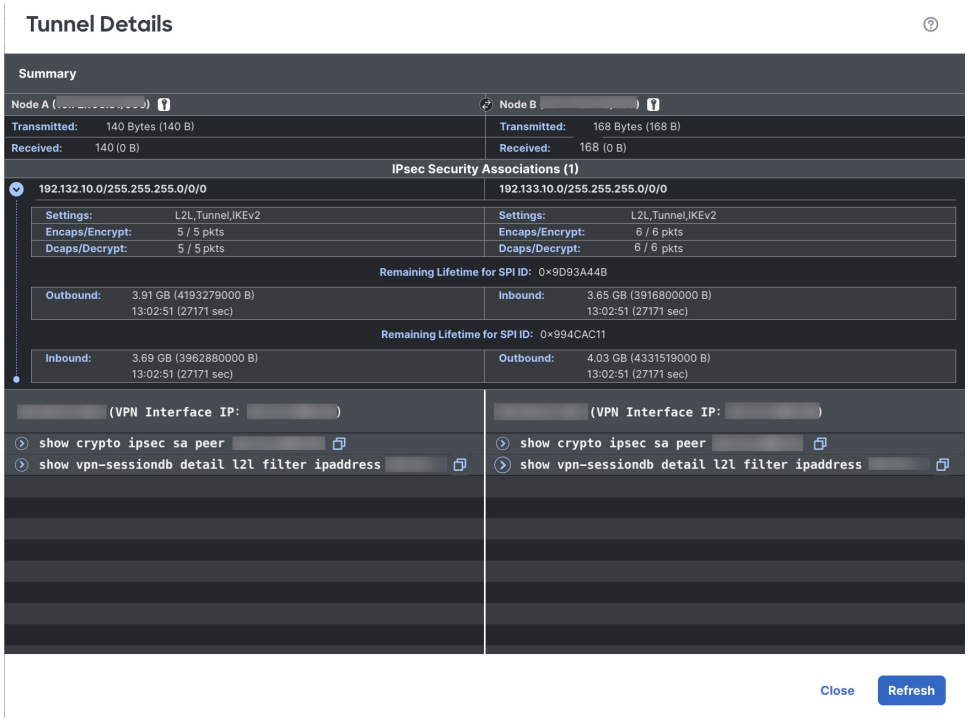
此表列出了使用防火墙管理中心配置的站点间VPN，包括SASE拓扑VPN。将鼠标悬停在拓扑上，然后点击 **视图** ( )，查看有关该拓扑的以下详细信息：

- **常规** - 显示有关节点的更多信息，例如 IP 地址和接口名称。
- **CLI 详细信息** - 显示以下命令的 CLI 输出：
  - **show crypto ipsec sa peer** <*node A/B_ip_address*>：显示在节点 A 和 B 之间构建的 IPsec SA。
  - **show vpn-sessiondb l2l filter ipaddress** <*node A/B_ip_address*>：显示有关 VPN 会话的信息。

  对于外联网设备，不会显示命令输出。

  从上述命令输出派生的有关 IKE 和 IPsec 会话的重要详细信息，以用户友好的汇总格式显示。您可以一次查看两个节点的详细信息。节点名称旁边的图标指定身份验证类型：预共享密钥或客户端证书。详细信息包括每个隧道的 IKE 统计信息和 IPsec SA 统计信息，如下所示：

图 *432:* 隧道状态 > 查看 > *CLI* 详细信息

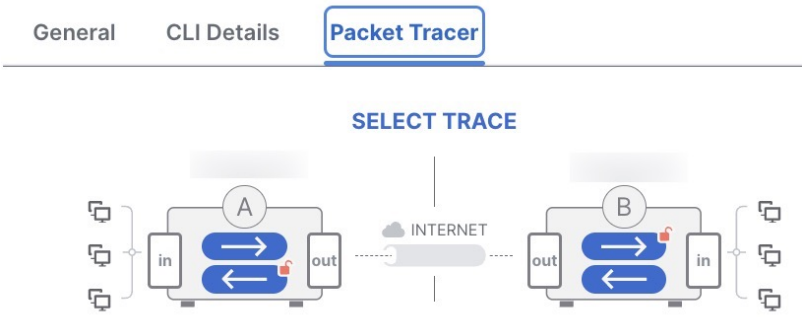


- **数据包跟踪器** - 使用数据包跟踪器来对威胁防御 VPN 隧道进行故障排除。

Packet Tracer

数据包跟踪器允许您对两台威胁防御设备之间的 VPN 隧道进行故障排除。您可以检查设备 A 和设备 B 之间的 VPN 连接是否正常。此工具将数据包注入设备并跟踪从入口端口到出口端口的数据包流量。在配置设备的入口接口以及受保护网络之后，该工具会模拟流量。数据包跟踪器会根据流量和路由查询、ACL、协议检查、NAT 和 QoS 等模块来评估数据包。

图 *433: Packet Tracer*



对于每台设备，该工具都会运行加密跟踪和解密跟踪（数据包被视为已解密的VPN流量）。您可以在设备的入口和出口端口之间运行四种不同的跟踪。点击各个加密和解密隧道即可启用或禁用跟踪。

运行跟踪时，该工具按以下顺序执行跟踪：

1. A 的加密跟踪。
2. B 的解密痕迹。
3. B 的加密跟踪。
4. A 的解密痕迹。

跟踪完成后，您可以查看跟踪的输出以及每个模块的结果。



注释 您不能对路由型（基于 VTI）的 VPN 运行解密跟踪。

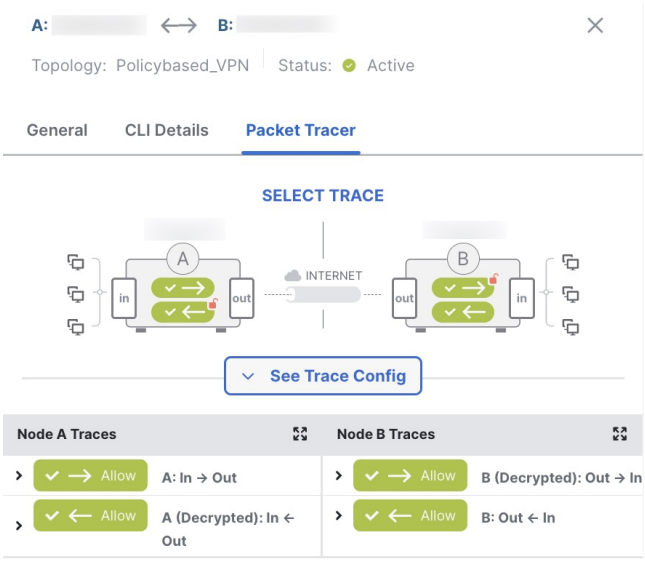
要运行数据包跟踪器，请执行以下操作：

1. 点击 **查看详细配置** 以查看 VPN 接口名称、VPN 接口 IP 地址、VTI 接口名称及 VTI 接口 IP 地址。
2. （可选）从 **协议** 下拉列表中选择协议。您可以选择 ICMP/8/0、TCP 或 UDP。

   ICMP/8/0 是默认选项。如果选择 ICMP/8/0，则 8 表示 ICMP 类型为回应请求，而 0 表示 ICMP 代码。如果选择 TCP 或 UDP，请从**目标端口 (Destination Port)** 下拉列表中选择目标端口。范围是从 0 到 65535。
3. 从**入口接口 (Ingress Interface)** 下拉列表中选择要在其上跟踪数据包的两个设备的入口接口。
4. 从 **受保护的网络 IP 地址** 字段中输入与入口接口相同的子网中的 IP 地址。
5. 点击**立即跟踪 (Trace Now)**。

   在启动跟踪后，您可以查看每个模块的跟踪是否成功。如果隧道关闭，则路径会显示为红色。如果隧道开启，则路径会显示为绿色。如果隧道已关闭，请点击 **重新跟踪** 以再次运行该工具。对于基于加密映射的 VPN，当隧道处于非活动状态且没有需要关注的流量时，初始跟踪可能为红色。点击 **重新跟踪** 以再次运行跟踪。

图 *434:* 成功跟踪后的数据包跟踪器



外联网节点 (Extranet Nodes)：您可以启动 VPN 隧道的数据包跟踪，其中一个节点作为外联网。对于外联网节点，您无法选择入口接口。数据包跟踪的其余步骤均相同。您无法在外联网端运行跟踪。

例如，如果节点 A 是托管威胁防御，而节点 B 是外联网：

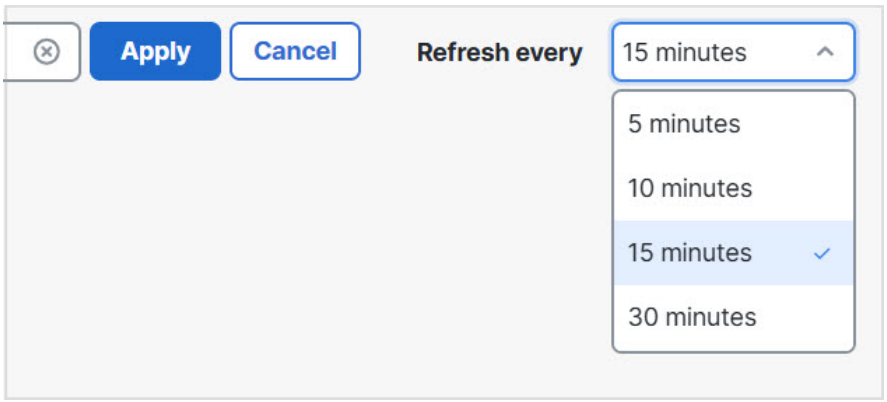
- 配置节点 A 的入口接口。
- 为节点 A 和 B 配置受保护的网络。
- 点击**立即跟踪 (Trace Now)**。跟踪显示的是节点 A，而不是节点 B。

自动数据刷新

表中的站点间 VPN 数据会定期刷新。您可以配置为以特定间隔刷新 VPN 监控数据，或者关闭自动数据刷新。

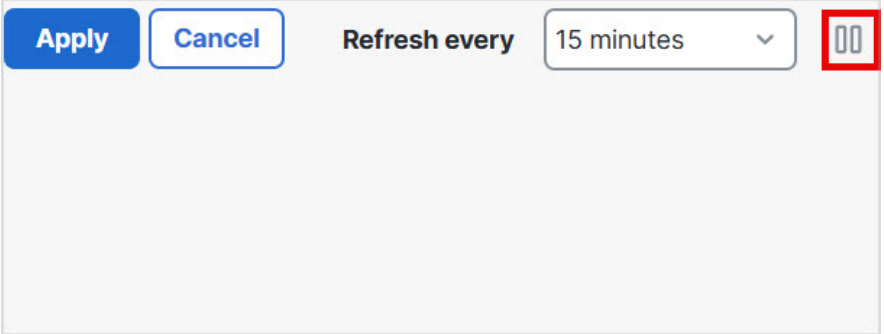
点击**刷新 (Refresh)** 间隔下拉列表，从可用的间隔时间中选择以刷新表中的数据。

图 *435:* 刷新隧道数据



点击**暂停 (Pause)** 可根据需要停止自动数据刷新。您可以点击同一按钮继续刷新隧道数据。

图 *436:* 暂停定期数据刷新



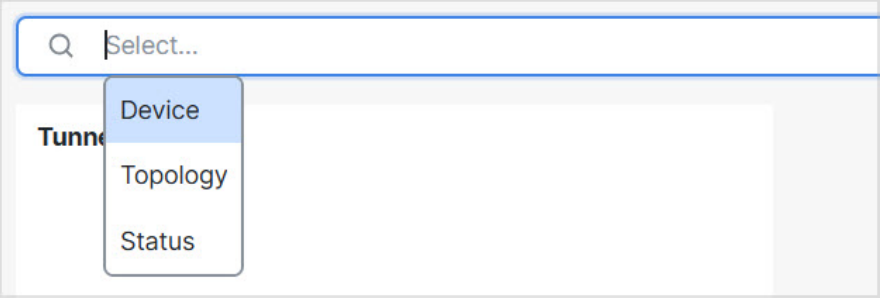
对站点间 VPN 监控数据进行过滤和排序

您可以按拓扑、设备和状态来过滤和查看 VPN 监控表中的数据。

例如，您可以查看特定拓扑中处于关闭状态的隧道。

在过滤器框中点击选择过滤条件，然后指定要过滤的值。

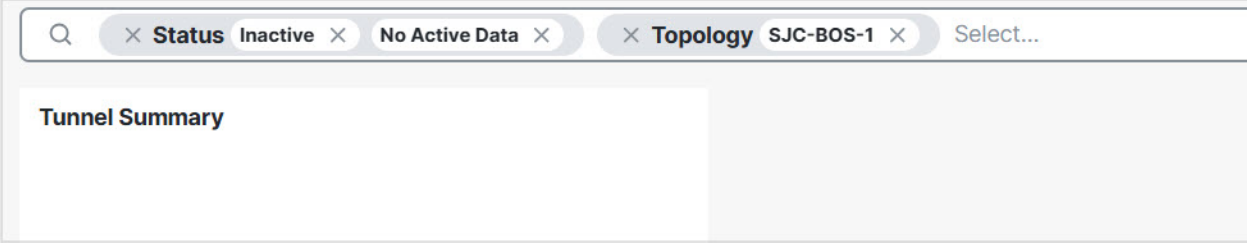
图 *437:* 过滤隧道数据



您可以根据需要使用多个过滤条件来查看数据。

例如，您可以选择只查看处于“开启”(Up) 和“关闭”(Down) 状态的隧道，并忽略处于“未知”(Unknown) 状态的隧道。

图 *438:* 示例：过滤隧道数据



排序数据 (Sort the data) - 要按列对数据进行排序，请点击列标题。

相关主题

关于站点间 VPN，第 1443 页
关于 Virtual Tunnel Interface，第 1462 页

站点间 VPN 连接事件监控

通过站点间 VPN 连接事件，您可以了解 VPN 是否加密连接，并帮助您解决连接问题，尤其是在多跳 VPN 部署中。防火墙管理中心 的事件控制面板显示加密或解密流量的 VPN 对等体的 IP 地址（对等体的 IKE 地址），并显示 VPN 操作，如下所示：

- 如果连接由 VPN 解密，则**解密对等体 (Decrypt Peer)** 列会显示接收流量的对等体地址 IP 地址，并将**解密 (Decrypt)** 显示为 VPN 操作。
- 如果连接由 VPN 加密，则**加密对等体 (Encrypt Peer)** 列会显示流量发送到的 VPN 对等体的 IP 地址，并将**加密 (Encrypt)** 显示为 VPN 操作。
- 如果VPN服务器级联连接，它将在一个隧道上解密，并在另一个隧道上重新加密。在这种情况下，事件中会同时显示 **加密对等体** 和 **解密对等体** IP 地址。 **VPN 操作** 列显示 **VPN 路由** 作为指示连接通过 VPN 服务器传输的操作。

如果启用绕过已解密流量的访问控制策略选项，则系统会绕过访问控制策略，并且不会记录已解密流量的事件。默认情况下，此选项处于禁用状态，VPN 隧道中的所有已解密流量都会经过 ACL 检查。

查看站点间 VPN 连接事件

访问 防火墙管理中心 的连接事件查看器，了解 VPN 是否加密连接流量，并检索 VPN 对等体详细信息。

开始之前

确保在访问控制规则中启用连接开始时和连接结束时的连接事件日志记录。

过程

步骤 1 选择**事件和日志** > **+ 显示更多** > **连接** > **事件**。

步骤 2 转到 **连接事件的表视图** 选项卡。

步骤 3 事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 **x** 图标以显示字段选择器。

步骤 4 选择以下列：

- 解密对等体
- 加密对等体
- VPN 操作

步骤 5 点击**应用 (Apply)**。

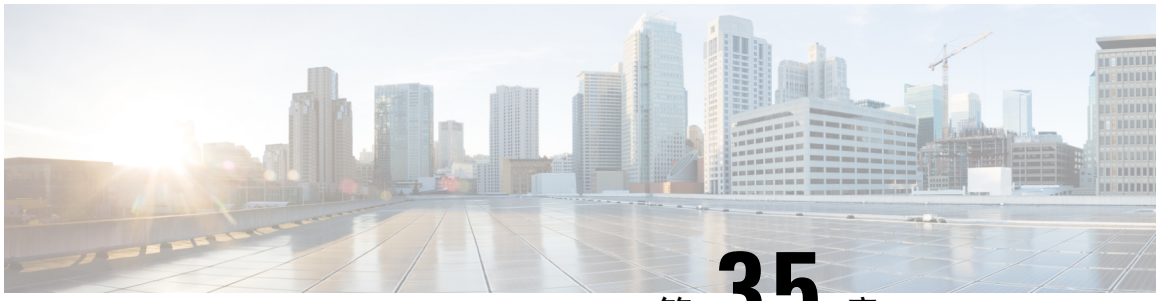
有关连接事件的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的连接和安全相关的连接事件。

站点间 VPN 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
查看虚拟隧道信息	7.4.1	任意	您可以在设备上查看基于路由的 VPN 的动态和静态 VTI 的详细信息。对于每个 VPN 拓扑，您还可以查看动态 VTI 的所有虚拟访问接口的详细信息。 新增/修改的屏幕：**设备** > **设备管理** > **编辑设备** > **接口**，然后点击**虚拟隧道**选项卡。
IPsec 流分流	7.4	任意	在 Cisco Secure Firewall 3100 和 Cisco Secure Firewall 4200 设备上的 VTI 环回接口上自动启用 IPsec 数据流分流。
Umbrella SASE 拓扑	7.3	任意	您可以配置 Umbrella SASE 拓扑，并在威胁防御设备和 Umbrella 之间部署 IPsec IKEv2 隧道。该隧道会将所有互联网绑定流量转发到 Umbrella 安全互联网网关 (SIG) 进行检查和过滤。
支持动态虚拟隧道接口	7.3	任意	您可以创建动态 VTI 并使用它在中心辐射型拓扑配置基于路由的站点间 VPN。
VTI 的 EIGRP IPv4 支持	7.3	任意	静态和动态 VTI 接口支持 EIGRP IPv4 路由。
VTI 支持 OSPFv2/v3 IPv4/v6	7.3	任意	静态和动态 VTI 接口支持 OSPFv2/v3 IPv4/v6 路由。
站点间 VPN 监控控制面板中的数据包跟踪器	7.3	任意	使用站点间 VPN 监控控制面板中的数据包跟踪器工具来对威胁防御 VPN 隧道进行故障排除。 新增/修改的屏幕： **概述** > **控制面板** > **站点间 VPN**
远程访问 VPN 控制面板	7.3	任意	使用远程访问 VPN 控制面板监控设备上主动远程访问 VPN 会话的实时数据。 新增/修改的屏幕： **概述** > **控制面板** > **远程访问 VPN**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
IPsec 流分流	7.2	任意	在 Cisco Secure Firewall 3100上，默认情况下会分流 IPsec 流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 您可以使用 FlexConfig 和 **flow-offload-ipsec** 命令更改配置。
站点间 VPN 过滤器	7.1	任意	添加了控制策略，以控制站点间 VPN 流量。
本地隧道 ID 支持	7.1	任意	对于站点间 VPN 上的每个终端，您可以配置要与对等体共享的唯一隧道 ID。
多 IKE 策略支持	7.1	任意	您可以为每个终端添加多个 IKEv1 和 IKEv2 策略对象。
站点间 VPN 监控控制面板	7.1	任意	使用站点间 VPN 监控控制面板，查看和监控站点间 VPN 隧道的状态。
备份基于路由的站点间 VPN 的虚拟隧道接口 (VTI) 。	7.0	任意	配置使用虚拟隧道接口的站点间VPN时，可以为隧道选择备份VTI。指定备用VTI可提供恢复能力，以便在主连接断开时，备用连接可能仍能正常工作。例如，可以将主 VTI 指向一个服务提供商的终端，将备用 VTI 指向其他服务提供商的终端。 通过选择基于路由作为点对点连接的 VPN 类型，您可以在站点间 VPN 向导中添加备份 VTI。
将VTI数量从每个接口 100 个增加到每个设备 1024 个	7.0	任意	支持的最大 VTI 数量从每个物理接口 100 个增强到每个设备 1024 个 VTI。
IPv6 支持	7.0	任意	您可以配置 IPv6 寻址的 VTI。虽然仅支持静态 IPv6 地址作为隧道源和目的地址，但不支持 VTI 上的 IPv6 BGP。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
删除和弃用弱密码	6.7	任意	已删除对不太安全的密码的支持。我们建议您在升级到 Firewall Threat Defense 6.70 以支持 DH 和加密算法之前更新 VPN 配置，以确保 VPN 正常工作。 更新 IKE 提议和 IPSec 策略以匹配 Firewall Threat Defense 6.70 中支持的策略，然后再部署配置更改。 从 Firewall Threat Defense 6.70 开始，以下安全性较低的密码已被删除或弃用： • 已弃用 IKEv1 的 **Diffie-Hellman GROUP 5**，并已为 IKEv2 将其删除 • Diffie-Hellman 组 2 和 24 已被删除。 • **加密算法**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 已被删除。 **注释** 在评估模式下或对不满足强加密导出控制要求的用户继续支持**DES**。 **NULL** 在 IKEv2 策略中已已删除，但在 IKEv1 和 IKEv2 IPsec 转换集中仍支持。
动态 RRI 支持	6.7	任意	基于 IKEv2 的静态加密映射支持动态反向路由。
面向站点间 VPN 的备用对等体	6.6	任意	您可以使用 防火墙管理中心 将备份对等体添加到站点间 VPN 连接。例如，如果您有两个 ISP，则可以将 VPN 连接配置为故障转移到备用 ISP（如果与第一个 ISP 的连接不可用）。 新增/经修改的页面： **设备 (Devices)** > **VPN** > **站点间 (Site to Site)**。在添加或编辑点对点或中心辐射型 FTD VPN 拓扑以添加终端时，**IP 地址 (IP Address)** 字段支持以逗号分隔的备份对等体。



第 35 章

SD-WAN

本章介绍管理中心支持的 SD-WAN 功能。

- SD-WAN 功能，第 1507 页
- 功能，第 1508 页
- 使用 SD-WAN 向导进行安全分支机构网络部署，第 1510 页
- SD-WAN 功能的使用案例，第 1525 页
- 监控 SD-WAN 拓扑，第 1525 页

SD-WAN 功能

软件定义的 WAN (SD-WAN) 解决方案取代了传统的 WAN 路由器，并且不受 WAN 传输技术的影响。SD-WAN 跨多个 WAN 连接提供基于策略的动态应用路径选择，并支持其他服务（例如 WAN 优化和防火墙）的服务链。

随着组织在多个分支机构扩展其运营，确保安全和简化的连接变得至关重要。部署安全的分支机构网络基础设施涉及复杂的配置，如果处理不当，不仅耗时，还容易出现配置错误。但是，组织可以通过利用 Cisco Secure Firewall Management Center（管理中心）和 Cisco Secure Firewall Threat Defense（威胁防御）设备来克服这些挑战，实现简化且安全的分支机构部署。

在本指南中，我们将探讨使用强大的防火墙解决方案简化安全分支机构部署的概念。通过集成 Cisco Secure Firewall 作为分支网络架构的基础组件，企业可以建立强大的安全基线，同时简化部署流程。这种方法使企业能够执行统一的安全策略，优化流量路由，并确保弹性连接。

Cisco Secure Firewall 支持的一些 SD-WAN 功能包括：

- **简化管理：**
  - SD-WAN 向导
  - SASE：Umbrella 自动隧道部署
  - 动态 VTI (DVTI) 中心辐射型拓扑简化
- **应用感知：**
  - 公共云和访客用户的直接互联网接入 (DIA)

- 使用应用作为匹配条件的策略型路由 (PBR)
- 为 Umbrella 提供本地隧道 ID 支持

- **增加可用带宽：**
  - ECMP 支持在多个 ISP 之间实现负载均衡和 VTI
  - 使用 PBR 的基于应用的负载均衡

- **高可用性，网络停机时间接近于零：**
  - 双 ISP 配置
  - 基于应用的接口监控优化路径选择。

- **安全弹性连接：**
  - 总部（中心）和分支机构（分支）之间的基于路由 (VTI) 的 VPN 隧道
  - IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPF 以及 IPv4 EIGRP over VTI
  - 对具有静态或动态 IP 的分支的 DVTI 支持

功能

下表列出了一些常用的 SD-WAN 功能：

特性	已引入	更多信息
使用 SD-WAN 向导配置设置，以通过 SD-WAN 隧道携带 SGT。	版本 10.0	使用 SD-WAN 向导进行安全分支机构网络部署，第 1510 页
支持中心的 ECMP 以及 SVTI 和 DVTI 的 BFD。	版本 10.0	使用 SD-WAN 向导进行安全分支机构网络部署，第 1510 页
使用 PBR 根据高级自定义应用检测器处理流量。	版本 10.0	策略型路由，第 1259 页
远程分支管理 (HA)，支持双 WAN	版本 7.7	Cisco SD-WAN 摘要控制面板，第 1525 页
针对自定义应用的 PBR 支持	版本 7.7	策略型路由，第 1259 页
SD-WAN 向导	版本 7.6	使用 SD-WAN 向导进行安全分支机构网络部署，第 1510 页

特性	已引入	更多信息
SD-WAN 摘要控制面板上的应用监控	版本 7.4.1	Cisco SD-WAN 摘要控制面板，第 1525 页
Cisco SD-WAN 摘要控制面板	版本 7.4	Cisco SD-WAN 摘要控制面板，第 1525 页
具有用户身份和 SGT 的策略型路由。	版本 7.4	策略型路由，第 1259 页
使用 HTTP 路径监控的策略型路由。	版本 7.4	策略型路由，第 1259 页
VTI 的环回接口支持	版本 7.3	关于环回接口，第 765 页
对站点间 VPN 的动态 VTI (DVTI) 支持	版本 7.3	动态 VTI，第 1464 页
Umbrella 自动隧道	版本 7.3	在 Umbrella 上部署 SASE 隧道，第 1488 页
VTI 支持 IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPF 以及 IPv4 EIGRP	版本 7.3	BGP，第 1213 页 OSPF，第 1175 页 EIGRP，第 1203 页
具有中心辐射型拓扑的基于路由的站点间 VPN	版本 7.2	创建基于路由的站点间 VPN，第 1471 页
具有路径监控的策略型路由	版本 7.2	策略型路由，第 1259 页
站点间 VPN 监控控制面板	版本 7.1	使用站点间 VPN 控制面板监控站点间 VPN ，第 1495 页
直接互联网接入/策略型路由	版本 7.1	策略型路由，第 1259 页
带 WAN 接口的等价多路径 (ECMP) 区域	版本 7.1	ECMP，第 1159 页
带 VTI 接口的等价多路径 (ECMP) 区域	版本 7.1	ECMP，第 1159 页
备份基于路由的站点间 VPN 的 VTI	版本 7.0	通过备用 VTI 隧道路由流量，第 1482 页
通过站点间 VPN 支持静态 VTI (SVTI)	版本 6.7	静态 VTI，第 1463 页

使用 SD-WAN 向导进行安全分支机构网络部署

管理中心允许您可以使用新的 SD-WAN 向导轻松配置集中式总部和远程分支机构站点之间的 VPN 隧道和路由配置。

什么是中心和分支？

中心：实现与一个或多个远程分支设备或分支之间的安全VPN连接的设备。中心还充当分支相互通信的网关。

分支：位于远程分支机构的设备，通过VPN连接到中心，以安全地访问中心背后的企业资源。分支通过中心相互通信。

使用 SD-WAN 向导的优势

- 简化并自动化 SD-WAN 网络的 VPN 和路由配置。
- 创建 VPN 隧道，并通过自动执行以下任务来简化配置过程：
  - 生成分支机构的隧道接口。
  - 将 IP 地址分配给这些隧道接口。
  - 为SD-WAN重叠网络配置BGP。这些配置可确保中心和辐射之间的无缝连接，以及通过中心的辐射到辐射之间的无缝连接。
- 提供无缝路由，因为中心充当路由反射器并启用以下功能：
  - 在分支之间提供连接。
  - 根据分支的主用和备用隧道决定最佳路径。
- 要求最少的用户输入。
- 一次轻松添加多个分支机构。
- 提供简单的双 ISP 配置。
- 启用网络扩展。

使用 SD-WAN 向导的准则和限制

准则

- 配置两个集线器的 DVTI 时，请确保它们具有相同的 IPsec 隧道模式（IPv4 或 IPv6）。
- 在双中心SD-WAN拓扑中，中心可以位于不同的地理位置，并且背后有不同的受保护网络。要确保这些网络之间的直接通信，请确保配置以下内容：

  - 两个中心之间的基于路由的点对点 VPN 拓扑（**安全连接** > **站点间 VPN 和 SD-WAN**，点击**添加** > **基于路由的 VPN**）。
  - 中心之间的动态路由协议（**设备** > **设备管理**，点击设备名称并点击**路由**）。

- 为分支配置 IP 地址池时，请确保执行以下操作：
  - 必须取消选中 **允许过载** 复选框。
  - 如果使用多个池，则其 IP 地址不得重叠。
  - IP 地址不得与辐条上的任何接口重叠。
- 创建安全区域或接口组时，请选择 **接口类型** 作为 **路由**。
- 使用 Spoke 安全区配置访问控制策略，以允许进出 Spoke 的隧道流量。
- 在 ECMP 区域中配置分支设备的静态 VTI，以均衡应用流量负载。如果不配置 ECMP 区域，当主路径发生故障时，其余路径将用作备用路径。请注意，必须在 ECMP 区域中配置分支设备的静态 VTI，而非物理接口。此配置不属于 SD-WAN 向导。
- 在具有分支双 ISP 的 SD-WAN 拓扑中，分支的隧道身份和隧道源必须是唯一的。
- 如果分支设备属于多个 SD-WAN 拓扑，请确保在每个 SD-WAN 拓扑中使用相同的本地社区标记和学习路由社区标记。请注意，本地社区标记和学习路由社区标记必须互不相同。
- 如果设备仅配置了 IPv6 地址，则必须使用具有 IPv4 地址的环回接口或物理接口配置 BGP 路由器 ID（**设备** > **设备管理**，点击**路由** > **常规设置** > **BGP**）。
- 为所有 SD-WAN VPN 拓扑中的所有隧道配置唯一的本地 IKE 身份。
- 确保 SD-WAN 拓扑中的分支设备没有相同的受保护网络。
- 为 SD-WAN 和基于路由的 VPN 使用不同的 DVTI，以避免 IPsec 配置文件冲突和错误。
- 在更改 DVTI 编号接口的 IP 地址前，请确保关闭 DVTI 虚拟模板。

限制

- 使用 SD-WAN 向导，您最多可以在 SD-WAN 拓扑中配置两个中心。
- 对于每个分支，每个拓扑只能使用一个 WAN 接口。但是，对于双 ISP 设置，您可以使用第二个 WAN 接口配置第二个 SD-WAN 拓扑。有关详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例，第 1517 页。
- SD-WAN 向导不支持以下各项：
  - IKEv1
  - 中心和辐射型不支持集群设备，因为集群设备上不支持 VTI。
  - 外联网中心和辐射点，例如 ASA、思科 IOS、思科 Viptela、Umbrella、Meraki 或供应商设备。

配置 SD-WAN 拓扑的许可证要求

确保在智能许可证中启用导出控制功能，以便在 防火墙管理中心 中配置 SD-WAN 拓扑。

要验证是否为您的智能许可证账户启用了出口控制功能，请选择 **管理** > **许可证** > **智能许可证**。

使用 SD-WAN 向导的前提条件。

- 您必须是管理员用户。
- 中心设备的版本必须为 7.6.0 及更高版本。
- 分支设备的版本必须为 7.3.0 及更高版本。
- Firewall Threat Defense 设备必须具有可通过互联网路由的公共 IP 地址。IP 地址可以是静态地址或动态地址。
- 为Firewall Threat Defense设备的接口分配适当的逻辑名称和 IP 地址。例如，使用 内部 表示连接到 LAN 的接口，使用 外部 表示连接到互联网或 WAN 的接口。
- 如果使用基于证书的身份验证，则必须在中心和分支中注册证书。
- 配置路由、NAT 和 AC 策略，以确保设备之间的底层连接。
- 中心设备必须为 10.0 及更高版本，才能在与中心动态 VTI 关联的虚拟访问接口上启用 ECMP。
- Firewall Threat Defense 设备必须为 10.0 及更高版本，才能在 SVTI 和 DVTI 上启用 BFD 路由协议。

使用 SD-WAN 向导配置 SD-WAN 拓扑

SD-WAN 向导允许您在集中式总部和远程分支机构站点之间轻松配置 VPN 隧道。

开始之前

确保您查看 使用 SD-WAN 向导的前提条件。 ，第 1512 页 和 使用 SD-WAN 向导的准则和限制 ，第 1510 页。

过程

步骤 1 选择 **安全连接** > **站点间 VPN 和 SD-WAN**，然后点击**添加 (Add)**。

步骤 2 在 **拓扑名称** 字段中，输入 SD-WAN VPN 拓扑的名称。

步骤 3 点击 **SD-WAN 拓扑** 单选按钮，然后点击 **创建**。

步骤 4 配置集线器：

a) 点击 **添加集线器**。

b) 从 **设备** 下拉列表中选择中心 。

c) 点击 **动态虚拟隧道接口** 下拉列表旁边的 + 以为中心添加动态 VTI。

系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。然而，您必须配置 **隧道源**和 **借用 IP 地址**。有关详细信息，请参阅向中心添加动态虚拟隧道接口 ，第 1517 页。

d) 点击**确定**。

e) 在**中心网关 IP 地址**字段，输入中心 VPN 接口的公共 IP 地址或分支所连接的动态 VTI 的隧道源。

如果接口具有静态 IP 地址，则系统会自动填充 IP 地址。如果集线器位于 NAT 设备后面，则必须手动配置 NAT 后的 IP 地址。

f) 从**分支隧道 IP 地址池**下拉列表中选择地址池，或者点击 + 创建池。

添加分支时，向导会自动生成分支隧道接口，并从此IP地址池将IP地址分配给这些分支接口。

g) 点击 **添加** 以保存中心配置。

h) （可选）要添加辅助中心，请重复步骤 4a 至步骤 4f。

i) 选中 **ECMP** 复选框，以在 10.0 及更高版本的中心设备的动态VTI上启用等价多路径(ECMP)。

中心上所有连接至同一分支的虚拟访问接口均被归入一个ECMP区域。此功能通过多条路径向分支设备均衡流量负载。

j) 点击**下一步 (Next)**。

步骤 5 配置分支：

点击 **添加** 分支以添加单个分支设备，或点击 **添加分支**（**批量添加**）以将多个分支添加到您的拓扑。

- 点击 **添加分支**。在 **添加分支** 对话框中，配置以下参数：

1. 从 **设备** 下拉列表中选择分支。
2. 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。
3. 选中 **本地隧道 (IKE) 身份** 为此设备到远程对等体的 VPN 隧道启用唯一且可配置的身份。默认情况下，此选项处于已启用状态。
4. 从 **身份类型** 下拉列表中，选择以下选项之一：
   - **密钥 ID**-（默认值）此值自动填充为 *<sd-wan topologyname>_<device_IP_address>*，例如，sdwantopo1_192.168.0.200。您还可以指定您选择的密钥 ID。
   - **邮件 ID**- 指定最多 127 个字符的邮件 ID。
   - **IP 地址**-分支 VPN 接口的 IP 地址。
   - **自动**- 用于预共享密钥身份验证的辐条 VPN 接口的 IP 地址或用于基于证书的身份验证的证书可分辨名称 (DN)。
   - **主机名**-分支的完全限定主机名。
5. 点击 **保存** 以保存分支配置。

- 点击 **添加分支**（**批量添加**）。在 **添加批量分支** 对话框中，配置以下参数：

  1. 从 **可用设备** 列表中选择一个或多个设备，然后点击 **添加** 以将设备移至 **所选设备**。
  2. 使用以下方法之一选择分支的 VPN 接口：
     - 点击 **接口名称模式** 单选按钮，指定一个字符串以匹配分支的互联网或 WAN 接口的逻辑名称，例如，outside*、wan*。

       如果辐射具有多个具有相同模式的接口，则会为拓扑选择与模式匹配的第一个接口。
     - 点击 **安全区域** 单选按钮，从下拉列表中选择具有分支的 VPN 接口的安全区域，或点击 **+** 创建安全区域。
  3. 点击**下一步 (Next)**。

     该向导将验证轮辐是否具有具有指定模式的接口。仅向拓扑添加经过验证的设备。
  4. 点击**添加 (Add)**。
  5. 点击**下一步 (Next)**。

对于每个分支，向导会自动选择集线器的 DVTI 作为隧道源 IP 地址。

注释
如果中心的隧道源 IP 地址是 IPv6 地址，则向导会自动选择分支的所选接口的第一个 IPv6 地址。要编辑分支隧道源的 IPv6 地址，请点击分支旁边的编辑图标，然后选择一个 **IP 地址** 下拉列表中的 IPv6 地址，然后点击 **保存**。

步骤 6 为 SD-WAN 拓扑中的设备配置身份验证设置：

a) **身份验证类型**- 对于设备身份验证，可以使用手动预共享密钥、自动生成的预共享密钥或证书。
   - **预共享手动密钥**-指定此 VPN 连接的预共享密钥。
   - **预共享自动密钥**-（默认值）向导会自动定义此 VPN 连接的预共享密钥。在 **预共享密钥长度** 字段中指定密钥长度。范围为 1 到 127。
   - **证书 (Certificate)** - 当您将证书用作身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并适用其相互进行身份验证。

b) 从 **转换集** 下拉列表中选择一个或多个算法。
c) 从 **IKEv2 策略** 下拉列表中选择一个或多个算法。
d) 点击**下一步 (Next)**。

步骤 7 配置 SD-WAN 设置：

此步骤涉及自动生成分支隧道接口，以及重叠网络的 BGP 配置。

a) 从 **分支隧道接口安全区域** 下拉列表中选择一个安全区域，或点击 **+** 以创建一个安全区域，向导会自动将分支的自动生成的静态虚拟隧道接口 (SVTI) 添加到该安全区域。
b) 选中**在 VPN 重叠拓扑上启用 BGP** 复选框以自动执行 BGP 配置，例如覆盖网络隧道接口之间的邻居配置以及来自中心和分支的直接连接的 LAN 接口的基本路由重新分发。

c) 在 **自治系统编号** 字段中，输入自治系统 (AS) 编号。

自治系统 (AS) 编号是具有单一路由策略的网络的唯一编号。BGP 使用 AS 编号标识网络。分支 BGP 邻居配置是根据相应中心的 AS 编号生成的。范围是从 0 到 65536。

- 如果所有中心和辐射点都位于同一区域，则默认情况下，**64512** 是 AS 编号。
- 如果主中心和辅助中心位于不同的区域，则为主中心和分支配置 **64512** 作为 AS 编号，并且为辅助中心配置其他编号。

d) 在 **本地路由的社区标记** 字段，输入用于标记已连接和重新分发的本地路由的 BGP 社区属性。此属性可轻松实现路由过滤。

e) 选中 **重新分发连接的接口** 复选框，从下拉列表中选择一个接口组，或点击 **+** 以创建具有连接的内部或 LAN 接口的接口组，以便在重叠拓扑上重新分发 BGP 路由。

f) 选中 **启用BGP的多路径** 复选框，允许同时使用多个BGP路由到达同一目的地。此选项使BGP能够跨多个链路对流量进行负载均衡。

请注意，启用此选项后，BGP 多路径仅对分支设备启用。

g) （可选）请选中 **辅助中心在不同的自治系统** 中复选框。仅当此拓扑中有辅助中心时，才会显示此复选框。

h) 在**远程 AS 编号**字段中，输入辅助中心的自治系统 (AS) 编号。

i) 在 **获知路由的社区标记** 字段，输入 BGP 社区属性，用于标记通过 VPN 隧道从其他 SD-WAN 对等体获知的路由。仅当辅助集线器具有不同的AS编号时，才需要对eBGP配置使用此属性。仅当您在 SD-WAN 拓扑中配置了两个中心时，才会显示此字段。

j) 点击**下一步 (Next)**。

步骤 8 配置**高级设置**。

a) 从**发送至对等体的身份**下拉列表中，选择对等体在 IKE 协商期间用于标识自身的身份。

- **autoOrDN** -（默认值）根据连接类型确定 IKE 协商：预共享密钥使用 IP 地址，证书身份验证使用证书 DN。
- **IP 地址** - 使用交换 ISAKMP 身份信息的主机的 IP 地址。
- **主机名** - 使用交换 ISAKMP 身份信息的主机的完全限定域名。此名称包含主机名和域名。

b) 配置 **TrustSec (SGT) 设置**。

启用通过虚拟隧道接口进行 SGT 传播 - Cisco TrustSec 使用安全组标记 (SGT) 控制网络访问并实施流量策略。此选项在 VPN 拓扑的 SVTI 和 DVTI 上启用 SGT 传播。 要启用通过特定 SVTI 或 DVTI 进行 SGT 传播，请在各个设备中进行配置。请注意，Firewall Threat Defense 设备必须为 10.0.0 及更高版本。

c) 配置**双向转发检测 (BFD) 设置**。

启用双向转发检测路由 — BFD 是用于检测转发路径故障的协议。此选项可在 SVTI 和 DVTI 上启用 BFD 路由协议。当 BFD 检测到路径故障时，流量会通过新识别的路径重新路由。请注意，Firewall Threat Defense 设备必须为 10.0.0 及更高版本。

1. 从**间隔**下拉列表中，选择发送 BFD 控制数据包的时间单位（微秒或毫秒）。

2. 在**乘数**字段中，输入宣布对等体不可用之前允许连续丢失的 BFD 控制数据包数量。范围为 3 到 50 个数据包。
3. 在**最小发送和接收间隔**字段中，输入 BFD 控制数据包的最小发送和接收间隔。范围介于 50 到 999 毫秒或 50000 到 999000 毫秒之间。

步骤 9 点击 **完成** 以保存并验证 SD-WAN 拓扑。

您可以在 **站点间 VPN 摘要** 页面（**安全连接** > **站点间 VPN 和 SD-WAN**）中查看拓扑。将配置部署到所有设备后，您可以在此页面中查看所有隧道的状态。

下一步做什么

- 查看自动生成的分支 SVTI 及其 IP 地址 - 点击分支配置旁的编辑按钮，然后点击 **查看生成的隧道接口**。
- 建议在分支设备的 SVTI 上启用 ECMP。选择 **设备** > **设备管理**，然后点击**路由** > **ECMP**。请注意，在中心设备上启用 ECMP 时，分支设备的 SVTI 上不会自动启用 ECMP，必须在 SVTI 上手动启用 ECMP。
- 在中心和辐射点上部署配置。选择**部署**。选择设备并点击**部署**。
- 验证 SD-WAN 拓扑的隧道状态。有关详细信息，请参阅验证 SD-WAN 拓扑的隧道状态，第 1522 页。
- 为分支的隧道接口安全区域配置 ACL。选择**策略** > **安全策略** > **访问控制**。
- 建议在中心设备上启用 BGP 多路径。要在中心设备上启用 BGP 多路径，请执行以下操作：
  1. 选择 ECMP **设备** > **设备管理**，然后点击**路由**。
  2. 在**常规设置**下，点击 **BGP**。
  3. 选中**启用 BGP** 复选框以启用 BGP。
  4. 在 **AS 编号**字段中，输入在 SD-WAN 拓扑中配置的 AS 编号。
  5. 点击**保存**。
  6. 在左侧窗格中，选择 **BGP** > **IPv4 或 IPv6**，然后点击**常规**选项卡。
  7. 在**通过多个路径转发数据包**部分中，点击编辑图标。
  8. 配置**路径数量**和 **IBGP 路径数量**的值。建议将这些值配置为 8。
- 有关使用 SD-WAN 向导的配置示例的详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例，第 1517 页
- 在每个分支上，根据 WAN 接口的应用性能指标为应用感知路由或智能路径选择配置 PBR 策略。有关更多信息，请参阅 使用直接互联网接入 (DIA) 将应用流量从分支机构路由到互联网。

向中心添加动态虚拟隧道接口

在 SD-WAN 向导中，必须为每个集线器配置 DVTI。DVTI 使用虚拟模板为每个 VPN 会话动态生成独一无二的虚拟访问接口。

开始之前

在 SD-WAN 向导中，点击 **添加集线器**，然后从 **设备** 下拉列表中选择集线器。

过程

步骤 1 点击 **动态虚拟隧道接口 (Dynamic Virtual Tunnel Interface)** 下拉列表旁边的 **+** 以为中心添加 DVTI。

系统将显示 **添加虚拟隧道接口** 对话框，其中包含预填充的默认配置。

1. **隧道类型**：动态。
2. **名称**: <*tunnel_source_interface_logical name*>_dynamic_vti_<*tunnel_ID*。例如，outside_dynamic_vti_1。
3. **已启用** 复选框：默认选中。
4. **模板 ID**：DVTI 的唯一 ID。
5. **隧道源**：作为 DVTI 源的物理接口，默认情况下会被自动填充。
6. **IPsec 隧道模式**：默认为 IPv4。

步骤 2 从 **安全区域** 下拉列表中选择动态 VTI 的安全区域。

步骤 3 从 **借用 IP** 下拉列表中选择物理或环回接口，动态 VTI 接口将继承此 IP 地址。

确保使用不同于隧道源 IP 地址的 IP 地址。我们建议您使用环回 IP 地址。

步骤 4 点击 **确定** 以保存动态 VTI。

使用 SD-WAN 向导部署双 ISP 的配置示例

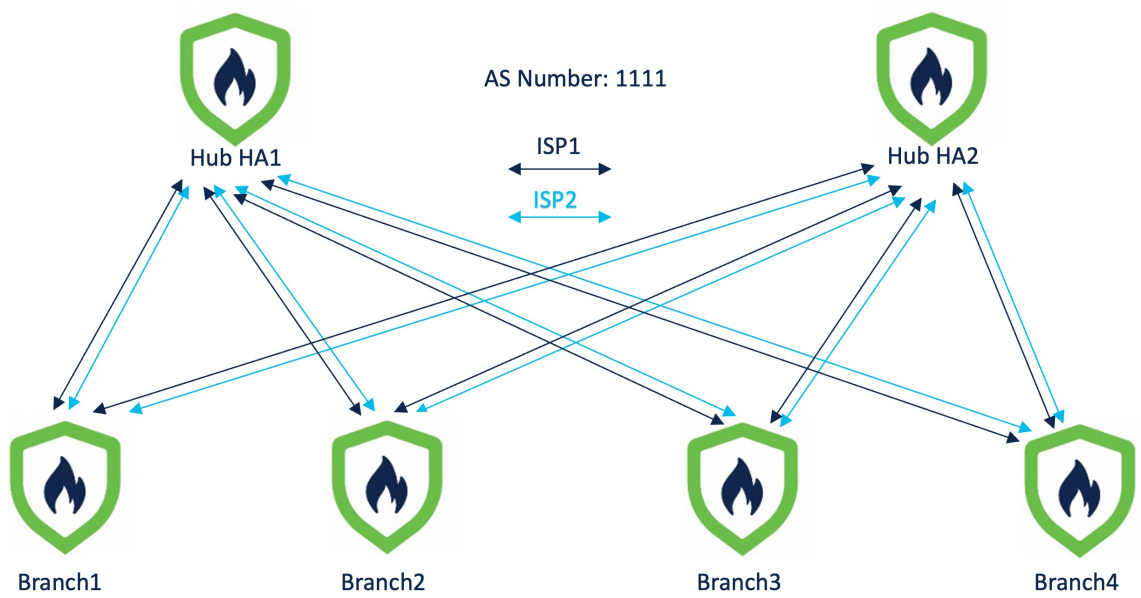
双 ISP 部署：同一区域中的两个中心和四个分支

在以下拓扑中，中心和辐射点位于单个区域中，AS 编号为 1111。中心和辐射点使用内部边界网关协议 (iBGP) 作为路由协议来交换路由信息。

- 中心 HA1 和中心 HA2 是总部的中心威胁防御设备。
- Branch1、Branch2、Branch3 和 Branch4 是分支机构的分支威胁防御设备。
- ISP1 是每个分支到 ISP1 的 VPN 接口。

- ISP2 是每个分支到 ISP2 的 VPN 接口。

图 *439:* 双 *ISP* 拓扑具有相同区域的两个中心和四个分支



要配置此拓扑，必须使用 SD-WAN 向导创建以下两个 SD-WAN 拓扑：

SD-WAN 拓扑 1

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支1、分之2、分支3、分支4
AS 编号	1111
VPN 接口（分支隧道源）	ISP1
隧道数量	8

SD-WAN 拓扑 1 中的隧道总数为 8。

SD-WAN 拓扑 2

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2

参数	值
分支	分支1、分之2、分支3、分支4
AS 编号	1111
VPN 接口（分支隧道源）	ISP2
隧道数量	8

SD-WAN 拓扑 2 中的隧道总数为 8。

此双 ISP 部署的 VPN 隧道总数为 16。



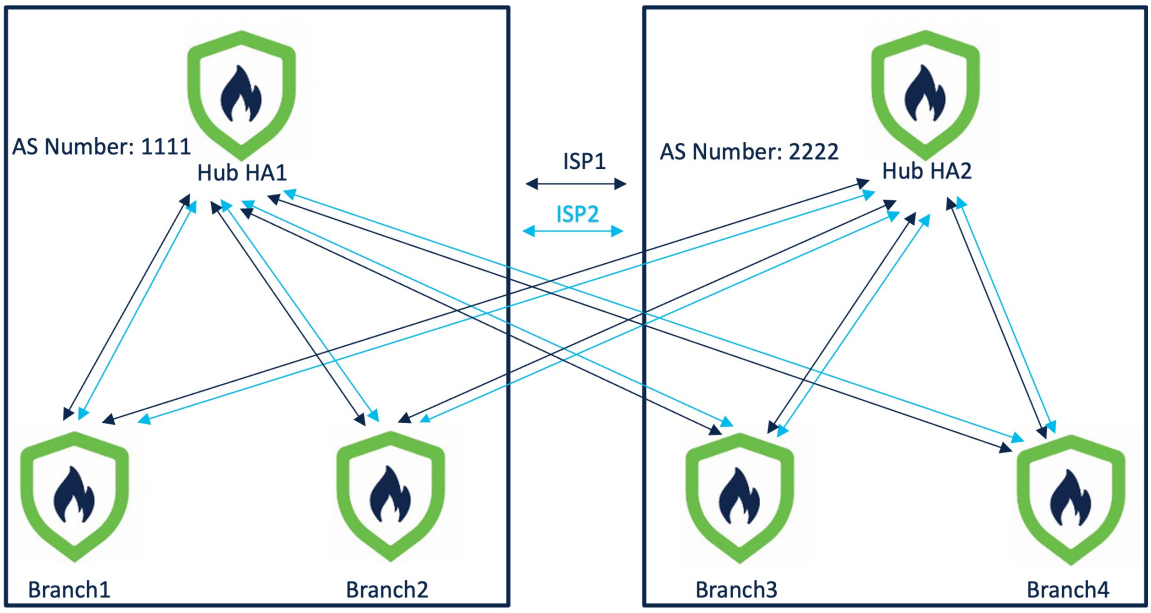
注释 如果集线器位于不同的地理位置，并且背后有不同的受保护网络，为确保这些网络之间的直接通信，请使用基于路由的 VPN 向导在两个集线器之间配置基于点对点路由的 VPN 拓扑。

双 ISP 部署：不同区域中的两个中心和四个分支

在以下双 ISP 拓扑中，集线器位于不同的区域，每个区域都有两个直连辐射点。集线器及其直连分支使用内部边界网关协议 (iBGP) 作为路由协议，而集线器使用外部边界网关协议 (eBGP) 交换路由信息。

- 中心 HA1 和中心 HA2 是总部的中心威胁防御设备。
- Branch1、Branch2、Branch3 和 Branch4 是分支机构的分支威胁防御设备。
- HQ1、Branch1 和 Branch2 位于一个区域，AS 编号为 1111。
- HQ2、Branch3 和 Branch4 位于一个区域，AS 编号为 2222。
- ISP1 是每个分支到 ISP1 的 VPN 接口。
- ISP2 是每个分支到 ISP2 的 VPN 接口。

图 *440:* 双 *ISP* 拓扑具有不同区域的两个中心和四个分支



要配置此拓扑，必须使用 SD-WAN 向导创建以下四个 SD-WAN 拓扑：

SD-WAN 拓扑 1

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支机构 1 和 分支机构 2
AS 编号	1111
辅助 AS 编号	2222
VPN 接口（分支隧道源）	ISP1

SD-WAN 拓扑 1 中的隧道数量为 4。

SD-WAN 拓扑 2

参数	值
主中心	集线器 HA1
辅助集线器	集线器 HA2
分支	分支机构 1 和 分支机构 2

参数	值
AS 编号	1111
辅助 AS 编号	2222
VPN 接口（分支隧道源）	ISP2

SD-WAN 拓扑 2 中的隧道数量为 4。

SD-WAN 拓扑 3

参数	值
主中心	集线器 HA2
辅助集线器	集线器 HA1
分支	分支机构 3 和分支机构 4
AS 编号	2222
辅助 AS 编号	1111
VPN 接口（分支隧道源）	ISP1

SD-WAN 拓扑 3 中的隧道数量为 4。

SD-WAN 拓扑 4

参数	值
主中心	集线器 HA2
辅助集线器	集线器 HA1
分支	分支机构 3 和分支机构 4
AS 编号	2222
辅助 AS 编号	1111
VPN 接口（分支隧道源）	ISP2

SD-WAN 拓扑 4 中的隧道数量是 4。

此双 ISP 部署的 VPN 隧道总数为 16。

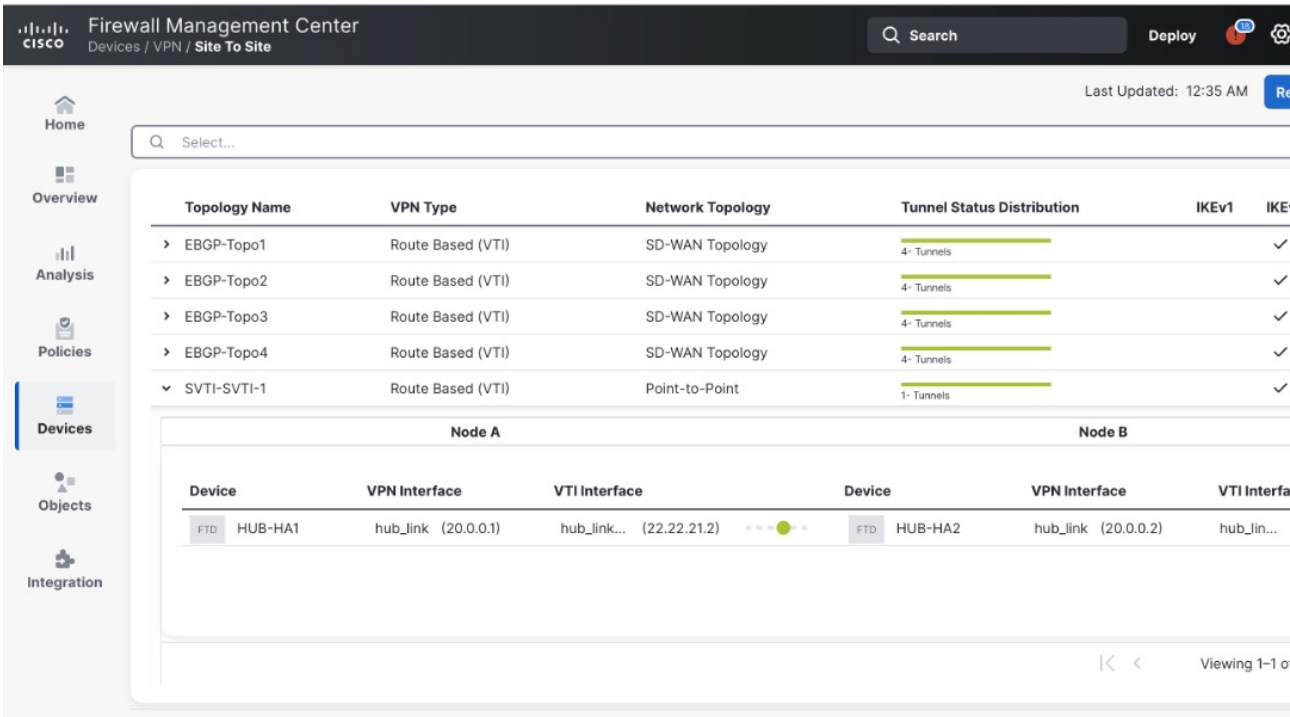
注释 如果集线器位于不同的地理位置，并且背后有不同的受保护网络，为确保这些网络之间的直接通信，请使用基于路由的 VPN 向导在两个集线器之间配置基于点对点路由的 VPN 拓扑。

验证 SD-WAN 拓扑的隧道状态

在站点间 VPN 摘要页面上验证隧道状态

要验证 SD-WAN 拓扑的 VPN 隧道是否已启动，请选择**安全连接** > **站点间 VPN 和 SD-WAN**。

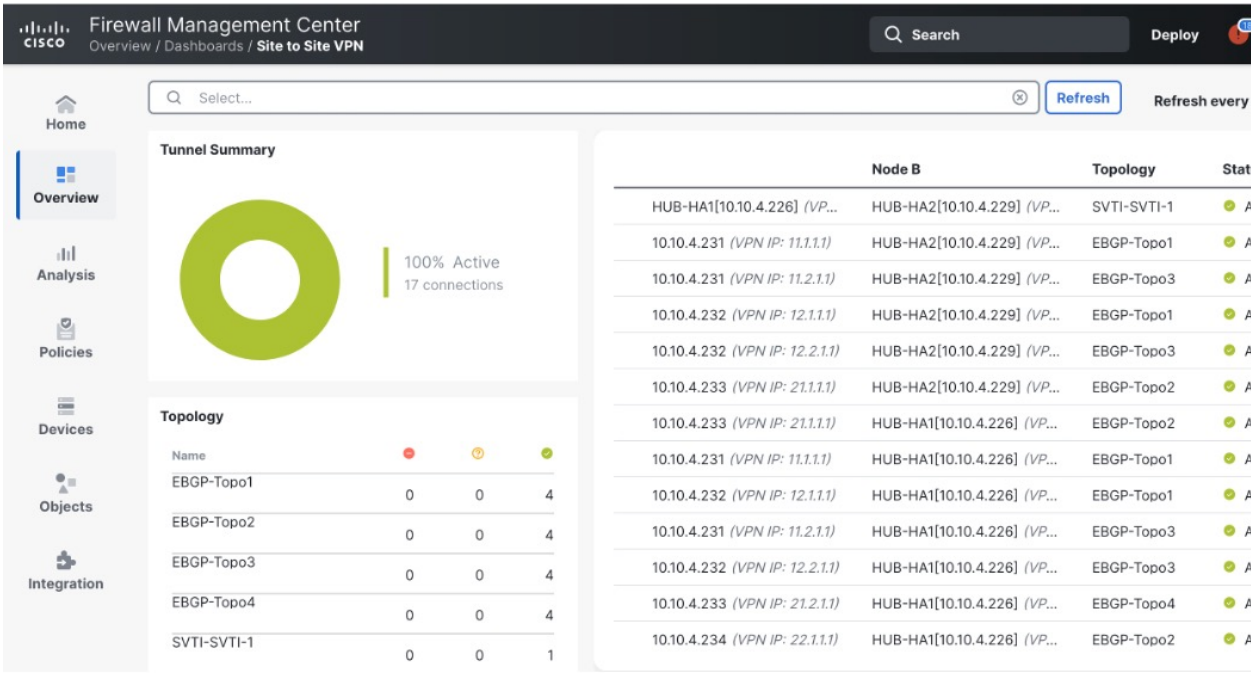
以下是五个 SD-WAN 拓扑，其中两个中心和四个分支位于不同的区域，连接到双 ISP：



在站点间 VPN 控制面板上验证隧道状态

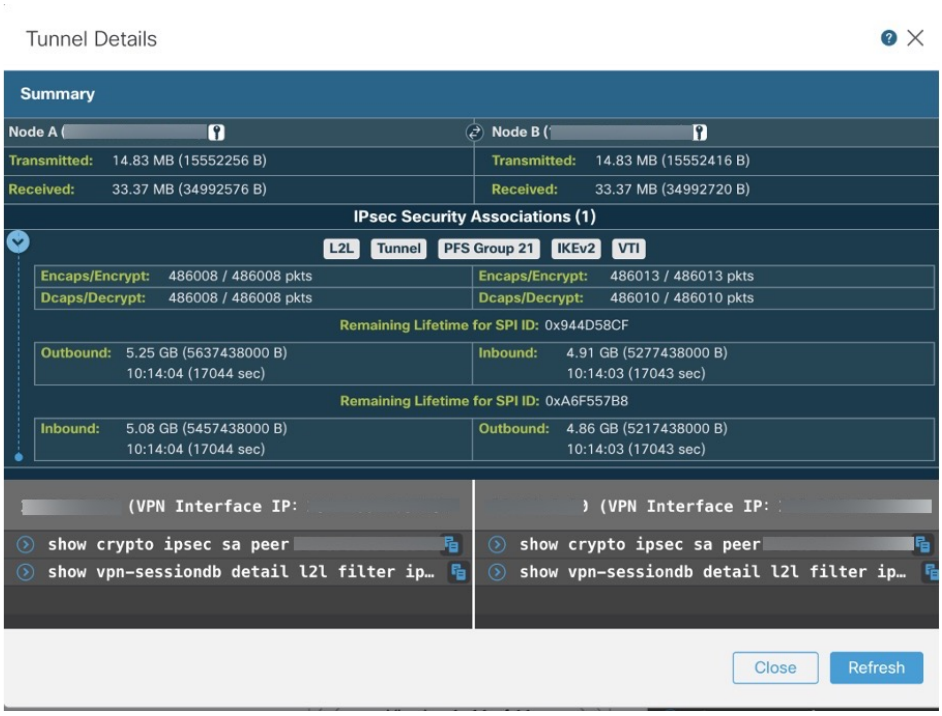
要查看 SD-WAN VPN 隧道的详细信息，请选择**洞察和报告** > **VPN 控制面板** > **站点间 VPN**。

以下是 SD-WAN 拓扑的 VPN 隧道，其中两个中心和四个分支位于不同的区域，连接到双 ISP：



要查看每个 VPN 隧道的更多详细信息，请执行以下操作：

1. 将鼠标悬停在隧道上。
2. 点击 **查看完整信息** (👁) 图标。系统将显示包含隧道详细信息和更多操作的窗格。
3. 点击侧窗格中的 **CLI 详细信息** 选项卡，查看 IPsec 安全关联的 show 命令和详细信息。



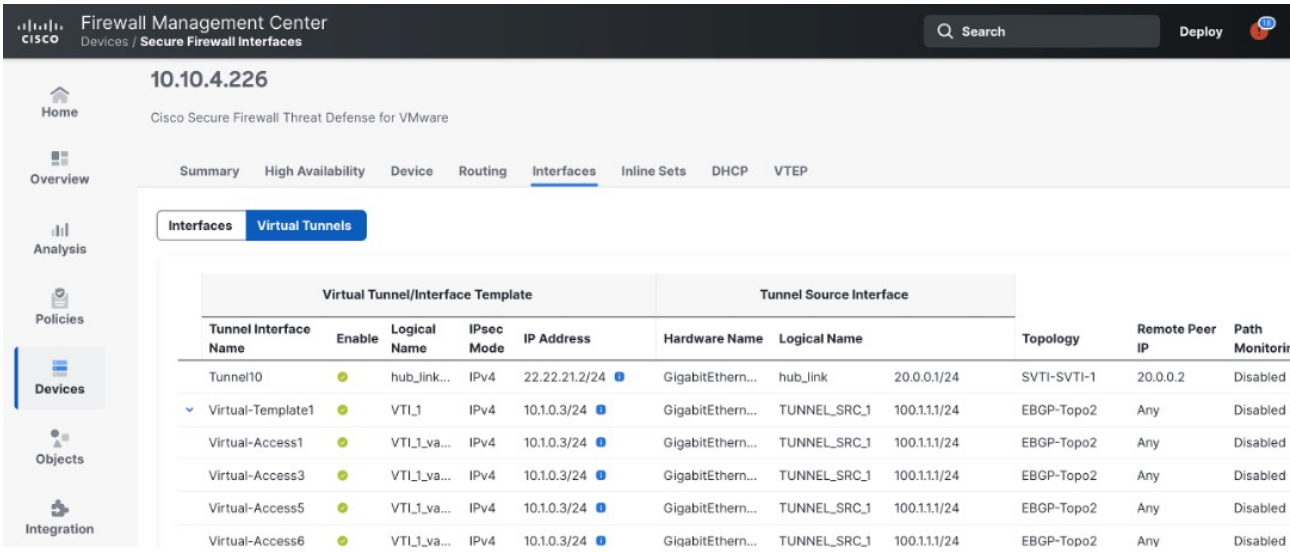
查看设备的虚拟隧道接口

要查看中心的动态 VTI 和分支的静态 VTI，请执行以下操作：

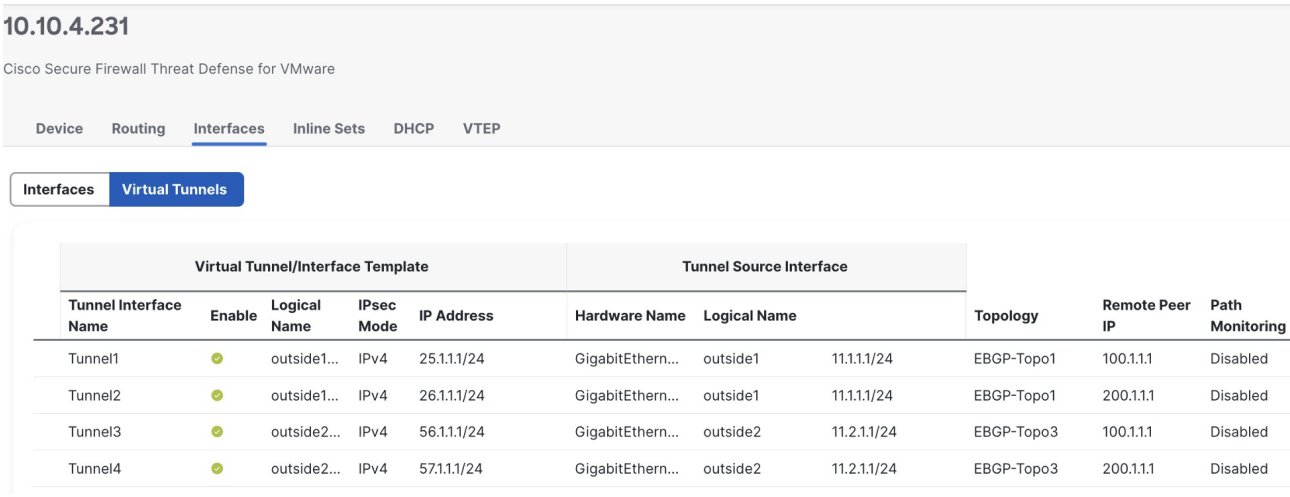
1. 选择**设备** > **设备管理**。
2. 点击中心或分支设备的编辑图标。
3. 点击**接口 (Interface)** 选项卡。
4. 点击**虚拟隧道 (Virtual Tunnels)** 选项卡。

   您可以查看每个 VTI 的详细信息，如名称、IP 地址、IPsec 模式、隧道源接口详细信息、拓扑结构和远程对等 IP。

下图显示了集线器的 DVTI 动态创建的虚拟接入接口示例：



下图显示了 SD-WAN 向导在轮辐上创建的静态隧道虚拟接口 (SVTI) 的示例：



SD-WAN 向导从中心的 IP 地址池将 IP 地址分配给这些隧道接口。

验证中心和分支上的路由

要验证 SD-WAN 拓扑的中心和辐射点的 BGP 配置，请执行以下操作：

1. 选择**设备** > **设备管理**。
2. 点击中心或分支设备的编辑图标。
3. 点击**设备 (Device)** 选项卡。
4. 点击 **常规 (General)** 卡中的 **CLI** 。系统将显示 **CLI 故障排除 (CLI Troubleshoot)** 窗口。
5. 在 **命令** 字段中输入以下命令，然后点击 **执行**：
   - **show route**
   - **show bgp summary**

SD-WAN 功能的使用案例

使用《Cisco Secure Firewall Threat Defense SD-WAN 设计和部署指南》，借助 Firewall Threat Defense 和防火墙管理中心来设计和部署 SD-WAN 架构。本指南介绍设计原则、配置工作流程和最佳实践。

如需了解利用 Cisco Secure Firewall 支持的 SD-WAN 功能的主要使用案例，请使用这些指南。

- 使用动态虚拟隧道接口 (DVTI) 简化分支机构与中心的通信
- 使用直接互联网接入 (DIA) 将应用流量从分支机构路由到互联网
- 使用 Umbrella 自动隧道保护互联网流量
- 为远程员工提供安全连接：使用中的 DIA、Umbrella 自动隧道和 DVTI
- 使用注册密钥和设备模板配置具有双 ISP 的 SD-WAN 分支机构
- 使用序列号和设备模板配置具有双 ISP 的 SD-WAN 分支机构

监控 SD-WAN 拓扑

-

Cisco SD-WAN 摘要控制面板

SD-WAN 摘要控制面板（**概述** > > **控制面板** > **SD-WAN 摘要** 分析 ）提供 WAN 设备及其接口的快照。**见解与报告** > **VPN 控制面板** > **SD-WAN 摘要**此控制面板可帮助您：

- 确定底层网络和重叠网络 (VPN) 拓扑的问题。

- 使用现有的 **运行状况监控**、 **设备管理**和 **站点间监控** 页面解决 VPN 问题。
- 监控 WAN 接口的应用性能指标。威胁防御系统会根据这些指标引导应用流量。

WAN 设备必须满足以下条件之一：

- 设备必须是一个 VPN 对等体。
- 设备必须有 WAN 接口。

WAN 接口必须满足以下条件之一：

- 接口已启用基于 IP 地址的路径监控。
- 接口具有策略型路由 (PBR) PBR 策略，并配置了至少一个应用来对其进行监控。

有关 PBR 策略和路径监控的详细信息，请参阅 策略型路由 ， 第 1259 页。

点击 **上行链路决策** 以查看 **VPN 故障排除** 页面。您可以查看 ID 为 880001 的系统日志。这些系统日志显示威胁防御接口，它通过这些接口根据配置的 PBR 策略引导流量。

要查看上述系统日志并查看此控制面板上的数据，请确保查看使用 SD-WAN 摘要控制面板的前提条件。

对于集群，此控制面板仅显示控制节点的应用性能指标，而不显示数据节点的应用性能指标。

使用 SD-WAN 摘要控制面板的前提条件

- 您必须是管理员、安全分析师或运维用户才能查看控制面板。
- 威胁防御设备必须为 7.2 或更高版本。
- 在 WAN 接口上启用基于 IP 的路径监控和基于 HTTP 的应用监控。
  1. 选择**设备** > **设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击要编辑的接口旁边的编辑图标。
  4. 点击 **路径监控 (Path Monitoring)** 选项卡。
  5. 选中**启用基于 IP 的监控 (Enable IP based Monitoring)** 复选框。
  6. 选中**启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框。
  7. 点击**确定 (OK)**。
- 配置 PBR 策略，其中至少有一个应用配置为对其进行监控：
  1. 选择**设备** > **设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击**路由**。

4. 在左侧窗格，点击 **策略型路由**。
5. 点击**添加 (Add)**。
6. 从 **入口接口** 下拉列表中，选择接口。
7. 点击 **添加** 以配置转发操作。
8. 配置相关参数。
9. 点击**保存**。

- 要查看 WAN 的应用性能指标，您必须：
  - 威胁防御设备必须是版本 7.4.1。
  - 在运行状况策略中启用 SD-WAN 模块的数据收集。
    1. 选择**故障排除** > **+ 显示更多** > **运行状况** > **策略** 。
    2. 点击**编辑运行状况策略 (Edit health policy)** 图标。
    3. 在 **运行状况模块** 选项卡，在 **SD-WAN**下，点击 **SD-WAN 监控** 切换按钮。
  - 为 PBR 策略配置应用。
    1. 选择**对象** > **访问列表** > **扩展**。
    2. 点击访问列表旁边的编辑图标，然后为 PBR 策略添加应用。
  - 使用四种应用指标之一为策略配置转发操作。
    1. 选择**设备** > **设备管理**。
    2. 点击要编辑的设备旁边的编辑图标。
    3. 点击**路由**。
    4. 在左侧窗格，点击 **策略型路由**。
    5. 点击要编辑的策略旁边的编辑图标。
    6. 在 **编辑策略型路由** 对话框中，点击相应 ACL 旁边的编辑图标。
    7. 在 **编辑转发操作** 对话框中，从 **接口排序** 下拉列表中选择以下选项之一：
       - **最小抖动**
       - **最大平均意见得分**
       - **最短往返时间**
       - **最小丢包率**

       如果选择 **接口优先级** 或 **顺序**，则不会在接口上启用应用监控。

- 在 WAN 接口上配置 ECMP：
  1. 选择**设备** > **设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击**路由**。
  4. 在左侧窗格中，点击 **ECMP**。
  5. 点击 **添加** 并指定 ECMP 区域的名称。
  6. 点击 **添加** ，将接口从 **可用接口** 移至 **所选接口**。
  7. 点击**确定 (OK)**。
- 确保流量通过接口。
- 在每个 WAN 设备上启用 DNS 检查，以便威胁防御设备可以执行 DNS 监听，并配置受信任的 DNS 服务器：
  1. 选择**设备** > **平台设置**。
  2. 点击要编辑的威胁策略旁边的编辑图标。
  3. 在左侧窗格中，点击 **DNS**。
  4. 点击 **DNS 设置** 选项卡。
  5. 选择 **启用按设备 DNS 域名解析** 复选框。
  6. 点击 **受信任的 DNS 服务器** 选项卡。
  7. 执行以下操作之一：
     - 点击 **Trust Any DNS 服务器** 切换按钮。
     - 请在 **指定 DNS 服务器**下，点击 **编辑**来添加受信任的 DNS 服务器。

- 要在点击**上行链路决策 (Uplink Decisions)** 时查看系统日志，必须执行以下操作：
  - 选择 **设备** > **平台设置**并创建或编辑威胁防御策略。
  - 在左侧窗格中，点击**系统日志 (Syslog)**。
  - 点击**日志记录设置 (Logging Setup)** 选项卡。
  - 选中**启动日志记录 (Enable Logging)** 复选框为威胁防御设备开启数据平面系统日志记录。
  - 点击**所有日志 (All Logs)** 单选按钮以启用对所有故障排除系统日志消息的日志记录。

    或者

    点击 **VPN 日志记录 (VPN Logs)** 单选按钮以启用仅记录 VPN 故障排除消息。
  - 点击**保存**。

使用 SD-WAN 摘要控制面板监控 WAN 设备和接口

SD-WAN 摘要控制面板在 **概述选项卡** 上具有以下 构件：

- 排名靠前的应用， 第 1529 页
- WAN 连接， 第 1529 页
- VPN 拓扑， 第 1529 页
- WAN 接口吞吐量， 第 1530 页
- 设备清单， 第 1530 页
- WAN 设备运行状况， 第 1530 页

排名靠前的应用

此构件显示根据吞吐量排名的前 10 个应用。

从 **显示最后时间** 下拉列表，选择构件数据的时间范围。范围为 15 分钟到两周。

WAN 连接

此构件提供 WAN 接口的状态摘要。它显示处于 **在线**、 **离线** 或 **无数据** 状态的 WAN 接口的数量。请注意，您无法使用此构件监控子接口。

点击 **查看所有接口**，以在“运行状况监控器”页面中查看有关接口的更多详细信息。

如果 WAN 接口处于 **离线** 或 **无数据** 状态，您可以从运行状况监控页面进行故障排除：

1. 在 **监控** 窗格中，展开 **设备**。
2. 点击相应的 WAN 设备可查看设备特定的运行状况详细信息。
3. 点击 **接口** 选项卡可查看特定时间的接口状态和汇聚流量统计信息。

   或者，您可以点击 **查看系统和故障排除详细信息**。系统将显示运行状况监控页面，其中包含所有必要的详细信息。

VPN 拓扑

此构件提供站点间 VPN 隧道状态的摘要。它显示 **活动**、 **非活动**和 **无活动数据** VPN 隧道的数量。

点击 **查看所有连接**，在 **站点间 VPN 监控** 控制面板中查看 VPN 隧道详细信息。

如果隧道处于 **非活动** 或 **无活动数据** 状态，您可以使用 **站点间 VPN 监控控制** 面板进行故障排除。在**隧道状态 (Tunnel Status)** 构件中，将光标悬停在拓扑上，点击 **视图** () 并执行以下操作之一：

- 点击 **CLI 详细信息** 选项卡以查看 VPN 隧道的详细信息。
- 点击 **数据包跟踪器** 选项卡，为拓扑使用数据包跟踪器工具。

WAN 接口吞吐量

此构件会监控所选时间段内 WAN 接口的平均吞吐量。

接口吞吐量分为四个频段。这些详细信息有助于成本规划和资源配置。从**显示最后时间**下拉列表，选择构件数据的时间范围。范围是从 15 分钟到两周。

点击 **查看运行状况监控**，以在“运行状况监控”页面中查看有关接口的更多详细信息。

设备清单

此构件根据型号列出所有托管设备并对其进行分组。

点击 **查看设备管理**，在 **设备管理** 页面中查看有关设备的更多详细信息。

WAN 设备运行状况

此构件根据 WAN 设备的运行状况显示设备计数。您可以查看出现错误、警告或处于 **禁用** 状态的设备数量。

点击 **查看运行状况监控**，查看警报并快速识别、隔离和解决问题。

如果设备的运行状况受到影响，您可以从运行状况监控页面进行故障排除。

1. 在 **监控** 窗格中，展开 **设备**。
2. 点击相应的 WAN 设备可查看设备特定的运行状况详细信息。
3. 点击 **查看系统和故障排除详细信息**。系统将显示运行状况监控页面，其中包含所有必要的详细信息。

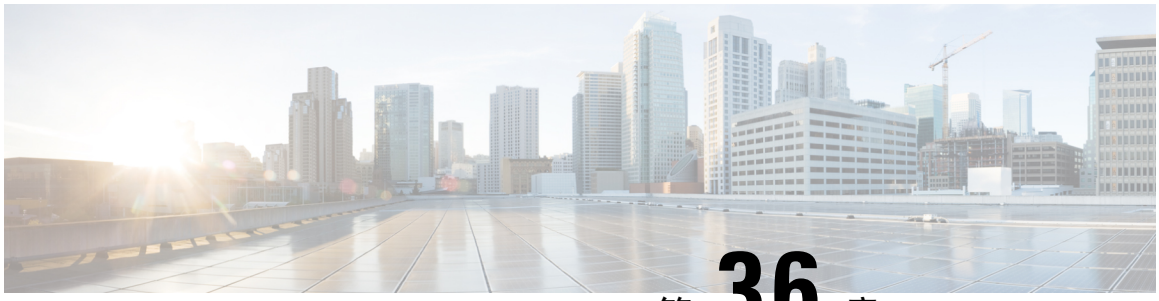
设备可能由于多种原因而处于 **禁用** 状态，包括以下原因：

- 禁用管理接口。
- 设备已关闭。
- 设备正在升级。

使用 SD-WAN 摘要控制面板监控 WAN 接口的应用性能指标

在 **应用监控** 选项卡中，您可以选择 WAN 设备并查看相应 WAN 接口的应用性能指标。这些指标包括抖动、往返时间 (RTT)、平均意见得分 (MOS) 和丢包。

默认情况下，指标数据每 5 分钟刷新一次。您可以更改刷新时间；范围为 5 到 30 分钟。您可以以表格和图形格式查看指标。对于每个 WAN 接口，表中列出了指标的最新值。对于图形数据，您可以选择最多 24 小时的时间间隔来查看相应 WAN 接口的指标数据。



第 36 章

远程访问 VPN

远程访问虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程访问 VPN。

- 远程访问 VPN 概述， 第 1531 页
- 远程接入 VPN 的许可证要求， 第 1537 页
- 远程接入 VPN 的要求和前提条件， 第 1537 页
- 远程访问 VPN 的准则和限制， 第 1538 页
- 配置新的远程访问 VPN 连接， 第 1541 页
- 创建现有远程接入 VPN 策略的副本， 第 1551 页
- 设置远程访问 VPN 策略的目标设备， 第 1551 页
- 将本地领域与远程接入 VPN 策略相关联， 第 1552 页
- 其他远程访问 VPN 配置， 第 1552 页
- 自定义远程接入 VPN AAA 设置， 第 1608 页
- 高级 Secure Client 配置， 第 1628 页
- 远程访问 VPN 示例， 第 1637 页
- 监控远程访问 VPN， 第 1642 页
- 远程接入 VPN 的功能历史记录， 第 1644 页

远程访问 VPN 概述

Cisco Secure Firewall Threat Defense 提供安全的网关功能，支持远程访问 SSL 和 IPsec-IKEv2 VPN。全隧道客户端， 安全客户端，可通过 SSL 和 IPsec-IKEv2 安全地连接远程用户的安全网关。客户端与 Firewall Threat Defense 协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接

安全客户端 是终端设备上通过远程 VPN 连接 Firewall Threat Defense 设备的唯一受支持客户端。该客户端为远程用户提供了 SSL 或 IPsec-IKEv2 VPN 客户端，而无需网络管理员在远程计算机上安装和配置客户端。连接后，即可从安全网关中部署适用于 Windows、Mac 和 Linux 的 安全客户端。从平台应用商店可安装适用于 Apple iOS 和 Android 设备的 安全客户端 应用。

使用远程访问 VPN 策略向导可设置 SSL 和 IPsec-IKEv2 远程访问 VPN 的基本功能。然后，根据需要增强策略配置并将其部署到您的 Firewall Threat Defense 安全网关设备。

远程访问 VPN 功能

下表介绍了 Cisco Secure Firewall Threat Defense 远程访问 VPN 的功能：

表 *89*: 远程访问 *VPN* 功能

	说明
Cisco Secure Firewall Threat Defense 远程访问 VPN 功能	• 使用 安全客户端 的 SSL 和 IPsec-IKEv2 远程访问。 • Secure Firewall Management Center 支持所有组合，如 IPv4 隧道上的 IPv6。 • 对 防火墙管理中心 和 防火墙设备管理器的配置支持。特定于设备的覆盖。 • 支持 Secure Firewall Management Center和 Firewall Threat Defense HA 环境。 • 支持多个接口和多个 AAA 服务器。 • 使用 RADIUS CoA 或 RADIUS 动态授权提供快速遏制威胁支持。 • 支持 Cisco 安全客户端 版本 4.7 或更高版本的 DTLS v1.2 协议。 • Secure Client 客户端模块支持远程访问 VPN 连接的其他安全服务。 • VPN 负载均衡。

	说明
AAA 功能	• 使用自签名或 CA 签名的身份证书的服务器身份验证。 • 使用 RADIUS 或 LDAP 或 AD 的基于 AAA 用户名和密码的远程身份验证。 • RADIUS 组和用户授权属性，以及 RADIUS 记帐。 • 提供使用其他 AAA 服务器进行辅助身份验证的双重身份验证支持。 • 使用 VPN 身份的 NGFW 访问控制集成。 • 使用 Secure Firewall Management Center Web 界面的 LDAP 或 AD 授权属性。 • 支持使用 SAML 2.0 的单一登录。 • 支持使用 Microsoft Azure 的多个身份提供程序信任点，这些信任点可以具有相同实体ID的多个应用，但具有唯一身份证书。 • 根据地理位置限制远程访问 VPN 连接。
VPN 隧道功能	• 地址分配。 • 拆分隧道 • 拆分 DNS。 • 客户端防火墙 ACL。 • 最大连接和空闲时间的会话超时。
远程访问 VPN 监控功能	• 新的 VPN 控制面板构件，按持续时间、客户端应用等各个特性显示 VPN 用户。 • 远程访问 VPN 事件，包括身份验证信息，如用户名和 OS 平台。 • 使用 Firewall Threat Defense统一 CLI 提供的隧道统计信息。

安全客户端 组件

安全客户端 部署

远程接入 VPN 策略可包括 安全客户端映像 和 安全客户端配置文件，以便分发到连接终端。您也可以使用其他方法分发客户端软件。请参阅 Cisco Secure Client（包括 AnyConnect）管理指南，版本 5 中的 部署 *Cisco Secure Client* 一章。

在先前未安装客户端的情况下，远程用户可以在他们的浏览器中输入配置为接受 SSL 或 IPsec-IKEv2 VPN 连接的接口的 IP 地址。除非安全设备被配置为将 http:// 请求重定向到 https://，否则远程用户必须以 https://地址形式输入 URL。在用户输入 URL 后，浏览器将连接该接口并显示登录屏幕。

在用户登录后，如果安全网关将用户识别为需要 VPN 客户端，则会下载与远程计算机的操作系统匹配的客户端。下载后，客户端会自行安装和配置、建立安全连接并在连接停止后自行保留或卸载（取决于安全设备配置）。如果是以前安装的客户端，登录后 Firewall Threat Defense 安全网关会检查客户端版本，并根据需要进行升级。

安全客户端 操作

当客户端与安全设备协商连接时，客户端将使用传输层安全 (TLS) 以及（可选）或数据报传输层安全 (DTLS) 协议进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

当 IPsec-IKEv2 VPN 客户端发起到安全网关的连接时，协商包括通过互联网密钥交换 (IKE) 验证设备，然后使用 IKE 扩展身份验证 (Xauth) 进行用户验证。系统会将群组配置文件推送到 VPN 客户端，并创建 IPsec 安全关联 (SA) 来完成 VPN。

安全客户端配置文件 和编辑器

安全客户端配置文件 是一组以 XML 文件形式存储的配置参数，VPN 客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

您可以使用 安全客户端配置文件编辑器配置配置文件。此编辑器是一款方便的基于 GUI 的配置工具，作为 安全客户端 软件包的一部分提供。该程序可独立于 防火墙管理中心 而运行。

远程访问 VPN 身份验证

远程访问 VPN 服务器身份验证

Cisco Secure Firewall Threat Defense 安全网关通常使用证书来识别和验证自己到 VPN 客户端终端的连接。

当使用远程访问 VPN 策略向导时，您可以在目标 Firewall Threat Defense 设备上注册选定的证书。在向导中的**访问和证书**阶段，选择“在目标设备上注册所选的证书对象”选项。证书注册过程将在指定设备上自动执行。完成远程访问 VPN 策略配置时，您可以在设备证书主页下查看已注册证书的状态。该状态清晰指明了证书注册是否成功。您的远程访问 VPN 策略配置现已完成，可以进行部署。

有关如何获得安全网关证书（也称为PKI注册）的信息，请参阅证书，第2743页。此章详细说明了如何配置、注册和维护网关证书。

远程访问 VPN 客户端 AAA

对于SSL和IPsec-IKEv2，可只使用用户名和密码、只使用证书或同时使用这两种方法对远程用户进行身份验证。

注释 如果您的部署中正在使用客户端证书，则必须将它们添加到独立于Cisco Secure Firewall Threat Defense或Secure Firewall Management Center的客户端平台中。不提供SCEP或CA服务等设施来为客户端填充证书。

AAA服务器支持使用托管设备作为安全网关来确定用户身份（身份验证）、允许用户执行的操作（授权）以及用户执行的操作（记帐）。AAA服务器的一些示例有RADIUS、LDAP/AD、TACACS+和Kerberos.。对于Firewall Threat Defense设备上的远程访问VPN，支持使用AD、LDAP和RADIUS AAA服务器进行身份验证。

请参阅 了解权限和属性的策略实施 部分以了解更多有关远程访问 VPN 授权的信息。

在添加或编辑远程访问 VPN 策略之前，必须配置要指定的领域和 RADIUS 服务器组。有关详细信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页和添加 RADIUS 服务器组，第 2620 页。

如果没有配置 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器，只能解析 IP 地址。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关相集成。

注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；`domain\username` 或 `username@domain` 格式无效。（Active Directory 将此用户名视为 *logon* 名称，有时也视为 `sAMAccountName`。）有关详细信息，请参阅 MSDN 上的用户命名属性。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接进行身份验证后，远程用户将接受 *VPN* 身份。Cisco Secure Firewall Threat Defense安全网关上的身份策略将使用此 VPN 身份来识别和过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。使用访问控制策略可阻止或允许远程用户访问您的网络资源。

有关详细信息，请参阅关于身份策略，第 2211 页和访问控制策略，第 1701 页部分：

相关主题

配置远程访问 VPN 的 AAA 设置，第 1555 页

了解权限和属性的策略实施

Cisco Secure Firewall Threat Defense设备支持将用户授权属性（也称为用户权利或权限）应用于来自外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或 Firewall Threat Defense设备上的组策略的 VPN 连接。如果 Firewall Threat Defense设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

Firewall Threat Defense设备按照以下顺序应用属性：

1. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
2. **在 Firepower Threat Defense 设备上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS Class 属性 IETF-Class-25 (OU=group-policy) 值， Firewall Threat Defense 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
3. **连接配置文件 (也称为隧道组) 分配的组策略** - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。



注释 Firewall Threat Defense设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。如果分配给连接配置文件的组策略上的属性没有被用户属性或来自 AAA 服务器的上述组策略所覆盖，则这些属性将用于用户会话。

相关主题

配置远程访问 VPN 的 AAA 设置 ， 第 1555 页

了解 AAA 服务器连接

必须能够从 Firewall Threat Defense 设备访问 LDAP、AD 和 RADIUS AAA 服务器以实现预期目的：仅用户身份处理、仅 VPN 身份验证或这两种活动。AAA 服务器在远程接入 VPN 中被用于以下活动：

- **用户身份处理 (User-identity handling)** - 必须能够通过管理接口访问服务器。

  在 Firewall Threat Defense 设备上管理接口具有区别于数据接口的单独路由过程和配置。

- **VPN 身份验证 (VPN authentication)** - 必须能够通过一个数据接口或管理接口来访问服务器。

  要使用管理接口，您必须明确选择管理接口作为源接口。不能使用其他管理专用接口。

要为两个活动使用相同的 AAA 服务器，建议将管理接口指定为源接口。

有关不同接口的详细信息，请参阅常规防火墙接口 ， 第 753 页。

部署后，请使用以下 CLI 命令从 Firewall Threat Defense设备监视和故障排除 AAA 服务器连接：

- **show aaa-server** 显示 AAA 服务器统计信息。
- **show network** 并且 **show network-static-routes** 或者查看管理接口默认路由和静态路由。
- **show route** 查看数据流量路由表项。

- **ping system** 和 **traceroute system** 以验证通过管理接口到 AAA 服务器的路径。
- **ping interface** *ifname* 和 **traceroute** *destination* 验证通过数据接口到 AAA 服务器的路径。
- **test aaa-server authentication** 和 **test aaa-server authorization** 测试 AAA 服务器上的身份验证和授权。
- **clear aaa-server statistics** *groupname* 或 **clear aaa-server statistics protocol** *protocol* 按组或协议清除 AAA 服务器统计信息。
- **aaa-server** *groupname* **active host** *hostname* 激活发生故障的 AAA 服务器；或 **aaa-server** *groupname* **fail host** *hostname* 使 AAA 服务器发生故障。
- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization** 和 **debug aaa accounting**。

远程接入 VPN 的许可证要求

威胁防御 许可证

Firewall Threat Defense FTD 远程访问 VPN 需要 强加密 和以下 安全客户端许可证之一：

- Secure Client Advantage
- Secure Client Premier
- 仅限 Secure Client VPN

远程接入 VPN 的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

远程访问 VPN 的准则和限制

远程访问 VPN 策略配置

- 您仅可通过使用向导来添加新的远程访问 VPN 策略。您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存任何策略。
- 两个用户必须 不 同时编辑远程访问 VPN 策略，但 Web 界面不会阻止同时编辑。如果发生这种情况，保留最后保存的配置。
- 如果为 Cisco Secure Firewall Threat Defense 设备分配了远程访问 VPN 策略，则无法将该设备从一个域移至另一个域。
- 使用 ECMP 时，远程访问 VPN 不支持 SSL。我们建议您使用 IPsec-IKEv2。
- 远程访问 VPN 不支持集群。
- 如果存在配置错误的 Firewall Threat Defense NAT 规则，远程访问 VPN 连接可能会失败。
- 如果使用 DHCP 向客户端提供 IP 地址，并且客户端无法获取地址，请检查 NAT 规则。适用于 RA VPN 网络的任何 NAT 规则都应包括路由查找选项。路由查找可以帮助确保 DHCP 请求通过适当的接口发送到 DHCP 服务器。
- 只要使用的是 IKE 端口 500/4500 或 SSL 端口 443 或有一些 PAT 转换处于活动状态，则无法在同一端口上配置 安全客户端 IPSec-IKEv2 或 SSL 远程访问 VPN，因为无法在这些端口上启动服务。配置远程访问 VPN 之前，不得在 Firewall Threat Defense 设备上使用这些端口。
- 在使用向导配置远程访问 VPN 时，可以创建内联证书注册对象，但不能使用它们安装身份证书。证书注册对象用于在被配置为远程访问 VPN 网关的 Firewall Threat Defense设备上生成身份证书。在将远程访问 VPN 配置部署到该设备之前，在该设备上安装身份证书。

  有关如何根据证书注册对象安装身份证书的更多信息，请参阅对象管理器，第 2610 页。
- ECMP 区域接口可在启用 IPsec 的远程访问 VPN 中使用。
- ECMP 区域接口不能在启用 SSL 的远程访问 VPN 中使用。如果属于安全区域或接口组的所有远程访问 VPN 接口也属于一个或多个 ECMP 区域，则部署远程访问 VPN（启用 SSL）配置会失败。但是，如果只有属于安全区域或接口组的一些远程访问 VPN 接口也属于一个或多个 ECMP 区域，则远程访问 VPN 配置的部署会成功排除这些接口。
- 更改远程访问 VPN 策略配置后，请重新部署对 Firewall Threat Defense 设备的更改。部署配置更改所需的时间取决于多个因素，例如策略和规则的复杂性，发送到设备的配置的类型和数量以及内存和设备型号。在部署远程访问 VPN 策略更改之前，请查看 部署配置更改的最佳实践，第 178 页。
- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。
- Firewall Threat Defense 如果第三方客户端发送空用户代理， 不接受远程访问 VPN 会话。

- 您可以使用 FlexConfig 配置浏览器代理。
- 在具有高可用性的远程分支部署 (RBD) 中，当您中断高可用性对时，备用设备的 RBD WAN 接口上的 RA VPN 策略分配和 VPN 配置将被删除。
- 如果领域的目录超过 16 个目录，则在 RA VPN 连接期间仅部署领域中的前 16 个目录。
- 当在 Firewall Threat Defense 上禁用 **已解密流量的绕过访问控制策略** 并且 ISE 发出 DACL 时，首先将流量与 ACP 进行匹配：如果允许，则继续进行 DACL 检查；如果被拒绝，则将绕过 DACL 匹配。

并发 VPN 会话容量规划（Firewall Threat Defense Virtual 型号）

最大并发 VPN 会话数由 Firewall Threat Defense Virtual 安装的智能许可授权层管理，并通过速率限制器实施。根据已许可的设备型号，设备上允许的并发远程访问VPN会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firewall Threat Defense Virtual5	50
Firewall Threat Defense Virtual10	250
Firewall Threat Defense Virtual20	250
Firewall Threat Defense Virtual30	250
Firewall Threat Defense Virtual50	750
Firewall Threat Defense Virtual100	10,000

并发 VPN 会话容量规划 （硬件型号）

最大并发VPN会话数受特定于平台的限制约束，而与许可证无关。根据设备型号，设备上允许的并发远程访问VPN会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000

设备型号	最大并发远程访问 VPN 会话数
Cisco Secure Firewall 3110	3000
Cisco Secure Firewall 3120	6000
Cisco Secure Firewall 3130	15,000
Cisco Secure Firewall 3140	20,000
Firepower 4100，所有型号	10,000
Firepower 9300 设备，所有型号	20,000
ISA 3000	25

有关其他硬件型号的容量，请联系您的销售代表。



注释 一旦达到每个平台的最大会话限制，Firewall Threat Defense设备就会拒绝 VPN 连接。连接通过系统日志消息来拒绝。请参阅系统日志消息指南中的系统日志消息 %ASA-4-113029 和 %ASA-4-113038。有关详细信息，请参阅 Cisco Secure Firewall ASA 系列系统日志消息。

控制 VPN 的密码使用

为防止使用大于 DES 的密码，在 防火墙管理中心中的下列位置提供了预部署检查：

设备 > 平台设置，点击 **编辑**，然后点击**SSL**。

安全连接 > 远程访问 VPN中，点击 **编辑**，然后从 “**高级**” 下拉列表中选择 **IPsec**。

有关 SSL 设置和 IPsec 的详细信息，请参阅 SSL ，第 1007 页 和 配置远程访问 VPN IPsec/IKEv2 参数 ，第 1586 页。

身份验证、授权和记帐

在拓扑中的每台设备上配置 DNS，以便使用远程访问 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名的 URL 和具有 FQDN 或主机名的 CA 服务器；只能解析 IP 地址。

您可以使用**平台设置 (Platform Settings)** 来配置 DNS。有关详细信息，请参阅DNS ，第 977 页和DNS 服务器组 ，第 2640 页。

客户端证书

如果您的部署中正在使用客户端证书，则必须将它们添加到独立于 Cisco Secure Firewall Threat Defense 或 Secure Firewall Management Center的客户端平台中。不提供 SCEP 或 CA 服务等设施来为客户端填充证书。

不支持的 安全客户端 功能

唯一支持的 VPN 客户端是思科 安全客户端。不支持任何其他客户端或本机 VPN。在 VPN 连接方面不支持无客户端 VPN；它只用于使用 Web 浏览器部署 Secure Client 客户端。

注释 在 Firewall Threat Defense 设备上使用多个 安全客户端 软件包可能会增加内存使用量并影响设备的性能。我们建议您不要在低端威胁防御设备上使用多个安全客户端软件包，以避免因内存耗尽而导致连续重启。

在连接到 Firewall Threat Defense 安全网关时，不支持以下 安全客户端 功能：

- TACACS、Kerberos（KCD 身份验证和 RSA SDI）以及 SDI。

配置新的远程访问 VPN 连接

本节介绍如何使用 Cisco Secure Firewall Threat Defense 设备作为 VPN 网关和 Cisco 安全客户端 作为 VPN 客户端配置新的远程访问 VPN 策略。

步骤	相应操作	更多信息
1	查看准则和前提条件。	远程访问 VPN 的准则和限制，第 1538 页 配置远程访问 VPN 的前提条件，第 1541 页
2	使用向导来添加新的远程访问 VPN 策略。	创建新的远程访问 VPN 策略，第 1542 页
3	更新设备上部署的访问控制策略。	在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 1545 页
4	（可选）如果在设备上配置了 NAT，请配置 NAT 免除规则。	（可选）配置 NAT 豁免，第 1546 页
5	配置 DNS。	配置 DNS，第 1547 页
6	添加 Secure Client 配置文件。	添加 安全客户端配置文件 XML 文件，第 1547 页
7	部署远程访问 VPN 策略。	部署配置更改，第 180 页
8	（可选）验证远程访问 VPN 策略配置。	检验配置，第 1550 页

配置远程访问 VPN 的前提条件

- 部署 Cisco Secure Firewall Threat Defense 设备并配置 Secure Firewall Management Center，以便在启用导出控制功能的情况下管理具有所需许可证的设备。有关详细信息，请参阅VPN 许可，第 1432 页。

- 配置用于为每台充当远程访问 VPN 网关的 Firewall Threat Defense 设备获取身份证书的证书注册对象。
- 配置远程访问 VPN 策略使用的任何 AD 或 LDAP 域。
- 确保 Firewall Threat Defense 设备可以访问 AAA 服务器。配置路由（**设备** > **设备管理**，点击**编辑**图标。从左侧窗格中选择**路由**），以确保与 AAA 服务器的连接。

  对于远程访问 VPN 双重身份验证，请确保Firewall Threat Defense设备可以访问主身份验证服务器和辅助身份验证服务器。
- 要启用 Firewall Threat Defense 远程访问 VPN 功能，购买并启用以下思科 Secure Client 许可证之一：Secure Client Advantage、 Secure Client Premier或 仅限 Secure Client VPN 。
- 从思科软件下载中心下载最新的 Secure Client 映像文件。

  在您的 Secure Firewall Management Center Web 界面上，转至 并添加新的 Secure Client 映像文件。
- 创建一个安全区或接口组，包含用户将访问的网络接口，用于VPN连接。请参阅接口，第2655页。
- 从 Cisco 软件下载中心下载 安全客户端配置文件编辑器 以创建 安全客户端配置文件。您可以使用独立配置文件编辑器创建新的或修改现有的 安全客户端配置文件。

创建新的远程访问 VPN 策略

远程访问 VPN 策略向导将指导您快速轻松地设置具备基本功能的远程访问 VPN。您可以根据需要通过指定其他属性来增强策略配置并将其部署到您的 Cisco Secure Firewall Threat Defense安全网关设备。

开始之前

- 确保满足配置远程访问 VPN 的前提条件，第 1541 页中列出的所有前提条件。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击**添加 (Add)** 使用远程访问 VPN 策略向导来新建具有基本策略配置的远程访问 VPN 策略。

您必须完成整个向导才能创建新的策略；如果在完成向导之前取消，则不会保存策略。

步骤 3 选择目标设备和协议。

您在这里选择的 Firewall Threat Defense 设备将用作 VPN 客户端用户的远程访问 VPN 网关。

您可以在创建远程访问 VPN 策略或稍后更改设备时选择 Firewall Threat Defense 设备。请参阅设置远程访问 VPN 策略的目标设备，第 1551 页。

您可以选择 **SSL** 或 **IPSec-IKEv2**，或同时选择两种VPN协议。 Firewall Threat Defense 支持两种协议通过 VPN 隧道在公共网络上建立安全连接。

注释
Firewall Threat Defense 不支持使用 NULL 加密的 IPSec 隧道。如果已选择 IPSec-IKEv2，请确保不为 IPSec IKEv2 提议选择 NULL 加密。请参阅配置 IKEv2 IPsec 方案对象，第 2732 页。

有关 SSL 设置，请参阅SSL ，第 1007 页。

步骤 4 点击**下一步 (Next)**。

步骤 5 配置 **连接配置文件** 和 **组策略** 设置。

连接配置文件将指定一组参数，用于定义远程用户如何连接到VPN设备。参数包括身份验证的设置和属性、VPN 客户端的地址分配以及组策略。配置远程访问 VPN 策略时，Firewall Threat Defense设备将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。

有关详细信息，请参阅配置连接配置文件设置，第 1552 页。

步骤 6 配置**身份验证、授权和记账 (Authentication, Authorization & Accounting)** 设置。

有关配置的信息，

- AAA 设置，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页
- LDAP 属性映射，请参阅配置 LDAP 属性映射，第 1578 页
- SAML 2.0 单点登录身份验证，请参阅配置 SAML 单点登录身份验证，第 1625 页

步骤 7 配置**客户端地址分配 (Client Address Assignment)** 设置。

客户端 IP 地址可由 AAA 服务器、DHCP 服务器和 IP 地址池分配。选择多个选项时，IP 地址分配将按照 AAA 服务器、DHCP 服务器和 IP 地址池的顺序进行。AAA 服务器分配客户端 IP 地址仅支持 Realm 和 RADIUS 授权。确保已配置 realm 或 RADIUS 服务器以提供客户端 IP 地址。

步骤 8 配置**组策略 (Group Policy)** 设置。

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问 VPN 体验的 VPN 用户。您可以使用组策略配置用户授权配置文件、IP 地址、安全客户端 设置、VLAN 映射和用户会话设置等属性。RADIUS 授权服务器将会分配组策略，或从当前连接配置文件中获取。有关详细信息，请参阅配置组策略，第 1577 页。

步骤 9 点击**下一步 (Next)**。

步骤 10 选择 VPN 用户将用于连接到远程访问 VPN 的 **安全客户端映像**。

安全客户端通过企业资源的全 VPN 调配为远程用户提供到 Cisco Secure Firewall Threat Defense 设备的安全 SSL 或 IPSec (IKEv2) 连接。在 Firewall Threat Defense设备上部署远程访问 VPN 策略后，VPN 用户可以在其浏览器中输入所配置设备接口的 IP 地址，以下载并安装 Secure Client。

有关配置客户端配置文件和客户端模块的信息，请参阅组策略 Secure Client 选项，第 2727 页。

步骤 11 点击**下一步 (Next)**。

步骤 12 配置**传入 VPN 访问的网络接口 (Network Interface for Incoming VPN Access)**。

接口对象可对网络分段，帮助您管理和分类流量数据流。安全区域对象只是对接口进行分组。这些组可以跨多个设备；您还可以在单个设备上配置多个区域接口对象。有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

（可选）如果需要，选中**在成员接口上启用 DTLS (Enable DTLS on member interfaces)** 复选框。DTLS 仅适用于 SSL协议。

步骤 13 配置**设备证书 (Device Certificates)**。

设备证书（也称为身份证书）可识别连接至远程访问客户端的 VPN 网关。选择用于对 VPN 网关进行身份验证的证书。从**证书注册 (Certificate Enrollment)** 下拉列表中选择证书，或点击 **+** 添加证书。

您可以选择 ACME 证书以对 VPN 网关进行身份验证。ACME 证书可自动执行 SSL 和 TLS 证书的生命周期管理，包括自动续约。

步骤 14 配置**服务访问控制 (Service Access Control)**。

您可以在运行 7.7 或更高版本的 Firewall Threat Defense 设备上使用服务访问对象，以便控制对远程客户访问 VPN 的访问。该对象可在 VPN 验证前为客户端提供基于地理位置的访问控制。默认情况下，RAVPN 没有访问控制，远程客户端可以从任何地理位置进行连接，除非由服务访问对象指定。有关详细信息，请参阅基于地理位置管理远程用户的 VPN 访问，第 1604 页和配置服务访问对象，第 2628 页。

步骤 15 配置 **VPN 流量访问控制 (Access Control for VPN Traffic)**。

默认情况下，VPN 隧道中的所有已解密流量受制于访问控制策略。选中**绕过已解密流量 (sysopt permit-vpn) 的访问控制策略 (Bypass Access Control policy for decrypted traffic [sysopt permit-vpn])** 复选框，从访问控制策略中绕过解密流量。此选项会绕过访问控制策略检查，但 VPN 过滤器 ACL 以及从 AAA 服务器下载的身份验证 ACL 仍适用于 VPN 流量。

注释
如果选择此选项，则无需更新在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 1545 页中指定的远程访问 VPN 的访问控制策略。

步骤 16 点击**下一步 (Next)**。

步骤 17 查看远程访问 VPN 策略配置**摘要**。

“摘要”页面显示到目前为止已配置的所有远程访问VPN设置，并提供指向在所选设备上部署远程访问 VPN 策略之前需要执行的其他配置的链接。

如有需要，请点击**返回 (Back)** 以更改配置。

步骤 18 点击**完成 (Finish)**，以完成远程访问 VPN 策略的基本配置。

在完成远程访问 VPN 策略向导后，将出现策略列表页面。稍后，设置 DNS 配置，为 VPN 用户配置访问控制，然后启用 NAT 豁免（如有必要），以完成基本远程访问 VPN 策略配置。

下一步做什么

使用远程访问 VPN 控制面板监控设备上主动远程访问 VPN 会话的实时数据。**洞察与报告** > **VPN 控制面板** > **远程访问 VPN**您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。有关详细信息，请参阅远程访问 VPN 控制面板，第 1642 页。

在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略

部署远程访问 VPN 策略之前，必须使用允许目标 Cisco Secure Firewall Threat Defense 设备上的 VPN 流量的规则更新访问控制策略。此规则必须允许来自外部接口的所有流量，其中源设备作为定义的 VPN 池网络，目标设备作为公司网络。



注释 如果在“访问接口”选项卡上选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，则无需更新远程访问 VPN 的访问控制策略。

启用或禁用所有 VPN 连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。

有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1571 页。

开始之前

使用远程访问 VPN 策略向导完成远程访问 VPN 策略配置。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要更新的访问控制策略旁边的 **编辑** 。

步骤 3 请点击 **添加规则**来添加新规则。

步骤 4 指定规则的 **名称** 并选择 **启用**。

步骤 5 选择 **操作**、 **允许** 或 **信任**。

步骤 6 在 **区域** 选项卡上选择以下选项：

a) 从可用区域中选择外部区域，然后点击**添加到源 (Add to Source)**。

b) 从可用区域中选择内部区域，然后点击**添加到目标 (Add to Destination)**。

步骤 7 在 **网络** 选项卡上选择以下选项：

a) 从可用网络中选择内部网络（内部接口和/或公司网络），然后点击 **添加到目标**。

b) 从 **可用网络** 中选择 VPN 地址池网络，然后点击 **添加到源网络**。

步骤 8 配置其他所需的访问控制规则设置，然后点击**添加 (Add)**。

步骤 9 保存此规则和访问控制策略。

（可选）配置 NAT 豁免

NAT 豁免将豁免转换地址，并允许已转换的主机和远程主机发起与受保护主机的连接。与身份 NAT 一样，请不要限制特定接口上的主机转换；必须对通过所有接口的连接使用 NAT 豁免。但是，借助 NAT 豁免，您可以在确定要转换的实际地址时指定实际地址和目标地址（类似于策略 NAT）。使用静态身份 NAT 以考虑访问列表中的端口。

为远程访问或站点间 VPN 配置静态身份 NAT 时，必须使用路由查找选项配置 NAT。如果没有路由查询，Firewall Threat Defense 会将流量向外发送到在 NAT 命令中指定的接口，无论路由表显示什么。例如，您不希望 Firewall Threat Defense 通过不正确的接口发送 DHCP 范围流量；它永远不会返回到接口 IP 地址。路由查询选项允许 Firewall Threat Defense 将流量直接发送到接口 IP 地址，而不是通过接口。对于从VPN客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。

开始之前

检查部署有远程访问 VPN 策略的目标设备上是否配置了 NAT。如果已在目标设备上启用 NAT，您必须定义 NAT 策略，为 VPN 流量设置豁免。

过程

步骤 1 在您的 Secure Firewall Management Center Web 界面上，点击 **策略** > **网络策略** > **NAT** 。

步骤 2 选择要更新的 NAT 策略，或点击 **新建策略** 以使用允许所有连接的连接的 NAT 规则创建 NAT 策略。

步骤 3 点击**添加规则**，以添加 NAT 规则。

步骤 4 在“添加 NAT 规则”窗口中，选择以下内容：

a) 为“NAT 规则”选择**手动 NAT 规则**。

b) 为“类型”选择**静态**。

c) 点击 **接口对象** ，然后选择源和目标接口对象。

注释
此接口对象必须与在远程访问 VPN 策略中选择的接口相同。

有关详细信息，请参阅配置远程访问 VPN 的访问接口 ， 第 1571 页。

a) 点击 **转换** 并选择源和目标网络：

- **原始源** 和 **转换后的源**
- **原始目标** 和 **转换后的目标**

步骤 5 在“高级”选项卡中，选择**不在目标接口上使用代理 ARP**。

不在目标接口上使用代理 ARP -为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。

步骤 6 点击**确定**。

配置 DNS

在每台 Firewall Threat Defense设备上配置 DNS，以便使用远程访问 VPN。如果没有 DNS，设备将无法解析 AAA 服务器名称、命名 URL 和具有 FQDN 或主机名的 CA 服务器。它只能解析 IP 地址。

过程

步骤 1 使用“平台设置”配置DNS服务器详细信息和域查找接口。有关详细信息，请参阅DNS，第977页和DNS 服务器组，第 2640 页。

步骤 2 如果可以通过 VNP 网络访问 DNS 服务器，则在组策略中配置拆分隧道，以允许 DNS 流量通过远程访问 VPN 隧道。有关详细信息，请参阅配置组策略对象，第 2724 页。

添加 安全客户端配置文件 XML 文件

安全客户端配置文件 是一组以 XML 文件形式存储的配置参数，客户端使用该文件来配置客户端的操作和外观。这些参数（XML 标记）包括主机名称和地址以及设置，用于启用更多客户端功能。

安全客户端配置文件 编辑器是一款基于 GUI 的配置工具，作为 安全客户端 软件包的一部分提供，您可以使用此编辑器来创建 安全客户端配置文件 。该程序可独立于 防火墙管理中心 而运行。有关安全客户端配置文件 编辑器的详细信息，请参阅 Cisco Secure Client（包括 AnyConnect）管理员指南。

开始之前

Cisco Secure Firewall Threat Defense 远程访问 VPN 策略要求将 安全客户端配置文件 的任务分配给 VPN 客户端。您可以将客户端配置文件连接到组策略。

您可以从 Cisco 软件下载中心下载 安全客户端配置文件 编辑器。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑** 。

步骤 3 点击要添加的 Secure Client 配置文件上的 **编辑** 。

步骤 4 点击 **编辑组策略**。如果您选择添加新的组策略，请点击 **添加**。

步骤 5 选择 **安全客户端** > **配置文件**。

步骤 6 从 **客户端配置文件** 下拉列表中选择一个配置文件。如果您选择添加新的客户端配置文件，请点击 **添加** 并执行以下操作：

a) 指定配置文件 **名称**。

b) 点击 **浏览** 并选择 安全客户端配置文件 XML 文件。

注释
对于双因素身份验证，也要确保在 Secure Client 配置文件中将超时设置为 60 秒或更长。

c) 点击**保存**。

步骤 7 保存更改。

（可选）配置分割隧道

拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。如果要允许 VPN 用户在连接到远程访问 VPN 时访问外部网络，则您可以配置分割隧道。要配置拆分隧道列表，必须创建标准访问列表或扩展访问列表。

有关详细信息，请参阅配置组策略，第 1577 页。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要为其配置分割隧道的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 在请求的连接配置文件上，点击 **编辑** 。

步骤 4 点击 **添加** 以添加组策略，或者点击 **编辑组策略**。

步骤 5 选择 **常规** > **分割隧道**。

步骤 6 从 **IPv4 拆分隧道** 或 **IPv6 拆分隧道** 列表中，选择**排除下面指定的网络**；然后选择要从 VPN 流量中排除的网络。

默认设置允许所有流量通过 VPN 隧道。

步骤 7 点击**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后从下拉列表中选择一个访问列表或添加新的访问列表。

步骤 8 如果您选择添加新的标准或扩展访问列表，请执行以下操作：

a) 为新访问列表指定**名称 (Name)**，然后点击**添加 (Add)**。

b) 从 **操作** 下拉列表中选择 **允许** 。

c) 选择允许通过 VPN 隧道的网络流量并点击 **添加**。

步骤 9 保存更改。

相关主题

访问列表，第 2625 页

（可选）配置动态分割隧道

通过动态分割隧道，您可以根据 DNS 域名微调分割隧道。您可以配置远程接入 VPN 隧道中必须包含或排除的域。排除的域不会被阻止。相反，流向这些域的流量将保留在VPN隧道之外。例如：您可以将流量发送到公共互联网上的 Cisco WebEx，从而释放 VPN 隧道中的带宽，以用于发往受保护网络中服务器的流量。有关配置此功能的详细信息，请参阅 在 FMC 管理的 FTD 上配置 AnyConnect 动态拆分隧道。

开始之前

您可以使用 防火墙管理中心 和 Firewall Threat Defense 从 7.0 或更高版本配置此功能。如果您有旧版本的 防火墙管理中心，可以按照 使用 FMC 进行 Firepower 威胁防御的高级 AnyConnect VPN 部署中的说明使用 FlexConfig 进行配置。

过程

步骤 1 将组策略配置为使用动态拆分隧道。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击要为其配置动态分割隧道的远程访问 VPN 策略旁边的 **编辑** 。
c) 在请求的连接配置文件上，点击 **编辑** 。
d) 点击 **编辑组策略**。

步骤 2 在 **添加/编辑组策略** 对话框中配置 Cisco Secure 客户端 自定义属性。

a) 点击Cisco Secure 客户端选项卡。
b) 点击 **自定义属性** ，然后点击 **+**。
c) 从 **Cisco Secure 客户端 属性** 下拉列表中选择 **动态分割隧道** 。
d) 点击 **+** 创建新的自定义属性对象。
e) 输入自定义属性对象的名称。
f) **包含域**-指定将包含在远程访问 VPN 隧道中的域名。

   您可以在隧道中包含将根据 IP 地址排除的域。

g) **排除域**-指定将从远程访问 VPN 中排除的域名。

   排除的域未被阻止，流向这些域的流量将保留在 VPN 隧道之外。

h) 点击**保存**。
i) 点击**添加 (Add)**。

步骤 3 验证已配置的自定义属性，然后点击 **保存**，以保存组策略。

步骤 4 点击**保存**以保存连接文件。

步骤 5 点击**保存**以保存远程访问 VPN 策略。

下一步做什么

1. 在 Firewall Threat Defense上部署配置。
2. 验证 Firewall Threat Defense 和 Secure Client上配置的动态拆分隧道配置。有关详细信息，请参阅验证动态分割隧道配置 ， 第 1550 页。

验证动态分割隧道配置

在 Firewall Threat Defense

使用以下命令验证动态分割隧道配置：

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *<group-policy-name>*

在 Secure Client

点击统计信息 () 图标，然后选择 **VPN > 统计信息**。您可以在动态拆分排除/包含类别下确认域。

检验配置

过程

步骤 1 在外部网络上的计算机上打开 Web 浏览器。

步骤 2 输入配置 Firewall Threat Defense 远程访问 VPN 网关的 URL。

步骤 3 提示时，输入用户名和密码，然后点击 **登录**。

注释
如果在系统上安装 安全客户端 ，则会自动建立与 VPN 的连接。

如果未安装 安全客户端 ，VPN 会提示您下载 安全客户端 。

步骤 4 下载 安全客户端 （如果尚未安装）并连接到 VPN。
安全客户端 自行安装。成功进行身份验证后，您将连接到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关。适用的身份或 QoS 策略根据您的远程访问 VPN 策略配置实施。

创建现有远程接入 VPN 策略的副本

复制现有的远程接入 VPN 策略，以便创建具有所有设置（包括连接配置文件和访问接口）的新策略。然后，您可以将设备分配给新策略，同时根据需要在分配的设备上部署 VPN。



注释 具有远程访问 VPN 只读权限的用户无法创建 VPN 的副本。域中拥有只读权限的用户可以复制远程访问 VPN。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要复制的策略上的 **复制** 。

步骤 3 为新的远程访问 VPN 指定 **名称** 。

步骤 4 点击**确定**。

下一步做什么

要将设备分配给新策略，请参阅 设置远程访问 VPN 策略的目标设备 ， 第 1551 页。

设置远程访问 VPN 策略的目标设备

在创建远程访问 VPN 策略后，您可以将策略分配给威胁防御设备。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** () 。

步骤 3 点击**策略分配**。

步骤 4 执行以下任一操作：

- 要将设备、高可用性对或设备组分配给策略，请在 **可用设备** 列表中将其选中，然后点击 **添加**。您还可以拖放可用设备进行选择。
- 要删除设备分配，请点击**所选设备 (Selected Devices)** 列表中的设备、高可用性对或设备组旁边的 **删除** ()。

步骤 5 点击**确定**。

步骤 6 点击保存。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

将本地领域与远程接入 VPN 策略相关联

您可以将本地领域与远程接入 VPN 策略相关联，以启用本地用户身份验证。

有关创建和管理领域的信息，请参阅管理领域，第 2048 页。

有关为远程接入 VPN 配置本地用户认证的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

过程

步骤 1 选择安全连接 > 远程访问 VPN。
步骤 2 点击要编辑的远程访问 VPN 策略旁边的 编辑 (✎) 。
步骤 3 点击本地领域旁边的链接。
步骤 4 从列表中选择 本地领域服务器，或点击 添加 以添加新的本地领域。
步骤 5 点击确定。
步骤 6 点击保存。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

其他远程访问 VPN 配置

配置连接配置文件设置

远程访问VPN策略包含针对特定设备的连接配置文件。这些策略与创建隧道本身有关，如如何完成AAA，以及如何为VPN客户端分配地址（DHCP或地址池）。它们还包括用户属性，这些属性将在Firewall Threat Defense设备上配置或从 AAA 服务器上获取的组策略中确定。设备还将提供名为 *DefaultWEBVPNGroup* 的默认连接配置文件。该连接配置文件是使用列表中显示的向导配置的。

如果您决定为不同的VPN用户组授予不同的权限，那么您可以为每个用户组添加特定的连接配置文件，并在远程访问 VPN 策略中维护多个连接配置文件。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择 **连接配置文件 (Connection Profile)**，然后点击 **编辑 (Edit)**。

步骤 4 （可选）如果您选择添加新的连接配置文件，请点击**添加 (Add)**。

步骤 5 配置 VPN 客户端的 IP 地址。
配置 VPN 客户端的 IP 地址，第 1553 页

步骤 6 （可选）更新远程访问 VPN 的 AAA 设置。
配置远程访问 VPN 的 AAA 设置，第 1555 页

步骤 7 （可选）创建或更新别名。
创建或更新连接配置文件的别名，第 1570 页

步骤 8 保存更改。

配置 VPN 客户端的 IP 地址

客户端地址分配允许您为远程访问 VPN 用户分配 IP 地址。

您可以从本地 IP 地址池、DHCP 服务器和 AAA 服务器为远程 VPN 客户端分配 IP 地址。首先由 AAA 服务器分配，然后由其他服务器分配。在**高级**选项卡中配置**客户端地址分配**策略，以定义分配条件。仅在连接配置文件的关联组策略或系统默认组策略 **DfltGrpPolicy** 中未定义 IP 池时，才会使用此连接配置文件中定义的 IP 池。

IPv4 地址池 - SSL VPN 客户端将在连接到 Firewall Threat Defense设备时收到新 IP 地址。地址池定义远程客户端可以接收的地址范围。可分别为 IPv4 和 IPv6 地址添加最多六个池。

注释 可以使用 防火墙管理中心 中现有 IP 池的 IP 地址，也可以使用**添加 (Add)** 选项来创建新的池。此外，您可以使用 **对象** > **地址池** 路径在 防火墙管理中心 中创建 IP 池。有关详细信息，请参阅地址池，第 2630 页。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。
系统将列出现有的远程访问策略。

步骤 2 选择远程访问 VPN 策略，然后点击编辑图标。

步骤 3 选择要更新的连接配置文件，然后点击编辑图标。

步骤 4 在**客户端地址分配 (Client Address Assignment)** 选项卡下，执行以下操作：

步骤 5 点击**地址池 (Address Pools)** 旁边的 +：

a) 点击**地址池 (Address Pools)** 旁边的 + 以添加 IP 地址，然后选择 **IPv4** 或 **IPv6** 以添加相应的地址池。从**可用池(Available Pools)** 中选择 IP 地址池，然后点击**添加 (Add)**。

注释
如果在多台 Cisco Secure Firewall Threat Defense 设备之间共享远程访问 VPN 策略，请牢记所有设备都将共享同一地址池，除非使用设备级对象覆盖，将每台设备的全局定义替换为一个唯一地址池。在设备不使用 NAT 的情况下，需要多个唯一地址池，以免重叠地址。

b) 在**地址池 (Address Pools)** 窗口中点击**可用池 (Available Pools)** 旁边的 +，以添加新的 IPv4 或 IPv6 地址池。如果选择 IPv4 池，请提供起始和结束 IP 地址。如果选择包括新的 IPv6 地址池，请输入介于范围 1-16384 之间的**地址数量**。在多台设备之间共享对象时，选择**允许覆盖**选项可以避免与 IP 地址冲突。有关详细信息，请参阅地址池，第 2630 页。

c) 点击**确定**。

如果您计划编辑 IP 地址池，则建议您在维护时间窗口期间执行以下步骤：

1. 从远程访问 VPN 取消分配设备。
2. 选择设备并点击**部署 (Deploy)**。

   此部署会从设备中删除所有远程访问 VPN 配置，终止远程访问 VPN 会话，而不会重新建立会话。
3. 点击 IP 地址池旁边的编辑图标可对其进行编辑，如有需要，可在 防火墙管理中心 上编辑任何其他远程访问 VPN 配置。
4. 将设备分配给更新后的远程访问 VPN 策略。
5. 在设备上部署配置。

   远程访问 VPN 客户端可以在维护窗口后连接到设备。

步骤 6 点击 **DHCP 服务器 (DHCP Servers)** 旁边的 + 以添加 DHCP 服务器：

注释
只能通过 IPv4 地址配置 DHCP 服务器地址。

a) 指定名称和 DHCP（动态主机配置协议）服务器地址作为网络对象。点击 **添加**，然后从对象列表中选择服务器。点击 **删除** 以删除 DHCP 服务器。

b) 点击 **新对象** 页面中的 **添加** 以添加新网络对象。输入新对象名称、说明、网络，然后选择**允许覆盖**选项（如果适用）。有关详细信息，请参阅创建网络对象，第 2660 页和允许对象覆盖，第 2618 页。

c) 点击**确定**。

步骤 7 点击**保存**。

相关主题

配置连接配置文件设置，第 1552 页

配置远程访问 VPN 的 AAA 设置

开始之前

- 确保在终端上部署所需的计算机和用户证书。有关 Firewall Threat Defense 证书的信息，请参阅管理 Firewall Threat Defense 证书，第 2744 页。
- 使用所需的证书配置 安全客户端 配置文件。有关详细信息，请参阅《*Cisco Secure Client*（包括 *AnyConnect*）管理员指南》。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择要更新 AAA 设置的连接配置文件，然后点击 **编辑 AAA** 。

步骤 4 为 **身份验证**选择以下选项：

- **身份验证方法** - 确定在允许用户访问网络和网络服务之前对其进行标识的方式。这种方法通过要求提供有效的用户凭据（通常是用户名和密码）来控制访问。它也可能包括来自客户端的证书。受支持的身份验证方法有**仅 AAA**、**仅客户端证书**和 **AAA + 客户端证书**。

  何时选择以下**身份验证方法**：

  - **仅 AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，必须手动选择 **授权服务器** 和 **记帐服务器** 。
  - **SAML** - 使用 SAML 单点登录服务器对每个用户进行身份验证。有关详细信息，请参阅使用 SAML 2.0 的单点登录身份验证，第 1623 页。

    覆盖身份提供程序证书-选择此选项可使用连接配置文件或 SAML 应用特定的 IdP 证书覆盖 SAML 提供程序的主身份提供程序证书。从 IdP 下拉列表中选择证书。

    Microsoft Azure 可以为同一实体 ID 支持多个应用。每个应用（映射到不同的连接配置文件）都需要唯一的证书。如果要在当前连接配置文件中保留单点登录对象的现有实体 ID 并使用其他 IdP 证书，则可以选择此选项。

    这启用每个 Microsoft Azure SAML 身份提供程序支持多个 SAML 应用。

    主身份证书在单点登录服务器对象中配置。

    有关配置单点登陆服务器对象的详细信息，请参阅添加单点登录服务器，第 2623 页。

    选择您的 **SAML 登录体验** 以配置用于 SAML Web 身份验证的浏览器：

    - **VPN 客户端嵌入式浏览器**-选择此选项可使用 VPN 客户端嵌入式浏览器进行 Web 身份验证。身份验证仅适用于 VPN 连接。

- **默认操作系统浏览器**-选择此选项可配置默认操作系统或支持 WebAuthN（用于 Web 身份验证的 FIDO2 标准）的本地浏览器。此选项启用单点登录 (SSO) 支持 Web 身份验证方法，例如生物识别身份验证。

  默认浏览器需要外部浏览器软件包进行 Web 身份验证。默认情况下配置软件包 默认-外部-浏览器-软件包。您可以通过编辑远程访问 VPN 策略并在**高级**下选择文件来更改默认外部浏览器软件包，选择 **AnyConnect 客户端映像安全客户端映像**，然后点击**软件包文件**。

  您还可以通过选择添加新的软件包文件。**对象** > **对象管理** > **VPN** > **AnyConnect 文件** > **添加 AnyConnect 文件**。

- **仅客户端证书** - 使用客户端证书对每个用户进行身份验证。客户端证书必须在 VPN 客户端终端上配置。默认情况下，用户名派生自客户端证书字段 CN 和 OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

  选择 **启用多个证书身份验证** 以使用计算机和用户证书对 VPN 客户端进行身份验证。

  如果已启用多个证书身份验证，则可以选择以下证书之一来映射用户名和对 VPN 用户进行身份验证：

  - **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
  - **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。

  注释
  如果未启用多证书身份验证，则默认情况下使用用户证书（第二证书）进行身份验证。

  如果选择**映射特定字段**选项（包括客户端证书中的用户名），则**主**字段和**辅助**字段将分别显示默认值：**CN**（**公用名**）和**OU**（**组织单位**）。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

  与**映射特定字段**选项相关的“主”字段和“辅助”字段包含以下公用值：

  - C（国家/地区）
  - CN（公用名）
  - DNQ（DN 限定符）
  - EA（邮件地址）
  - GENQ（代系限定符）
  - GN（名字）
  - I（首字母）
  - L（地区）
  - N（名字）
  - O（组织）

- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- **客户端证书和 AAA** - 每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择身份验证所需的证书和 AAA 配置。

  无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **客户端证书和 SAML** - 每个用户都使用客户端证书和 AAA 服务器进行身份验证。选择所需的证书和 SAML 配置以进行身份验证。
  - **允许仅在证书中的用户名与 SAML 相同时允许连接**-仅当证书中的用户名与 SAML 单点登录用户名匹配时，选择仅允许 VPN 连接。
  - **从客户端证书中使用用户名进行授权**-选择从客户端证书中选择用户名进行授权时，必须配置要从客户端证书中选择的字段。

    您可以选择将特定字段映射为用户名，也可以使用整个可分辨名称 (DN) 进行授权：
    - **映射特定字段**- 从客户端证书中选择要包含的用户名，则 **主要** 和 **辅助** 字段将分别显示默认值： **CN**（**公用名**） 和 **OU**（**组织单位**） 。
    - **使用整个 DN 作为用户名**- 系统将自动检索用户身份用于授权。

  您还可以创建动态访问策略 (DAP)，以将用户特定的 SAML 断言属性或用户名与 DAP 证书属性进行匹配。请参阅为 DAP 记录配置 AAA 条件设置，第 1654 页。

- **身份验证服务器** - 身份验证是在允许用户访问网络和网络服务之前对其进行标识的方式。身份验证需要有效的用户凭证和/或证书。您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。

  如果您已添加服务器或创建身份验证服务器，请从列表中选择身份验证服务器：
  - **LOCAL**-使用来自 Firewall Threat Defense 的本地数据库进行用户身份验证。要配置本地身份验证，Firewall Threat Defense 必须为版本 7.0 及更高版本。
    - **本地领域** - 选择本地领域或点击 **添加** 以配置领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。
  - **领域** - 配置 LDAP 或 AD 领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。

- **RADIUS 服务器组** - 使用 RADIUS 服务器添加 RADIUS 服务器组对象。请参阅添加 RADIUS 服务器组，第 2620 页。
- **单点登录服务器** - 为 SAML 身份验证创建单点登录服务器对象。请参阅添加单点登录服务器，第 2623 页。

回退到本地身份验证 - 使用本地数据库对用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 安全客户端 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问 VPN 身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

  必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA 服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

  注释
  默认情况下，无需辅助身份验证。

  身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

  - **回退到本地身份验证** - 使用本地数据库对此用户进行身份验证，即使 AAA 服务器组不可用，只要已配置本地数据库，即可建立 VPN 隧道。

  选择 **辅助身份验证的用户名**以下的选项：

  - **提示：** 在登录 VPN 网关时，提示用户输入用户名和密码。
  - **使用主身份验证用户名：** 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。
  - **映射客户端证书中的用户名：** 预填充客户端证书中的辅助用户名。

    如果已启用多个证书身份验证，则可以选择以下证书之一：

    - **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
    - **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。
    - 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

      有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。
    - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)：** 用户通过 安全客户端 VPN 客户端连接时，预填充客户端证书中的辅助用户名。

- **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

- **使用 VPN 会话的辅助用户名：** 辅助用户名用于在 VPN 会话期间报告用户活动。

步骤 5 为 **授权**选择以下选项：

- **身份验证服务器** - 身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。当您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。授权需要进行身份验证。

  要了解有关远程访问 VPN 授权工作原理的更多信息，请参阅 了解权限和属性的策略实施，第 1536 页。

  在连接配置文件中配置了 RADIUS 服务器以进行用户授权时，远程访问 VPN 系统管理员可以为用户或用户组配置多个授权属性。在 RADIUS 服务器上配置的授权属性可以特定于用户或用户组。用户通过身份验证后，这些特定的授权属性将被推送到 Firewall Threat Defense设备。

  注释
  从授权服务器获得的AAA服务器属性覆盖了之前在组策略或连接配置文件上可能已经配置的属性值。

- 如果需要，请选择**仅当用户位于授权数据库中时才允许连接**。

  启用该选项后，系统检查客户端的用户名必须存在于授权数据库中，才可以成功进行连接。如果授权数据库中不存在该用户名，则连接被拒绝。

- 当您选择领域作为授权服务器时，必须配置 LDAP 属性映射。您可以选择用于身份验证和授权的单个服务器或其他服务器。点击 **配置 LDAP 属性映射** 以添加用于授权的 LDAP属性映射。

  注释
  Firewall Threat Defense 不支持将 SAML 身份提供程序用作授权服务器。如果 SAML 身份提供程序后面的 Active Directory 可通过 防火墙管理中心 和 Firewall Threat Defense 访问，则可以按照以下步骤配置授权：

  - 为 AD 服务器添加领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。
  - 选择领域对象作为远程访问 VPN 连接配置文件中的授权服务器。
  - 为所选领域配置 LDAP 属性映射。

  有关配置 LDAP 属性映射的信息，请参阅 配置 LDAP 属性映射，第 1578 页。

步骤 6 为 **记帐**选择以下选项：

- **记账服务器** - 记账用于跟踪用户正在访问的服务和他们正在使用的网络资源量。当激活 AAA 记帐时，网络访问服务器会向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后系统

可以分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

指定将用于对远程访问 VPN 会话进行记帐的 RADIUS 服务器组对象。

步骤 7 选择 **高级设置**以下的选项：

- **从用户名删除领域** - 在将用户名传递到 AAA 服务器之前，选择要从用户名删除领域。例如，如果选择此选项并提供域\用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。
- **从用户名删除组** - 在将用户名传递到 AAA 服务器之前，选择要从用户名删除组名称。默认情况下，此选项处于取消选中状态。

  注释
  领域是管理域。启用这些选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。

- **密码管理 (Password Management)**：启用远程访问 VPN 用户的密码管理。选择以提前通知密码到期或密码到期的日期。

步骤 8 点击**保存**。

相关主题

了解权限和属性的策略实施 ， 第 1536 页
管理领域 ， 第 2048 页

Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性

Firewall Threat Defense设备支持将用户授权属性（也称为用户权利或权限）应用到来自外部RADIUS服务器的 VPN 连接，这些连接被配置为用于远程接入 VPN 策略中的身份验证和/或授权。

注释 Cisco Secure Firewall Threat Defense 设备支持具有供应商 ID 3076 的属性。

以下用户授权属性由 RADIUS 服务器发送到 Firewall Threat Defense设备。

- RADIUS 属性 146 和 150 是从 Firewall Threat Defense设备发送到 RADIUS 服务器，以提出身份验证和请求授权。
- 所有三个属性（146、150 和 151）都是从 Firewall Threat Defense设备发送到 RADIUS 服务器，以提出开始记账、临时更新和停止请求。

*表 90: 从 **Cisco Secure Firewall Threat Defense** 发送到 **RADIUS** 服务器的 **RADIUS** 属性*

属性	属性编号	语法、类型	单值或多值	说明或值
连接配置文件名称或隧道组名称	146	字符串	单值	1 到 253 个字符

属性	属性编号	语法、类型	单值或多值	说明或值
客户端类型	150	整数	单值	2 = Secure Client SSL VPN, 6 = Secure Client IPsec VPN (IKEv2)
会话类型	151	整数	单值	1 = Secure Client SSL VPN, 2 = Secure Client IPsec VPN (IKEv2)

表 *91:* 支持的 *RADIUS* 授权属性

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
Access-Hours	是	1	字符串	单值	时间范围的名称，例如工作时间
Access-List-Inbound	是	86	字符串	单值	这两个访问列表属性都使用 Firewall Threa 设备上配置的 ACL 名称。使用 Smart CL 列表对象类型创建 ACL（依次选择**设备** > **Smart CLI** > **对象**）。 此类 ACL 用于控制入站流量（流量进入 Threat Defense 设备）或出站流量（流量离 Threat Defense 设备）。
Access-List-Outbound	是	87	字符串	单值	
Address-Pools	是	217	字符串	单值	Firewall Threat Defense 设备上定义的网络对 用于识别将作为地址池供客户端连接远程 时使用的子网。在 **对象** 页面上定义网络对 将网络对象与组策略或连接配置文件相关
Allow-Network-Extension-Mode	是	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	是	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	是	67	字符串	单值	可能的值：UID、OU、O、CN、L、SP、 T、N、GN、SN、I、GENQ、DNQ、SEF use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	是	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	是	15	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 安全客户端 SSL TLS/DTLS Clientless SSL。
Banner2	是	36	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 安全客户端 SSL TLS/DTLS Clientless SSL。如果进行了相应的配置， 字符串会连接到 Banner1 字符串。

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
Cisco-IP-Phone-Bypass	是	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	是	75	整数	单值	0 = 已禁用 1 = 已启用
Client Type	是	150	整数	单值	1 = 思科 VPN 客户端 (IKEv1) 2 = Secure Clie VPN 3 = 无客户端 SSL VPN 4 = 直接转发代 L2TP/IPsec SSL VPN 6 = Secure Client IPsec (IKEv2)
Client-Type-Version-Limiting	是	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	是	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	是	122	整数	单值	0 = 已禁用 1 = 已启用
Framed-Interface-Id	是	96	字符串	单值	分配的 IPv6 接口 ID。与 Framed-IPv6-Prefix 用以创建完整的已分配 IPv6 地址。例如： Framed-Interface-ID =1:1:1:1与 Framed-IPv6-P =2001:0db8::/64 组合可提供分配的IP地址 2001:0db8::1:1:1:1。
Framed-IPv6-Prefix	是	97	字符串	单值	分配的 IPv6 前缀和长度。与 Framed-Interfac 合以创建完整的已分配 IPv6 地址。例如：前 2001:0db8::/64 与 Framed-Interface-Id=1:1:1:1 提供IP地址 2001:0db8::1:1:1:1。通过分配前缀 为/128 的完整 IPv6 地址（例如， Framed-IPv6-Prefix=2001:0db8::1/128），可以 属性分配IP地址而不使用 Framed-Interface-Id
Group-Policy	是	25	字符串	单值	为远程访问 VPN 会话设置组策略。您可以使 其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	换行符 (\n) 分隔的 DNS 域列表
IE-Proxy-PAC-URL	是	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
IE-Proxy-Server-Policy		81	整数	单值	1 = 无修改 2 = 无代理 3 = 自动检测 4 = 使设置
IKE-KeepAlive-Confidence-Interval	是	68	整数	单值	10 到 300 秒
IKE-Keepalive-Retry-Interval	是	84	整数	单值	2 到 10 秒
IKE-Keep-Alives	是	41	布尔值	单值	0 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	是	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	是	16	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅适用于= NT 域 4 = SDI 5 = 内部 6 = RADIUS 到Kerberos/Active Directory
IPsec-Auth-On-Rekey	是	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	是	60	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	是	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要作为防火墙策略推送到客户端的过称
IPsec-Client-Firewall-Filter-Optional	是	58	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	是	28	字符串	单值	指定要发送到客户端的单个默认域名（1符）。
IPsec-IKE-Peer-ID-Check	是	40	整数	单值	1 = 必需 2 = 如果对等证书支持 3 = 不检
IPsec-IP-Compression	是	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	是	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	是	34	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	是	35	整数	单值	4001 到 49151。默认值为 10000。
IPsec-Required-Client-Firewall-Capability	是	56	整数	单值	0 = 无 1 = 远程 FW Are-You-There (AYT)略 2 = 策略推送的 CPP 4 = 来自服务器的
IPsec-Sec-Association		12	字符串	单值	安全关联的名称

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
IPsec-Split-DNS-Names	是	29	字符串	单值	指定要发送到客户端的辅助域名列表（1 到2符）。
IPsec-Split-Tunneling-Policy	是	55	整数	单值	0 = 无拆分隧道 1 = 拆分隧道 2 = 允许本地 L
IPsec-Split-Tunnel-List	是	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 AC称。
IPsec-Tunnel-Type	是	30	整数	单值	1 = LAN 到 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 已禁用 1 = 已启用
IPv6-Address-Pools	是	218	字符串	单值	IP 本地池 IPv6 的名称
IPv6-VPN-Filter	是	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8无状态 15= 40/128 位加密/需要无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用
Member-Of	是	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设略。
MS-Client-Subnet-Mask	是	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 到 86400 秒
NAC-Settings	是	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 到 1800 秒
Perfect-Forward-Secrecy-Enable	是	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8无状态 15= 40/128 位加密/需要无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	是	5	字符串	单值	IP 地址

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
Primary-WINS	是	7	字符串	单值	IP 地址
Privilege-Level	是	220	整数	单值	介于 0 和 15 之间的整数。
Required-Client- Firewall-Vendor-Code	是	45	整数	单值	1 = 思科系统（使用思科集成客户端） 2 = 3 = NetworkICE 4 = Sygate 5 = 思科系统 入侵防御安全代理）
Required-Client-Firewall-Description	是	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	是	46	整数	单值	思科系统公司产品： 1 = 思科入侵防御安全代理或思科集成客 Zone Labs 产品： 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defende Sygate 产品： 1 = Personal Firewall 2 = P Firewall Pro 3 = 安全代理
Required-Individual-User-Auth	是	49	整数	单值	0 = 已禁用 1 = 已启用
Require-HW-Client-Auth	是	48	布尔值	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	是	6	字符串	单值	IP 地址
Secondary-WINS	是	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	是	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客 Session Subtype 的适用条件是 Session Typ 性仅具有以下值：1、2、3 和 4。
Session Type	是	151	整数	单值	0 = 无1 = Secure Client SSL VPN 2 = Secu IPSec VPN (IKEv2) 3 = 无客户端 SSL VP 户端邮件代理5 = 思科 VPN 客户端 (IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN
Simultaneous-Logins	是	2	整数	单值	0 到 2147483647
Smart-Tunnel	是	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	是	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	是	139	字符串	单值	智能隧道自动登录名称列表（附带域名）

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
Strip-Realm	是	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	是	131	字符串	单值	0 = 已禁用 1 = 已启用 3 = 启用默认服务 5 = 认无客户端 （未使用 2 和 4）
SVC-Ask-Timeout	是	132	整数	单值	5 到 120 秒
SVC-DPD-Interval-Client	是	108	整数	单值	0 = 关 5-3600 秒
SVC-DPD-Interval-Gateway	是	109	整数	单值	0 = 关） 5-3600 秒
SVC-DTLS	是	123	整数	单值	0 = 错误 1 = 正确
SVC-Keepalive	是	107	整数	单值	0 = 关 15-600 秒
SVC-Modules	是	127	字符串	单值	字符串（模块的名称）
SVC-MTU	是	125	整数	单值	MTU 值 256-1406 字节
SVC-Profiles	是	128	字符串	单值	字符串（配置文件的名称）
SVC-Rekey-Time	是	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	是	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	是	85	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	是	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2T 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 互斥。 0 - 11、16 - 27、32 - 43、48 - 59 是合
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
VLAN	是	140	整数	单值	0 到 4094
WebVPN-Access-List	是	73	字符串	单值	访问列表名称
WebVPN ACL	是	73	字符串	单值	设备上的 WebVPN ACL 的名称
WebVPN-ActiveX-Relay	是	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	是	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	是	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	是	101	整数	单值	0 = 已禁用 1 = 已启用

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Content-Filter-Parameters	是	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 的 Cookie
WebVPN-Customization	是	113	字符串	单值	自定义的名称
WebVPN-Default-Homepage	是	76	字符串	单值	URL，例如 http://example-example.com
WebVPN-Deny-Message	是	116	字符串	单值	有效字符串（最多 500 个字符）
WebVPN-Download_Max-Size	是	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	是	94	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	是	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	是	95	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	是	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP *.cisco.com、192.168.1.*、wwwin.cisco.co
WebVPN-Hidden-Shares	是	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	是	228	布尔值	单值	已启用（如果无客户端主页将通过智能隧
WebVPN-HTML-Filter	是	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = C
WebVPN-HTTP-Compression	是	120	整数	单值	0 = 关 1 = Deflate 压缩
WebVPN-HTTP-Proxy-IP-Address	是	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https 如 http=10.10.10.10:80、https=11.11.11.11:
WebVPN-Idle-Timeout-Alert-Interval	是	148	整数	单值	0 到 30 0 = 已禁用。
WebVPN-Keepalive-Ignore	是	121	整数	单值	0 到 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。
WebVPN-Port-Forwarding-Enable	是	97	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	是	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	是	99	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-List	是	72	字符串	单值	端口转发列表名称

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Port-Forwarding-Name	是	79	字符串	单值	字符串名称（例如，“Corporate-Apps”）。 此文本将替换无客户端门户主页上的默认字 “Application Access”。
WebVPN-Post-Max-Size	是	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	是	149	整数	单值	0 到 30 0 = 已禁用。
WebVPN Smart-Card-Removal-Disconnect	是	225	布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Smart-Tunnel	是	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	是	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
WebVPN-Smart-Tunnel-Auto-Start	是	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	是	227	字符串	单值	“e networkname”、“i networkname”或“a 一，其中 networkname 是指智能隧道网络列 称，e表示不包含的隧道，i表示指定的隧道， 所有隧道。
WebVPN-SSL-VPN-Client-Enable	是	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep- Installation	是	105	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Required	是	104	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSO-Server-Name	是	114	字符串	单值	有效字符串
WebVPN-Storage-Key	是	162	字符串	单值	
WebVPN-Storage-Objects	是	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	是	107	整数	单值	15 到 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	是	108	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	是	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	是	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	是	109	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-Rekey-Time	是	110	整数	单值	4 到 10080 分钟，0 = 关闭
WebVPN-SVC-Rekey-Method	是	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）

属性名称	Firewall Threat Defense	属性编号	语法/类型	单值或多值	说明或值
WebVPN-SVC-Compression	是	112	整数	单值	0（关闭）、1（Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	是	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	是	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	是	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	是	93	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-URL-List	是	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	是	160	字符串	单值	
WebVPN-VDI	是	163	字符串	单值	设置列表

表 *92:* 发送到 *Cisco Secure Firewall Threat Defense* 的 *RADIUS* 属性

属性	属性编号	语法、类型	单值或多值	说明或值
Address-Pools	217	字符串	单值	Firewall Threat Defense 设备上定义的网络对象名称，用于识别将作为地址池供客户端连接远程访问 VPN 时使用的子网。在**对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。
可下载 ACL	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		通过 Cisco-AV-Pair 配置来支持。
过滤器 ACL	86, 87	字符串	单值	过滤器 ACL 由 RADIUS 服务器中的 ACL 名称引用。它要求 Firewall Threat Defense设备上已经存在 ACL 配置，以便可以在 RADIUS 授权期间使用该配置。 86=Access-List-Inbound 87=Access-List-Outbound

属性	属性编号	语法、类型	单值或多值	说明或值
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在远程访问 VPN **组策略**页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	允许用户建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 Firewall Threat Defense设备的子接口上配置此 VLAN。

您必须将从 ISE 返回的 IE-Proxy-Server-Method 属性的值设置为以下值之一：

- IE_PROXY_Method_PACFILE: 8
- IE_PROXY_Method_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_Method_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_Method_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

Firewall Threat Defense 仅当上述值之一用于 IE-Proxy-Server-Method 属性时，才会提供代理设置。

创建或更新连接配置文件的别名

别名包含特定连接配置文件的备用名称或 URL。远程访问 VPN 管理员可以启用或禁用别名和别名 URL。VPN 用户可以在连接到 Cisco Secure Firewall Threat Defense设备时选择别名。可以开启或关闭在此设备上配置的所有连接的别名，以开启或关闭别名显示。您还可以配置别名URL列表，您的终端在启动远程访问 VPN 连接时可以从该列表中进行选择。如果用户使用别名 URL 进行连接，则系统将使用与别名 URL 匹配的连接配置文件自动记录它们。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要修改的策略上的**编辑 (Edit)**。

步骤 3 在要为其创建或更新别名的连接配置文件上点击**编辑 (Edit)**。

步骤 4 点击 **别名**。

步骤 5 要添加别名，请执行以下操作：

a) 点击**别名 (Alias Names)** 下的**添加 (Add)**。

b) 指定**别名**。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 6 要添加别名 URL，请执行以下操作：

a) 点击 **URL 别名 (URL Alias)** 下的**添加 (Add)**。
b) 从列表中选择 **别名 URL** 或创建新的 URL 对象。有关详细信息，请参阅创建 URL 对象，第 2705 页。
c) 选中每个窗口中的**已启用**复选框以启用别名。
d) 点击**确定**。

步骤 7 保存更改。

相关主题

配置连接配置文件设置，第 1552 页

配置远程访问 VPN 的访问接口

访问接口表列出了包含设备接口的接口组和安全区域。它们配置用于远程访问 SSL 或 IPsec IKEv2 VPN 连接。该表显示每个接口组或安全区域的名称、接口使用的接口信任点以及是否启用了数据报传输层安全(DTLS)。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 点击**访问接口 (Access Interface)** 选项卡。

步骤 4 要添加访问接口，请点击 **+**，并在**添加访问接口 (Add Access Interface)** 对话框中为以下选项指定值：

a) **访问接口** - 选择接口所属的接口组或安全区域。

接口组或安全区域必须是路由类型。远程访问 VPN 连接不支持其他接口类型。

b) 通过选择以下选项将**协议**对象与访问接口关联：

- **启用 IPSet-IKEv2** - 选择此选项可启用 **IKEv2** 设置。
- **启用 SSL** - 选择此选项可启用 **SSL** 设置。
  - 选择**启用数据报传输层安全**。

    选中此选项后，将在接口上启用数据报传输层安全 (DTLS)，并允许 Cisco Secure Client 的 AnyConnect VPN 模块使用两个同步隧道（一个 SSL 隧道和一个 DTLS 隧道）建立 SSL VPN 连接。

启用 DTLS 可避免与某些 SSL 连接相关的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。

要配置 SSL 设置以及 TLS 和 DTLS 版本，请参阅 关于 SSL 设置，第 1007 页。

要配置 Cisco Secure Client 的 AnyConnect VPN 型号的 SSL 设置，请参阅 组策略 Secure Client 选项，第 2727 页。

- 选中 **配置接口特定身份证书** 复选框，然后从下拉列表中选择 **接口身份证书** 。

  如果不选择接口身份证书，则默认使用 **信任点**。

  如果不选择接口身份证书或信任点，则默认使用 **SSL 全局身份证书** 。

c) 点击**确定** 以保存更改。

步骤 5 在 **访问设置**下选择以下选项：

- **允许用户选择将登录的连接配置文件 (Allow Users to select connection profile while logging in)** - 如果您有多个连接配置文件，选中此复选框将允许用户在登录期间选择正确的连接配置文件。必须为 **IPsec-IKEv2** VPN 选择此选项。
- **启用仅 HTTP VPN Cookie** - 选中此复选框可限制对浏览器及其 HTTP 会话的 Cookie 数据访问，确保数据仅对服务器可用。此选项有助于防御跨站脚本攻击。

步骤 6 使用以下选项配置 **SSL 设置**：

- **Web 访问端口号** - 用于 VPN 会话的端口。默认端口为 443。
- **DTLS 端口号** - 要用于 DTLS 连接的 UDP 端口。默认端口为 443。
- **SSL 全域身份证书**-如果未提供 **接口特定身份证书** ，则选定的 **SSL 全局身份证书** 将用于所有关联的接口。

  您可以选择 ACME 证书以对 VPN 网关进行身份验证。ACME 证书可自动执行 SSL 和 TLS 证书的生命周期管理，包括自动续约。

步骤 7 对于 **IPsec-IKEv2 设置**，请从列表中选择 **IKEv2 身份证书** 或添加身份证书。

步骤 8 配置**服务访问控制 (Service Access Control)**。从**服务访问对象 (Service Access Object)** 下拉列表中选择服务访问对象，或点击 + 创建新对象。

您可以在运行 7.7 或更高版本的 Firewall Threat Defense 设备上使用服务访问对象，以便控制对远程客户访问 VPN 的访问。该对象可在 VPN 验证前为客户端提供基于地理位置的访问控制。默认情况下，RA VPN 没有访问控制，远程客户端可以从任何地理位置进行连接，除非由服务访问对象指定。有关详细信息，请参阅基于地理位置管理远程用户的 VPN 访问，第 1604 页和配置服务访问对象，第 2628 页。

步骤 9 在 **VPN 流量的访问控制** 部分下，如果要绕过访问控制策略，请选择以下选项：

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** - 默认情况下，已解密流量要经过访问控制策略的检查。启用“为已解密的流量绕过访问控制策略”选项会绕过 ACL 检查，但 VPN 过滤器 ACL 以及从 AAA 服务器下载的身份验证 ACL 仍适用于 VPN 流量。

注释
如果选择此选项，则无需更新在 Cisco Secure Firewall Threat Defense 设备上更新访问控制策略，第 1545 页中指定的远程访问 VPN 的访问控制策略。

步骤 10 点击**保存**，保存接口更改。

相关主题
接口，第 2655 页

配置远程访问 VPN 的高级选项

思科 安全客户端 映像

安全客户端 映像

安全客户端通过企业资源的全 VPN 调配为远程用户提供到 Firewall Threat Defense 设备的安全 SSL 或 IPsec (IKEv2) 连接。如果先前没有安装客户端，远程用户可以输入为在其浏览器中接受无客户端 VPN 连接所配置的接口的 IP 地址，以下载并安装 Secure Client。Firewall Threat Defense设备下载与远程计算机的操作系统匹配的客户端。下载后，客户端安装并建立安全连接。如果先前已安装客户端，当用户进行身份验证时， Firewall Threat Defense 设备将检查客户端的版本并在必要情况下升级客户端。

远程访问 VPN 管理员将新的或附加的 Secure Client 映像与 VPN 策略相关联。管理员可以取消关联不受支持的或生命周期终止的客户端程序包。

Secure Firewall Management Center通过使用文件包名称确定操作系统的类型。如果用户重命名文件而不指示操作系统信息，则必须从列表框中选择有效的操作系统类型。

通过访问 Cisco 软件下载中心来下载 Secure Client 映像文件。

相关主题
将 安全客户端 映像添加到 Secure Firewall Management Center，第 1573 页

将 安全客户端 映像添加到 Secure Firewall Management Center

您可以使用 **安全客户端文件**对象将 安全客户端 映像上传到 Secure Firewall Management Center。有关详细信息，请参阅文件对象，第 2737 页。有关客户端映像的详细信息，请参阅思科 安全客户端 映像，第 1573 页。

过程

步骤 1 选择 **安全连接** > **远程访问 VPN**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)**选项卡。

步骤 2 点击**添加 (Add)** 以添加 安全客户端 映像。

步骤 3 在 **安全客户端映像 (Secure Client Images)** 对话框的**可用安全客户端映像 (Available Secure Client Images)**中点击**添加 (Add)**。

步骤 4 为可用的 安全客户端 映像输入**名称 (Name)** 和**说明 (Description)**（可选）。

步骤 5 点击**浏览 (Browse)**，找到想要上传的客户端映像。

步骤 6 点击**保存** 以便将映像上传到 防火墙管理中心。

在将客户端映像上传到 Secure Firewall Management Center 时，会自动显示映像的操作系统信息。

步骤 7 要更改客户端映像的顺序，请点击**显示重新排序按钮 (Show Re-order buttons)**，然后向上或向下移动客户端映像。

相关主题

思科 安全客户端 映像 ， 第 1573 页

更新远程接入 VPN 客户端的 安全客户端映像

当 思科软件下载中心提供新的 安全客户端 更新时，您可以手动下载软件包并将其添加到远程接入 VPN 策略，以便根据其操作系统在 VPN 客户端系统上升级新的客户端软件包。

开始之前

此部分中的说明可帮助您更新连接 Cisco Secure Firewall Threat Defense VPN 网关的远程接入 VPN 客户端的新 安全客户端 客户端映像。更新 安全客户端 映像之前，确保完成以下配置：

- 从思科软件下载中心下载最新的 安全客户端 映像文件。
- 在您的 Secure Firewall Management Center Web 界面上，转到，并添加新的 Secure Client 映像文件。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 从**高级**下拉菜单中，选择 **AnyConnect 客户端映像Secure Client 映像**，然后点击**添加**。

步骤 4 从 **可用的安全客户端映像** 中选择客户端图像文件，然后点击 **添加**。

如果未列出所需的客户端映像，点击 **添加** 浏览并上传映像。

步骤 5 点击**确定**。

步骤 6 保存远程访问 VPN 策略。

在部署远程访问 VPN 策略更改之后，新的 安全客户端 映像将在 Cisco Secure Firewall Threat Defense 设备上更新，该设备配置为远程接入 VPN 网关。当新的 VPN 用户连接到 VPN 网关时，用户将根据客户端系统的操作系统获取要下载的新 Secure Client 映像。对于现有 VPN 用户， Secure Client 映像将在其下一个 VPN 会话中更新。

将思科 安全客户端 外部浏览器软件包添加到 Secure Firewall Management Center

如果您的本地磁盘上有一个 安全客户端 外部浏览器软件包镜像，请使用此程序将其上传到 Secure Firewall Management Center。上传外部浏览器软件包后，您可以为远程访问 VPN 连接更新外部浏览器软件包。

您可以使用 **安全客户端文件**对象将外部浏览器软件包文件上传到 Secure Firewall Management Center。有关详细信息，请参阅文件对象 ，第 2737 页。

要点回顾

- 只能向 Firewall Threat Defense 设备添加一个外部浏览器软件包。
- 将外部浏览器软件包添加到 防火墙管理中心 后，只有在远程接入 VPN 配置中启用外部浏览器后，才会将浏览器推送到 Firewall Threat Defense。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**，选择并编辑列出的远程访问策略，然后选择**高级 (Advanced)**选项卡。

步骤 2 点击 **安全客户端映像** 页面的 **安全客户端外部浏览器包** 部分中的 **添加** 。

步骤 3 输入 安全客户端 软件包的 **名称** 和 **说明** 。

步骤 4 点击 **浏览** 并找到要上传的外部浏览器软件包文件。

步骤 5 点击**保存**以便将映像上传到 Secure Firewall Management Center。

注释
如果要使用现有外部浏览器软件包来更新远程访问 VPN 连接，请从 **软件包文件** 下拉列表中选择该文件。

步骤 6 保存远程访问 VPN 策略。

相关主题

思科 安全客户端 映像 ，第 1573 页

远程接入 VPN 地址分配策略

Firewall Threat Defense设备可以使用 IPv4 或 IPv6 策略将 IP 地址分配给远程接入 VPN 客户端。如已配置多个地址分配方法，则 Firewall Threat Defense设备将尝试每一个选项，直到找到一个 IP 地址为止。

IPv4 或 IPv6 策略

您可以使用 IPv4 或 IPv6 策略对远程接入 VPN 客户端的 IP 地址进行寻址。首先，您必须尝试使用 IPv4 策略，然后再尝试使用 IPv6 策略。

- **使用授权服务器**- 在每个用户的基础上从外部授权服务器检索地址。如果使用已配置 IP 地址的授权服务器，建议使用此方法。只有基于 RADIUS 的授权服务器支持地址分配。AD/LDAP 则不支持。此方法适用于 IPv4 和 IPv6 分配策略。
- **使用 DHCP** - 从在连接配置文件中配置的 DHCP 服务器获取 IP 地址。您还可以通过在组策略中配置 DHCP 网络范围来定义 DHCP 服务器可以使用的 IP 地址的范围。如果使用 DHCP，则在**对象** > **网络**中配置服务器。此方法适用于 IPv4 分配策略。

  有关 DHCP 网络范围配置的详细信息，请参阅组策略常规选项，第 2725 页。
- **使用内部地址池** - 内部配置的地址池是分配地址池以进行配置的最简单方法。如果使用此方法，请在**对象** > **地址池** 窗格中创建 IP 地址池，并在连接配置文件中做出相同的选择。此方法适用于 IPv4 和 IPv6 分配策略。
- **允许释放 IP 地址一段时间之后对其重新使用** - 在 IP 地址返回到地址池之后，延迟一段时间方可重新使用。增加延迟有助于防止防火墙在快速重新分配 IP 地址时遇到的问题。默认情况下，延迟设置为零。如果要延长延迟，请输入取值范围为 0 至 480 内的分钟数，以便延迟 IP 地址重新分配。此配置元素适用于 IPv4 分配策略。

相关主题

配置连接配置文件设置，第 1552 页
远程访问 VPN 身份验证，第 1534 页

配置证书映射

通过证书映射，您可以根据证书的字段内容定义匹配连接配置文件的用户证书的规则。证书映射提供安全网关上的证书身份验证。

规则或证书映射在证书映射对象，第 2721 页中定义。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择 **高级** > **证书映射**。

步骤 4 从 **连接配置文件映射的常规设置** 窗格中选择以下选项：

选择是基于优先级的，如果没有找到第一个选择的匹配项，则继续向下匹配列表中的选项。当满足规则时，匹配完成。如果不满足规则，则使用默认的连接配置文件（在底部列出）用于此连接。选择以下任意选项或所有选项，以建立身份验证并确定应映射到客户端的连接配置文件（隧道组）。

- **如果组 URL 和证书映射匹配不同的连接配置文件，则使用组 URL**。
- **使用配置的规则将证书匹配到连接配置文件**- 启用此功能可以使用连接配置文件映射中定义的规则。

注释

配置证书映射意味着采用基于证书的身份验证方法。系统将提示远程用户输入客户端证书，而不考虑配置的身份验证方法。

步骤 5 在**证书到连接配置文件映射 (Certificate to Connection Profile Mapping)** 部分下，点击**添加映射 (Add Mapping)**，以便为此策略创建证书到连接配置文件的映射。

a) 选择或创建 **证书映射名称** 对象。

b) 选择当满足证书映射对象中的规则时想要使用的 **连接配置文件** 。

c) 点击**确定 (OK)** 以创建映射。

步骤 6 点击**保存**。

配置组策略

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。



注释 Firewall Threat Defense 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时 AAA 服务器识别的组策略对象；如果未指定组策略对象，则使用为 VPN 连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 选择**高级 (Advanced)** > **组策略 (Group Policies)** > **添加 (Add)**。

步骤 4 从**可用组策略 (Available Group Policy)** 列表中选择组策略并点击**添加 (Add)**。您可以选择与此远程访问 VPN 策略关联的一个或多个组策略。

步骤 5 点击**确定** 以完成组策略选择。

步骤 6 保存更改。

相关主题

配置组策略对象 ， 第 2724 页

配置 LDAP 属性映射

LDAP 属性名称将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。属性映射将 Active Directory（AD）或 LDAP 服务器中存在的属性与 Cisco 属性名称等同起来。您可以将任何标准 LDAP 属性映射到公认的供应商特定属性 (VSA)。您可以将一个或多个 LDAP 属性映射到一个或多个 Cisco LDAP 属性。当 AD 或 LDAP 服务器在远程访问 VPN 连接建立期间向 Firewall Threat Defense 设备返回身份验证时， Firewall Threat Defense 设备可以使用该信息调整 Secure Client 如何完成连接。

当您想要为 VPN 用户提供不同的访问权限或 VPN 内容时，您可以在 VPN 服务器上配置不同的 VPN 策略，并根据其凭证将这些策略集分配给每个用户。您可以在 Firewall Threat Defense 中通过使用 LDAP 属性映射配置 LDAP 授权来实现此目的。要使用 LDAP 将组策略分配给用户，您必须配置映射 LDAP 属性的映射。

LDAP 属性映射包括三个组件：

- **领域 (Realm)** - 指定 LDAP 属性映射的名称；名称根据所选领域生成。
- **属性名称映射 (Attribute Name Map)** - 将 LDAP 用户或组属性名称映射到 Cisco 可理解的名称。
- **属性值映射 (Attribute Value Map)** - 将 LDAP 用户或组属性中的值映射到所选名称映射的 Cisco 属性值.

LDAP 属性映射中使用的组策略将被添加到远程访问 VPN 配置中的组策略列表。从远程访问 VPN 配置中删除组策略也会删除相关的 LDAP 属性映射。

在版本 6.4 到 6.6 中，只能使用 FlexConfig 配置 LDAP 属性映射。有关详细信息，请参阅 使用 FlexConfig 配置 AnyConnect 模块和配置文件。

在 7.0 及更高版本中，可以使用以下程序：

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 在列表中选择现有的远程访问策略，然后点击相应的**编辑**图标。

步骤 3 点击 **高级** > **LDAP 属性映射**。

步骤 4 点击**添加 (Add)**。

步骤 5 在配置 LDAP 属性映射页面上，选择要配置属性映射的 **领域** 。

步骤 6 点击**添加 (Add)**。

您可以配置多个属性映射。每个属性映射都要求您配置名称映射和值映射。

注释
确保在创建 LDAP 属性映射时遵循以下准则：

- 为 LDAP 属性至少配置一个映射；不允许多个具有相同 LDAP 属性名称的映射。
- 配置至少一个名称映射以创建 LDAP 属性映射。

- 如果属性映射未与远程访问 VPN 配置中的任何连接配置文件关联，您可以删除任何 LDAP 属性映射。
- 对 与 Cisco 和 LDAP 属性名称和值使用 LDAP 属性映射中的正确拼写和大写。

a) 指定 **LDAP 属性名称**，然后从列表中选择所需的 **Cisco 属性名称** 。
b) 点击 **添加值映射** 并指定 **LDAP 属性值** 和 **Cisco 属性值**。

重复此步骤以添加更多值映射。

步骤 7 点击**确定** 以完成 LDAP 属性映射配置。

步骤 8 点击 **保存** 以保存对 LDAP 属性映射的更改。

示例

有关详细示例，请参阅 为 FTD 配置具有 LDAP 身份验证和授权的 RA VPN。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1555 页
了解权限和属性的策略实施，第 1536 页

配置 VPN 负载均衡

关于 VPN 负载均衡

Firewall Threat Defense 中的 VPN 负载均衡允许您对两台或更多设备进行逻辑分组，并在设备之间平均分配远程接入 VPN 会话。VPN 负载均衡会在负载均衡组中的设备之间共享 Secure Client VPN 会话。

VPN 负载均衡基于简单的流量分配，而不考虑吞吐量或其他因素。VPN 负载均衡组由两台或更多 Firewall Threat Defense 设备组成。一台设备充当导向器，而其他设备是成员设备。组中的设备不需要是完全相同的类型，也不需要具有相同的软件版本和配置。支持远程接入 VPN 的任何 Firewall Threat Defense 设备都可以加入负载均衡组。 Firewall Threat Defense 支持使用 AnyConnect 安全客户端 SAML 身份验证进行 VPN 负载均衡。

VPN 负载均衡组中的所有主用设备都会承载会话负载。VPN 负载均衡可以将流量定向至组中负载最低的设备，在所有设备之间分配负载。这样可以高效地利用系统资源，提供更高的性能和高可用性。

VPN 负载均衡的组件

以下是 VPN 负载均衡的组件：

- **负载均衡组 (Load-balancing group)** - 由两台或多台 Firewall Threat Defense 设备组成的虚拟组，用于共享 VPN 会话。

  VPN 负载均衡组可以包含相同版本或混合版本的 Firewall Threat Defense 设备；但设备必须要支持远程接入 VPN 配置。

请参阅配置 VPN 负载均衡的组设置，第 1580 页和配置负载均衡的其他设置，第 1581 页。

- **导向器 (Director)** - 由组中的一个设备充当导向器。它会在组中的其他成员之间分配负载，并参与为 VPN 会话提供服务。

  导向器会监控组中的所有设备、追踪每台设备的负载情况，然后相应地分配会话负载。导向器的角色不会与某台物理设备绑定；它可以在设备之间切换。例如，如果当前的导向器发生故障，该组的一台成员设备会接管该角色，立即成为新的导向器。

- **成员 (Members)** - 组中除导向器以外的设备均被称为成员。它们会参与负载均衡并共享远程接入 VPN 连接。

  配置参与设备的设置，第 1582 页。

VPN 负载均衡的前提条件

- **证书 (Certificates)** - Firewall Threat Defense 的证书必须包含连接重定向到的导向器和成员的 IP 地址或 FQDN。否则，证书将被视为不可信。证书必须使用使用者替代名称 (SAN) 或通配符证书
- **组 URL (Group URL)** - 在连接配置文件中添加 VPN 负载均衡组 IP 地址的组 URL。指定组 URL，以便用户在登录时无需再选择组。
- **IP 地址池 (IP Address Pool)** - 为成员设备选择唯一的 IP 地址池，并覆盖 防火墙管理中心 中每个成员设备的 IP 池。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。

VPN 负载均衡准则和限制

- 默认情况下会禁用 VPN 负载均衡。您必须显式启用 VPN 负载均衡。
- 只有协同定位的 Firewall Threat Defense 设备才能被添加到负载均衡组中。
- 一个负载均衡组必须至少有两台 Firewall Threat Defense 设备。
- Firewall Threat Defense 高可用性的设备可以加入负载均衡组。
- 网络地址转换 (NAT) 后面的设备也可以作为负载均衡组的一部分。
- 当成员或导向器设备发生故障时，该设备提供的远程接入VPN连接会被丢弃。您必须再次启动 VPN 连接。
- 每台设备上的身份证书必须具有使用者替代名称 (SAN) 或通配符。

配置 VPN 负载均衡的组设置

您可以启用VPN负载均衡，并配置适用于负载均衡组所有成员的组设置。在创建组时，您可以配置负载均衡的参与设置。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 点击**启用成员设备之间的负载均衡 (Enable Load balancing between member devices)** 切换按钮以启用负载均衡。
系统将打开 **编辑组配置** 页面。组参数适用于负载均衡组下的所有设备。

步骤 5 如果适用，请指定 **组 IPv4 地址** 和 **组 IPv6 地址** 。

此处指定的 IP 地址用于整个负载均衡组，而导向器将为传入 VPN 连接打开此 IP 地址。

步骤 6 为负载均衡组选择 **通信接口** 。点击 **添加** 以添加接口组或安全区域。

通信接口是一个专用接口，导向器和成员都会通过该接口共享有关其负载的信息。

步骤 7 输入用于在组中的导向器和成员之间进行通信的 **UDP 端口** 。默认端口为 9023。

步骤 8 启用 **IPsec 加密** 切换按钮，为导向器和成员之间的通信激活 IPsec 加密。

启用加密后会使用预共享密钥在导向器和成员之间建立 IPsec 隧道。

当您在启用了 **IPsec 加密 (IPsec Encryption)** 选项的情况下升级或降级 Firewall Threat Defense 设备时，请确保 防火墙管理中心 和 Firewall Threat Defense 之间的配置没有不匹配，以防部署失败。

步骤 9 输入用于 IPsec 加密的 **加密密钥** 。

步骤 10 点击**确定**。

配置负载均衡的其他设置

VPN 负载均衡的其他设置包括 FQDN 和 IKEv2 重定向。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果已经完成，打开 **启用成员设备之间的负载均衡** 切换按钮以启用负载均衡。

步骤 5 点击**设置**。

步骤 6 打开 **将 FQDN 发送到对等设备而不是 IP** 切换按钮以启用使用完全限定域名的重定向。

默认情况下，Firewall Threat Defense 只会将 VPN 负载均衡重定向中的 IP 地址发给客户端。

步骤 7 选择 **IKEv2 重定向** 阶段之一：

- 在 SA 身份验证期间重定向
- 在 SA 初始化期间重定向

步骤 8 点击**确定**。

步骤 9 保存更改。

配置参与设备的设置

设备参与设置将确定设备如何在 VPN 负载均衡中共享负载。在设备上启用 VPN 负载均衡，并定义设备特定属性，从而配置参与设备。这些值因设备而异。您可以为参与负载均衡的设备提供优先级编号。优先级越高，设备就越有可能成为导向器，而不是其他设备。但您不能选择某个设备作为该组的导向器。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程接入 VPN 策略旁边的 **编辑** 。

步骤 3 点击**高级 (Advanced)** > **负载均衡 (Load Balancing)**。

步骤 4 如果尚未启用负载均衡，打开 **启用成员设备之间的负载均衡** 切换按钮以启用负载均衡。

步骤 5 配置**设备参与 (Device Participation)** 设置：

设备参与 部分列出了所选远程访问 VPN 配置的目标设备。可以配置这些设备，为分担传入 VPN 会话的负载。

a) 打开 **负载均衡** 切换按钮，为设备启用负载均衡，然后点击 **编辑**。

b) 输入设备**优先级**。

默认情况下，设备优先级会被设为 5。您可以从 1 到 10 中选择一个数字。

c) 如果设备位于 NAT 之后，请为 VPN 接口 IP 地址指定 **IPv4 NAT** 或 **IPv6 NAT** 地址。

d) 点击**确定**。

步骤 6 点击**保存**以保存远程访问 VPN 策略设置。

配置远程接入 VPN 的 IPsec 设置

只有在配置远程接入 VPN 策略时选择 IPsec 作为 VPN 协议时，IPsec 设置才适用。否则，可以使用“编辑访问接口”对话框启用 IKEv2。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1571 页。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击 **Advanced**。

IPsec 设置列表将显示在屏幕左侧的导航窗格中。

步骤 4 使用导航窗格编辑下列 IPsec 选项：

a) **加密映射** -“加密映射”页面列出了在其上启用了 IKEv2 协议的接口组。启用 IKEv2 协议的接口将自动生成加密映射。要编辑加密映射，请参阅配置远程接入 VPN 加密映射，第 1583 页。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1571 页。

b) **IKE 策略** - 当 安全客户端 终端使用 IPsec 协议进行连接时，“IKE 策略”页面将列出适用于所选 VPN 策略的所有 IKE 策略对象。有关详细信息，请参阅 远程接入 VPN 中的 IKE 策略，第 1585 页。要添加新的 IKE 策略，请参阅 配置 IKEv2 策略对象，第 2735 页。 Firewall Threat Defense 仅支持 安全客户端 IKEv2 客户端。不支持第三方标准 IKEv2 客户端。

c) **IPsec/IKEv2 参数** -“IPsec/IKEv2 参数”页面使您可以修改 IKEv2 会话设置、IKEv2 安全关联设置、IPsec 设置和 NAT 透明度设置。有关详细信息，请参阅配置远程访问 VPN IPsec/IKEv2 参数，第 1586 页。

步骤 5 点击**保存**。

配置远程接入 VPN 加密映射

对于已启用 IPsec-IKEv2 协议的接口，将自动生成加密映射。可在**访问接口 (Access Interface)** 中，为选定的 VPN 策略添加或删除接口组。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1571 页。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **加密映射 (Crypto Maps)**，选择表中的一行并点击**编辑 (Edit)** 以编辑加密映射选项。

步骤 4 选择 **IKEv2 IPsec 提议 (IKEv2 IPsec Proposals)** 并选择对指定将使用哪些身份验证和加密算法来保护隧道中的流量安全的集合进行转换。

步骤 5 选择**启用反向路由注入 (Enable Reverse Route Injection)** 以启用静态路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。

步骤 6 选择**启用客户端服务 (Enable Client Services)** 并指定端口号。

客户端服务服务器提供 HTTPS (SSL) 访问，以允许 安全客户端下载程序接收软件升级、配置文件、本地化和自定义文档、CSD、SCEP 以及客户端所需的其他文件下载。如果选择此选项，请指定客户端服务端口号。如果不启用客户端服务服务器，用户将无法下载 安全客户端可能需要的任何文件。

注释
您可以使用与在同一设备上运行的 SSL VPN 相同的端口。即使配置了 SSL VPN，您也必须选择此选项，以便通过 SSL 为 IPsec-IKEv2 客户端启用文件下载。

步骤 7 选择**启用完全向前保密 (Enable Perfect Forward Secrecy)**，然后选择**模数组 (Modulus group)**。

使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享或私有密钥。如果选择此选项，也请选择在**模数组 (Modulus Group)** 列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。

模数组是用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。选择要在远程接入 VPN 配置中允许的模数组。

- 1 - Diffie-Hellman 组 1（768 位模数）。
- 2 - Diffie-Hellman 组 2（1024 位模数）。
- 5 - Diffie-Hellman 组 5（1536 位模数，可为 128 为密钥提供较好的保护，但组 14 更好）。如果使用的是 AES 加密，请使用此组（或更高的组）。
- 14 - Diffie-Hellman 组 14（2048 位模数，可为 128 为密钥提供较好的保护）。
- 19 - Diffie-Hellman 组 19（256 位椭圆曲线字段大小）。
- 20 - Diffie-Hellman 组 20（384 位椭圆曲线字段大小）。
- 21 - Diffie-Hellman 组 21（521 位椭圆曲线字段大小）。
- 24 - Diffie-Hellman 组 24（2048 位模数和 256 位素数阶子组）。

步骤 8 指定**生命周期持续时间（秒）(Lifetime Duration [seconds])**。

安全关联 (SA) 的生命周期（以秒为单位）。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商就越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。

可指定 120 到 2147483647 秒之间的值。默认值为 28800 秒。

步骤 9 指定**生命周期大小（千字节）(Lifetime Size [kbytes])**。

使用特定安全关联的 Ipsec 对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。

可指定 10 到 2147483647 千字节之间的值。默认值为 4,608,000 千字节。没有规范允许使用无限数据。

步骤 10 选择以下 **ESPv3 设置 (ESPv3 Settings)**：

- **验证传入 ICMP 错误消息 (Validate incoming ICMP error messages)** - 选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。
- **启用“不分段”策略 (Enable 'Do Not Fragment' Policy)** - 定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位，然后从**策略 (Policy)** 列表选择以下一项。
  - 复制 - 维护 DF 位。
  - 清除 - 忽略 DF 位。
  - 设置 - 设置和使用 DF 位。
- 选择**启用数据流机密性 (TFC) 数据包 (Enable Traffic Flow Confidentiality [TFC] Packets)** - 启用虚拟 TFC 数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用 **Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

  注释
  启用流量保密性 (TFC) 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。请参阅组策略高级选项，第 2730 页。

  - 突发 - 指定 1 到 16 字节之间的值。
  - 负载大小 - 指定 64 到 1024 字节之间的值。
  - 超时 - 指定 10 到 60 秒之间的值。

步骤 11 点击**确定**。

相关主题

接口，第 2655 页

远程接入 VPN 中的 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

注释 Firewall Threat Defense仅支持将 IKEv2 用于远程接入 VPN。

与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑创建多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置远程接入 IPsec VPN 时，需要 IKE 策略。

配置远程接入 *VPN IKE* 策略

IKE 策略表指定，当 安全客户端端点使用 IPsec 协议进行连接时适用于所选 VPN 配置的所有 IKE 策略对象。有关详细信息，请参阅远程接入 VPN 中的 IKE 策略 ， 第 1585 页。



注释 Firewall Threat Defense仅支持用于远程接入 VPN 的 IKEv2。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击**高级 (Advanced)** > **IKE 策略 (IKE Policy)**。

步骤 4 点击**添加 (Add)** 从可用的 IKEv2 策略中选择，或添加新的 IKEv2 策略并指定以下选项：

- **名称 (Name)** - IKEv2 策略的名称。
- **说明 (Description)** - IKEv2 策略的可选说明
- **优先级** — 当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）
- **完整性 (Integrity)** - IKE 策略中使用的散列算法的完整性算法部分。
- **加密 (Encryption)** - 用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的加密算法。
- **PRF 散列 (PRF Hash)** - IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv2 中，您可以为这些元素指定不同的算法。
- **DH 组 (DH Group)** - 用于加密的 Diffie-Hellman 组。

步骤 5 点击**保存**。

配置远程访问 VPN IPsec/IKEv2 参数

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 从可用 VPN 策略列表中，选择要修改其设置的策略。

步骤 3 点击 **高级 (Advanced)** > **IPsec**> **IPsec/IKEv2 参数 (IPsec/IKEv2 Parameters)**。

步骤 4 为 **IKEv2 会话设置**选择以下选项：

- **发送至对等体的身份**-选择对等体将在 IKE 协商期间用于标识自身的身份：
  - **自动**-按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
  - **IP 地址**-使用交换 ISAKMP 身份信息的主机的 IP 地址。
  - **主机名称**-使用交换 ISAKMP 身份信息的主机的完全限定域名 (FQDN)。此名称包含主机名和域名。
- **在断联隧道上启用通知**-当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。
- **请勿允许设备重新引导直至所有会话被终止**-选中以支持等待所有活动在系统重启之前自动终止。默认情况下将禁用此复选框。

步骤 5 为 **IKEv2 安全关联 (SA) 设置**选择以下选项：

- **Cookie 质询**-是否向对等体设备发送 Cookie 质询，以响应 SA 发起的数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：
  - **自定义**-指定 **向质询传入 Cookie 发出挑战的阈值**，这是指允许进行协商的总 SA 数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。默认为 50%。
  - 始终-始终选择向对等设备发送 cookie 质询。
  - 从不-选择从不向对等设备发送 cookie 质询。
- **允许协商的 SA 数量**-限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。默认为 100%。
- **允许的最大 SA 数量**-限制 ASA 上允许的 IKEv2 连接的数量。

步骤 6 为 **IPsec 设置**选择以下选项：

- **解密前启用分片**-此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。
- **路径最大传输单元老化**-选中以启用 PMTU（路径最大传输单元）老化，设置 SA（安全关联）的 PMTU 的间隔。
- **值重置间隔**-输入 SA（安全关联）的 PMTU 值重置为其原始值的分钟数。有效范围是 10 到 30 分钟，默认值为不受限制。

步骤 7 为 **NAT 设置**选择以下选项：

- **保持连接消息穿越** - 选择是否启用 NAT 保持连接消息穿越。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。如果选择此选项，请配置在分支和中间设备之间发送的保持连接信号之间的间隔（以秒为单位），以指示会话处于活动状态。此值可以介于 10 到 3600 秒之间。默认值为 20 秒。

- 间隔-设置 NAT 保持连接间隔，范围从 10 秒到 3600 秒。默认值为 20 秒。

步骤 8 点击保存。

自定义 Cisco Secure Client

您可以使用管理中心配置安全客户端自定义，并将其部署到 VPN 头端。当用户从安全客户端连接时，威胁防御设备会将这些自定义分发到终端。管理员可以在终端上自定义以下元素：

表 *93*: 管理中心中可用的安全客户端自定义

可以定制	说明	更多信息
GUI 文本和消息	自定义或本地化安全客户端 GUI 文本和信息/错误消息。	自定义和本地化安全客户端 GUI 文本和消息，第 1590 页
图标和图像	自定义 Secure Client GUI 的徽标、图像或图标。	自定义安全客户端图标和图像，第 1591 页
脚本	当客户端建立或断开 VPN 会话时，在终端设备上部署脚本。	使用安全客户端在终端设备上部署脚本，第 1592 页
二进制文件	使用安全客户端 API 部署自定义应用。	使用思科安全客户端 API 部署自定义应用，第 1594 页
自定义安装程序转换	自定义安全客户端安装程序。	自定义安全客户端安装程序，第 1595 页
本地化安装程序转换	本地化客户端安装程序。	本地化客户端安装程序，第 1595 页

安全客户端自定义的准则和限制

准则

- 确保将 xml 文件导入到定义为 `DfltCustomization` 的对象中。导入自定义对象时，防火墙管理中心 会检查 XML 代码的有效性。

  例如：

  ```
  hostname# import webvpn customization DfltCustomization
  disk0:/csm/defaultcustomizationwebvpn.xml
  ```

- 在部署自定义命令之前，将 Windows Cisco Secure Client 头端部署包添加到远程访问 VPN 政策。在支持 Windows、MacOS 或 Linux 客户端时，必须包含此包。

一般限制

- 如果使用 CLI 在威胁防御上直接配置了早于 7.4 的任何自定义设置，则管理中心会在部署期间删除这些自定义设置。
- 无集群支持。

表 *94:* 安全客户端自定义的限制

可以定制	限制

GUI 文本和消息自定义	• 在使用此自定义之前，必须重新启动安全客户端。
	• 不支持从右到左的语言。
	• 由于硬编码字段的长度要求，有些字符串在 GUI 中会截断。
	• 某些消息在客户端中进行了硬编码。例如：
	  • 状态消息（更新期间）
	  • 不受信任的服务器消息。
	  • 延期更新消息
	• 本地化是特定于版本的。
	如果管理员基于旧版安全客户端的模板创建了转换表，则新消息不会向远程用户显示。管理员必须将最新的模板与转换表合并，以便该表包含新邮件。您可以使用 Get text 等第三方工具执行合并。

图标和图像自定义	• 在使用此自定义之前，必须重新启动安全客户端。 • 自定义对象名称必须与安全客户端 GUI 文件名匹配。每个操作系统的文件名都不同，并且区分大小写。有关每个操作系统的文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。 • 如果图像大小不正确，则图像无法正确显示。管理中心或威胁防御设备不验证映像大小。 • MacOS 不支持自定义安全客户端图像和图标。
部署自定义脚本	• 安全客户端只运行一个 OnConnect 和一个 OnDisconnect 脚本；然而，这些脚本可能会启动其他脚本。 • 脚本只能执行用户有权调用的功能。 • 您无法从登录前启动 (SBL) GUI 启动 OnConnect 脚本。

可以定制	限制
使用 Cisco 安全客户端 API（二进制）部署自定义应用	• 使用此自定义后，如果在管理中心部署更新版本的安全客户端，客户端将下载更新并替换您的自定义 UI。
自定义客户端安装程序	• 此自定义仅适用于 Windows。

自定义和本地化安全客户端 GUI 文本和消息

您可以自定义安全客户端 GUI 文本和信息/错误消息。您还可以自定义以首选语言显示的 GUI 文本和所有消息。

自定义 GUI 文本和消息

要自定义 GUI 文本或消息，可以编辑消息文件中的消息。您可以更新消息，以在错误消息中包含更多详细信息。例如：

- 修改登录对话框中的任何标签，例如将 **密码** 修改为 **域密码**。
- 在错误消息中添加您的支持联系人详细信息。

本地化 GUI 文本和消息

威胁防御设备使用转换表来转换安全客户端中显示的标签和用户消息。当用户连接到远程接入 VPN 时，安全客户端会识别终端上设置的区域设置并下载转换文件。威胁防御设备支持 128 种区域设置。默认情况下，安全客户端以英语安装。

- 对于思科安全客户端 5.0，各种语言的默认本地化文件是应用的一部分。
- 对于 AnyConnect 客户端 4.x，您可以从 Cisco.com 下载几种语言的本地化文件，并将其上传到管理中心。

如何自定义安全客户端 *GUI* 文本和消息

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 从安全客户端软件包或 Cisco.com 获取基本模板或转换文件。例如，AnyConnect.po。

步骤 2 使用文本编辑器添加翻译或自定义标签或消息。

步骤 3 更新与每个 **msgid** 对应的 **msgstr** 字符串。

步骤 4 保存文件。

步骤 5 创建新的安全客户端自定义对象。

a) 选择**对象** > **VPN** > **安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **GUI 文本和消息**。
e) 从 **语言** 下拉列表中，选择要为其添加翻译的语言。
f) 点击 **浏览** 并选择翻译文件。支持的文件扩展名包括 .po、.mo 和 .txt。

步骤 6 将自定义添加到远程接入 VPN 策略。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级** > **安全客户端自定义** > **本地化**。
d) 点击 **+** 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 7 点击**保存**。

步骤 8 选择 **部署** > **部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义，第 1596 页。

自定义安全客户端图标和图像

您可以使用管理中心自定义 Secure Client GUI 的徽标、图像和图标。

要自定义 Secure Client GUI 的徽标、图像和图标，必须在管理中心创建 Secure Client 自定义对象。此自定义对象的名称必须与安全客户端 GUI 文件名匹配。每个操作系统的文件名都不同，并且区分大小写。有关每个操作系统的文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。

例如，如果要替换 Windows 客户端的公司徽标，则必须创建名称为 `company_logo` 的自定义对象，并将此自定义对象添加到远程接入VPN策略。如果为自定义对象使用不同的名称，则安全客户端安装程序不会更改组件。但是，如果部署自己的可执行文件来自定义 GUI，则自定义对象可以具有任何名称。

所有映像文件的位置：

- Windows: **%PROGRAMFILES%\Cisco\Cisco Secure Client\res**
- Linux：**/opt/cisco/secureclient/resources** 或 **/opt/cisco/anyconnect/resources**
- macOS：不支持

注释 建立远程访问VPN连接后，徽标或图像将下载到客户端目录。确保重新启动客户端，更新后的徽标或图像才会显示在您的客户端中。

如何自定义安全客户端映像和图标

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 使用正确的扩展名和大小创建图标或图像。

如果图像大小不正确，则图像无法正确显示。管理中心或威胁防御设备不验证映像大小。

有关文件名、扩展名和大小的详细信息，请参阅 思科安全客户端管理员指南。

步骤 2 创建新的安全客户端自定义对象。

a) 选择**对象** > **VPN** > **安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义对象的名称和说明。

确保自定义对象名称与安全客户端 GUI 文件名匹配。有关文件名的详细信息，请参阅 思科安全客户端管理员指南。

d) 从 **自定义类型** 下拉列表中，选择 **图标和图像**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择文件。支持的文件扩展名包括 .png、.ico 和 .jpeg。
g) 重复步骤 2a - f 以添加多个图标和图像。

步骤 3 将自定义对象添加到远程接入 VPN 策略。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级** > **安全客户端自定义** > **图标和图像**。
d) 点击 + 以选择文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署** > **部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义，第 1596 页。

使用安全客户端在终端设备上部署脚本

发生以下事件时，您可以通过安全客户端下载和运行脚本：

- 使用威胁防御建立新的客户端 VPN 会话。此事件触发的脚本是 OnConnect 脚本，因为该脚本需要此文件名前缀。重新连接 VPN 会话不会触发此脚本。
- 使用威胁防御断开客户端 VPN 会话。此事件触发的脚本是 OnDisconnect 脚本，因为该脚本需要此文件名前缀。

这些脚本异步运行，不会延迟连接建立或断开连接。它们可以是任何扩展名，并且必须在终端上可执行。安全客户端通过文件名识别 OnConnect 脚本和 onDisconnect 脚本。它查找名称以 OnConnect 或 OnDisconnect 开头的文件，并忽略文件扩展名。

此功能的一些示例如下：

- VPN 连接后刷新组策略。
- 在 VPN 连接上安装网络驱动器。
- 在 VPN 断开连接时卸载网络驱动器。

要启用脚本，请在 VPN 配置文件上选中 **启用脚本** 选项 。默认情况下，客户端不会启动脚本。客户端不要求以特定语言编写脚本。它需要在客户端计算机上安装可以运行脚本的应用。为了保证客户端可以启动脚本，脚本必须从命令行运行。

只有在用户登录并建立 VPN 会话后，安全客户端才能启动脚本。您无法从登录前启动 (SBL) GUI 启动 OnConnect 脚本。您必须在 VPN 配置文件上选中 **启用 Post SBL On Connect 脚本** 选项，才能在用户登录后触发脚本。安全客户端是 32 位应用。在 64 位 Windows 版本中运行脚本时，AnyConnect 将使用 cmd.exe 的 32 位版本。

如何为安全客户端添加自定义脚本

开始之前

1. 配置远程接入 VPN。
2. 在 VPN 配置文件中启用脚本。
3. 将 VPN 配置文件添加到远程访问 VPN 组策略。

过程

步骤 1 为平台创建 OnConnect 和 OnDisconnect 脚本。

步骤 2 创建新的安全客户端自定义对象。

a) 选择**对象** > **VPN** > **安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **脚本**。
e) 从 **平台** 下拉列表中选择平台。
f) 选择以下一个选项：

- **On Connect**：选择 OnConnect 脚本。
- **On Disconnect**：选择 OnDisconnect 脚本。

g) 点击 **浏览** 并选择要在终端上执行的脚本。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级** > **安全客户端自定义** > **本地化**。
d) 点击 + 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署** > **部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

下一步做什么

验证安全客户端自定义。有关详细信息，请参阅验证安全客户端自定义，第 1596 页。

使用思科安全客户端 API 部署自定义应用

对于 Windows、Linux 或 MacOs 计算机，您可以创建和部署使用安全客户端 API 的自定义客户端。您可以使用此客户端二进制文件替换安全客户端 GUI 或 CLI 二进制文件。

可执行文件能够调用您导入管理中心的任何资源文件，例如徽标图像。部署自己的可执行文件时，您可以对资源文件使用任意文件名。

下表列出了不同操作系统的客户端可执行文件的文件名：

表 *95:* 安全客户端可执行文件的文件名

客户端操作系统	客户端 GUI 文件	客户端 CLI 文件
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
MacOS	管理中心部署不支持。但是，您可以为使用其他方法（例如 Altiris Agent）替换客户端 GUI 的 macOS 部署可执行文件。	vpn

如何使用 *Cisco Secure Client API* 部署自定义应用

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 使用思科安全客户端 API 创建自定义应用。

步骤 2 创建新的安全客户端自定义对象。

a) 选择**对象** > **VPN** > **安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从 **自定义类型** 下拉列表中，选择 **二进制文件**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择自定义应用。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级** > **安全客户端自定义** > **二进制文件**。
d) 点击 + 选择转换文件。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署** > **部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

自定义安全客户端安装程序

您可以通过创建使用客户端安装程序部署的自定义转换来自定义安全客户端 GUI。您可以将转换导入管理中心并将其部署到威胁防御设备。威胁防御使用客户端安装程序将此转换部署到终端。

注释 此自定义仅适用于 Windows。

本地化客户端安装程序

您可以翻译 Cisco Secure Client 安装程序显示的消息。管理中心使用转换功能来翻译安装程序显示的消息。该转换会更改安装，但会保持原始安全签名的 MSI 不变。这些转换仅翻译安装程序屏幕，而不翻译客户端 GUI 屏幕。

Cisco Secure Client 的每个版本都包括本地化转换，管理员可在上传含有新软件的 Cisco Secure Client 软件包时将转换上传到管理中心。如果您使用我们的本地化转换，请确保在上传新的 Cisco Secure Client 软件包时用 Cisco.com 的最新版本更新这些转换。

如何自定义或本地化客户端安装程序

开始之前

配置一个或多个远程访问 VPN IKE 策略。

过程

步骤 1 创建自定义或本地化转换。

步骤 2 创建新的安全客户端自定义对象。

a) 选择**对象** > **VPN** > **安全客户端自定义**。
b) 点击 **安全客户端自定义**。
c) 输入自定义的名称和说明。
d) 从**自定义类型 (Customization Type)** 下拉列表中，选择**自定义安装程序转换 (Customized Installer Transform)** 或**本地化安装程序转换 (Localized Installer Transform)**。
e) 从 **平台** 下拉列表中选择平台。
f) 点击 **浏览** 并选择转换。

步骤 3 将自定义添加到远程接入 VPN 策略。

a) 选择**安全连接** > **远程访问 VPN**。
b) 点击远程接入 VPN 策略的编辑图标。
c) 点击 **高级 > 安全客户端自定义 > 自定义安装程序转换**或 **本地化安装程序转换**。
d) 点击 **+** 选择转换。
e) 点击 **添加 (Add)**。
f) 点击**确定**。

步骤 4 点击**保存**。

步骤 5 选择 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

验证安全客户端自定义

验证部署

在部署完成后，请在管理中心中验证部署。点击 **脚本详细信息** （）) 图标以验证为自定义生成的命令。

示例

1. 以下示例显示 GUI 文本和消息自定义的脚本详细信息：使用自定义提示保护客户端 en_us 本地化。

```
import webvpn translation-table AnyConnect language en-us disk0:/AnyConnect_en-us.po
```

2. 以下示例显示自定义图标和图像的脚本详细信息：将 Secure Client 徽标自定义为 ABC 徽标。

```
import webvpn AnyConnect-customization type resource platform win name company_logo.png
 disk0:/company_logo.png
```

3. 以下示例显示自定义 OnConnect 和 OnDisconnect 脚本的脚本详细信息。连接时脚本装载网络驱动器，断开连接脚本卸载网络驱动器。

```
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnConnect_mount.bat disk0:/mount.bat
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnDisconnect_unmount.bat disk0:/unmount.bat
```

使用威胁防御命令验证自定义

在威胁防御上使用以下命令验证自定义设置：

- **show import webvpn translation-table detailed**：显示可用的转换表。

```
HQ-FTD# show import webvpn translation-table detailed
 Translation Tables' Templates:
   AnyConnect           ia4DaAXNSvl5pZboQRGJcs9KMXY=
   customization
 Translation Tables:
   fr                   customization        BWWodsOt1PbvDvYOp8hLb3W7a64=
   ja                   customization        lNvUk1+qTLNZyNrBcApMQPHnm1M=
   ru                   customization        UqyKyUAcjR+xTGUtdiIFnoIiW5U=
```

- **show import webvpn AnyConnect-customization detailed**：显示安全客户端自定义的详细信息。

```
HQ-FTD# show import webvpn AnyConnect-customization detailed
OEM resources for AnyConnect client:
  linux-64/binary/scripts_OnConnect_conn.sh           w6+n7z80D/8AR+ul2f7DvTmcDTw=
  linux-64/binary/scripts_OnDisconnect_discon.sh      jx5LJC2XBEmEkGeww59CAkszvnI=
  linux-64/resource/company-logo.png                  GsfBDroqGSQEEwuBDS/3DJNVv88=
  win/binary/scripts_OnConnect_mount.bat              dzjfsLYYft/XMlPlzskKl+Wv1bw=
  win/binary/scripts_OnDisconnect_unmount.bat         k6xlKhF1l2IRyJu08+sdYXgKNgM=
  win/resource/company_logo.png                       cmEvxwqvtaS+Pz/6sb9n3NZudS4=
```

验证安全客户端中的自定义

- 在安全客户端中，点击 **消息历史记录** 选项卡以验证是否已下载自定义设置。

  使用 DART 工具查看客户端诊断。

表 *96:* 验证安全客户端中的自定义

可以定制	验证
GUI 文本和消息自定义	• 验证安全客户端是否在以下位置具有语言本地化或自定义文件： • Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<language-code>\LC_MESSAGES (AnyConnect 版本 4.9 及更早版本) • Windows: %ProgramData%\Cisco\Cisco Secure Client\l10n\<language-code>\LC_MESSAGES (Secure Client 版本 5.0 及更早版本) • 对于 Mac OS 和 Linux: /opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES /opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES • 验证本地化或自定义文件的内容，并确认它们是否具有自定义或本地化字符串。例如：AnyConnect.mo
图像和图标自定义	• 验证安全客户端是否在以下位置具有自定义文件： • Windows: %PROGRAMFILES%\ Cisco\Cisco AnyConnect Secure Mobility Client\res\ (AnyConnect 版本 4.10 及更早版本) • Windows: %PROGRAMFILES%\ Cisco\Cisco Secure Client\UI\res (Cisco Secure Client 5.0 及更高版本) • Linux：/opt/cisco/anyconnect/resources 或 /opt/cisco/secureclient/resources • 验证自定义图标或图像文件的内容。
自定义 OnConnect 和 OnDisconnect 脚本	• 验证自定义脚本是否位于以下位置： • Windows: %ProgramData%\Cisco\Cisco Secure Client\Script (Cisco Secure Client 5.0 及更高版本) • Windows: %ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Script (AnyConnect 版本 4.9 及更早版本) • Mac OS 和 Linux：/opt/cisco/anyconnect/script or /opt/cisco/secureclient/vpn/script • 验证脚本。

配置 安全客户端 管理 VPN 隧道

只要客户端系统通电，管理 VPN 隧道就会提供与企业网络的连接，而无需 VPN 用户连接到 VPN。这有助于组织通过软件补丁和更新让终端保持最新状态。在建立用户发起的VPN隧道后，管理隧道将断开连接。

本部分提供有关在 Firewall Threat Defense上配置 安全客户端 管理 VPN 隧道的信息。使用 防火墙管理中心 Web 界面在 Firewall Threat Defense 上配置 安全客户端 管理隧道需要以下设置：

- 具有基于证书的身份验证和组 URL 的**连接配置文件**。
- **为服务器配置了组 URL 和备份服务器（如果需要）的Secure Client 管理 VPN 配置文件**。
- 包含管理 VPN 配置文件（其中明确包含网络的分割隧道、客户端绕行协议且无横幅）的**组策略**。

有关配置 安全客户端 管理 VPN 隧道的详细说明，请参阅 在 Firewall Threat Defense 上配置 安全客户端 管理 VPN 隧道 ， 第 1600 页。

安全客户端 管理 VPN 隧道的要求和前提条件

软件和配置要求

在使用 Firewall Threat Defense Web 界面在 防火墙管理中心 上配置 安全客户端 管理隧道之前，请确保您已具备以下条件：

- 确保您使用的是 Firewall Threat Defense 和 防火墙管理中心 版本 6.7.0 或更高版本。
- 下载 安全客户端 安全客户端 VPN Webdeploy 软件包 4.7 或更高版本，并将其上传到 Firewall Threat Defense 远程访问 VPN。
- 确保在连接配置文件中配置证书身份验证。
- 确保未在组策略中配置横幅。
- 检查管理隧道组策略中的分割隧道配置。

证书要求

- Firewall Threat Defense 必须具有远程访问 VPN 的有效身份证书，并且 Firewall Threat Defense 上必须存在来自本地证书颁发机构 (CA) 的根证书。
- 连接到管理 VPN 隧道的终端必须具有有效的身份证书。
- Firewall Threat Defense 的身份证书的 CA 证书必须安装在终端上，而终端的 CA 证书必须安装在 Firewall Threat Defense 上。
- 同一本地 CA 颁发的身份证书必须存在于计算机存储区中。

  证书存储区（适用于 Windows）和/或系统密钥链中（适用于 macOS）。

安全客户端 管理 VPN 隧道的限制

- 安全客户端 管理 VPN 隧道仅支持证书身份验证，而不支持基于 AAA 的身份验证。
- 不支持公共或专用代理设置。
- 在已连接管理 VPN 隧道时，不支持安全客户端 升级和 AnyConnect 模块下载。

在 Firewall Threat Defense 上配置 安全客户端 管理 VPN 隧道

过程

步骤 1 使用向导来创建远程访问 **VPN** 策略配置：

有关配置远程访问 VPN 的信息，请参阅配置新的远程访问 VPN 连接，第 1541 页。

步骤 2 配置管理 **VPN** 隧道的连接配置文件设置：

注释
建议创建仅用于 安全客户端 管理 VPN 隧道的新连接配置文件。

a) 编辑已创建的远程访问 VPN 策略。
b) 选择并编辑将用于管理 VPN 隧道的连接配置文件。
c) 在 **AAA** 中，选择**身份验证方法**并点击**仅客户端证书**。根据需要配置授权和记账设置。
d) 点击连接配置文件的**别名 (Aliases)** 选项卡。
e) 在连接配置文件的 URL 别名和 **URL 别名**下，点击**添加 (+) (Add [+])**。
f) 点击**启用 (Enabled)** 以启用 URL。
g) 点击**确定**，然后点击**保存**以保存连接配置文件设置。

有关连接配置文件设置的详细信息，请参阅配置连接配置文件设置，第 1552 页。

步骤 3 使用 安全客户端配置文件编辑器来创建管理隧道配置文件：

a) 从 Cisco 软件下载中心 下载 安全客户端 **VPN 管理隧道独立配置文件编辑器**（如果尚未下载）。
b) 使用 VPN 用户的所需设置来创建管理隧道配置文件并保存文件。
c) 使用您在连接配置文件中配置的组 URL 来配置服务器列表中的服务器。

有关使用配置文件编辑器来创建管理配置文件的详细信息，请参阅 *Cisco Secure Client（包括 AnyConnect）管理员指南*。

步骤 4 创建管理隧道对象：

a) 在 Secure Firewall Management Center Web 接口上，导航至
b) 点击 **添加安全客户端文件**。
c) 指定 安全客户端 文件的 **名称** 。
d) 点击**浏览 (Browse)** 并选择已保存的管理隧道配置文件。
e) 点击 **文件类型** 下拉列表，然后选择 **安全客户端管理 VPN 配置文件**。
f) 点击**保存**。

注释
您还可以在创建或更新组策略的 安全客户端 设置时创建管理隧道对象。请参阅组策略 Secure Client 选项，第 2727 页。

步骤 5 将管理配置文件与组策略关联并配置组策略设置：

您必须将管理 VPN 配置文件添加到与用于管理隧道 VPN 连接的连接配置文件关联的组策略。当用户连接时，系统会下载管理 VPN 配置文件以及已映射到组策略的用户 VPN 配置文件，从而启用管理 VPN 隧道功能。

注意
无横幅 (No Banner)：检查并确保未在组策略设置中配置横幅。您可以在**组策略 (Group Policy)** > **常规设置 (General Settings)** > **横幅 (Banner)** 下检查横幅设置。

a) 编辑为管理 VPN 隧道创建的连接配置文件。
b) 点击**编辑组策略** > **安全客户端** > **管理配置文件** 编辑组策略并选择 **AnyConnect 安全客户端**，然后点击**管理配置文件**。
c) 点击**管理 VPN 配置文件 (Management VPN Profile)** 下拉列表，然后选择您创建的管理配置文件对象。

   注释
   您还可以点击 + 并添加新的 安全客户端 管理 VPN 配置文件对象。

d) 点击**保存**。

步骤 6 在组策略中配置分割隧道：

a) 点击**编辑组策略**，然后选择**常规**，然后点击**分割隧道**。
b) 从 IPv4 或 IPv6 分割隧道的下拉菜单中，选择**下面指定的隧道网络 (Tunnel networks specified below)**。
c) 选择拆分隧道网络列表类型：**标准访问列表 (Standard Access List)** 或**扩展访问列表 (Extended Access List)**，然后选择所需的访问列表以允许流量通过管理 VPN 隧道。
d) 点击**保存**，保存分割隧道设置。

安全客户端自定义属性

安全客户端 管理 VPN 隧道要求分割默认包含隧道配置。如果要在组策略中配置 安全客户端 自定义属性，以使用分割隧道来部署管理VPN隧道，您可以配置安全客户端自定义属性对象 (**对象** > **VPN** > **自定义属性**) 。

步骤 7 部署、验证和监控远程访问 **VPN** 策略：

a) 将管理 VPN 隧道配置部署到 Firewall Threat Defense。

   注释
   客户端系统必须连接到 Firewall Threat Defense 远程访问 VPN 一次，才能将管理隧道 VPN 配置文件下载到客户端计算机。

b) 您可以在 **AnyConnect 安全移动客户端安全移动客户端**中验证 安全客户端 管理 VPN 隧道，然后选择 **VPN** 并点击**统计信息**。

您还可以使用 **show vpn-sessiondb anyconnect** 命令在 Firewall Threat Defense 命令提示符后检查管理 VPN 会话详细信息。

c) 在 防火墙管理中心 Web 界面上，点击 **分析** 以查看管理隧道会话信息。

相关主题

配置连接配置文件设置，第 1552 页
Firewall Threat Defense组策略对象，第 2724 页

多证书身份验证

基于多个证书的身份验证能够让 Firewall Threat Defense 验证计算机或设备的证书，以确保设备是企业发放的设备，此外还可以验证用户的身份证书，以允许在 SSL 或 IKEv2 EAP 阶段使用 Secure Client 来进行 VPN 访问。

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果未选中此选项，则只能对计算机或用户执行证书身份验证，而不能同时对两者执行证书身份验证。

多重证书身份验证的准则和限制

注释 配置多证书身份验证时，请确保在思科 Secure Client 配置文件设置中将 **AutomaticCertSelection** 的值设置为 true。

- 多证书身份验证当前会将证书数量限制为两个。
- Secure Client 必须指明支持多证书身份验证。如果不是这样，网关将使用其中一种旧版身份验证方法，否则连接将失败。安全客户端 版本 4.4.04030 或更高版本支持基于多证书的身份验证。
- 安全客户端 仅支持基于 RSA 的证书。
- 在 安全客户端 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

配置多证书身份验证

开始之前

在配置多证书身份验证之前，请确保配置了用于获取每台 Firewall Threat Defense 设备的身份证书的证书注册对象。有关详细信息，请参阅证书映射对象，第 2721 页。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑 (Edit)**。

注释
如果尚未配置远程接入 VPN，请点击**添加 (Add)** 以创建新的远程接入 VPN 策略。

步骤 3 选择并**编辑**连接配置文件，以便配置多证书身份验证。

步骤 4 点击 **AAA** 设置，然后选择**身份验证方法 (Authentication Method)** > **仅客户端证书 (Client Certificate Only)** 或**客户端证书和 AAA (Client Certificate & AAA)**。

注释
如果您选择了客户端证书和 AAA 身份验证方法，请选择**身份验证服务器 (Authentication Server)**

步骤 5 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。

步骤 6 选择一个证书以便**映射客户端证书中的用户名**：

- **第一个证书** - 选择此选项以映射从 VPN 客户端发送的计算机证书中的用户名。
- **第二个证书** - 选择此选项以映射从客户端发送的用户证书中的用户名。

如果启用仅证书身份验证，从客户端发送的用户名会被用作 VPN 会话用户名。如果启用了 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

注释
如果选择**映射特定字段 (Map specific field)** 选项（包括客户端证书中的用户名），则**主 (Primary)** 字段和**辅助 (Secondary)** 字段将分别显示默认值：**CN**（**公用名**）和 **OU**（**组织单位**）。

如果选择**使用整个 DN**（**可分辨名称**）**作为用户名**选项，系统将自动检索用户身份。可分辨名称 (DN) 是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

如果您选择了客户证书和 AAA 身份验证，请选择 **在用户登录窗口预填证书中的用户名** 选项，以便在用户通过 Cisco Secure Client 的 AnyConnect VPN 模块连接时预填充辅助用户名。

- **在登录窗口隐藏用户名**： 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。

步骤 7 为远程访问 VPN 配置所需的 AAA 设置和连接配置文件设置。

步骤 8 保存连接配置文件和远程访问 VPN 配置并将其部署在您的 Firewall Threat Defense 设备上。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1555 页

基于地理位置管理远程用户的 VPN 访问

您可以根据用户所在的地理位置对其远程访问VPN 连接进行管理。通过配置允许或拒绝来自特定国家或地区的VPN连接，可以满足合规性要求并增强安全性。不符合这些基于位置的条件的连接会被阻止，然后进行身份验证，详细信息记录在 防火墙管理中心（设备 > 故障排除 > 故障排除日志）。**故障排除 > + 显示更多 > 高级 > 故障排除日志**

此功能支持 Secure Client 的所有版本。

前提条件

Firewall Threat Defense 设备的必须为 7.7.0 或更高版本。

基于地理位置管理远程用户 VPN 访问的工作流程

步骤	任务	更多信息
1	定义策略以允许对远程客户端进行基于地理位置的访问控制。	配置服务访问对象， 第 2628 页
2	使用该策略更新远程访问 VPN 配置。	配置远程访问 VPN 的访问接口， 第 1571 页
3	在设备上部署配置。	—
4	在客户端连接到 Firewall Threat Defense 设备之后： 1. 在**远程访问 VPN (Remote Access VPN)** 控制面板中验证活动远程访问 VPN 会话。 2. 在 **故障排除 > + 显示更多 > 高级 > 故障排除日志** 验证被拒绝的远程访问 VPN 会话的日志。	监控服务访问策略并进行故障排除， 第 1605 页

基于地理位置管理远程接入 VPN 用户的准则和限制

准则

- 在服务访问对象中，如果使用地理位置对象（国家/地区、大洲或地理位置对象），请仅在一个规则中使用该对象。
- 按照正确的顺序配置服务访问规则，因为这些规则不能重新排序。

限制

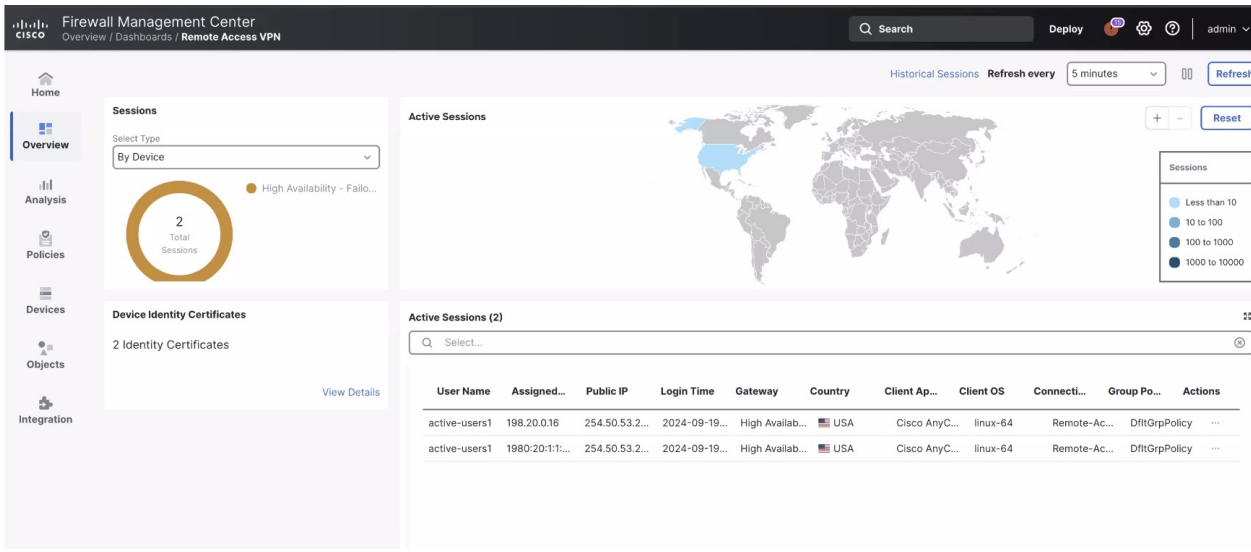
- 不支持群集。

- 基于地理位置的未分类 IP 地址不按其地理来源进行分类。对于此类未分类的 IP 地址，防火墙管理中心 会实施默认服务访问策略操作。
- 来自 IETF RFC1918 地址的连接，无论服务访问策略设置如何，都允许用于基于地理位置的远程访问 VPN。

监控服务访问策略并进行故障排除

在远程访问 VPN 控制面板中监控活动的远程访问 VPN 会话

选择**洞察与报告** > **VPN 控制面板** > **远程访问 VPN**。

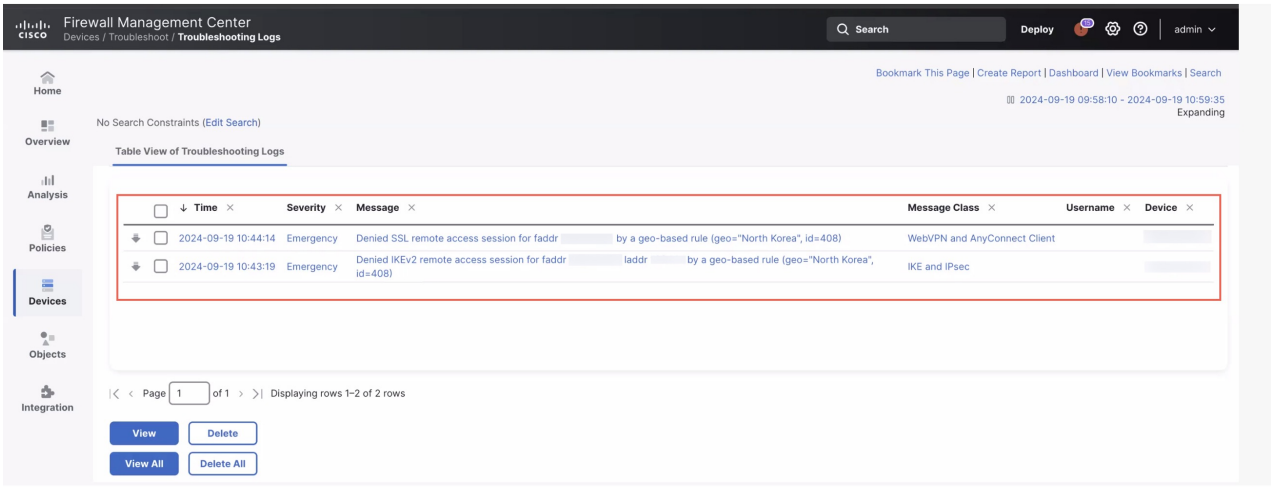


监控被拒绝的远程访问 VPN 会话

在 **故障排除** > **+ 显示更多** > **高级** > **故障排除日志** 处监控被拒绝的远程访问 VPN 会话。要查看拒绝的远程访问 VPN 会话，则必须在 Firewall Threat Defense 中配置系统日志设置：

1. 选择 **设备** > **平台设置**并创建或编辑威胁防御策略。
2. 在左侧窗格中，点击**系统日志 (Syslog)**。
3. 点击**日志记录设置 (Logging Setup)** 选项卡。
4. 选中 **Enable Logging** 复选框。
5. 点击 **VPN 日志 (VPN Logs)** 单选按钮。
6. 在**日志记录级别 (Logging Level)** 下拉列表中，选择 **6 信息 (6 - informational)**。
7. 点击**保存**。

注释 如果为**所有日志 (All Logs)** 选项配置的**日志记录级别**介于 0 和 2 之间，则您无法查看拒绝的远程访问 VPN 会话。



验证服务访问策略

在 Firewall Threat Defense 设备 CLI 中，运行以下命令：

- **show running-config service-access**：显示用户定义的服务访问策略。

```
firepower#show running-config service-access
   service-access deny geolocation OBJGRP_Asia1
   service-access permit interface outside ra-ssl-client geolocation OBJGRP_India
   service-access deny ra-ikev2 geolocation any
```

- **show service-access**：显示用户定义的服务访问策略的详细信息。

```
firepower# show service-access
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
2 any              : ra-ikev2 ra-ssl-client (deny) hits = 123
  Last hit time    : 11:23:12.032 IST Tue Jul 17 2024
  object-group     : any


firepower# show service-access detail
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
  geolocation      : Egypt(818) Jordan(400)
                     Iran (Islamic Republic of)(364)
                     Saudi Arabia(682)
```

- **show geodb**：显示地理位置表的详细信息。

  show geodb {**ipv4** | **ipv6** | **counters** | **context**} [**location** *country_name* | **lookup** *ip_address*] [**detail**]

- **show geodb** {**ipv4** | **ipv6**}：显示 IPv4 或 IPv6 地址映射总数。

```
firepower# show geodb ipv4
 Geolocation Table - IPv4
 Total number of mappings available: 532507
 Last geolocation data read time:  17:02:13.000 IST Thu Jul 18 2024
 Running geolocation update version: 2024-02-15-019
```

- **show geodb** {**ipv4** | **ipv6**} **location** *country_name* **detail**：显示 IPv4 或 IPv6 地址映射的详细信息。

```
firepower# show geodb ipv4 location Antarctica detail
Geolocation Table - IPv4
id=0x00007fff82c284e0, geo_id=10, hits=0
        range_lower=77.70.176.176, range_upper=77.70.176.183
id=0x00007fff82cca360, geo_id:10, hits=0
     range_lower=79.110.169.69, range_upper=79.110.169.69
Total number of mappings available: 28
```

- **show geodb counters**：显示活动会话、允许会话和被拒绝会话的详细信息。

```
firepower# show geodb counters
current   - ongoing sessions
permitted - cumulative permitted sessions
denied    - cumulative denied sessions
Location                current          permitted      denied
Egypt                     0                  0             5
India                     45                 1345          45
```

- **show geodb** {**ipv4** | **ipv6lookup** *ip_address*：显示特定 IPv4 或 IPv6 地址的地理位置。

```
firepower# show geodb ipv4 lookup 223.223.128.24
Geolocation of 223.223.128.24 is "India" (356) with id=0x000015114d0aa330
Matching network range: 223.223.128.0 - 223.223.159.255
```

服务访问策略故障排除

- 系统日志

  启用远程访问 VPN 服务访问系统日志：

  1. 选择**设备** > **平台设置**。
  2. 创建或编辑平台设置策略。
  3. 在左侧窗格中，点击**系统日志 (Syslog)**。
  4. 点击**日志记录设置 (Logging Setup)** 选项卡并选中**启用日志记录 (Enable Logging)** 复选框。
  5. 点击**系统日志设置 (Syslog Settings)** 选项卡，并启用服务访问系统日志 751031 和 716166 的系统日志。

- 命令

  - 使用 **show running-config service-access** 和 **show service-access** 命令查看用户定义的服务访问策略的详细信息。

- 使用 **show geodb** 命令查看地理位置表的详细信息。
- 使用 **debug geolocation <debug-level>** 命令发送到捕获与地理位置相关的调试日志。调试级别可以是 1（错误）、2（警告）、3 和 4（信息）、5（调试）或 255（全部调试）。
- 使用 **clear geodb counters** 命令清除地理位置表计数器，例如服务访问策略的命中计数。但是，使用该命令无法清除位置的实际允许和拒绝计数器；只有在重启设备后才能清除这些计数器。

自定义远程接入 VPN AAA 设置

本节提供有关自定义远程接入 VPN 的 AAA 首选项的信息。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

通过客户端证书对 VPN 用户进行身份验证

使用向导创建新的远程接入 VPN 策略或稍后编辑策略时，可以使用客户端证书配置远程接入 VPN 身份验证。

开始之前

配置用于为每台充当 VPN 网关的 Firewall Threat Defense设备获取身份证书的证书注册对象。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程访问VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA** > **身份验证方法 (Authentication Method)** > **仅限客户端证书 (Client Certificate Only)**。

使用此身份验证方法，用户可以使用客户端证书进行身份验证。必须在VPN客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段CN和OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”字段和“辅助”字段来映射适当的字段。

如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。 **主** 字段和 **辅助** 字段将显示默认值：**CN**（**公用名**）和**OU**（**组织单位**）。如果选择**使用整个DN作为用户名**选项，系统将自动检索用户身份。可分辨名称(DN)是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

- 与 **映射特定字段** 选项相关的“主”和“辅助”字段包含以下公共值：
  - C（国家/地区）
  - CN（公用名）

- DNQ（DN 限定符）
- EA（邮件地址）
- GENQ（代系限定符）
- GN（名字）
- I（首字母）
- L（地区）
- N（名字）
- O（组织）
- OU（组织单位）
- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1552 页
添加证书注册对象，第 2671 页

通过客户端证书和 AAA 服务器配置 VPN 用户身份验证

在配置远程接入VPN身份验证以便同时使用客户端证书和身份验证服务器时，会使用客户端证书验证和 AAA 服务器来完成 VPN 客户端身份验证。

开始之前

- 配置用于为每台充当 VPN 网关的 Firewall Threat Defense 设备获取身份证书的证书注册对象。
- 配置在远程访问 VPN 策略配置中使用的 RADIUS 服务器组对象和任何 AD 或 LDAP 领域。

- 确保可以通过 Cisco Secure Firewall Threat Defense设备访问 AAA 服务器，以使远程接入 VPN 配置生效。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 在要更新身份验证的远程接入 VPN 策略上点击 **编辑** ，或点击 **添加** 以创建新的身份验证。

步骤 3 如果选择创建新的远程接入 VPN 策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 转到 **AAA** ，然后从 **身份验证方法** 下拉列表中选择 **客户端证书和 AAA**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA - 完成两种类型的身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。

  - **客户端证书**-使用客户端证书对用户进行身份验证。您必须在 VPN 客户端终端上配置客户端证书。默认情况下，用户名分别派生自客户端证书字段CN和OU。如果使用客户端配置文件中的任何其他字段指定了用户名，请使用 **主字段** 和 **辅助字段** 来映射相应的字段。

    如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名)** 和 **OU (组织单位)**。如果选择**使用整个 DN 作为用户名**选项，系统将自动检索用户身份。可分辨名称(DN)是由单个字段组成的唯一标识，可在将用户与连接配置文件匹配时用作标识符。DN 规则用于增强的证书身份验证。

    与**映射特定字段**选项相关的“主”和“辅助”字段包含以下公共值：

    - C（国家/地区）
    - CN（公用名）
    - DNQ（DN 限定符）
    - EA（邮件地址）
    - GENQ（代系限定符）
    - GN（名字）
    - I（首字母）
    - L（地区）
    - N（名字）
    - O（组织）
    - OU（组织单位）

- SER（序列号）
- SN（姓氏）
- SP（省）
- T（职务）
- UID（用户 ID）
- UPN（用户主体名称）

- 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1552 页
添加证书注册对象，第 2671 页

通过 VPN 会话管理密码更改

通过密码管理，远程访问 VPN 策略管理员可以为远程访问 VPN 用户配置密码到期时的通知设置。密码管理在使用身份验证方法“仅 AAA”和“客户端证书和 AAA”的 AAA 设置中可用。有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要编辑的远程访问 VPN 策略旁边的 **编辑** 。

步骤 3 在包含 AAA 设置的连接配置文件上点击 **编辑** 。

步骤 4 选择 **AAA** > **高级设置** > **密码管理**。

步骤 5 选中 **启用密码管理** 复选框并选择以下选项之一：

- 通知用户 - 在密码到期之前；在框中指定天数。
- 在密码到期当天通知用户。

步骤 6 保存更改。

相关主题

配置连接配置文件设置，第 1552 页

向 RADIUS 服务器发送记账记录

远程接入 VPN 中的记账记录有助于 VPN 管理员跟踪用户访问的服务以及他们使用的网络资源量。记账信息包括用户会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。

您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。激活 AAA 记账时，网络访问服务器会向所配置的记账服务器报告用户活动。您可以将 RADIUS 服务器配置为记账服务器，以便将所有用户活动信息从 防火墙管理中心 发送到 RADIUS 服务器。

注释 您可以在远程接入 VPN AAA 设置中使用相同的 RADIUS 服务器或单独的 RADIUS 服务器进行认证授权和记账。

开始之前

- 使用将向其发送身份验证请求或记账记录的 RADIUS 服务器配置 RADIUS 组对象。有关详细信息，请参阅RADIUS 服务器组选项，第 2620 页。
- 确保可从 Firewall Threat Defense 设备访问 RADIUS 服务器。在 **设备** > **设备管理** 上，在您的 Secure Firewall Management Center 上配置路由，然后点击 **编辑** ()。然后，点击**路由**选项卡以确保连接到 RADIUS 服务器。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 在要配置 RADIUS 服务器的远程访问策略上点击 **编辑**，或创建新的远程访问 VPN 策略。

步骤 3 在包含 AAA 设置的连接的配置文件上点击 **编辑**，然后选择 **AAA**。

步骤 4 从 **记帐服务器** 下拉列表中选择 RADIUS 服务器。

步骤 5 保存更改。

相关主题

配置连接配置文件设置，第 1552 页
配置远程访问 VPN 的 AAA 设置，第 1555 页

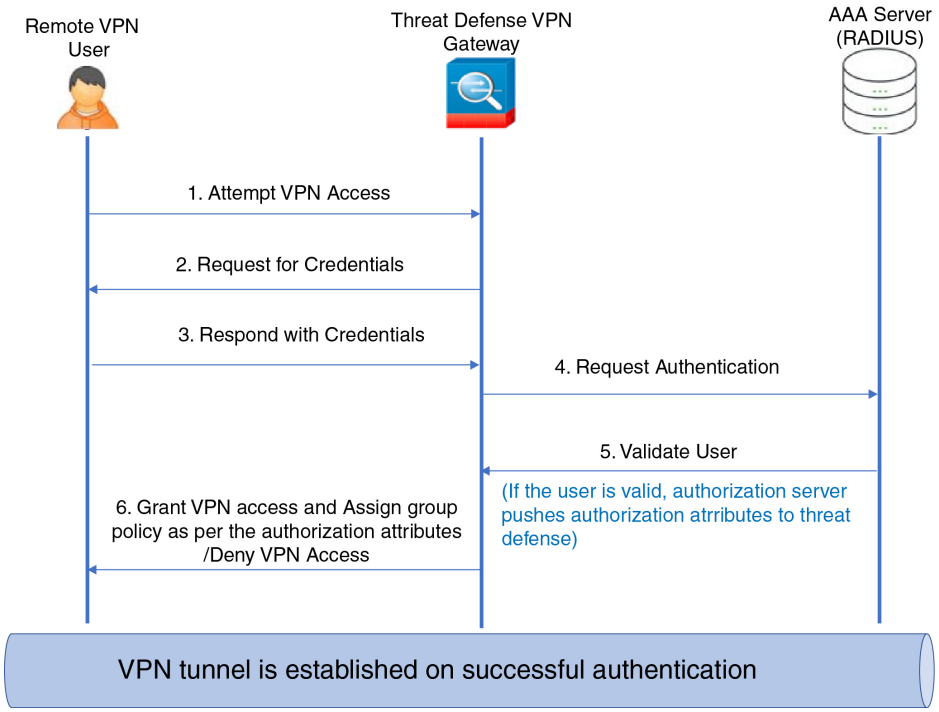
将组策略选择委派给授权服务器

在建立 VPN 隧道时，将确定应用于用户的组策略。您可以在使用向导来创建远程接入 VPN 策略时为连接配置文件选择组策略，也可以稍后再更新连接配置文件的连接策略。但是，您可以配置 AAA (RADIUS) 服务器以分配组策略，或者从当前连接配置文件中获取。如果 Firewall Threat Defense 设备从与连接配置文件上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

您可以配置 ISE 或 RADIUS 服务器，通过发送 IETF RADIUS 属性 25 并映射到相应的组策略名称来为此用户或用户组设置授权配置文件。您可以为用户或用户组配置特定组策略，以便推送可下载 ACL、设置横幅、限制 VLAN，并配置将 SGT 应用于会话的高级选项。建立 VPN 连接时，这些属性将应用于属于该组的所有用户。

有关更多信息，请参阅《思科身份服务引擎管理员指南》中的“配置标准授权策略”部分和Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 1560 页。

图 *441: AAA* 服务器的远程接入 *VPN* 组策略选择



相关主题

配置组策略对象，第 2724 页
配置连接配置文件设置，第 1552 页

授权服务器覆盖组策略或其他属性的选择

当远程访问 VPN 用户连接 VPN 时，系统会将连接配置文件中配置的组策略和其他属性分配给用户。但是，远程访问 VPN 系统管理员可以通过配置 ISE 或 RADIUS 服务器为用户或用户组设置授权配置文件，将组策略和其他属性的选择委派给授权服务器。用户通过身份验证后，这些特定的授权属性将被推送到 Firewall Threat Defense设备。

开始之前

确保使用 RADIUS 作为身份验证服务器来配置远程访问 VPN 策略。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 如果尚未配置，请选择 RADIUS 或 ISE 作为授权服务器。

步骤 4 选择**高级** > **组策略**，并添加所需的组策略。有关组策略对象的详细信息，请参阅配置组策略对象，第 2724 页。

您只可将单个组策略映射到连接配置文件；但是，您可以在远程访问VPN策略中创建多个组策略。可以在 ISE 或 RADIUS 服务器中引用这些组策略，并将其配置为通过在授权服务器中分配授权属性来覆盖连接配置文件中配置的组策略。

步骤 5 在目标 Firewall Threat Defense设备上部署配置。

步骤 6 在授权服务器上，使用 IP 地址和可下载 ACL 的 RADIUS 属性创建授权配置文件。

在选择用于远程访问VPN的授权服务器中配置组策略后，组策略将覆盖用户通过身份验证后在远程访问 VPN 用户的连接配置文件中配置的组策略。

相关主题

配置组策略对象，第 2724 页

拒绝用户组的 VPN 访问

如果您不希望通过身份验证的用户或用户组使用 VPN，则可以配置组策略以拒绝 VPN 接入。您可以在远程访问 VPN 策略中配置组策略，并在 ISE 或 RADIUS 服务器配置中引用此策略以进行授权。

开始之前

确保已使用远程访问策略向导配置远程访问 VPN，并已为远程访问 VPN 策略配置身份验证设置。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择**高级组策略**。

步骤 4 选择组策略，点击**编辑 (Edit)** 或添加新增组策略。

步骤 5 选择**高级会话设置**并将**每个用户同时登录数**设置为 0 （零）。
这会阻止用户或用户组连接到 VPN，哪怕只有一次。

步骤 6 点击**保存**以保存组策略，然后保存远程访问 VPN 配置。

步骤 7 配置 ISE 或 RADIUS 服务器，为此用户/用户组设置授权配置文件，以发送 IETF RADIUS 属性 25 并映射到相应的组策略名称。

步骤 8 配置 ISE 或 RADIUS 服务器作为远程访问 VPN 策略中的授权服务器。

步骤 9 保存和部署远程访问 VPN 策略。

相关主题

配置连接配置文件设置，第 1552 页

限制用户组的连接配置文件选择

如果要在用户或用户组上强制实施单个连接配置文件，可以选择禁用连接配置文件，以便用户在使用 Cisco Secure Client 的 AnyConnect VPN 模块连接时无法选择组别名或 URL。

例如，如果您的组织要为不同的VPN用户组（如移动用户、公司分发的笔记本电脑用户或个人笔记本电脑用户）使用特定配置，则可以配置特定于每个用户组的连接配置文件，并在用户连接VPN时应用适当的连接配置文件。

默认情况下，Cisco Secure Client 的 AnyConnect VPN 模块将显示在 防火墙管理中心 中配置并在 Firewall Threat Defense 上部署的连接配置文件列表（按连接配置文件名称、别名或别名 URL）。如果未配置自定义连接配置文件，Cisco Secure Client 的 AnyConnect VPN 模块将显示 *DefaultWEBVPNGroup* 连接配置文件。使用以下程序实施用户组的单个连接配置文件。

开始之前

- 在 Secure Firewall Management Center Web 界面中，使用远程访问 VPN 策略向导配置远程访问 VPN，将身份验证方法设置为“仅客户端证书”或“客户端证书 + AAA”。从证书中选择用户名字段。
- 配置 ISE 或 RADIUS 服务器以进行授权，并将组策略与授权服务器关联。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 选择远程访问策略，然后点击 **编辑**。

步骤 3 选择 **访问接口** ，然后禁用 **允许用户在登录时选择连接配置文件**。

步骤 4 点击**高级** **证书映射**。

步骤 5 选择 **使用配置的规则将证书与连接配置文件匹配**。

步骤 6 选择**证书映射名称**，或点击**添加**图标以添加证书规则。

步骤 7 选择**连接配置文件 (Connection Profile)** 并点击**确定**。
使用此配置，当用户从 Cisco Secure Client 的 AnyConnect VPN 模块连接时，用户将具有映射的连接配置文件，并将进行身份验证以使用 VPN。

相关主题

配置组策略对象，第 2724 页
配置连接配置文件设置，第 1552 页

更新远程接入 VPN 客户端的 Secure Client 配置文件

Secure Client 客户端配置文件是一个 XML 文件，其中包含管理员定义的最终用户要求以及作为 安全客户端的一部分部署在VPN客户端系统上的身份验证策略。它使最终用户可以使用预配置的网络配置文件。

您可以使用基于 GUI 的 安全客户端配置文件编辑器（一个独立的配置工具）来创建他们。此独立配置文件编辑器可用于创建新的或修改现有的安全客户端配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关详细信息，请参见相应版本的 Cisco Secure Client（包括 AnyConnect）管理员指南中的 安全客户端配置文件编辑器 一章。

开始之前

- 确保已使用远程接入策略向导配置远程接入 VPN，并已在 Firewall Threat Defense设备上部署配置。请参阅创建新的远程访问 VPN 策略，第 1542 页。
- 在您的 Secure Firewall Management Center Web 界面上，转至 并添加新的 Secure Client 映像。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑**。

步骤 3 选择包含要编辑的客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **编辑组策略** > **安全客户端** > **配置文件**。

步骤 5 从列表中选择一个客户端配置文件 XML 文件，或者点击**添加 (Add)** 以添加新的客户端配置文件。

步骤 6 保存组策略、连接配置文件，然后保存远程接入 VPN 策略。

步骤 7 部署更改。

客户端配置文件的更改将在 VPN 客户端连接到远程接入 VPN 网关时在 VPN 客户端上进行更新。

相关主题

配置组策略对象，第 2724 页

RADIUS 动态授权

Cisco Secure Firewall Threat Defense 可以使用 RADIUS 服务器进行 VPN 远程接入和防火墙直接转发代理会话的用户授权（按用户使用动态访问控制列表 [ACL] 或 ACL 名称）。要实施动态授权或 RADIUS 授权更改 (RADIUS CoA) 的动态 ACL，您必须配置 RADIUS 服务器以支持它们。在用户尝试进行身份验证时，RADIUS 服务器会向 Firewall Threat Defense 发送可下载的 ACL 或 ACL 名称。ACL 允许或拒绝访问特定服务。身份验证会话到期时，Cisco Secure Firewall Threat Defense会删除 ACL。

相关主题

添加 RADIUS 服务器组，第 2620 页
接口，第 2655 页
配置 RADIUS 动态授权，第 1617 页
Cisco Secure Firewall Threat Defense 的 RADIUS 服务器属性，第 1560 页

配置 RADIUS 动态授权

准备工作：

- 如果在 RADIUS 服务器中引用接口，则只能在安全区域或接口组中配置一个接口。
- 启用动态授权的 RADIUS 服务器需要 Cisco Secure Firewall Threat Defense 6.3 或更高版本才能使动态授权生效。
- Cisco Secure Firewall Threat Defense 6.2.3 或更低版本不支持 RADIUS 服务器中的接口选择。在部署期间，接口选项将被忽略。
- Firewall Threat Defense 终端安全评估 VPN 不支持通过动态授权或 RADIUS 授权来更改 (CoA) 更改组策略。

表 *97:* 过程

	相应操作	更多信息
步骤 1	登录 Secure Firewall Management Center Web 界面。	
步骤 2	使用动态授权配置 RADIUS 服务器对象。	RADIUS 服务器组选项，第 2620 页
步骤 3	通过已启用授权更改 (CoA) 的接口配置到 ISE 服务器的路由，以通过路由或特定接口建立 Firewall Threat Defense到 RADIUS 服务器的连接。	RADIUS 服务器组选项，第 2620 页 配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页
步骤 4	配置远程访问 VPN 策略，选择您通过动态授权创建的 RADIUS 服务器组对象。	创建新的远程访问 VPN 策略，第 1542 页
步骤 5	使用“平台设置”配置 DNS 服务器详细信息和域查找接口。	配置 DNS，第 1547 页 DNS 服务器组，第 2640 页
步骤 6	在远程访问 VPN 组策略中配置分割隧道，以允许 DNS 流量通过 VPN 隧道。	配置组策略对象，第 2724 页
步骤 7	部署配置更改。	部署配置更改，第 180 页

双因素身份验证

您可以为远程访问VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如RSA令牌或密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 RSA 服务器的关系绑定到主身份验证源。

Cisco Secure Firewall Threat Defense 支持 RSA 令牌和 Duo Push 身份验证请求，并将任何 RADIUS 或 AD 服务器作为双因素认证过程中的第一因素，向 Duo Mobile 提出第二因素。

配置 RSA 双因素身份验证

关于此任务：

您可以将 RADIUS 或 AD 服务器配置为 RSA 服务器中的身份验证代理，并将 Secure Firewall Management Center中的服务器用作远程接入 VPN 中的主身份验证源。

使用此方法时，用户必须使用 RADIUS 或 AD 服务器中配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

在此配置中，通常会使用单独的 RADIUS 服务器 （例如，Cisco ISE 提供的 RADIUS 服务器) 提供授权服务。将第二个 RADIUS 服务器配置为授权、配置或记账服务器。

准备工作：

在 Cisco Secure Firewall Threat Defense上配置 RADIUS 双因素身份验证之前，请确保完成以下配置：

在 RSA 服务器上

- 将 RADIUS 或 Active Directory 服务器配置为身份验证代理。
- 生成并下载配置 (*sdconf.rec*) 文件。
- 创建令牌配置文件，将令牌分配给用户，并将令牌分发给用户。下载并在远程接入VPN客户端系统上安装令牌。

有关详细信息，请参阅 RSA SecureID 套件文档。

在 ISE 服务器上

- 导入 RSA 服务器上生成的配置 (*sdconf.rec*) 文件。
- 添加 RSA 服务器作为外部身份源并指定共享密钥。

表 *98:* 过程

	相应操作	更多信息
步骤 1	登录 Secure Firewall Management Center Web 界面。	
步骤 2	创建 RADIUS 服务器组。	RADIUS 服务器组选项，第 2620 页

	相应操作	更多信息
步骤 3	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 RADIUS 或 AD 服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器组选项，第 2620 页 **注释** RADIUS 或 AD 服务器必须与在 RSA 服务器中配置为身份验证代理的服务器相同。 对于双因素身份验证，也要确保在 安全客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
步骤 4	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程访问 VPN 策略，第 1542 页
步骤 5	选择 RADIUS 作为身份验证服务器，然后选择新创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置，第 1555 页
步骤 7	部署配置更改。	部署配置更改，第 180 页

配置 Duo 双因素身份验证

关于此任务：

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。（您不能通过 LDAPS 使用与 Duo 云服务的直接连接。）

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 云和 Web 服务器以及关联的 RADIUS 服务器上配置的用户名进行身份验证。用户必须输入 RADIUS 服务器中配置的密码，后跟以下 Duo 代码之一：

- **Duo-passcode**。例如，*my-password*,123456。
- **push**。例如，*my-password*,**push**。使用 push 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。
- **sms**。例如，*my-password*,**sms**。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。
- **phone**。例如，*my-password*,**phone**。使用**电话**通过电话呼叫来进行身份验证。

有关登录选项及示例的详细信息，请参阅https://guide.duo.com/anyconnect。

准备工作：

在 Firewall Threat Defense上使用 Duo 身份验证代理配置双因素身份验证之前，确保完成以下配置：

- 在开始部署 Duo 之前，为远程接入 VPN 用户配置有效的主身份验证（RADIUS 或 AD）。
- 在网络中的 Windows 或 Linux 计算机上安装 Duo 代理服务，以将 Duo 与 Cisco Secure Firewall Threat Defense远程接入 VPN 集成。此 Duo 代理服务器也可充当 RADIUS 服务器。

  从以下位置下载并安装最新的 Duo 身份验证代理：

  - **Windows：** https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux：** https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - 在 https://duo.com/docs/checksums#duo-authentication-proxy 上验证校验和。

- 配置 Duo 身份验证文件 `authproxy.cfg`。按照 https://duo.com/docs/cisco-firepower#configure-the-proxy 页面上的说明配置身份验证配置设置。

  `authproxy.cfg` 配置文件必须包含 RADIUS 或 ISE 服务器、Firewall Threat Defense设备的详细信息、Duo 代理服务器详细信息、集成密钥、密钥以及 API 主机详细信息。

- 确保 `authproxy.cfg` 文件中具有正确的 API 主机信息。
- 在 **Duo 安全服务器** > **Duo 管理面板**> **应用** > **思科 ONE RADIUS VPN** 下，在新安装的 Duo 代理服务器中配置其他所需设置，例如辅助身份验证因素。

表 *99:* 过程

	相应操作	更多信息
步骤 1	登录 Secure Firewall Management Center Web 界面。	
步骤 2	创建 RADIUS 服务器组。	RADIUS 服务器组选项，第 2620 页
步骤 3	在新 RADIUS 服务器组中创建 RADIUS 服务器对象，将 Duo 代理服务器作为主机，超时时间为 60 秒或更长。	RADIUS 服务器选项，第 2622 页 **注释** 对于双因素身份验证，也要确保在 安全客户端配置文件 配置文件 XML 文件中将超时更新为 60 秒或更长。
步骤 4	使用向导配置新的远程接入 VPN 策略，或者编辑现有的远程接入 VPN 策略。	创建新的远程访问 VPN 策略，第 1542 页
步骤 5	选择 RADIUS 作为身份验证服务器，然后选择使用 Duo 代理服务器创建的 RADIUS 服务器组作为身份验证服务器。	配置远程访问 VPN 的 AAA 设置，第 1555 页

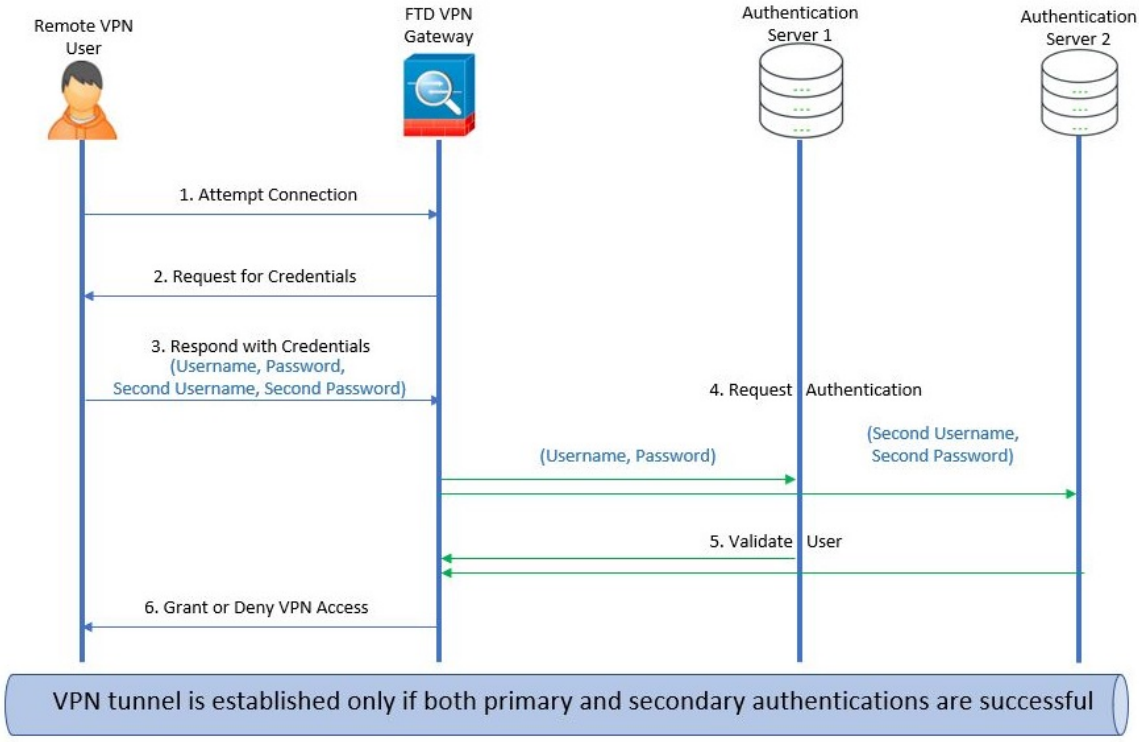
	相应操作	更多信息
步骤 7	部署配置更改。	部署配置更改，第 180 页

辅助身份验证

Cisco Secure Firewall Threat Defense 中的辅助身份验证或双重身份验证，通过使用两个不同的身份验证服务器，为远程访问 VPN 连接额外添加了一层安全性。启用辅助身份验证后， 安全客户端 VPN 用户必须提供两组凭证才能登录 VPN 网关。

Cisco Secure Firewall Threat Defense 远程访问 VPN 支持仅 AAA 和客户端证书以及 AAA 身份验证方法的辅助身份验证。

图 *442:* 远程访问 *VPN* 辅助或双重身份验证



相关主题

配置远程访问 VPN 辅助身份验证，第 1621 页

配置远程访问 VPN 辅助身份验证

当远程访问VPN身份验证配置为同时使用客户端证书和身份验证服务器时，使用客户端证书验证和 AAA 服务器完成 VPN 客户端身份验证。

开始之前

- 配置两个身份验证(AAA)服务器-主要和辅助身份验证服务器，以及所需的身份证书。身份验证服务器可以是 RADIUS 服务器以及 AD 或 LDAP 领域。
- 确保可以通过 Cisco Secure Firewall Threat Defense 设备访问 AAA 服务器，以使远程访问访问 VPN 配置生效。配置路由（在 **设备 > 设备管理** 中点击 **编辑** (✎)）。然后，点击**设备 > 路由**），以确保与 AAA 服务器的连接。

过程

步骤 1 在 Secure Firewall Management Center Web 界面上，选择**安全连接 > 远程访问 VPN**。

步骤 2 在远程访问策略，然后点击 **编辑**；或者点击 **添加** 以创建新的远程访问 VPN 策略。

步骤 3 对于新的远程访问VPN策略，请在选择连接配置文件设置时配置身份验证。对于现有配置，选择包含客户端配置文件的连接配置文件，然后点击**编辑**。

步骤 4 点击 **AAA > 身份验证方式， AAA** 或 **客户端证书和 AAA**。

- 何时选择以下**身份验证方法**：

  客户端证书和 AAA-使用客户端证书和 AAA 服务器已完成身份验证。

  - **AAA** - 如果选择 **RADIUS** 作为**身份验证服务器**，则授权服务器默认也采用此选择。从下拉列表中选择**记帐服务器**。每当从“身份验证服务器”下拉列表中选择 **AD** 和 **LDAP** 时，都必须手动分别选择**授权服务器**和**记帐服务器**。
  - 无论选择哪种身份验证方法，选择或取消选择**仅当用户位于授权数据库中时才允许连接**。

- **使用辅助身份验证** - 除主身份验证之外，还配置了辅助身份验证，以便为 VPN 会话提供额外的安全保护。辅助身份验证是仅适用于**仅 AAA** 和**客户端证书和 AAA** 身份验证方法。

  辅助身份验证是一项可选功能，该功能要求 VPN 用户在 安全客户端 登录屏幕上输入两组用户名和密码。您还可以配置为从身份验证服务器或客户端证书预填充辅助用户名。仅当主身份验证和辅助身份验证均成功时，才会授予远程访问VPN身份验证。如果任何一个身份验证服务器无法访问或一个身份验证失败，VPN 身份验证将被拒绝。

  必须在配置辅助身份验证前，为辅助用户名和密码配置辅助身份验证服务器组（AAA服务器）。例如，可以将主身份验证服务器设置为 LDAP 或 Active Directory 领域，将辅助身份验证设置为 RADIUS 服务器。

  注释
  默认情况下，无需辅助身份验证。

  身份验证服务器 - 为 VPN 用户提供辅助用户名和密码的辅助身份验证服务器。

  选择 **辅助身份验证的用户名**以下的选项：

  - **提示：** 在登录 VPN 网关时，提示用户输入用户名和密码。

- **使用主身份验证用户名：** 用户名从主身份验证服务器获取，用于主身份验证和辅助身份验证；必须输入两个密码。
- **映射客户端证书中的用户名：** 预填充客户端证书中的辅助用户名。
  - 如果选择**映射特定字段**选项，其中包括来自客户端证书的用户名。则**主**和**辅助**字段将显示默认值：**CN (公用名称)** 和 **OU (组织单位)**。如果选择**使用整个 DN（可分辨名称）作为用户名**选项，系统将自动检索用户身份。

    有关主字段和辅助字段映射的详细信息，请参阅**身份验证方法**说明。
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)：** 用户通过 安全客户端 VPN 客户端连接时，预填充客户端证书中的辅助用户名。
    - **在登录窗口隐藏用户名：** 辅助用户名是从客户端证书预填充的，但对用户隐藏，确保用户不会修改预填充的用户名。
- **使用 VPN 会话的辅助用户名：** 辅助用户名用于在 VPN 会话期间报告用户活动。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

相关主题

配置连接配置文件设置，第 1552 页

使用 SAML 2.0 的单点登录身份验证

关于 SAML 单点登录身份验证

安全断言标记语言（SAML）是一种开放标准，用于通过用户在其他情景中的会话将其登录到应用中。当用户登录其 Active Directory（AD）域或内联网时，组织已经知道用户的身份。他们使用此身份信息通过使用 SAML 将用户登录到其他应用，例如基于 Web 的应用。单个应用无需存储凭证，用户无需记住和管理单个应用的不同凭证集。SAML 单点登录 (SSO) 通过将用户的身份从一个位置（身份提供程序）传输到另一个位置（服务提供商）来工作。

通过 Cisco Secure Firewall Threat Defense 进行 SAML 单点登录

Cisco Secure Firewall Threat Defense 设备支持使用 安全客户端对远程访问 VPN 连接进行 SAML 2.0 单点登录 (SSO) 身份验证。您需要执行以下操作，才能在 Cisco Secure Firewall Threat Defense上配置 SAML 2.0 SSO：

- **身份提供程序 (IdP)** - Duo Access Gateway 充当身份提供程序以执行用户身份验证并发出断言。
- **服务提供商 (SP)** - Firewall Threat Defense 设备充当服务提供商并从身份提供商获取身份验证断言。
- **VPN 客户端** - 安全客户端会通过嵌入式浏览器来执行 SAML 2.0 身份验证。

SAML 2.0 的准则和限制

- Firewall Threat Defense 支持以下 SAML 身份验证签名：
  - 包含 RSA 和 HMAC 的 SHA1
  - 包含 RSA 和 HMAC 的 SHA2
- Firewall Threat Defense 支持 SAML 2.0 重定向-POST 绑定，所有 SAML IdP 也支持此功能。
- Firewall Threat Defense 仅用作 SAML SP。在网关模式或对等模式下，它不能用作身份提供程序。
- 如果您的身份策略与与 SAML 域匹配的 AD 领域相关联，则可以对通过 SAML 身份验证的用户实施访问策略。但是，它不适用于 Azure AD SAML，因为它需要从 Azure AD 的租户 ID 到威胁防御设备上关联领域 ID 的额外映射。
- 不支持在 DAP 评估中使用 SAML 身份验证属性（类似于从 AAA 服务器发送的 RADIUS 身份验证响应中的 RADIUS 属性）。Firewall Threat Defense 支持对 DAP 策略启用 SAML 的组策略；但是，在使用 SAML 身份验证时，您无法检查用户名属性，因为用户名属性已被 SAML 身份提供程序屏蔽。
- Firewall Threat Defense 管理员需要确保 Firewall Threat Defense 与 SAML IdP 之间的时钟同步，从而正确处理身份验证断言并确保正确的超时行为。
- Firewall Threat Defense 管理员有责任在 Firewall Threat Defense 和 IdP 上维护有效的签名证书，并考虑以下因素：
  - 在 Firewall Threat Defense 上配置 IdP 时，必须配置 IdP 签名证书。
  - Firewall Threat Defense 不会对从 IdP 接收的签名证书执行吊销检查。
- SAML 断言中有 NotBefore 和 NotOnOrAfter 条件。Firewall Threat Defense SAML 配置的超时与这两个条件如下交互：
  - 如果 NotBefore 与超时之和早于 NotOnOrAfter，则超时将覆盖 NotOnOrAfter。
  - 如果 NotBefore + 超时晚于 NotOnOrAfter，则 NotOnOrAfter 生效。
  - 如果不存在 NotBefore 属性，Firewall Threat Defense 将拒绝登录请求。如果不存在 NotOnOrAfter 属性且未设置 SAML 超时，Firewall Threat Defense 将拒绝登录请求。
- Firewall Threat Defense 不适用于使用内部 SAML 的部署中的 Duo，由于在双因素身份验证（推送、代码、密码）的质询/响应期间发生 FQDN 更改，这会强制到客户端代理的 Firewall Threat Defense 进行身份验证。
- 将 SAML 与 安全客户端配合使用时，还需遵守这些准则：
  - 在嵌入式浏览器中不允许不受信任的服务器证书。
  - CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
  - 在网络浏览器中建立的 SAML 身份验证不会与 安全客户端 共享，反之亦然。

- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管安全客户端 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，安全客户端 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 Firewall Threat Defense 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- 使用内部 IdP 登录后，您将无法访问包含 SSO 的内部服务器。
- SAML IdP NameID 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。

- SAML 不支持登录前启动 (SBL)。
- 不支持通过 SAML 断言接收多个属性。
- 防火墙使用身份提供商实体 ID 作为从 防火墙管理中心 (**对象** > **AAA服务器** > **单点登录服务器**) 中创建的单一登录服务器对象的 SAML 对象名称。因此，您不能在单个防火墙上使用具有相同身份提供商实体 ID 的多个 SAML 对象。

配置 SAML 单点登录身份验证

开始之前

在使用 Firewall Threat Defense 远程访问 VPN 配置 SAML 单点登录之前，请确保已完成以下操作：

- 使用 Duo 创建帐户。
- 下载并安装 Duo Access Gateway。
- 从您的 SAML身份提供程序（Duo）获取以下信息。
  - 身份提供程序实体 ID URL
  - 登录 URL
  - 注销 URL
  - 标识提供程序证书
- 创建 SAML 单点登录服务器对象。有关详细信息，请参阅添加单点登录服务器，第 2623 页。



注释 在使用远程访问 VPN 策略向导创建一个新的策略时，您可以在**连接配置文件 (Connection Profile)** 设置中创建一个单点登录服务器对象。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。

步骤 2 点击要为其配置 SAML 身份验证的远程访问 VPN 策略旁边的**编辑 (Edit)**。如果要创建新策略，请点击**添加 (Add)**。

步骤 3 点击要修改的连接配置文件上的**编辑 (Edit)**。

步骤 4 选择 **AAA** 设置，然后从**身份验证方式 (Authentication Method)** 下拉列表中选择 **SAML**。

步骤 5 选择所需的 SAML 单点登录服务器作为**身份验证服务器**。

步骤 6 配置远程访问 VPN 所需的设置。

步骤 7 在您的 Firewall Threat Defense 设备上保存和部署远程访问 VPN 策略。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1555 页

配置 SAML 授权

关于 SAML 授权

SAML 授权支持在 AAA 和动态访问策略 (DAP) 框架内的 SAML 断言中提供的用户属性。您可以在身份提供程序上将SAML断言属性配置为名称-值对，然后它们会被解析为字符串。接收的属性可供 DAP 使用，以便在 DAP 记录中定义选择条件时使用这些属性。SAML 断言 *cisco_group_policy* 会被用于确定要应用于 VPN 会话的组策略。

动态访问策略属性表示

在 DAP 表中，DAP 属性按以下格式表示：

```
aaa.saml.name = "value”
```

示例，*aaa.saml.department = ” finance"*

此属性可用于 DAP 选择，如下所示：

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

多值属性

DAP 中也支持多值属性，并且 DAP 表已建立索引：

```
aaa.saml.name.1 = "value”
aaa.saml.name.2 = "value"
```

Active Directory memberOf 属性

Active Directory (AD) memberOf 属性接受与通过 LDAP 查询的处理方式一致的特殊处理。

组名称由 DN 的 CN 属性来表示。

从授权服务器接收的属性示例：

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us”
```

动态访问策略属性：

```
aaa.saml.memberOf.1 = "FTD-VPN-Group”
aaa.saml.memberOf.2 = "Domain Admins"
```

cisco_group_policy 属性的解释

组策略可以通过 SAML 断言属性来指定。当 Firewall Threat Defense 接收到属性“cisco_group_policy”时，相应的值会被用于选择连接组策略

配置 SAML 授权

开始之前

确保您已在服务器（例如 DUO）上配置单点登录，并完成所需的身份提供程序 (IdP) 和服务提供商 (SP) 设置。

有关详细信息，请参阅使用 SAML 2.0 的单点登录身份验证，第 1623 页。

过程

步骤 1 配置单点登录服务器对象（如果尚未配置）。

a) 选择**对象** > **AAA服务器** > **单点登录服务器**。

b) 点击**添加单点登录服务器 (Add Single Sign-on Server)**。

c) 输入单点登录服务器详细信息，然后点击 **保存**。

有关详细信息，请参阅添加单点登录服务器，第 2623 页。

步骤 2 在远程接入 VPN 连接配置文件中配置 SAML 身份验证 。

a) 选择**安全连接** > **远程访问 VPN**。

b) 点击要为其配置 SAML 授权或创建新策略的远程访问 VPN 策略上的 **编辑** 。

c) 编辑所需的连接配置文件，然后选择 **AAA**。

d) 从 **身份验证服务器** 下拉列表中选择单点登录服务器对象。

e) 保存远程访问 VPN 配置。

步骤 3 匹配 DAP 策略中的 SAML 条件。

a) 选择**安全连接** > **动态**。

b) 创建新的 DAP 或编辑现有组。

c) 创建 DAP 记录或编辑现有记录。

d) 点击**AAA 条件 (AAA Criteria)** > **SAML 条件 (SAML Criteria)** > **添加 SAML 条件 (Add SAML Criteria)**。

e) 根据 SSO 服务器返回的 SAML 断言来创建 SAML 条件。

步骤 4 部署远程访问 VPN 配置。

相关主题

配置连接配置文件设置，第 1552 页
Firewall Threat Defense组策略对象，第 2724 页

高级 Secure Client 配置

在 Firewall Threat Defense上配置 Secure Client 模块

Secure Client 可以与各种 Cisco 终端安全解决方案集成，并使用不同的 Secure Client 模块提供增强的安全性。

您可以使用托管前端 Firewall Threat Defense 向终端分发和管理 Secure Client 模块。当用户连接到 Firewall Threat Defense时，它会在终端上下载并安装 Secure Client 和所需的模块。

在版本 6.7 及更高版本中，您可以使用由 防火墙管理中心管理的前端 Firewall Threat Defense将 Secure Client 模块分发到终端并进行管理。然后，这些模块与相应的 Cisco 终端安全解决方案集成。

在版本 6.4 到 6.6 中，您可以使用 FlexConfig 在 Firewall Threat Defense 上启用这些模块和配置文件。有关详细信息，请参阅 使用 FlexConfig 配置 AnyConnect 模块和配置文件。

优势

如果使用 Firewall Threat Defense 向终端分发和管理 Secure Client 模块，则可以轻松执行以下任务：

- 分发和管理每个终端上的 Secure Client 模块和配置文件。
- 在每个终端上升级 Secure Client 。

Secure Client 模块类型

AMP 启用程序

使用此模块在终端上部署 Secure Endpoint。该模块将 Secure Endpoint 从企业内本地托管的服务器推送到终端。此模块提供了额外的安全代理，可以检测网络中可能发生的潜在恶意软件威胁、删除这些威胁并保护企业免受危害。

在 Cisco Secure Client 5.0 中，AMP 启用程序仅适用于 macOS。适用于 Windows 的 Cisco Secure Client 提供与 Cisco Secure Endpoint 的完全集成。

ISE 终端安全评估

使用此模块通过 Cisco Identity Services Engine (ISE) 执行终端安全状态检查，例如防病毒软件、反间谍软件、操作系统等，并评估终端的合规性。ISE提供下一代身份和访问控制策略。ISE终端安全评估可执行客户端评估。客户端从头端获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回头端。

网络可视性

使用此模块通过网络可视性模块监控终端应用的使用情况。您可以发现潜在的行为异常并做出明智的网络设计决策。这可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。可将使用情况数据与 Cisco Stealthwatch 等 NetFlow 分析工具共享。

Umbrella 漫游安全

使用此模块通过 Cisco Umbrella 漫游安全服务实现 DNS 层安全。此外，Cisco Umbrella 订用还将提供内容过滤、多重策略、稳健性报告、Active Directory 集成等更多功能。

网络安全

使用此模块启用由 Cisco Talos 提供支持的 Cisco Secure Web Appliance (SWA)。此模块会通过阻止有风险的网站和测试未知网站，然后再允许用户访问这些网站，从而为终端提供保护。它可以通过本地 WSA 或基于云的 Cisco Cloud Web Security 部署 Web 安全。此模块不是版本 4.5 和 Secure Client 5.0 的 AnyConnect 软件包的一部分。

网络访问管理器

此模块提供安全的第 2 层网络，并执行设备身份验证以访问有线和无线网络。网络访问管理器对安全访问所需的用户及设备身份和网络访问协议进行管理。

网络访问管理器在 macOS 或 Linux 上不支持。

登录前开始

登录前启动 (SBL) 允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。安装 SBL 模块后，必须在 Secure Client VPN 配置文件中启用 SBL，并将其添加到远程接入 VPN 组策略。

议价授权请求工具 (DART)

诊断和报告工具 (DART) 会整理系统日志和其他诊断信息，以排除 AnyConnect 安装和连接问题。您可以将此数据发送到 Cisco TAC 进行故障排除。

默认情况下，6.7 及更高版本的新 RA VPN 组策略中未启用 DART。在 6.6 及更早版本中，默认情况下启用 DART。

反馈

客户体验反馈 (CEF) 模块提供有关您使用和启用的功能和模块的信息。此信息将让我们了解用户体验，从而让 Cisco 继续改善 Cisco Secure Client的质量、可靠性、性能和用户体验。 Secure Client 不会将反馈模块下载到终端。反馈数据将发送到 Cisco 反馈服务器。

配置 Secure Client 模块的前提条件

- 根据您要使用的模块配置关联的产品。
- 从 Cisco 软件下载中心 将以下 Secure Client相关软件包下载到本地主机。
  - 适用于所需平台的 Cisco Secure Client 前端部署包。

    此软件包适用于前端，包含所有 Secure Client 模块。对于 Windows，文件名为 cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg。
  - 配置文件编辑器：为需要配置文件的模块创建配置文件。

    Secure Client 需要某些模块的 Secure Client 配置文件。配置文件包含用于启用模块和连接到相应安全服务的配置。配置文件编辑器仅支持 Windows。

    如果模块需要客户端配置文件，请参阅以下列表：

Secure Client 模块	需要客户端配置文件
AMP 启用程序	是
ISE 终端安全评估	是
网络访问管理器	是
网络可视性模块	是
Umbrella 漫游安全模块	是
反馈	是
网络安全	是
诊断和报告工具 (DART)	否
登录前开始	否

- 许可
  - 您需要以下安全客户端许可证之一： Secure Client Premier、 Secure Client Advantage或 仅限 Secure Client VPN
  - 您的 防火墙管理中心 基础版 许可证必须允许出口控制功能。

    选择 **管理** > **许可证** > **智能许可证** 在管理中心验证此功能。

配置 Secure Client 模块的准则

- AnyConnect 4.8 及更高版本以及 Secure Client 5.0 支持所有 Secure Client 模块。
- 不同的模块支持具有不同文件扩展名的配置文件。下表列出了模块及其配置文件支持的文件扩展名：

表 *100:* 配置文件支持的文件扩展名

模块	文件扩展名
AMP 启用程序	*.xml、*.asp
反馈	*.xml
ISE 终端安全评估	*.xml、*.isp
网络访问管理器	*.xml、*.nsp
网络可视性	*.xml、*.nvmsp
Umbrella 漫游安全	*.xml、*.json
网络安全	*.xml、*.wsp、*.wso

- 每个客户端模块只能添加一个条目。您可以编辑或删除模块的条目。
- 如果您计划在 Windows 操作系统上使用 ISE 终端安全评估和网络访问管理器模块，则必须在使用 ISE 终端安全评估模块之前安装网络访问管理器。
- 如果启用 Umbrella 漫游安全模块，请确保禁用 VPN 组策略中的分割隧道下的 **始终通过隧道发送 DNS 请求** 选项。
- 如果要使用 SBL，则必须在 Secure Client VPN 配置文件中启用 SBL。

使用 Firewall Threat Defense安装 Secure Client 模块

开始之前

确保您查看 配置 Secure Client 模块的前提条件，第 1630 页 和 配置 Secure Client 模块的准则，第 1630 页 主题。

过程

步骤 1 如果需要，管理员可为所需 Secure Client 模块创建配置文件。

步骤 2 管理员使用 防火墙管理中心 来：

a) 配置模块并在远程接入 VPN 组策略中添加配置文件。

b) 在 Firewall Threat Defense上部署配置。

步骤 3 用户使用 Secure Client 启动 Firewall Threat DefenseVPN 连接。

步骤 4 Firewall Threat Defense 对用户进行身份验证。

步骤 5 Secure Client 检查更新。

步骤 6 Firewall Threat Defense 在终端上分发 Secure Client 模块和配置文件。

下一步做什么

使用 Secure Client 模块配置远程接入 VPN 组策略，第 1632 页。

使用 Secure Client 模块配置远程接入 VPN 组策略

要使用由 防火墙管理中心管理的 Firewall Threat Defense 安装和更新终端上的 Secure Client 模块，必须使用模块配置更新远程访问 VPN 组策略 Secure Client 。

开始之前

确保您已在 防火墙管理中心中配置远程接入 VPN 策略。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。
步骤 2 选择远程访问 VPN 策略，然后点击**编辑 (Edit)**。
步骤 3 选择一个连接配置文件，然后点击**编辑 (Edit)**。
步骤 4 点击**编辑组策略 (Edit Group Policy)**。
步骤 5 点击 **安全客户端** 选项卡。
步骤 6 点击 **客户端模块**。
步骤 7 点击 +。
步骤 8 从**客户端模块 (Client Module)** 下拉列表中选择一个模块。
步骤 9 从 **要下载的配置文件** 下拉列表中选择模块的配置文件，或点击 + 添加配置文件。
步骤 10 选中 **启用模块下载** 复选框以在终端上下载模块。
步骤 11 点击**添加 (Add)**。
步骤 12 如果要添加更多模块，请重复步骤 7 至 11。
步骤 13 点击**保存**。

下一步做什么

1. 在威胁防御上部署配置。
2. 启动 Secure Client，选择 VPN 配置文件，然后连接到 VPN。 Secure Client 在其上安装已配置的模块。
3. 确认配置。有关详细信息，请参阅验证 Secure Client 模块配置，第 1633 页。

验证 Secure Client 模块配置

在 Firewall Threat Defense

在 Firewall Threat Defense 上使用以下命令查看配置文件和 Secure Client 模块配置：

- **show disk0:**-查看配置文件及其配置。
- **show run webvpn** - 查看安全客户端配置的详细信息。
- **show run group-policy<ravpn_group_policy_name>** - 查看安全客户端的 RA VPN 组策略的详细信息。
- **show vpn-sessiondb anyconnect** - 查看活动安全客户端 VPN 会话的详细信息。

在终端上

1. 使用 Secure Client 与 Firewall Threat Defense建立 VPN 连接。
2. 验证已配置的模块是否已作为 Secure Client的一部分下载并安装。
3. 验证配置的配置文件（如果有）在 所有操作系统的配置文件位置中记录的位置是否可用。

在 防火墙管理中心

您可以使用远程访问 VPN 控制面板（**洞察与报告** > **VPN 控制面板** > **远程访问 VPN**）监控 防火墙管理中心 上的远程接入 VPN 活动会话。您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。

在移动设备上配置基于应用的（Per App VPN）远程访问 VPN

当您使用 Secure Client 从移动设备建立 VPN 连接时，所有流量（包括来自个人应用的流量）都通过 VPN 路由。

对于在 Android 或 iOS 上运行的移动设备，可以限制使用 VPN 隧道的应用。这种基于应用的远程访问 VPN 称为 Per App VPN。要使用 Per App VPN，您必须安装和配置第三方移动设备管理器 (MDM) 应用。在 MDM 中，您要定义可通过 VPN 隧道使用的已批准应用的列表。您可以在 Firewall Threat Defense 头端启用 Per App VPN，以便您的 MDM 可以在移动设备上应用您的策略。

优势

将远程访问 VPN 限制为已批准的应用的好处包括：

- 性能 - 限制企业网络上的 VPN 流量并释放 VPN 前端的资源。
- 保护 - 保护企业 VPN 隧道免受移动设备上未经批准的恶意应用的影响。

配置 Per App VPN 隧道的前提条件和许可

前提条件

- 安装和配置第三方移动设备管理器 (MDM)。

  您必须在 MDM 本身而非 Firewall Threat Defense 头端设备中配置允许在 VPN 中使用的应用。

- 您可以从 Cisco 软件下载中心下载 Cisco AnyConnect Enterprise Application 选择器。

  您需要此工具来定义 Per App VPN 策略。

许可

- Secure Client Premier，或 Secure Client Advantage。
- 基础版许可证必须允许出口控制功能。

  要在 防火墙管理中心 中验证此功能，请选择 **管理** > **许可证** > **特定许可证**。

确定移动应用的应用 ID

在配置 Firewall Threat Defense 前端以允许来自移动设备的基于应用的 VPN 之前，您必须确定应在隧道中允许哪些应用。

我们强烈建议您在用户移动设备上的移动设备管理器 (MDM) 中配置 Per-App 策略。这样可以简化前端配置。如果您决定要在前端配置允许的应用列表，则必须确定每种类型的终端上每个应用的应用 ID。

应用 ID（在 iOS 中称为捆绑包 ID）是反向 DNS 名称。您可以使用星号作为通配符。例如，*.* 表示所有应用，com.cisco.* 表示所有 Cisco 应用。

要确定应用 ID，请执行以下操作：

- **Android**-在网络浏览器中转至 Google Play，然后选择应用类别。点击要允许的应用（或悬停在该应用上），然后查看 URL。应用 ID 位于 URL 中的 **id=** 参数上。例如，Facebook Messenger 的 URL 如下，因此应用 ID 是 com.facebook.orca。

  https://play.google.com/store/apps/details?id=com.facebook.orca

  对于通过 Google Play 无法获得的应用（例如您自己的应用），下载一个程序包名称查看器应用以提取该应用 ID。Cisco 不为任何可用的应用背书，但这些应用之一应能够满足您的需求。

- **iOS**-没有直接的方法来获取捆绑包 ID。以下是一种查找方法：

  1. 使用桌面 web 浏览器（例如 Chrome）搜索应用名称。
  2. 在搜索结果中，查找从 Apple App Store 下载该应用的链接。例如，Facebook Messager 将类似于：

     https://apps.apple.com/us/app/messenger/id454638411

  3. 复制 **id** 字符串后面的数字。在本例中，即 **454638411**。

4. 打开一个新的浏览器窗口，然后将该数字添加到以下 URL 的末尾：

   https://itunes.apple.com/lookup?id=

   在本例中，即： https://itunes.apple.com/lookup?id=454638411

5. 系统将提示您下载文本文件，该文件通常命名为 1.txt。下载文件。
6. 在文本编辑器（例如写字板）中打开文件，然后搜索 bundleId。例如：

   "bundleId":"com.facebook.Messenger",

   在本例中，捆绑包 ID 为 com.facebook.Messenger。以此作为应用 ID。

拥有应用 ID 列表后，您可以如所解释配置策略。

配置基于应用的 VPN 隧道

安装并配置 MDM 软件后，您可以在 Firewall Threat Defense 头端设备上启用 Per App VPN。在头端启用后，您的 MDM 软件将控制通过 VPN 连接到企业网络的应用。

开始之前

- 确保您已在 防火墙管理中心中远程访问 VPN 策略。
- 使用 MDM 配置 Per App VPN，并将每台设备注册到 MDM 服务器。
- 下载 Cisco AnyConnect 企业应用选择器。

过程

步骤 1 使用 Cisco AnyConnect 企业应用选择器定义 Per App VPN 策略。

我们建议您创建一个简单的 **全部允许** 策略，并在 MDM 中定义允许的应用。但是，您可以从头端指定要允许和控制列表的应用列表。如果要包括特定应用，请使用唯一名称和应用的应用 ID 为每个应用创建单独的规则。有关获取应用 ID 的详细信息，请参阅 确定移动应用的应用 ID。

要使用 AnyConnect 企业应用选择器创建支持 Android 和 iOS 平台的 **全部允许** 策略，请执行以下操作：

a) 从下拉列表中选择 **Android** 作为平台类型，并配置以下选项：

- **友好名称 (Friendly Name)** - 输入策略的名称。例如，Allow_All。
- **App ID**-输入 *.* 以匹配所有可能的应用。
- 其他选项保持不变。

b) 从下拉列表中选择 **iOS** 作为平台类型，并配置以下选项：

- **友好名称 (Friendly Name)** - 输入策略的名称。例如，Allow_All。

- **App ID**-输入 *.* 以匹配所有可能的应用。
- 其他选项保持不变。

c) 依次选择 **策略 > 查看策略** 以获取策略的 base64 编码字符串。

此字符串包含允许 Firewall Threat Defense 查看策略的加密 XML 文件。复制此值。在 Firewall Threat Defense上配置 Per App VPN 时需要此字符串。

步骤 2 使用 防火墙管理中心 在 Firewall Threat Defense 头端设备上启用 Per App。

a) 选择**安全连接** > **远程访问 VPN**。
b) 选择远程访问 VPN 策略，然后点击**编辑 (Edit)**。
c) 选择一个连接配置文件 ，然后点击**编辑 (Edit)**。
d) 点击**编辑组策略 (Edit Group Policy)**。
e) 点击 **安全客户端** 选项卡。
f) 点击 **自定义属性** ，然后点击 +。
g) 从 **安全客户端 属性** 下拉列表中选择 **Per App VPN** 。
h) 从 **自定义属性对象** 下拉列表中选择对象，或点击 **+** 添加对象。

为 Per App VPN 添加新的自定义属性对象时，请输入 Cisco AnyConnect 企业应用选择器中的名称、说明和 base64 编码策略字符串。

i) 点击**保存**。
j) 点击 **添加** ，然后点击 **保存**。

步骤 3 在 防火墙管理中心上部署更改。

下一步做什么

1. 启动 Secure Client，选择 VPN 配置文件，然后连接到 VPN。
2. 确认配置。有关详细信息，请参阅验证每个应用配置 ， 第 1636 页。

验证每个应用配置

在 Firewall Threat Defense

在 Firewall Threat Defense 上使用以下命令查看 Per App 配置：

- **show run webvpn**
- **show run group-policy<ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

在终端上

终端与 Firewall Threat Defense建立 VPN 连接后：

1. 点击视图 **统计信息** 图标 Secure Client。
2. **隧道模式 (Tunnel Mode)** 将是“应用隧道”(Application Tunnel)，而不是“隧道所有流量”(Tunnel All Traffic)。
3. **隧道应用 (Tunneled Apps)** 将列出您在 MDM 中启用隧道的应用。

远程访问 VPN 示例

如何限制每个用户的 安全客户端 带宽

本节介绍如何限制 VPN 用户使用 Secure Client 到 Cisco Secure Firewall Threat Defense 远程访问 VPN 网关连接时消耗的最大带宽。您可以通过使用 Firewall Threat Defense策略中的服务质量（QoS）限制最大带宽，以确保单个用户或组或多个用户不会接管整个资源。通过此配置，您可以优先处理关键流量，防止带宽占用和管理网络。如果当流量超出最大速率，Firewall Threat Defense 会丢弃超额流量。

步骤	相应操作	更多信息
1	创建和设置领域。	创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页
2	为新创建的领域中可用的用户或组创建 QoS 策略和 QoS 规则。	• 请参阅 创建 QoS 策略，第 1416 页 以创建 QoS 策略。 • 请参阅 配置 QoS 规则，第 1417 页 以创建 QoS 规则。
3	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程访问 VPN 策略，第 1542 页
4	部署远程访问 VPN 策略。	部署配置更改，第 180 页

如何对基于用户 ID 的访问控制规则使用 VPN 身份

步骤	相应操作	更多信息
1	创建和设置领域。	创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。
2	创建身份策略并添加身份规则。	• 请参阅 创建身份策略，第 2213 页 以创建身份策略。 • 请参阅 创建身份规则，第 2221 页 以创建身份规则。

步骤	相应操作	更多信息
3	将身份策略与访问控制策略相关联。	将其他策略与访问控制相关联，第 1719 页
4	配置远程访问 VPN 策略，并选择新创建的领域进行用户身份验证。	创建新的远程访问 VPN 策略，第 1542 页
5	部署远程访问 VPN 策略。	部署配置更改，第 180 页

配置Firewall Threat Defense多证书身份验证

基于多证书的身份验证

基于多证书的身份验证允许 Firewall Threat Defense 验证计算机或设备证书。可以在远程接入 VPN 连接配置文件中为基于证书的身份验证启用多个证书。它可以与 AAA 身份验证结合使用。远程接入 VPN 连接配置文件中的多证书选项允许通过证书同时对计算机和用户进行证书身份验证。除了对用户的身份证书进行身份验证以允许 RA VPN 访问之外，这样还可以确保设备是公司颁发的设备。管理员可以选择是从计算机证书还是用户证书获取会话的用户名。

如果配置了多个基于证书的身份验证，则会从 VPN 客户端获取两个证书：

- **第一个证书 (First Certificate)** - 对终端进行身份验证的计算机证书。
- **第二个证书 (Second Certificate)** - 对 VPN 用户进行身份验证的用户证书。

有关 Firewall Threat Defense 证书的详细信息，请参阅管理 Firewall Threat Defense 证书，第 2744 页。

限制

- 多证书身份验证当前会将证书数量限制为两个。
- 安全客户端 仅支持基于 RSA 的证书。
- 在 安全客户端 汇聚身份验证期间，仅支持基于 SHA256、SHA384 和 SHA512 的证书。
- 证书身份验证不能与 SAML 身份验证结合使用。

从证书预填充用户名

预填充用户名选项允许解析证书中的字段，并将其用于后续 AAA 身份验证（主和辅助）。在使用两个证书进行身份验证时，管理员可以为预填充功能选择应从中派生的用户名的证书。默认情况下，用于预填充的用户名检索自用户证书（从 安全客户端 接收的第二个证书）。如果启用“仅证书”(Certificate Only) 身份验证方法，预填充的用户名会被用作 VPN 会话用户名。如果启用 AAA 和证书身份验证，VPN 会话用户名将基于预填充选项。

为远程接入 VPN 配置多证书身份验证

1. 在 Secure Firewall Management Center Web 界面上，选择**安全连接** > **远程访问 VPN**。

2. 编辑现有远程访问策略，或者创建新的策略并进行编辑。

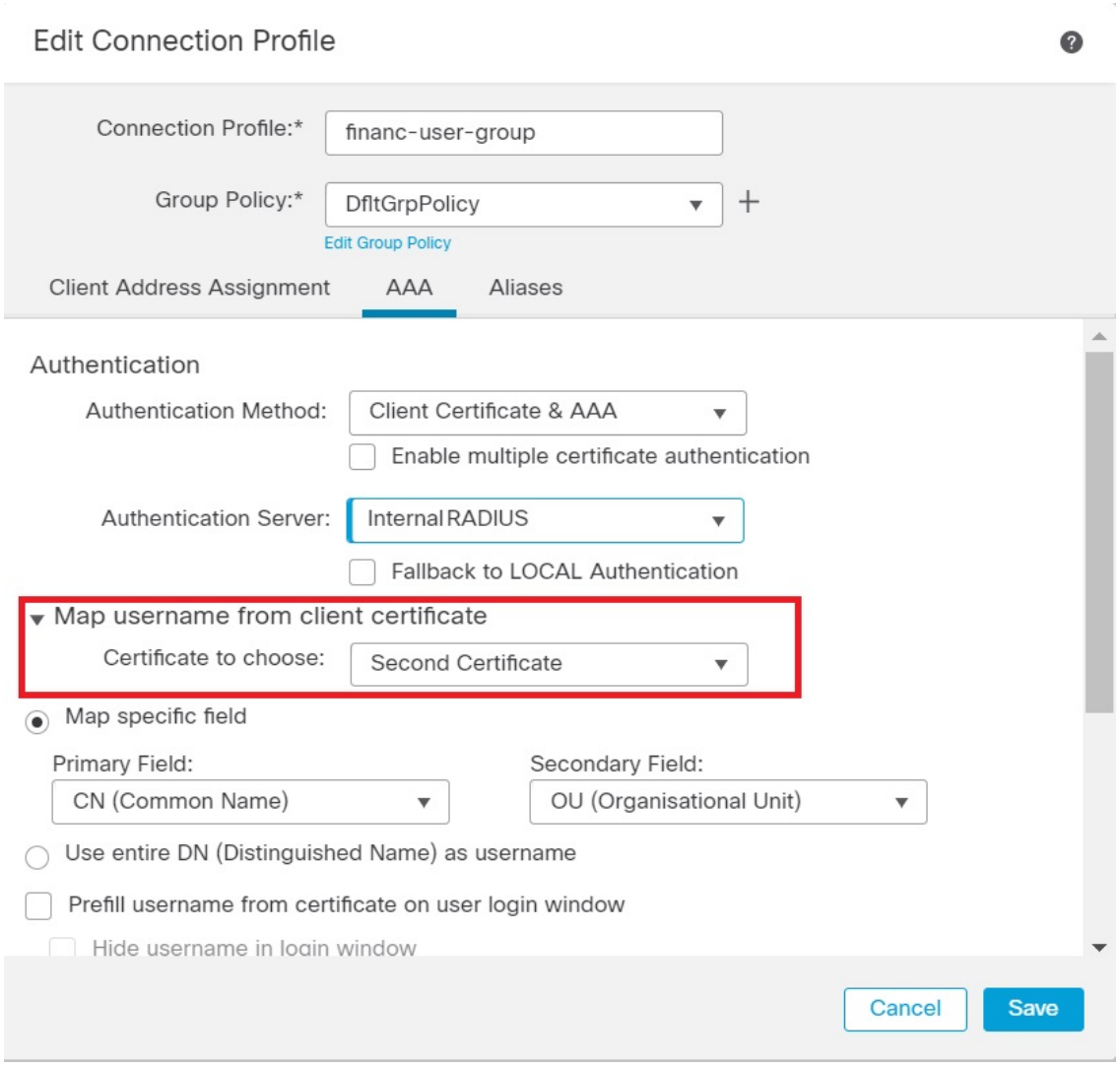
   请参阅创建新的远程访问 VPN 策略，第 1542 页。

3. 选择连接配置文件以配置多证书身份验证，然后点击**编辑 (Edit)**。

   请参阅配置连接配置文件设置，第 1552 页。

4. 选择 **AAA**，然后选择**身份验证方法 (Authentication Method)**：

   图 *443:*



- **仅客户端证书** - 使用客户端证书对用户进行身份验证。客户端证书必须在 VPN 客户端终端上配置。默认情况下，用户名分别派生自客户端证书字段 CN 和 OU。如果在客户端证书的其他字段中指定了用户名，请使用“主”(Primary) 和“辅助”(Secondary) 字段来映射适当的字段。
- **客户端证书和 AAA (Client Certificate & AAA)** - 使用 AAA 和客户端证书这两种身份验证类型来对用户进行身份验证。

5. 选择**启用多证书身份验证 (Enable multiple certificate authentication)**。
6. 选择**映射客户端证书中的用户名 (Map username from client certificate)**，然后从**可供选择的证书 (Certificate to choose)** 下拉列表中选择证书，以便从计算机证书或用户证书中选择 VPN 会话的用户名。
   - **第一个证书 (First Certificate)** - 映射计算机证书中的用户名。
   - **第二个证书 (Second Certificate)** - 映射用户证书中的用户名，以便对 VPN 用户进行身份验证。
7. 配置所需的连接配置文件设置和远程访问 VPN 设置。
8. 保存连接配置文件和远程访问 VPN 策略。在 Firewall Threat Defense 上部署远程访问 VPN 策略。

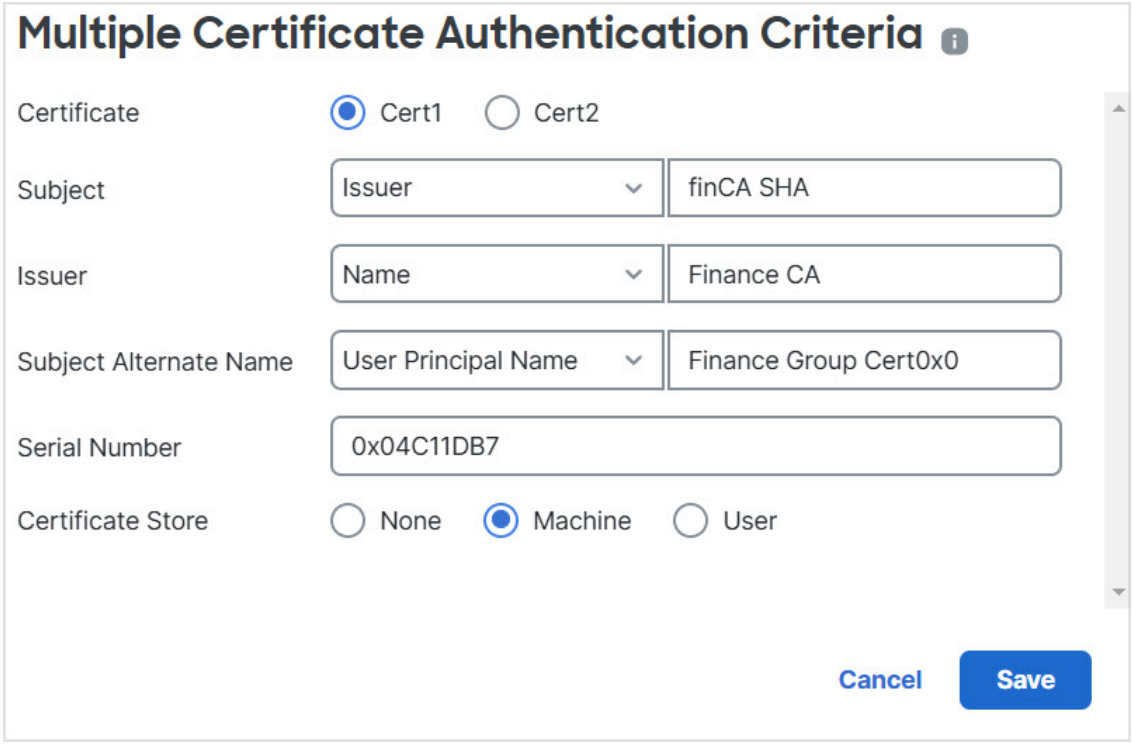
有关远程访问 VPN AAA 设置的信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

DAP 中的证书配置

您也可以在 DAP 记录中配置证书条件属性。将在多证书身份验证期间从 VPN 客户端收到的用户和计算机证书加载到动态访问策略 (DAP)，以确保能够根据证书字段配置策略。您可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。

1. 选择**安全连接** > **动态**。
2. 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。
3. 选择现有的 DAP 记录，或创建新的 DAP 记录并对其进行编辑。
4. 选择**终端条件 (Endpoint Criteria)** > **证书 (Certificate)**。
5. 选择匹配条件**所有 (All)** 或**任何 (Any)**。
6. 点击**添加 (Add)** 以添加证书属性。

图 *444:*



7. 选择证书 **Cert1** 或 **Cert2**。
8. 选择**使用者 (Subject)** 并指定证书使用者值。
9. 选择**颁发机构 (Issuer)** 并指定证书颁发机构名称。
10. 选择**使用者替代名称 (Subject Alternate Name)**，并为使用者指定替代名称。
11. 指定**序列号 (Serial Number)**。
12. 选择**证书存储区 (Certificate Store)**：无、计算机或用户。

    此选项会添加一个条件来检查在终端上要从中挑选证书的存储区。
13. 点击**保存**以完成证书条件设置。

    配置所需的 DAP 记录设置，然后将 DAP 与远程接入 VPN 关联。

有关 DAP 的详细信息，请参阅动态访问策略 ，第 1649 页。

监控远程访问 VPN

远程访问 VPN 控制面板

远程访问虚拟专用网络 (RA VPN) 允许远程用户安全地连接到您的网络。通过 RA VPN 控制面板，您可以监控设备上活动 RA VPN 会话的实时数据。您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。

RA VPN 控制面板（**洞察与报告** > **VPN 控制面板** > **远程访问 VPN**）提供防火墙管理中心管理的威胁防御设备上的活动 RA VPN 会话快照。

控制面板提供：

- 基于位置的活动用户会话可视化。
- 有关活动用户会话的详细信息。
- 如果需要，通过终止会话来缓解用户会话问题。
- 按设备、加密类型、安全客户端版本、操作系统和连接配置文件分布的活动用户会话。
- 设备的设备身份证书到期详细信息。

控制面板具有以下构件：

- 活动会话（表格视图）
- 活动会话（地图视图）
- 会话
- 设备身份证书

活动会话（表格视图）

此构件提供已连接的活动 RA VPN 用户的表格视图。您可以查看活动 RA VPN 会话的详细信息，例如用户名、分配的 IP、公共 IP、登录时间、VPN 网关（威胁防御设备）、客户端应用、客户端操作系统、连接配置文件和组策略。您可以使用过滤器根据不同的条件来缩小搜索范围。您还可以对各个会话执行以下操作：

- 终止特定用户的会话。
- 终止连接到特定 VPN 网关的特定用户的所有会话。
- 终止连接到特定 VPN 网关的所有会话。

如果客户端设备支持双地址栈，并且 Firewall Threat Defense 设备上的 RA VPN 配置允许 IPv4 和 IPv6 地址池，那么当客户端与头端设备建立 RA VPN 会话时，它会为客户端的隧道接口分配一个 IPv4 和一个 IPv6 地址。RA VPN 会话有两个 IP 地址，即威胁防御设备上的 IPv4 和 IPv6 地址。防火墙管理中心 显示同一用户的两个会话，一个使用 IPv4 地址，另一个使用 IPv6 地址，会话计数为 2。

因此，即使根据设备上的 **show vpn-sessiondb l2l filter ipaddress** 命令，用户只有一个 RA VPN 会话，防火墙管理中心 也会显示两个不同的会话。

活动会话（地图视图）

该构件会显示交互式热度地图，以便直观地显示通过 RA VPN 会话连接到设备上的用户的位置。

- 具有用户会话的国家/地区会显示为蓝色阴影。
- 地图图例提供了一个比例，表示某个国家/地区的会话数与其蓝色阴影之间的相关性。
- 将鼠标指针悬停在地图上即可查看国家/地区名称和活动用户会话总数。
- 提供放大、缩小和重置选项。

会话

此构件允许您监控设备上活动 RA VPN 会话的实时数据。您可以根据以下条件来过滤和查看活动 RA VPN 会话的分布情况：

- 设备：显示每台设备的会话数。
- 加密类型：显示 Secure Client SSL 或 IPsec 会话的数量。
- Secure Client 版本：显示每个 Secure Client 版本的会话。
- 操作系统：显示每个操作系统的会话。例如，Windows、Linux、Mac、Mobile OS 等。
- 连接配置文件：显示每个连接配置文件的会话。

设备身份证书

此构件提供有关 RA VPN 网关身份证书到期的信息。您可以查看过期的证书和一个月内到期的证书。点击**查看详细信息 (View Details)**，在设备**设备** > **证书**页面中查看证书。

VPN 会话和用户信息

系统生成在网络上传达用户活动详细信息的事件，包括与 VPN 相关的活动。系统监视功能使您能够快速确定远程接入 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。或者，您可以根据需要注销远程接入 VPN 用户。

查看远程接入 VPN 活动会话

事件和日志 > **用户** > **活动会话**

使您可以使用支持信息（如用户名、登录持续时间、身份验证类型、分配的/公用 IP 地址、设备详细信息、客户端版本、终端消息、吞吐量、占用带宽的组策略、隧道组等）在任何给定的时间点查看当前登录的 VPN 用户。系统允许您过滤当前用户信息、注销用户以及从摘要列表中删除用户。

注释 如果在高可用性部署中配置了 VPN，则针对活动 VPN 会话显示的设备名称可以是识别用户会话的主要或辅助设备。

查看远程接入 VPN 用户活动

事件和日志 > 用户 > 用户活动

用于查看网络上用户活动的详细信息。系统记录历史事件，包括与VPN相关的信息，如连接配置文件信息、IP 地址、地理位置信息、连接持续时间、吞吐量和设备信息。

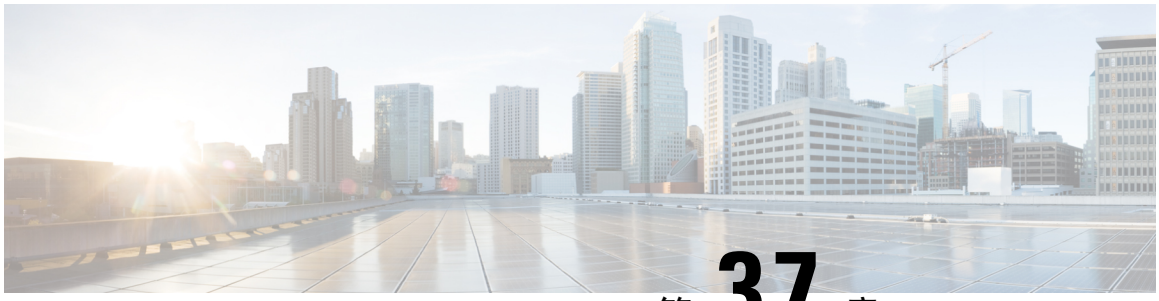
远程接入 VPN 的功能历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
基于地理位置的 RA VPN	7.7	7.7	现在，您可以根据国家或地区允许或阻止远程访问 VPN 连接。不符合基于位置的条件的连接会在验证前被阻止，并记录在案以备审核。 新增/修改的屏幕： • **对象** > **对象管理** > **访问列表** > **服务访问** • **设备** > **VPN** > **远程访问**
VTI环回接口上的IPsec流分流	7.4	任意	在 Cisco Secure Firewall 3100 和 Cisco Secure Firewall 4200 设备上，会在 VTI 环回接口上自动启用 IPsec 数据流分流。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
安全客户端自定义	7.4	任意	您可以配置安全客户端自定义并将其部署到 VPN 头端。当用户从安全客户端连接时，威胁防御会将这些自定义分发到终端： • GUI 文本和消息 • 图标和图像 • 脚本 • 二进制文件 • 自定义安装程序转换 • 本地化安装程序转换 新增/修改的屏幕： • **对象 > 对象管理 > VPN > 安全客户端自定义** > >**设备** > **远程访问** > **高级** > **安全客户端自定义**
WAN 摘要控制面板	7.4	任意	WAN 摘要控制面板提供 WAN 设备及其接口的快照。 新增/修改的屏幕： **概述** > **控制面板** > **WAN 摘要**
远程访问 VPN 控制面板	7.3	任意	远程访问 VPN (RA VPN) 控制面板，可让您监控设备上正在进行的远程访问 VPN 会话的实时数据。您可以借此快速定位与用户会话相关的问题，并缓解这些问题对网络和用户造成的影响。 新增/修改的屏幕： **洞察与报告** > **VPN 控制面板** > **远程访问 VPN**
支持证书的 SAML	7.2	任意	我们更新了远程接入 VPN 配置向导，以支持通过证书和 SAML 进行用户身份验证。您可以将远程接入 VPN 配置为在发起 SAML 身份验证之前对计算机或用户证书进行身份验证。
IPsec 流分流。	7.2	任意	在 Cisco Secure Firewall 3100上，默认情况下会分流 IPsec 流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 您可以使用 FlexConfig 和 **flow-offload-ipsec** 命令更改配置。
多个 IDP 信任点支持	7.1	任意	Secure Firewall Management Center 支持使用 Microsoft Azure 的多个身份提供程序信任点，这些信任点可以具有相同实体ID的多个应用，但具有唯一身份证书。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
AnyConnect VPN SAML 外部浏览器	7.1	任意	您现在可以配置 AnyConnect VPN SAML 外部浏览器，以启用其他身份验证选项，例如无密码身份验证、WebAuthN、FIDO、SSO、U2F 以及由于 Cookie 的持久性而改进的 SAML 体验。当您使用 SAML 作为远程访问 VPN 连接配置文件的主身份验证方法时，可以选择让 AnyConnect 客户端使用客户端的本地浏览器而不是 AnyConnect 嵌入式浏览器来执行 Web 身份验证。此选项可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证和 Yubikeys），也可选择此选项。 我们更新了远程访问 VPN 连接配置文件向导，现在您可以配置 **SAML 登录体验**。
多证书身份验证	7.0	任意	Secure Firewall Management Center 现在支持多种基于证书的 Firewall Threat Defense 身份验证，以验证机器或设备证书，确保设备是企业发放的设备，此外还可以验证用户的身份证书，以便允许使用 AnyConnect 客户端进行 VPN 接入。
VPN 负载均衡	7.0	任意	VPN 负载均衡会在逻辑上对两台或多台设备进行分组，并在分组的设备之间平均分配远程接入 VPN 会话，而不考虑吞吐量和其他流量参数。
AnyConnect 自定义属性	7.0	任意	Secure Firewall Management Center 现在支持 AnyConnect 自定义属性，同时提供配置 AnyConnect 客户端功能的基础设施，而无需在 Firewall Threat Defense上添加对这些功能的硬编码支持。
本地用户身份验证	7.0	任意	您现在可以使用 Secure Firewall Management Center Web 界面在 Firewall Threat Defense 上配置和管理用户，并为主要和辅助远程接入 VPN 身份验证配置本地用户。
选择性策略部署	7.0	任意	现在，您可以选择包括或排除在部署期间对远程接入 VPN 和站点间 VPN 配置的更改。
支持 AnyConnect 模块配置	6.7	任意	Secure Firewall Management Center 现在支持配置 AnyConnect 模块和配置文件以提高安全性。
支持 LDAP 授权	6.7	任意	您可以使用 Secure Firewall Management Center 为远程接入 VPN 配置 LDAP 授权。
远程接入 VPN 的 SAML 单点登录支持	6.7	任意	您可以为远程接入 VPN 将 SAML 2.0 服务器配置为单点登录身份验证服务器。
AnyConnect 管理 VPN 隧道支持	6.7	任意	Firewall Threat Defense 远程访问 VPN 支持配置 AnyConnect 管理 VPN 隧道，该隧道允许在企业终端通电时通过 VPN 连接到终端，而无需 VPN 用户连接到 VPN。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持数据报传输层安全 (DTLS) 1.2	6.6	任意	DTLS 1.2 现在是默认 SSL 密码组的一部分，并且它可以与 TLS 1.2 一起配置。



第 37 章

动态访问策略

动态访问策略(DAP)让您能够配置解决VPN环境动态问题的授权。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。

- Firewall Threat Defense 动态访问策略， 第 1649 页
- 动态访问策略的先决条件， 第 1651 页
- 动态访问策略的准则与限制， 第 1651 页
- 配置动态访问策略 (DAP)， 第 1652 页
- 将动态访问策略与远程访问 VPN 关联， 第 1662 页
- 动态访问策略历史记录， 第 1662 页

Firewall Threat Defense 动态访问策略

Cisco Secure Firewall Threat Defense 动态访问策略是一组访问控制属性，可以

- 解决 VPN 环境中多个组成员身份和终端安全的问题
- 根据定义的策略授予特定用户在特定会话中的访问权限，并且
- 适应具有影响每个 VPN 连接的多个变量的动态环境。

动态访问策略操作

VPN 网关在动态环境下运行。多个变量可能会影响每个 VPN 连接。例如，频繁更改内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点尝试登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。

您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。 Firewall Threat Defense 设备会通过从一个或多个 DAP 记录中选择或汇总属性，从而在用户身份验证期间生成DAP。然后，设备会根据远程设备的终端安全信息，以及经过身份验证的用户的AAA授权信息，选择这些 DAP 记录。然后，设备会将 DAP 记录应用至用户隧道或会话。

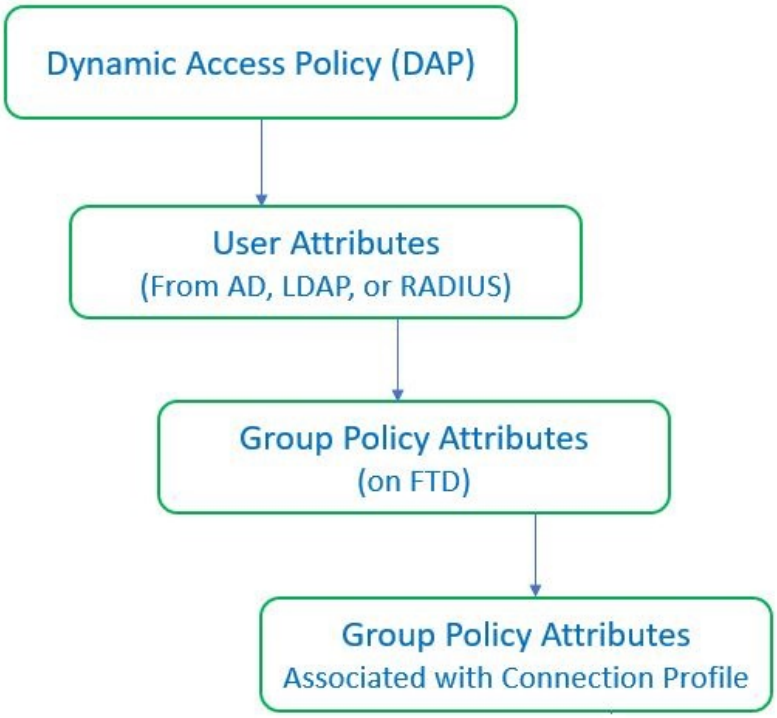
Firewall Threat Defense 设备中权限和属性的策略实施层次结构

Firewall Threat Defense 设备支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接。从 Firewall Threat Defense 上的 DAP、外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或从 Firewall Threat Defense 设备上的组策略应用属性。

如果 Firewall Threat Defense 设备收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果来自 DAP、AAA 服务器或组策略的属性之间存在冲突，从 DAP 获得的属性始终会被优先考虑。

Firewall Threat Defense 设备按以下顺序应用属性：

图 *445:* 策略实施流程



1. **FTD 上的 DAP 属性** - DAP 属性优先于所有其他的属性。
2. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
3. **FTD 上配置的组策略** — 如果 RADIUS 服务器为用户返回 RADIUS 类属性 IETF-Class-25 (OU=group-policy) 值，Firewall Threat Defense 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
4. **连接配置文件 (也称为隧道组) 分配的组策略**- 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。

注释 Firewall Threat Defense设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。对于用户会话，设备会使用您分配给连接配置文件的组策略上的属性，除非它们被来自AAA服务器的用户属性或组策略覆盖。

动态访问策略的先决条件

本文介绍了在配置 Dynamic Access Policy 功能之前必须满足的许可先决条件。

许可证先决条件

- Firewall Threat Defense 必须至少具有以下 Secure Client 许可证之一：
  - Secure Client Premier
  - Secure Client Advantage
  - 仅限 Secure Client VPN
- Firewall Threat Defense 基础版许可证必须允许出口控制功能。

一般先决条件

在配置动态访问策略之前，请确保您拥有 Cisco Secure Firewall 终端安全评估 软件包。您可以在 添加 Cisco Secure Firewall 终端安全评估 文件。

动态访问策略的准则与限制

在实施动态访问策略时，请考虑以下准则和限制：

- 只有当AAA服务器被配置为在对远程接入VPN会话进行身份验证或授权时返回正确的属性时，才能匹配 DAP 中的 AAA 属性。
- DAP 支持的最低 安全客户端 和 Cisco Secure Firewall 终端安全评估 软件包版本为 4.6。但是强烈建议使用最新版本的 安全客户端。
- DAP 不支持集群或多实例模式。
- 具有已分配 IPv4 或 IPv6 地址的 DAP 条件不适用于本地身份验证。

配置动态访问策略 (DAP)

创建动态访问策略

创建动态访问策略，根据 VPN 用户的终端安全状态和合规状态为他们启用条件访问控制。

动态访问策略评估终端属性和安全状态，以确定VPN用户的适当访问权限。这些策略与终端安全评估包配合使用，以实施安全合规。

Before you begin

在配置动态访问策略之前，请确保您拥有 Cisco Secure Firewall 终端安全评估 软件包。您可以在 添加 Cisco Secure Firewall 终端安全评估 文件。

过程

步骤 1 选择 **安全连接** > **动态**，然后点击**创建动态访问策略**。

步骤 2 为 DAP 策略指定**名称 (Name)** 和可选的**说明 (Description)**。

步骤 3 从下拉列表中选择 **Cisco Secure Firewall 终端安全软件包 (Secure Firewall Posture Package)**。

步骤 4 点击**保存**。

下一步做什么

要配置 DAP 记录，请参阅 创建动态访问策略记录

创建动态访问策略记录

动态访问策略 (DAP) 可以包含多个 DAP 记录，您可以在这些记录中配置用户和终端属性。您可以确定 DAP 内的 DAP 记录的优先级，以便 Firewall Threat Defense 设备在用户尝试 VPN 连接时选择和排序所需的条件。

过程

步骤 1 选择**安全连接** > **动态**。

步骤 2 编辑现有的动态访问策略，或者点击**创建动态访问策略 (Create Dynamic Access Policy)** 以创建新策略，然后编辑该策略。

步骤 3 点击**创建 DAP 记录 (Create DAP Record)**。

步骤 4 点击**常规 (General)**选项卡。

步骤 5 指定 DAP 记录的**名称 (Name)**。

步骤 6 为 DAP 记录输入**优先级 (Priority)**。

数值越低，优先级越高。

步骤 7 选择当 DAP 记录匹配时要执行的这些操作之一：

- **继续** - 将访问策略属性应用于会话。如果有的话，接下来会评估下一个 DAP 记录（优先级较低的下一个策略行）。
- **终止 (Terminate)** - 终止会话。
- **隔离 (Quarantine)** - 隔离连接。

步骤 8 选中 **在条件匹配时显示用户消息** 复选框并添加用户消息。

当 DAP 记录匹配， Firewall Threat Defense 将此消息显示给用户。

步骤 9 选中**对流量应用网络 ACL (Apply a Network ACL on Traffic)** 复选框，然后从下拉列表中选择访问控制列表。

步骤 10 选中**应用一个或多个 Secure Client 自定义属性 (Apply one or more Secure Client Custom Attributes)** 复选框，然后从下拉列表中选择自定义属性对象。

步骤 11 点击**保存**。

配置终端安全评估条件

对于 DAP 策略，可以使用唯一的终端 ID 配置文件、进程或注册表终端属性。这些 ID 可用作 Lua 脚本中的终端条件以配置 DAP 记录。

过程

步骤 1 选择**安全连接** > **动态**。

步骤 2 点击**创建动态访问策略 (Create Dynamic Access Policy)** 以创建新的 DAP 策略，然后编辑策略。

步骤 3 点击 DAP 策略旁边的编辑图标。

步骤 4 点击**添加终端安全评估条件 (Add Posture Assessment Criteria)**。

步骤 5 执行以下任一操作：

- 配置文件终端属性：
  1. 点击**文件 (File)** 单选按钮。
  2. 在**终端 ID (Endpoint ID)** 字段中，输入文件的唯一 ID。它可以是一个字符串或数字。
  3. 在**文件路径 (File Path)** 字段中，指定文件路径。
- 配置注册表终端属性：

1. 点击**注册表 (Registry)** 单选按钮。
2. 在**终端 ID (Endpoint ID)** 字段中，输入注册表的唯一 ID。它可以是一个字符串或数字。
3. 在**条目路径 (Entry Path)** 字段中，指定文件路径。

- 配置进程终端属性：
  1. 点击**进程 (Process)** 单选按钮。
  2. 在**终端 ID (Endpoint ID)** 字段中，输入进程的唯一 ID。它可以是一个字符串或数字。
  3. 在**进程名称 (Process Name)** 字段中，指定进程名称。

注释
终端 ID 一旦保存，就无法编辑。

步骤 6 点击**保存**。

下一步做什么

您可以使用 Lua 脚本来通过终端 ID 配置高级终端安全评估条件。有关详细信息，请参阅配置 DAP 高级设置，第 1661 页。

为 DAP 记录配置 AAA 条件设置

配置 AAA 条件设置以指定根据 AAA 授权和状态评估信息选择 DAP 记录并将其应用于用户会话的条件。

DAP 可提供一组限定的授权属性，这些属性可覆盖 AAA 提供的属性，从而补充 AAA 服务。Firewall Threat Defense 设备基于用户的 AAA 授权信息和会话的状态评估信息来选择 DAP 记录。Firewall Threat Defense 设备可根据此信息选择多个 DAP 记录，然后将其聚合以创建 DAP 授权属性。

过程

步骤 1 选择**安全连接** > **动态**。
步骤 2 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。
步骤 3 选择 DAP 记录或创建新记录，然后编辑 DAP 记录。
步骤 4 点击 **AAA 条件 (AAA Criteria)**。
步骤 5 选择**部分之间匹配条件**之一。

- 任意 (Any) - 匹配任意条件。
- 全部 (All) - 匹配所有条件。
- 无 (None) - 不匹配任何设定的条件。

步骤 6 点击添加 (Add) 以添加所需的思科 VPN 条件。

思科 VPN 条件包括组策略的属性、分配的 IPv4 地址、分配的 IPv6 地址、连接配置文件、用户名、用户名 2 和所需的 SCEP。

a) 选择属性并指定 值。
b) 点击添加其他条件以添加更多条件。
c) 点击保存。

步骤 7 选择 LDAP 条件、 RADIUS 条件或 SAML 条件 并指定 属性 ID 和 值 (。

步骤 8 点击保存。

Configure Endpoint Attribute Selection Criteria in DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The Firewall Threat Defense dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database that is associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the Firewall Threat Defense to choose it for a session. The Firewall Threat Defense selects only DAP records that satisfy every condition configured.

Procedure

步骤 1 Choose 安全连接 > 动态, and click **Create Dynamic Access Policy**.

步骤 2 Edit a DAP policy and then DAP record.

Note
Create a DAP policy and DAP record if not done already.

步骤 3 Click **Endpoint Criteria** and configure the following endpoint criteria attributes:

Note
You can create multiple instances of each type of endpoint attribute. There is no limit for the number of endpoint attributes for each DAP record.

- Add an Anti-Malware Endpoint Attribute to a DAP
- Add a Device Endpoint Attribute to a DAP
- Add Secure Client Endpoint Attributes to a DAP, on page 1657
- Add a NAC Endpoint Attribute to a DAP
- Add an Application Attribute to a DAP
- Add a Personal Firewall Endpoint Attribute to a DAP
- Add an Operating System Endpoint Attribute to a DAP

- Add a Process Endpoint Attribute to a DAP
- Add a Registry Endpoint Attribute to a DAP
- Add a File Endpoint Attribute to a DAP
- Add Multiple Certificate Authentication Attributes to DAP

步骤 4 Click **Save**.

Add an Anti-Malware Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Anti-Malware**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add anti-malware attributes.

步骤 4 Click **Installed** to indicate whether the selected endpoint attribute and its accompanying qualifiers are installed or not installed.

步骤 5 Choose **Enabled** or **Disabled** to activate or deactivate real-time malware scanning.

步骤 6 Select the name of the anti-malware **Vendor** from the list.

步骤 7 Select the anti-malware **Product Description**.

步骤 8 Choose the **Version** of the anti-malware product.

步骤 9 Specify the number of days since the **Last Update**.

You can indicate that an anti-malware update must occur in less than (<) or more than (>) the number of days you specify.

步骤 10 Click **Save**.

Add a Device Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record and choose **Endpoint Criteria** > **Device**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** and select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter for the following attributes:

- **Host Name**—Hostname of the device you are testing for. Use the computer’s host name only, not the fully qualified domain name (FQDN).

- **MAC Address**—MAC address of the network interface card you are testing for. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
- **BIOS Serial Number**—BIOS serial number value of the device you are testing for. The number format is manufacturer-specific.
- **Port Number**—Listening port number of the device.
- **Secure Desktop Version**—Version of the Host Scan image running on the endpoint.
- **OPSWAT Version**—The OPSWAT client version.
- **Privacy Protection**—None, Cache cleaner, Secure Desktop.
- **TCP/UDP Port Number**—TCP or UDP port in the listening state that you are testing for.

步骤 4 Click **Save**.

Add Secure Client Endpoint Attributes to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Secure Client**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** and select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter.

步骤 4 Select the **Client Version** and **Platform**.

步骤 5 Select the **Platform Version**, and specify the **Device Type** and **Device Unique ID**.

步骤 6 Add the **MAC Addresses** the MAC Address Pool.

Note
The MAC Address must be in the format XX-XX-XX-XX-XX-XX, where each X is a hexadecimal character. You can click **Add another MAC Address** to add more addresses.

步骤 7 Click **Save**.

Add NAC Endpoint Attributes to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **NAC**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add NAC attributes.

步骤 4 Set the operator to be equal to = or not equal to ≠ the posture token string. Enter the posture token string in the **Posture Status** box.

步骤 5 Click **Save**.

Add an Application Attribute to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Application**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add application attributes.

步骤 4 Choose equals (=) or does not equal (≠) and specify the **Client Type** to indicate the type of remote access connection.

步骤 5 Click **Save**.

Add a Personal Firewall Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Personal Firewall**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add personal firewall attributes.

步骤 4 Click **Installed** to indicate whether the personal firewall endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.

步骤 5 Choose **Enabled** or **Disabled** to activate or deactivate firewall protection.

步骤 6 Select the name of the firewall **Vendor** from the list.

步骤 7 Select the firewall **Product Description**.

步骤 8 Select the equals (=) or does not equal (≠) operator and choose the **Version** of the personal firewall product.

步骤 9 Click **Save**.

Add an Operating System Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Operating System** .

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add endpoint attributes.

步骤 4 Select the equals (=) or does not equal (≠) operator and then select the **Operating System**.

步骤 5 Select the equals (=) or does not equal (≠) operator and then specify the operating system **Version**.

步骤 6 Click **Save**.

Add a Process Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record.

步骤 2 Click the **Endpoint Criteria** tab.

步骤 3 Click **Process**.

步骤 4 Select the **Match Criteria** as **All** or **Any**.

步骤 5 Click + to add the process attributes.

步骤 6 Select **Exists** or **Does not exist**.

步骤 7 Specify the **Process Name**.

步骤 8 From the **Endpoint ID** drop-down list, choose the ID for the process or click + to configure a posture assessment criteria for the process. For more information, see 配置终端安全评估条件, on page 1653.

步骤 9 Click **Exists** or **Does not exist**.

步骤 10 Click **Save**.

Add a Registry Endpoint Attribute to a DAP

Scanning for registry endpoint attributes applies to Windows operating systems only.

Before you begin

Before configuring a Registry endpoint attribute, define the registry key for which you want to scan in the Host Scan window for Cisco Secure Desktop.

Procedure

步骤 1 Edit a DAP record.
步骤 2 Click the **Endpoint Criteria** tab.
步骤 3 Click **Registry**.
步骤 4 Select the **Match Criteria** as **All** or **Any**.
步骤 5 Click + to add registry attributes.
步骤 6 Select the **Entry Path** for the registry and specify the path.
步骤 7 From the **Endpoint ID** drop-down list, choose the ID for the registry or click + to configure a posture assessment criteria for the registry. For more information, see 配置终端安全评估条件, on page 1653.
步骤 8 Choose the existence of the registry, **Exists** or **Does not exist**.
步骤 9 Select the registry **Type** from the list.
步骤 10 Select the equals (=) or does not equal (≠) operator and enter the **Value** of the registry key.
步骤 11 Select **Case insensitive** to disregard the case of the registry entry while scanning.
步骤 12 Click **Save**.

Add a File Endpoint Attribute to a DAP

Procedure

步骤 1 Edit a DAP record.
步骤 2 Click the **Endpoint Criteria** tab.
步骤 3 Click **File**.
步骤 4 Select the Match Criteria **All** or **Any**.
步骤 5 Click + to add file attributes.
步骤 6 Specify the **File Path**.
步骤 7 From the **Endpoint ID** drop-down list, choose the ID for the file or click + to configure a posture assessment criteria for the file. For more information, see 配置终端安全评估条件, on page 1653.
步骤 8 Choose **Exists** or **Does not exist** to indicate the presence of the file.
步骤 9 Select less than (<) or greater than (>) and specify the **Last Modified** days for the file.
步骤 10 Select the equal to (=) or not equal to ≠ operator and enter the **Checksum**.
步骤 11 Click **Save**.

Add Certificate Authentication Attributes to a DAP

You can index each certificate to allow referencing to any of the received certificates, by the configured rules. Based on these certificate fields, you can configure DAP rules to allow or disallow connection attempts.

Procedure

步骤 1 Edit a DAP record and select **Endpoint Criteria** > **Certificate**.

步骤 2 Select the Match Criteria **All** or **Any**.

步骤 3 Click **Add** to add certificate attributes.

步骤 4 Select the certificate **Cert1** or **Cert2**.

步骤 5 Select the **Subject** and specify the subject value.

步骤 6 Select the **Issuer** and specify the issuer value.

步骤 7 Select the **Subject Alternate Name** and specify the subject value.

步骤 8 Specify the **Serial Number**.

步骤 9 Choose the **Certificate Store**: None, Machine, or User.

The VPN client sends the certificate store information.

步骤 10 Click **Save**.

配置 DAP 高级设置

当标准 AAA 与终端属性区域无法满足要求时，此任务允许使用 Lua 脚本配置 DAP 记录的选择条件。

您可以使用**高级**选项卡添加 AAA 与终端属性区域以外的选择条件。例如，在您将 Firewall Threat Defense配置为使用AAA属性（这些属性满足任意、所有指定条件，或者不需要满足指定条件）时，终端属性是累计的，并且必须全部满足。要让安全设备使用一个或另一个终端属性，您必须创建适当的 Lua 逻辑表达式，并在此处输入它们。

过程

步骤 1 选择**安全连接** > **动态**。

步骤 2 创建或编辑 DAP 记录。

步骤 3 点击**高级**选项卡。

步骤 4 选择 **AND** 或 **OR** 作为要在 DAP 配置上使用的匹配条件。

步骤 5 在 **用于高级属性匹配的 Lua 脚本** 字段中添加 Lua 脚本。

步骤 6 要在 Lua 脚本中使用端点标准 ID，请执行以下操作：

1. 将光标放在要插入终端条件 ID 的位置。

2. 从**终端条件 (Endpoint Criteria)** 下拉列表中选择条件 a
3. 从相邻的下拉列表中选择相应的 ID。

示例：

在本示例中，DAPTESTFILE、LIBAGENT、vpnagent 和 DUOAGENT 已插入 Lua 脚本：

```
EVAL(endpoint.file["DAPTESTFILE"].exists,"EQ","true") or
EVAL(endpoint.file["LIBAGENT"].exists,"EQ","true") and
EVAL(endpoint.process[""vpnagent""].exists,"EQ","true") and
EVAL(endpoint.registry[""DUOAGENT""].exists,"EQ","true")
```

步骤 7 点击**保存**。

将动态访问策略与远程访问 VPN 关联

您可以将动态访问策略 (DAP) 与远程访问 VPN 策略关联，以便在 VPN 会话身份验证和授权期间匹配动态访问策略属性。您可以在 Firewall Threat Defense 上部署远程访问 VPN。

过程

步骤 1 选择**安全连接** > **远程访问 VPN**。
步骤 2 点击要与动态访问策略关联的远程访问 VPN 策略旁边的 **编辑** 。
步骤 3 点击远程访问 VPN 中的链接以选择动态访问策略。
步骤 4 从 **动态访问策略** 下拉列表中选择策略，或点击 **创建新的动态访问策略** 以配置新的动态访问策略。
步骤 5 点击**确定**。
步骤 6 点击**保存**以保存远程访问 VPN 策略。

当远程访问 VPN 用户尝试连接时，VPN 会检查配置的动态访问策略记录和属性。VPN 根据匹配的动态访问策略记录创建动态访问策略，并对 VPN 会话执行适当的操作。

动态访问策略历史记录

本参考提供了动态访问策略功能的版本历史记录，包括引入时间及每个版本中的变更。

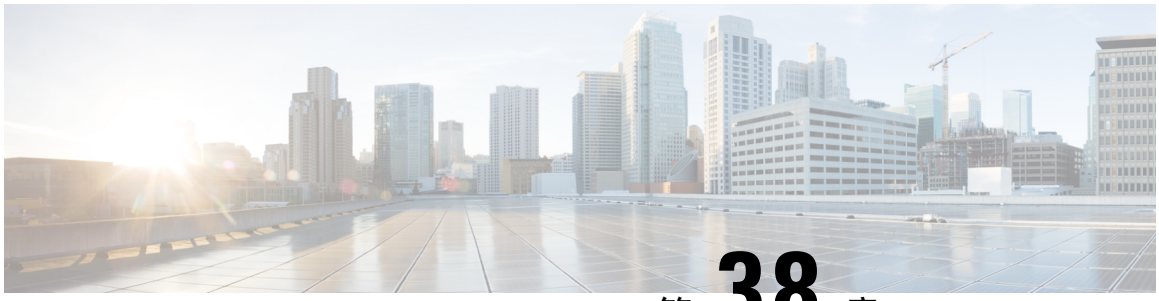
功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
轻松配置动态访问策略的安全评估条件	7.7	任意	对于 DAP 策略，可以使用唯一的终端 ID 配置文件、进程或注册表终端属性。这些 ID 可用作 Lua 脚本中的终端条件以配置 DAP 记录。 新增/修改的屏幕： • 设备 > 动态访问策略 > 添加/编辑策略 > 添加状态评估条件 • 设备 **(Devices)** > 动态访问策略 **(Dynamic Access Policy)** > 添加/编辑策略 **(Add/Edit Policy)** > 添加/编辑 **DAP** 记录 **(Add/Edit DAP Record)** > 高级 **(Advanced)** > 终端条件 **(Endpoint Criteria)**
动态访问策略	7.0	任意	引入了此功能。



第 VII 部分

零信任网络访问

- 零信任网络访问， 第 1667 页



第 38 章

零信任网络访问

以下主题提供有关 无客户端 Cisco Zero Trust 访问、通用零信任网络访问 的详细信息，以及如何配置和部署它们。

- 关于无客户端和通用 Zero Trust 网络访问， 第 1667 页
- 无客户端 Cisco Zero Trust 访问， 第 1668 页
- 通用零信任网络访问， 第 1683 页
- Zero Trust 网络访问历史记录， 第 1696 页

关于无客户端和通用 Zero Trust 网络访问

Zero Trust 访问 或 Zero Trust 网络访问 (ZTNA) 是指使用基于身份的访问来保护内部资源的进程，包括用户信任和终端安全评估。该流程先验证用户、设备和请求上下文，然后再允许访问内部资源和应用。仅在验证用户、了解请求上下文并评估任何风险后，它才会授予最低权限访问权限。

您可以在两个 ZTNA 部署模式之间进行选择：

- 无客户端 Cisco Zero Trust 访问
- 通用零信任网络访问

无客户端 Cisco Zero Trust 访问

无客户端零信任网络访问（无客户端 ZTNA）可对来自网络内部（本地）或外部（远程）的受保护的基于 Web 的资源和应用进行身份验证和授权访问。这是使用具有安全断言标记语言 (SAML) 身份验证的外部身份提供程序 (IdP) 来完成的。用户设备上不需要安装客户端软件。

无客户端 ZTNA 非常适合远程用户访问 Web 应用和非托管设备。

通用零信任网络访问

通用 Zero Trust 网络访问（通用 ZTNA）是一种基于客户端的解决方案，无论用户位于何处，它都可以提供对所有内部资源的基于身份的访问。它为每个应用和用户实施强认证、终端安全评估和流量检查。

通用 ZTNA 支持远程和本地用户。本地用户使用 Cisco Secure Firewall Threat Defense 设备访问受信任的网络。远程用户通过基于云的安全访问服务访问可信网络，该服务会在云中安全地评估策略并代理用户流量。

无客户端 Cisco Zero Trust 访问

无客户端 Cisco Zero Trust 访问 基于 Zero Trust 访问原则。Zero Trust 访问是一种消除隐式信任的 Zero Trust 安全模型。该模型在验证用户、请求的上下文以及分析风险（如果授予访问权限）后授予最低权限访问权限。

无客户端 Cisco Zero Trust 访问 允许您使用外部安全断言标记语言 (SAML) 身份提供程序 (IdP) 策略，从网络内部（本地）或外部（远程）对受保护的基于 Web 的资源和应用程序进行身份验证和授权访问。

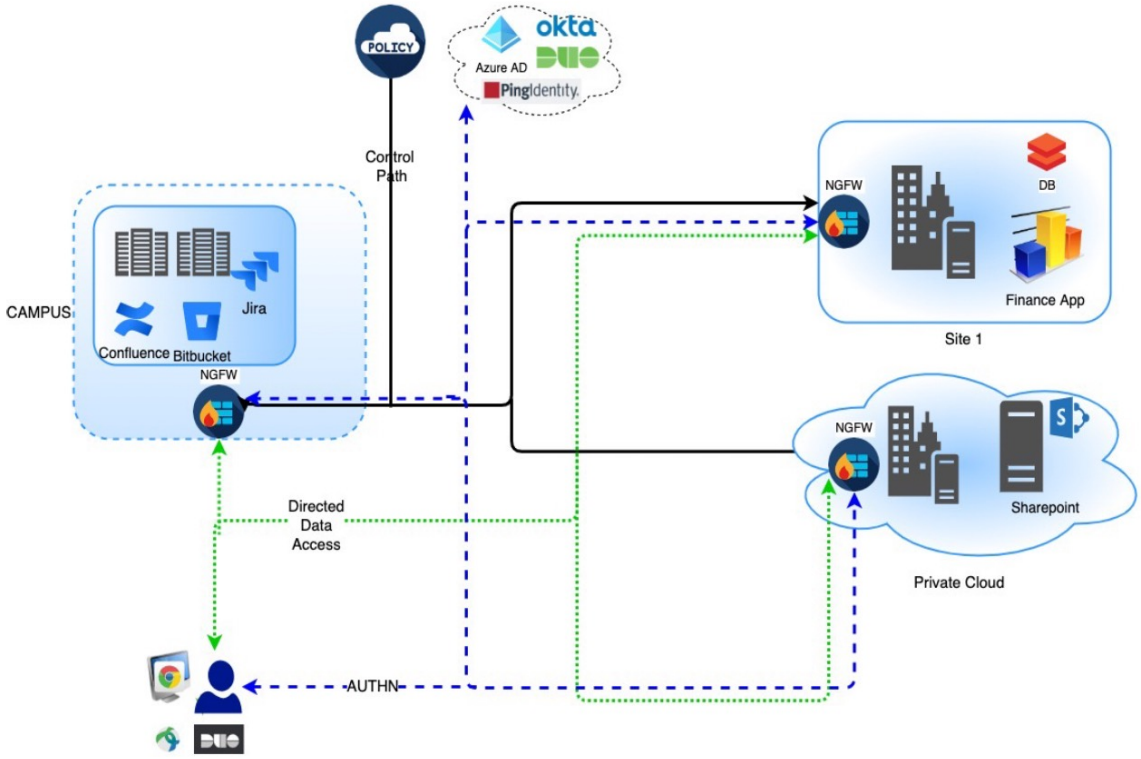
功能如下：

- 支持多个基于 SAML 的身份提供商，如 Duo、Azure Active Directory (Azure AD)、Okta 和其他身份提供商。
- 终端（客户端设备）上不需要思科 Cisco Secure 客户端 等客户端应用来进行安全访问。
- 通过浏览器进行访问和身份验证。
- 仅支持 TLS Web 应用。
- 通过代理（例如 Duo Health）支持客户端设备状态，使用该代理可以根据 Duo 中的策略评估设备的状态，并且可以基于相同的策略提供访问。可以与支持使用其代理（例如 Okta 或 PingID）进行安全评估的第三方身份提供程序一起执行相同的功能。
- 支持 HTTP 重定向 SAML 绑定。
- 支持应用组，便于在一组应用上启用 无客户端 Cisco Zero Trust 访问保护。
- 对 Zero Trust 应用流量利用威胁防御入侵和恶意软件防护。

您可以使用 Cisco Secure Firewall Management Center Web 界面创建 Zero Trust 应用策略，以便定义专用应用并向其分配威胁策略。该策略是应用特定的，其中管理员根据该应用的威胁感知来决定检测级别。

威胁防御如何与 Zero Trust 访问配合使用

图 *446:* 威胁防御部署



1. 远程或本地用户使用浏览器发送 HTTPS 请求，以从终端连接到应用。
2. HTTPS 请求被保护应用的防火墙拦截。
3. 防火墙将用户重定向到应用的已配置 IdP 进行身份验证。

注释 在图中，每个防火墙保护一组 Web 应用。用户可以在认证和授权后直接访问防火墙后面的应用。

4. 身份验证和授权过程完成后，防火墙允许用户访问应用。

为何使用 Zero Trust 网络访问？

Zero Trust 网络访问 (ZTNA) 通过要求每次连接都进行显式授权，提供安全、分段的访问。此方法减少了攻击面，并简化了安全迁移，无需增加设备。

ZTNA 利用您现有的威胁防御部署作为应用程序访问的实施点，实现分段和按应用程序授权。它为远程和本地用户建立独立的隧道。

此功能对用户隐藏网络，并确保他们只能访问已明确授权的应用程序。对网络中的一个应用进行授权不会为网络上的其他应用提供隐式授权，从而显着减少受攻击面。换句话说，对应用程序或资源的每次访问都必须经过明确授权。

通过在威胁防御中添加 Zero Trust 访问功能，您可以采纳更安全访问模型，而无需在网络中安装或管理额外设备。

无客户端 Cisco Zero Trust 访问 配置的组件

新的配置包括 Zero Trust 应用策略、应用组和应用。

- **Zero Trust 应用策略**-包括 Zero Trust 应用策略、应用组和应用。安全区域和安全控制设置在全局级别与所有未分组的应用和应用组关联。

  默认情况下，为策略分配全局端口池。从这个池中自动为配置的每个专用应用分配一个唯一的端口。

  Zero Trust 应用策略包括应用组、分组或未分组的应用。

- **应用组**- 由一组共享 SAML 身份验证设置的应用组成，可以选择性地共享安全区域和安全控制设置。

  应用组从全局策略继承安全区域和安全控制设置，并且可以覆盖这些值。

  创建应用组后，可以使用相同的 SAML IdP 配置对多个应用进行身份验证。属于应用组的应用继承应用组的 SAML 配置。这样就无需为每个应用配置 SAML 设置。创建应用组后，可以向其中添加新应用，而无需为其配置 IdP。

  当最终用户尝试访问属于组的应用时，用户将首次通过应用组的身份验证。当用户尝试访问属于同一应用组的其他应用时，系统会为用户提供访问权限，而不会再次重定向到 IdP 进行身份验证。这可以防止应用访问请求使 IdP 过载，并在启用限制的情况下优化 IdP 的使用。

- **应用**- 有两种类型：
  - **未分组的应用**- 是独立的应用。必须为每个应用配置 SAML 设置。应用从全局策略继承安全区域和安全控制设置，并且可以由应用覆盖。
  - **分组应用**- 是指在应用组下分组的多个应用。SAML 设置继承自应用组，无法被覆盖。但是，可以为每个应用覆盖安全区域和安全控制设置。

配置需要以下证书：

- **身份证书**- Firewall Threat Defense 使用此证书伪装成应用。Firewall Threat Defense 充当 SAML 服务提供商 (SP)。此证书必须是与专用应用的 FQDN 匹配的通配符或使用者备用名称 (SAN) 证书。它是受 Firewall Threat Defense保护的所有应用的通用证书。
- **IdP 证书**- IdP 为每个定义的应用或应用组提供一个证书。必须配置此证书，以便 Firewall Threat Defense 可以验证 IDP 对传入 SAML 断言的签名。

注释 IdP 证书通常包含在元数据文件中；否则，用户需要在应用配置期间随时可用 IdP 证书。

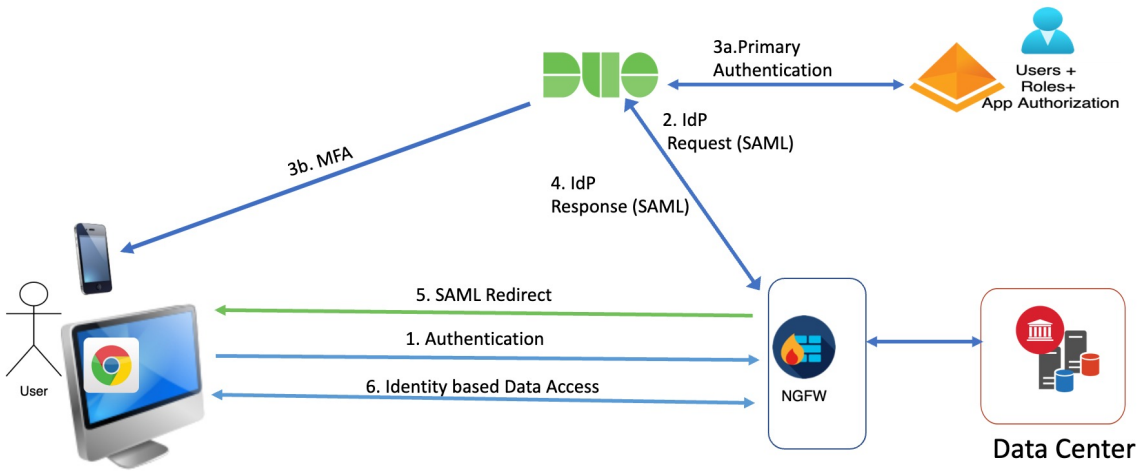
- **应用证书**- Firewall Threat Defense 使用此证书解密从用户到应用的加密流量，以进行检查。

注释 即使我们不执行 IPS/恶意软件检查，也需要此证书来验证信头中的 Cookie 以授权连接。

无客户端 Cisco Zero Trust 访问 工作流程

此图描绘了 Zero Trust 访问工作流程。

图 *447:* 无客户端 ***Zero Trust*** 网络访问工作流程



工作流程如下：

1. 用户在浏览器中键入应用 URL。
   - 如果 HTTPS 请求有效，则用户将被重定向到映射端口（步骤 6）。
   - 如果 HTTPS 请求无效，则发送用户进行身份验证（第 2 步）。
2. 用户被重定向到已配置的身份提供程序 (IdP)。
3. 1. 用户将被重定向到已配置的主身份验证源。
   2. 用户将使用已配置的辅助多因素身份验证（如果有）进行质询。
4. IdP 向威胁防御发送 SAML 响应。通过浏览器从 SAML 响应中检索用户 ID 和其他必要参数。

5. 用户被重定向到应用。
6. 验证成功后，允许用户访问应用。

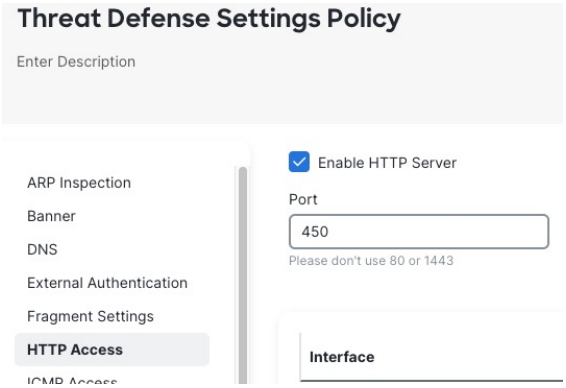
无客户端 Cisco Zero Trust 访问 的限制

- 仅支持启用了 TLS 的 Web 应用。所有流量都必须解密。
- 仅支持 SAML 身份提供程序。
- 支持 IPv6；但是，您只能使用同构网络地址转换 (NAT) 场景，例如 NAT66 和 NAT44。

  不支持 NAT64 和 NAT46 场景。
- 仅在启用了 Snort 3 时，才能对 Firewall Threat Defense 进行无客户端 Zero Trust 访问。
- 默认情况下，Firewall Threat Defense 设备会使用端口 443 进行安全通信。由于这与可能被配置为 Zero Trust 网络访问的启用 TLS 的应用使用的端口相同，因此，您必须更改设备的 HTTP 服务器端口。

  转至 **设备** > **平台设置**，然后编辑设备的威胁防御设置策略，点击 **HTTP 访问**，选中**启用 HTTP 服务器**复选框，并在该字段中输入 443 以外的端口。完成后，点击页面右上角的**保存**。

  下图显示了一个示例。



- 受保护的 Web 应用中的所有超链接都必须具有相对路径，并且在单个模式集群上不受支持。
- 在虚拟主机上或在内部负载均衡器后面运行的受保护 Web 应用必须使用相同的外部和内部 URL。
- 在启用了严格 HTTP 主机报头验证的应用上不受支持。
- 如果应用服务器托管多个应用并根据 TLS 客户端 Hello 中的服务器名称指示 (SNI) 报头提供内容，则 Zero Trust 应用配置的外部 URL 必须与该特定应用的 SNI 匹配。

Zero Trust 应用策略的前提条件

前提条件类型	说明
许可	• 具有出口管制功能的智能许可证账户 • （可选）IPS 和威胁许可证 - 如果使用安全控制，则为必填项。
配置	创建与专用应用的 FQDN 匹配的通配符或使用者备用名称 (SAN) 证书。有关详细信息，请参阅添加证书注册对象，第 2671 页。
	通过监管对专用应用的访问来创建安全区域。有关详细信息，请参阅创建安全区域和接口组对象，第 715 页。

管理 Zero Trust 应用策略

您可以创建、编辑和删除 Zero Trust 应用策略。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 管理 Zero Trust 访问策略：

- 创建 - 点击 **新建策略**。请参阅创建 Zero Trust 应用策略，第 1673 页
- 编辑 - 点击 **编辑** ()。请参阅编辑 Zero Trust 应用策略，第 1679 页
- 报告 - 点击 **报告** ()。
- 删除 - 点击 **删除** ()。

步骤 3 点击**保存**。

下一步做什么

在将配置部署到威胁防御之前，请确保没有警告。要部署配置更改，请参阅 Cisco Secure Firewall Management Center 管理指南中的部署配置更改。

创建 Zero Trust 应用策略

此任务配置 Zero Trust 应用策略。

开始之前

确保满足Zero Trust 应用策略的前提条件，第 1673 页中列出的所有前提条件。

过程

步骤 1 选择**策略** > **安全策略** > **Zero Trust 应用**。

步骤 2 点击**添加策略 (Add Policy)**。

步骤 3 在 **常规** 部分中，在 **名称** 字段中输入策略名称。说明字段是可选的。

步骤 4 在 **域名** 字段中输入域名。

确保域名已添加到 DNS。域名解析为访问应用的Firewall Threat Defense网关接口。域名用于为应用组中的所有专用应用生成 ACS URL。

如果在下一步中选择 ACME 证书作为策略的身份证书，则域名必须与 ACME 证书的公用名 (CN) 匹配。

注释
更改域名后，SAML 服务提供商 (SP) 元数据将随之更新。必须重新配置以下设置：

- 使用新 SAML SP 元数据的 IdP
- 使用新域名的 DNS 服务器

如果在更改域名后进行部署，系统将移除并重新添加所有应用，这会导致应用访问中断。

步骤 5 从 **身份证书** 下拉列表中选择现有证书。

点击 **添加** (+) 图标以配置证书注册对象。有关详细信息，请参阅 添加证书注册对象，第 2671 页。

可以选择 ACME 证书，将 Firewall Threat Defense 设备作为 SAML SP 进行身份验证，以用于 Zero Trust 应用策略。ACME 证书可自动执行 SSL 和 TLS 证书的生命周期管理，包括自动续约。

步骤 6 从 **安全区域** 下拉列表中选择安全区域。

点击 **添加** (+) 图标以添加新的安全区域。

要添加安全区域，请参阅 创建安全区域和接口组对象，第 715 页。

步骤 7 在 **全局端口池** 部分，显示默认端口范围。如果需要，请修改。端口值范围为 1024 到 65535。此池中的唯一端口分配给每个专用应用。

注释
此端口范围应避免与现有 NAT 范围发生任何冲突。

步骤 8 （可选）在 **安全控制** 部分，您可以添加入侵或恶意软件和文件策略：

- **入侵策略**- 从下拉列表中选择默认策略，或点击 **添加** (+) 图标以创建新的自定义入侵策略。有关详细信息，请参阅最新版本的 Cisco Secure Firewall Management Center Snort 3 配置指南中的创建自定义 Snort 3 入侵策略主题。

- **变量集**- 从下拉列表中选择默认变量集，或点击 **添加** (+) 图标以创建新的变量集。有关详细信息，请参阅 创建变量集，第 2716 页。

  注释
  要使用变量集，必须拥有托管设备的 Cisco Secure Firewall Threat Defense IPS 许可证。

- **恶意软件和文件策略**- 从下拉列表中选择现有策略。点击 **添加** (+) 图标来创建新的恶意软件和文件策略。有关详细信息，请参阅管理文件策略，第 2306 页。

步骤 9 点击**保存**保存策略。

下一步做什么

1. 创建应用组。请参阅创建应用组，第 1675 页。
2. 创建应用。请参阅创建应用，第 1676 页。
3. 将 Zero Trust 应用策略与设备关联。请参阅 为目标设备设置 Zero Trust 访问策略，第 1678 页
4. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

创建应用组

开始之前

创建 Zero Trust 应用策略，第 1673 页

过程

步骤 1 点击 **添加应用组**。

步骤 2 在 **应用组** 部分，在 **名称** 字段中键入名称，然后点击 **下一步**。

步骤 3 在 **SAML 服务提供商 (SP) 元数据** 部分，数据是动态生成的。复制 **实体 ID** 和 **断言使用者服务 (ACS) URL** 字段的值，或点击 **下载 SP 元** 数据以 XML 格式下载此数据，以便将其添加到 IdP。点击**下一步 (Next)**。

步骤 4 在 **SAML 身份提供程序 (IdP) 元数据** 部分，使用以下任一方法添加元数据：

- **XML 文件上传**- 选择文件或拖放 XML 文件。

  系统将显示 **实体 ID**、 **单点登录 URL**和 **IdP 证书** 的详细信息。

- **手动配置**- 执行以下步骤：
  - **实体 ID** - 输入在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。
  - **单点登录 URL** - 输入用于登录到 SAML 身份提供程序服务器的 URL。

- **IdP 证书** - 选择注册到威胁防御以验证由 IdP 签名的消息的 IdP 的证书。

  点击 **添加** (+) 图标来配置新的认证登记对象。有关详细信息，请参阅添加证书注册，第 2673 页。

- **稍后配置**- 如果没有 IdP 元数据，可以稍后配置。

点击**下一步 (Next)**。

步骤 5 在 **重新身份验证间隔** 部分中，在 **超时间隔** 字段中输入值，然后点击 **下一步**。

重新身份验证间隔允许您提供一个值，以确定用户何时必须再次进行身份验证。

步骤 6 在 **安全区域和安全控制** 部分，从父策略继承安全区域和威胁设置。您可以覆盖这些设置。点击**下一步 (Next)**。

步骤 7 检查配置摘要。在任何区域，点击 **编辑** 以修改详细信息。点击 **Finish**。

步骤 8 点击**保存**。

应用组已创建，并显示在“Zero Trust 应用”页面上。

下一步做什么

1. 创建应用，第 1676 页。
2. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

创建应用

使用此任务可创建已分组或未分组的应用。

开始之前

1. 创建 Zero Trust 应用策略，第 1673 页。
2. 创建应用组，第 1675 页（仅分组应用需要）。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 选择策略。

步骤 3 点击**添加应用 (Add Application)**。

步骤 4 在 **应用设置** 部分中，填写以下字段：

- **应用名称**-输入应用名称。

- **外部 URL**- 输入用户用于访问应用的 URL。
- **应用 URL**-默认情况下，外部 URL 用作应用 URL。取消选中 **使用外部 URL 作为应用 URL** 复选框来指定不同 URL。

  如果威胁防御使用内部 DNS，则应用程序 URL 必须与该 DNS 中的条目匹配，以确保它解析到应用程序。此外，如果输入的完全限定域名 (FQDN) 既可以是 IPv4，也可以是 IPv6 地址，则 FQDN 必须同时解析为 IPv4 和 IPv6。威胁防御不在这些类型的地址之间进行转换。
- **应用证书**- 选择专用应用的证书。点击 **添加** (+) 图标可配置内部证书对象。有关详细信息，请参阅 添加内部证书对象，第 2669 页。
- **源网络地址转换** — 源网络地址转换 (source NAT) 将数据包中的源 IP 地址转换为指定范围内的地址。

  启用**源网络地址转换**以指定 IP 地址范围。传入请求的源 IP 地址将转换为指定范围内的 IP 地址。源 NAT 同时适用于 IPv4 和 IPv6 地址。

  - **IPv4** — 从列表中选择 NAT 的源网络。点击 **添加** (+) 以创建网络对象。有关详细信息，请参阅 网络，第 2658 页。
  - **IPv6** — 从列表中选择 NAT 的源网络。点击 **添加** (+) 以创建网络对象。有关详细信息，请参阅 网络，第 2658 页。

  源 NAT 将传入请求的源 IP 地址转换为网络对象或对象组中指定的可路由 IP 地址。

  注释
  仅支持类型为“主机”或“范围”的对象或对象组。
- **应用组** - 从下拉列表中选择应用组。请参阅创建应用组，第 1675 页。

  注释
  此字段不适用于未分组的应用。

步骤 5 点击**下一步 (Next)**。

步骤 6 根据应用类型：

- 对于分组应用， **SAML 服务提供程序 (SP) 元数据**、 **SAML 身份提供程序 (IdP) 元数据** 和 **重新身份验证间隔** 继承自应用组，不需要由用户配置。
- 对于未分组的应用，请执行以下步骤：

  1. 在 **SAML 服务提供商 (SP) 元数据** 部分，数据是动态生成的。复制 IdP 的**实体 ID**、**断言使用者服务 (ACS) URL**，或点击**下载 SP 元数据**以 XML 格式下载此数据，以便将其添加到 IdP。点击**下一步 (Next)**。
  2. 在 **SAML 身份提供程序 (IdP) 元数据** 部分，使用以下任一方法添加元数据：
     - **XML 文件上传**- 选择文件或拖放 XML 文件。

       系统将显示 **实体 ID**、 **单点登录 URL**和 **IdP 证书** 的详细信息。
     - **手动配置**- 执行以下步骤：

- **实体 ID** - 输入在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。
- **单点登录 URL** - 输入用于登录到 SAML 身份提供程序服务器的 URL。
- **IdP 证书** - 选择注册到威胁防御以验证由 IdP 签名的消息的 IdP 的证书。

  点击 **添加** (+) 图标来配置新的认证登记对象。有关详细信息，请参阅添加证书注册，第 2673 页。

- **稍后配置** — 如果您没有 IdP 元数据，可以稍后配置。

点击**下一步 (Next)**。

3. 在 **重新身份验证间隔** 部分中，在 **超时间隔** 字段中输入值，然后点击 **下一步**。重新身份验证间隔允许您提供一个值，以确定用户何时必须再次进行身份验证。

步骤 7 在**安全区域和安全控制**部分，从策略或应用组继承安全区域和威胁设置。您可以覆盖这些设置。点击**下一步 (Next)**。

步骤 8 检查配置摘要。在任何区域，点击 **编辑** 以修改详细信息。点击 **Finish**。

步骤 9 点击**保存**。

该应用程序列在 Zero Trust 应用程序页面上，并默认启用。

下一步做什么

1. 为目标设备设置 Zero Trust 访问策略，第 1678 页。
2. 部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

为目标设备设置 Zero Trust 访问策略

每项 Zero Trust 策略可以多台设备为目标；每天设备每次只能部署一项策略。

开始之前

1. 创建 Zero Trust 应用策略，第 1673 页。
2. 创建应用组，第 1675 页。
3. 创建应用，第 1676 页。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 选择策略。

步骤 3 点击 **目标设备**。

步骤 4 使用以下任何方法之一，选择要部署策略的设备：

- 从 **可用设备** 列表中选择一个设备，然后点击 >> 或 **添加** () 图标。
- 要从 **所选设备** 列表中删除设备，请选择一个设备，然后点击 << 或 **删除** () 图标。

步骤 5 点击 **应用** 以保存策略分配。

步骤 6 点击**保存**保存策略。

下一步做什么

部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

编辑 Zero Trust 应用策略

您可以编辑 Zero Trust 应用策略、应用组或应用的设置。

过程

步骤 1 选择 **策略** > **安全策略** > **Zero Trust 应用**

步骤 2 点击要编辑的 Zero Trust 应用策略旁边的 **编辑** () 。

步骤 3 编辑 Zero Trust 应用策略。

您可以更改以下设置或执行以下操作：

- 名称和说明 - 点击策略名称旁边的 **编辑** ()，进行更改，然后点击 **应用**。
- 要修改策略设置，请执行以下操作：
  - 点击**设置**
  - 根据需要修改设置。

    重要事项
    编辑 SAML ACS URL 的域名会中断应用访问。

  - 点击**保存**。
- 要修改应用组设置，请执行以下操作：
  - 点击 **应用**。
  - 点击要编辑的应用组旁边的 **编辑** () 。

- 在每个部分中，根据需要点击 **编辑** 以修改设置

  重要事项
  编辑应用组名称会中断应用访问。

- 修改部分中的设置后，点击 **应用** 。
- 点击 **完成**。
- 点击**保存**。

- 要修改应用设置，请执行以下操作：
  - 点击 **应用**。
  - 点击要编辑的应用旁边的 **编辑** ( ) 。
  - 在每个部分中，点击 **编辑** 以根据需要修改设置。

    重要事项
    编辑应用名称会中断应用访问。

  - 修改部分中的设置后，点击 **应用** 。
  - 点击 **完成**。
  - 点击**保存**。

- 要启用、禁用或删除多个应用，请选择应用，点击所需的批量操作，然后点击 **保存**。

  注释
  这些操作也可通过右键点击菜单来执行。

  - 要启用所有应用，请点击 **批量操作** > **启用**。
  - 要禁用所有应用，请点击 **批量操作** > **禁用**。
  - 要删除所有应用，请点击 **批量操作** > **删除**。

- 点击 **返回 Zero Trust 应用 (Return to Zero Trust Application)** 以返回到策略页面。

下一步做什么

部署配置更改。请参阅 Cisco Secure Firewall Management Center 管理指南 中的部署配置更改。

监控 Zero Trust 会话

连接事件

部署 Zero Trust 应用策略后，新字段可用。要将字段添加到表视图：

1. 选择**事件和日志** > **+ 显示更多** > **连接** > **事件**。
2. 点击**连接事件的表视图 (Table View of Connection Events)** 选项卡。
3. 事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 **x** 图标以显示字段选择器。
4. 选择以下字段：
   - **身份验证源**
   - **Zero Trust 应用**
   - **Zero Trust 应用组**
   - **Zero Trust 应用主机**
   - **Zero Trust 应用策略**
   - **Zero Trust 源用户**
   - **Zero Trust 代理**
   - **Zero Trust 规则**
   - **Zero Trust 状态**
   - **Zero Trust 隧道 ID**
5. 点击**应用 (Apply)**。

有关连接事件的详细信息，请参阅 Cisco Secure Firewall Management Center 管理指南 中的连接和安全相关的连接事件 。

Zero Trust 控制面板

通过 Zero Trust 控制面板，您可以监控设备上活动 Zero Trust 会话的实时数据。

Zero Trust 控制面板提供由管理中心管理的排名靠前的 Zero Trust 应用和 Zero Trust 用户的摘要。选择 **洞察和报告** > **控制面板**，然后点击 **Zero Trust** 选项卡以访问控制面板。

控制面板具有以下构件：

- 热门 Zero Trust 应用
- 热门 Zero Trust 用户

CLI 命令

请登录设备 CLI 并使用以下命令：

CLI 命令	说明
show running-config zero-trust	查看 Zero Trust 配置的运行配置。
show running-config zero-trust-hybrid	查看通用 Zero Trust 配置的运行配置。
show zero-trust	显示运行时 Zero Trust 统计信息和会话信息。
show cluster zero-trust	显示集群中各节点的 Zero Trust 统计信息摘要。
clear zero-trust	清除 Zero Trust 会话和统计信息。
show counters protocol zero_trust	查看 Zero Trust 流命中的计数器。

诊断工具

诊断工具通过检测 Zero Trust 配置可能存在的问题来促进故障排除过程。诊断可以分为两种类型：

- **特定于应用的诊断**用于检测以下问题：
  - DNS 相关问题
  - 错误配置（例如套接字未打开）以及分类和 NAT 规则问题。
  - Zero Trust 策略或 SSL 规则的部署问题
  - 源 NAT 问题和 PAT 池耗尽问题
- **常规诊断** 用于检测以下问题：
  - 未启用强密码许可证
  - 无效应用证书
  - SAML 相关问题
  - 本地代理和集群批量同步问题

要运行诊断工具，请执行以下操作：

1. 点击要进行故障排除的 Zero Trust 应用旁边的诊断 ( )。系统将显示 **诊断** 对话框。
2. 从 **选择设备** 下拉列表中选择设备并点击 **运行**。诊断过程完成后，系统会在“报告”选项卡中生成 **报告** 。
3. 要查看、复制或下载日志，请点击 **日志** 选项卡。

通用零信任网络访问

通用零信任网络访问 (通用 ZTNA) 使管理员能够根据用户身份（包括用户信任和终端安全评估）专门允许访问内部网络资源，而无需像远程访问 VPN 那样授予对整个网络的访问权限。通用 ZTNA 是基于客户端的 ZTNA 解决方案，无论用户位于何处（远程或 本地部署），都能让用户安全访问内部资源和应用。

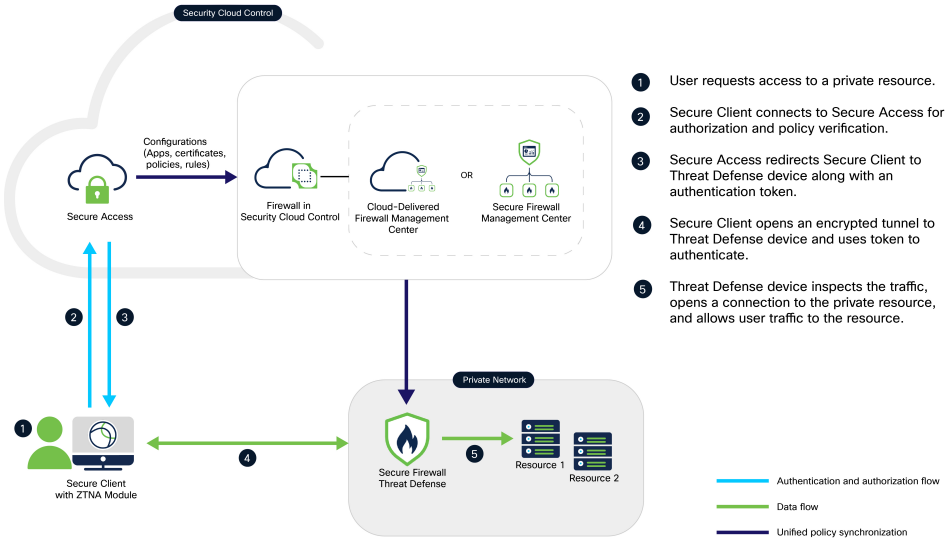
由于 通用 ZTNA 不假定授予一个应用的访问权限会隐式授权访问其他应用，因此网络攻击面得以减少。

通过强身份验证、终端安全评估验证和全面的流量检测，通用 ZTNA 确保实现最小权限、按应用、按用户的访问。它能有效保护混合环境中的应用。

通用 ZTNA 的组件

通用 ZTNA 的新配置包括安全云控制防火墙管理（以前称为 Cisco Defense Orchestrator）和“安全访问”，两者均在安全云控制平台上配置。安全云控制防火墙管理通过 Cisco Secure Firewall Management Center 来管理防火墙威胁防御设备。

图 *448:* 通用 *ZTNA* 的组件



- **安全云控制防火墙管理**：管理 Firewall Threat Defense 设备的 通用 ZTNA 策略配置和部署。威胁防御设备通过实施 通用 ZTNA 策略来保护 本地部署 资源。威胁防御会检测流量，并对流量实施入侵防御系统 (IPS)、文件和恶意软件策略。
- **安全访问**：安全访问定义用户的访问策略、终端安全评估和安全配置文件。它通过云对用户流量实施策略。
- **安全云控制平台**：安全云控制为安全访问和防火墙提供统一的安全管理平面，简化了跨两者的通用 ZTNA 策略管理。

- **安全客户端**：安全客户端安装在最终用户的设备上。它作为实施点拦截对受保护内部资源的连接请求，从而实现基于身份的安全访问。

以下部分介绍如何在威胁防御设备上启用通用 ZTNA。有关 通用 ZTNA 的完整配置，请参阅《通用 *Zero Trust* 网络访问配置指南》。

威胁防御如何与 通用 ZTNA 配合使用

启用 通用 ZTNA 的防火墙威胁防御设备是关键的实施点，通过将 Zero Trust 原则与防火墙功能相结合来保护私有资源。它通过以下方式保护私有资源：

- **实施访问并验证策略**：威胁防御设备拦截所有对私有资源的访问请求。它实施精细的、基于上下文的访问策略，在授予访问权限前验证用户身份、设备状态和上下文因素。仅允许满足最小权限标准的请求，阻止未经授权的资源访问尝试。
- **建立到资源的安全隧道**：验证访问策略后，威胁防御设备在用户设备和私有资源之间建立安全的加密隧道。此隧道确保私有资源不会直接暴露在网络中。
- **检测流量**：威胁防御设备持续检测流量，在威胁到达资源前将其阻止。设备应用入侵防御系统、文件和恶意软件检测功能来检测和阻止威胁。
- **微分段并防止横向移动**：设备通过将流量流限制为仅授权资源来实施微分段。这种隔离可防止网络内的横向移动，从而限制任何潜在漏洞的影响。

通用零信任网络访问 的前提条件

本主题讨论 通用零信任网络访问 (通用 ZTNA) 的要求和准则。

许可要求

- Cisco Secure Firewall Management Center 需要具有受控出口功能的智能许可证账户。它在 通用 ZTNA 的评估模式下无法运行。

  如果配置了入侵策略，Cisco Secure Firewall Threat Defense 设备需要 IPS 许可证。如果配置了恶意软件策略，设备需要 IPS 和恶意软件防御许可证。有关详细信息，请参阅《*Cisco Secure Firewall Management Center* 管理指南》中的“许可证”部分。

- 安全访问需要 Cisco Secure 专用访问 Essentials 或 Advantage 订用。

设备要求

- 所有 Secure Firewall Management Center 和 Cisco Secure Firewall Threat Defense 设备必须运行 7.7.10 及更高版本。
- 所有 Cisco Secure Firewall Threat Defense 设备必须配置为路由模式；不支持透明模式。

- 在安全云控制中为设备配置通用Zero Trust访问时，确保设备身份证书的注册类型是使用PKCS12文件格式创建的对象。不支持其他证书类型。如有必要，也可以从安全云控制创建新的证书对象，该对象支持 PKCS12 格式。请参阅配置安全设备。
- 配置域名系统 (DNS) 以解析私有资源的完全限定域名 (FQDN)。使用 Cisco Secure Firewall 上的平台设置 (Platform Settings) 菜单配置 DNS。请参阅接口和设备设置。
- 支持高可用性 (HA) 设备；它们显示为一个实体。
- 支持安全客户端（已启用 ZTNA 模块）5.1.10 及更高版本。

  客户端必须在支持可信平台模块 (TPM) 的平台（如 Windows 11）上运行。

证书类型准则

- **用户身份证书**：启用了 Zero Trust 访问的 Secure Client 在与 Secure Access 和 Firewall Threat Defense 进行双向传输层安全 (mTLS) 会话时出示用户身份证书，以请求访问私有资源。
- **防火墙威胁防御设备证书**：已启用通用 ZTNA 的 威胁防御设备使用设备证书与安全客户端和安全访问建立安全的 mTLS 连接。确保设备身份证书为 PKCS12 类型。

  如果已为设备注册手动证书，请先在防火墙管理中心上使用 **Devices** > **Certificates** > **Export Certificate** 菜单将其导出为 PKCS12 格式。使用导出的 PKCS12 文件创建新的 PKCS12 证书注册对象。
- **解密证书**：（可选）要解密发送到私有资源的流量，请在安全访问中为资源启用**解密**，并提供服务器证书和密钥。我们建议您使用由公开认可的证书颁发机构 (CA) 签名的证书。

支持的设备

本地防火墙管理中心和云交付型防火墙管理中心均可配置为管理设备。

仅支持具有 16 个或更多内核的设备。此类 Cisco Secure Firewall Threat Defense 型号包括：

- 1150
- 3105、3110、3120、3130、3140
- 4115、4125、4145、4112
- 4215、4225、4245
- FTDv

注释 您可以在 16 核 FTDv 上配置 通用 ZTNA。FTDv 的其他部署配置均不支持通用 ZTNA。

通用零信任网络访问 的限制

- 通用 ZTNA 不支持 IPv6。
- 启用 通用 ZTNA 的设备不会对通过站点间隧道的流量实施策略。
- 通用 ZTNA 不支持集群设备。
- 通用 ZTNA 不支持多实例模式下的设备。
- 通用 ZTNA 会话不支持巨型帧。
- 通用 ZTNA 仅支持全局 VRF。
- 通用 ZTNA 不支持 FTP 或 TFP 等由服务器发起数据连接或次要连接的协议。

  例如，主动模式 FTP 连接使用持久控制连接传输命令，并创建临时数据连接传输文件。通用 ZTNA 不支持此类由服务器发起的数据连接。

将防火墙管理中心与安全云控制集成

注释 此任务仅适用于本地防火墙管理中心。

将本地部署的 Secure Firewall Management Center 与 Security Cloud Control 集成使您能够配置您的 Secure Firewall Management Center 及其关联的 Cisco Secure Firewall Threat Defense 设备。这些设备随后可使用配置和管理 通用 ZTNA 所需的网络、专用资源和策略。

注释 通用 ZTNA 仅使用 安全接入 定义的访问策略。从 Secure Firewall Management Center 部署到威胁防御设备的任何其他访问控制策略和规则，在 通用 ZTNA 中都会被忽略。

开始之前

您的思科联系人必须将您的 Security Cloud Control 和 安全接入 系统纳入管理，并创建用户和租户。

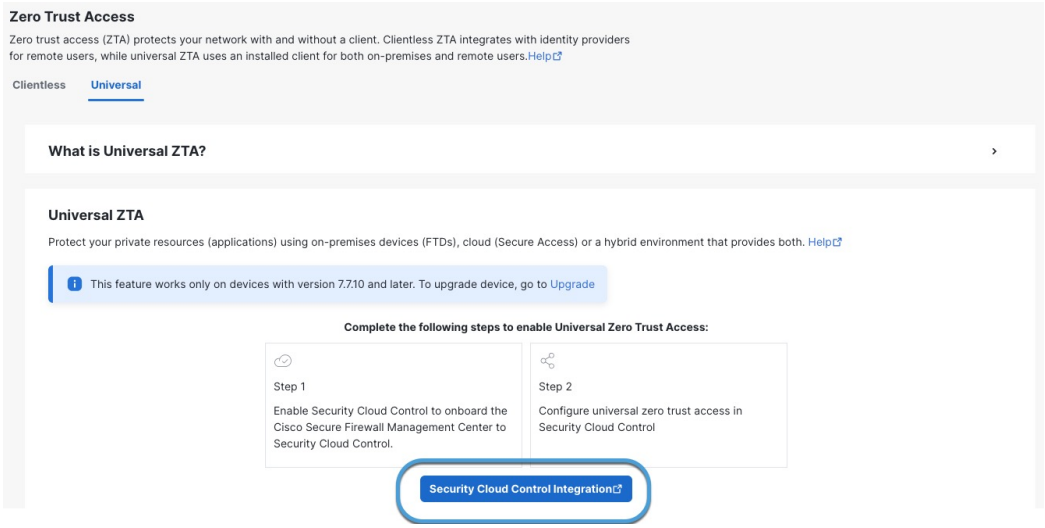
过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **Zero Trust 应用**。

步骤 3 点击**通用**选项卡。

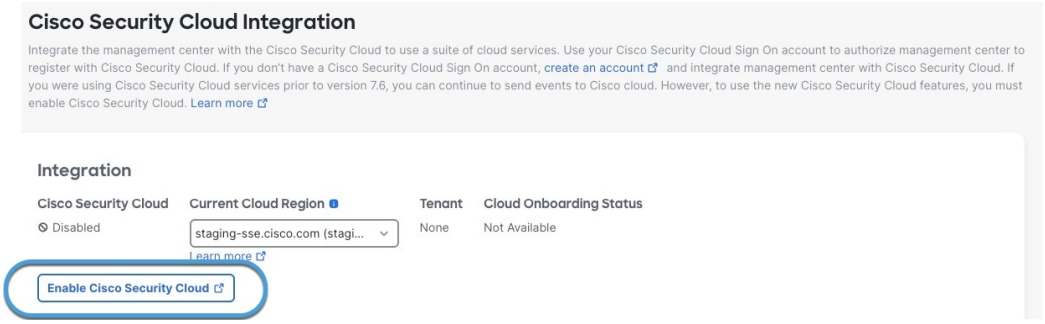
系统将显示“Zero Trust 访问”页面。



步骤 4 点击**安全云控制集成**。

步骤 5 在**当前云区域**列表中，点击您的 Security Cloud Control 区域的名称。

步骤 6 点击 **启用思科安全云**。

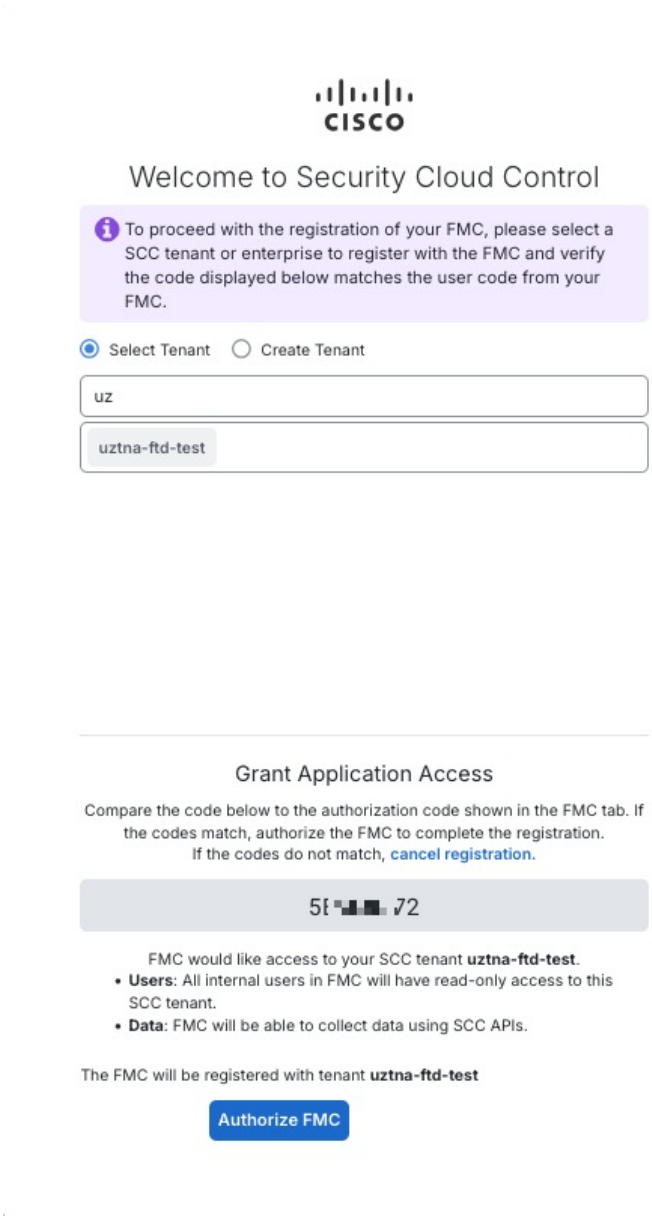


步骤 7 出现提示时，点击**继续使用思科 SSO**。

步骤 8 登录 Security Cloud Control。

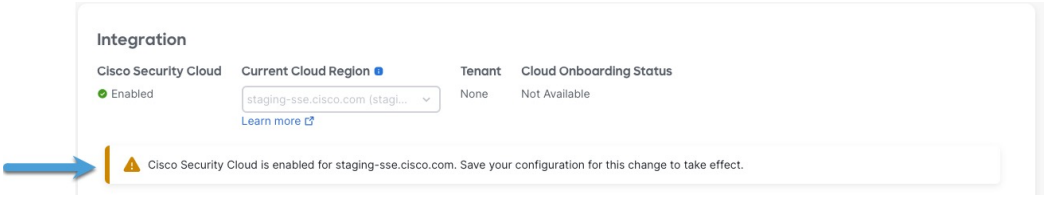
步骤 9 在**选择租户**列表中，点击租户名称。

步骤 10 在随后显示的页面上，点击**授权 FMC**。



步骤 11 出现提示时，关闭选项卡页面。

步骤 12 系统将显示一条确认消息，表明载入操作已成功。



步骤 13 点击页面底部的**保存**。

保存配置可能需要几分钟时间。配置保存后，页面会显示载入状态和租户名称。



步骤 14 有关此页面上其他选项的详细信息，请参阅安全云控制设置，第 1689 页。

安全云控制设置

以下主题讨论“Cisco Security Cloud 集成”页面上的设置，可通过在 Secure Firewall Management Center 上选择 **集成** > **安全云控制** 来访问该页面。

事件配置

在Security Cloud Control中监控选定的事件：

- **向云发送事件**：选中此复选框以在 Security Cloud Control 中监控事件；清除此复选框以不监控任何事件。

  您可以在 Security Cloud Control 中通过**防火墙** > **事件和日志**查看事件。
- **入侵事件**：如果您使用 IPS 策略，请选中此复选框以监控这些策略。
- **文件和恶意软件事件**：如果您使用文件或恶意软件策略，请选中此复选框以监控这些策略。
- **连接事件**：选中要监控的事件旁的复选框，**安全**（用于文件和 IPS 事件）或**全部**。

有关事件的详细信息，请参阅安全云控制中的事件类型。

思科安全云支持（可选）

（可选）选中复选框以启用以下功能：

- **启用 Cisco Success Network**：选中此复选框以启用《*Cisco Success Network* 从 *Cisco Secure Firewall Management Center*收集的遥测数据，版本 *7.7*》中讨论的统计信息收集。
- **启用思科支持诊断**：选中此复选框以启用*Cisco Secure Firewall Management Center* 管理指南中讨论的统计信息收集。

思科安全 AI 助手

选中复选框以启用《有效使用 Cisco AI Assistant for Security 管理您的威胁防御设备》中讨论的 AI 助手。

思科 XDR 自动化

选中复选框以启用思科 XDR 帮助中心中讨论的 XDR 工作流程自动化。

策略分析器和优化器

选中复选框以启用策略分析器；点击**了解更多**获取详情。

零接触调配 (ZTP)

选中复选框以启用*Cisco Secure Firewall Management Center* 管理指南中讨论的零接触配置。

配置安全设备

与您载入 Security Cloud Control 的 Secure Firewall Management Center 相关联的所有防火墙威胁防御设备都是安全设备，您可以：

- 将私有资源（即您希望通过基于身份的访问控制、IPS、恶意软件和其他保护措施进行保护的内部应用）与这些设备相关联。
- 部署 安全接入 访问规则。安全设备负责为 本地部署 用户、远程用户或两者实施访问规则。

执行以下步骤，在 威胁防御设备上启用**通用 Zero Trust 网络访问设置**。这些步骤包括配置设备 FQDN、内部接口、外部接口和 PKCS12 证书，以在设备上启用通用 ZTNA。

开始之前

完成将防火墙管理中心与安全云控制集成，第 1686 页中讨论的所有任务。

您必须知道每个设备的内部和外部网络接口名称：

- 内部接口（也称为 *DMZ* 接口）用于对本地用户应用访问规则。
- 外部接口用于对远程用户应用访问规则。

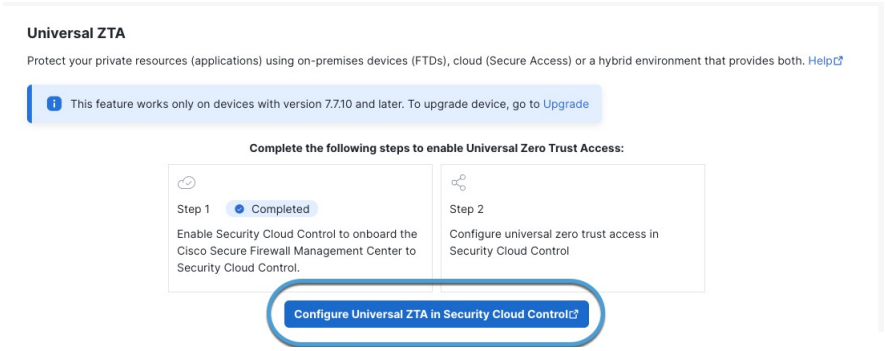
您可以为每个安全设备选择内部接口、外部接口或两种类型的接口。

过程

步骤 1 在 Secure Firewall Management Center 中，点击 **策略** > **安全策略** > **Zero Trust 应用**。

步骤 2 点击**在安全云控制中配置通用 ZTA**。

下图显示了一个示例。

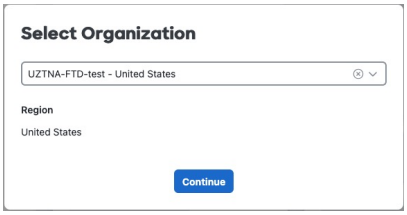


步骤 3 出现提示时，登录到 Security Cloud Control。

步骤 4 出现提示时，从下拉列表中选择您的组织，然后点击**继续**。

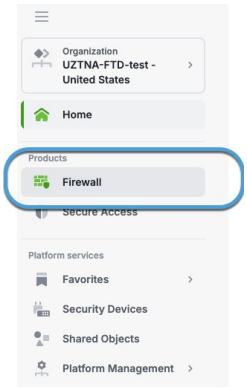
选择已配置安全访问和 Cisco Secure Firewall 微应用的组织。

下图显示了一个示例。



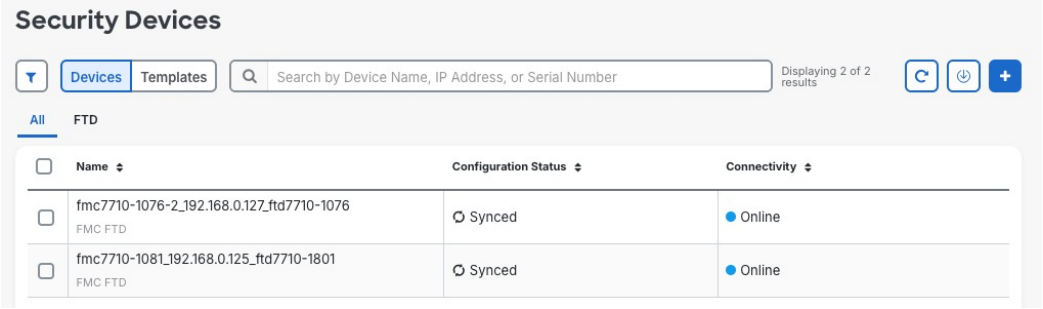
步骤 5 在 Security Cloud Control 中，在“产品”部分，点击**防火墙**。

下图显示了一个示例。



步骤 6 在“管理”部分，点击**安全设备**。

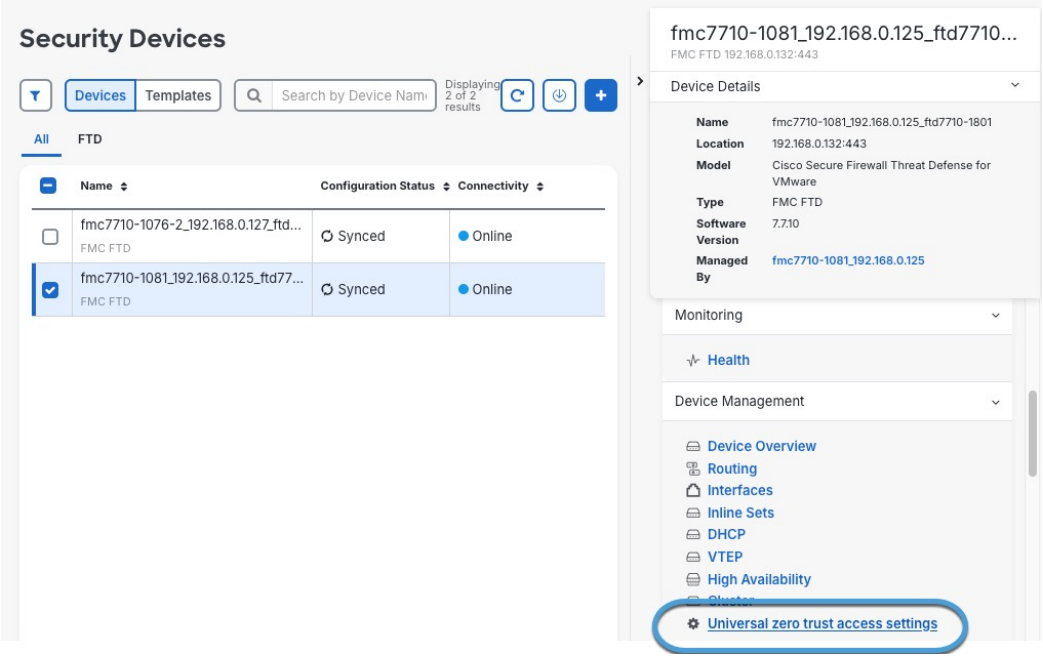
安全设备页面显示可用的安全设备。



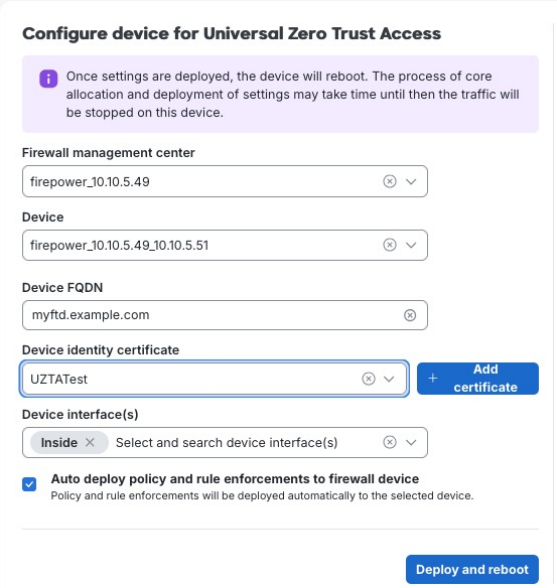
步骤 7 选中要添加到 通用零信任网络访问 配置中的设备旁边的复选框。

步骤 8 在右侧窗格中，点击**设备管理** > **通用 Zero Trust 访问设置**。

下图显示了一个示例。



步骤 9 在**为通用 Zero Trust 访问配置设备**页面上输入或编辑以下信息。



下表描述了要在设备上启用 通用 ZTNA 的配置。

项目	说明
防火墙管理中心	从下拉列表中，点击要用于策略部署、监控和其他任务的 Secure Firewall Management Center 的名称。
设备	从下拉列表中，点击要用于规则部署和实施的设备的名称。
设备 FQDN	输入安全设备的完全限定域名 (FQDN)。FQDN 也称为 TLS/SSL 证书的公用名。 Secure Access 将客户端重定向到此 FQDN 所代表的资源。 确保设备 FQDN 与设备身份证书的通用名称 (CN) 完全匹配，并且还必须匹配证书中的主题备用名称 (SAN)。

项目	说明
设备身份证书	**设备身份证书**的通用名称必须： • 与您在**设备 FQDN** 字段中输入的值完全匹配。 • 与证书中的使用者备用名称 (SAN) 匹配。 从下拉列表中，点击列表中现有身份证书的名称。 点击**添加证书**，以 **.p12** 格式（也称为 PKCS#12；请参阅 ssl.com 上的此文章）添加身份证书。 **注释** 通用 ZTNA 仅支持 PKCS#12 格式的证书注册。 在提供的字段中，输入用于标识证书的**名称**。然后复制粘贴、拖放或上传证书和私钥。如果证书已加密，请在提供的字段中输入其密码。 您也可以按照 ssl.com 上的什么是通配符证书？中的说明使用通配符证书。
设备接口	从下拉列表中，选中以下任一类型接口旁边的复选框。 • 内部网络接口（或 DMZ）：仅对本地用户部署访问规则。 • 外部网络接口：仅对远程用户部署访问规则。 • 两种类型的接口：对本地用户或远程用户部署访问规则。
自动将策略和规则实施部署到防火墙设备	选中此复选框，以便在 安全接入 上更新访问规则后，自动将其部署到设备。 在设备上，“自动部署”功能仅选择性地部署 通用 ZTNA 访问策略。它不会影响防火墙管理中心上的其他更改或配置。 **注释** 如果设备上存在与 通用 ZTNA 访问策略相互关联的其他依赖策略，防火墙配置状态会显示错误消息。然后部署会停止。在这种情况下，您应从防火墙管理中心手动部署 通用 ZTNA 访问策略。

步骤 10 点击**部署并重启**。

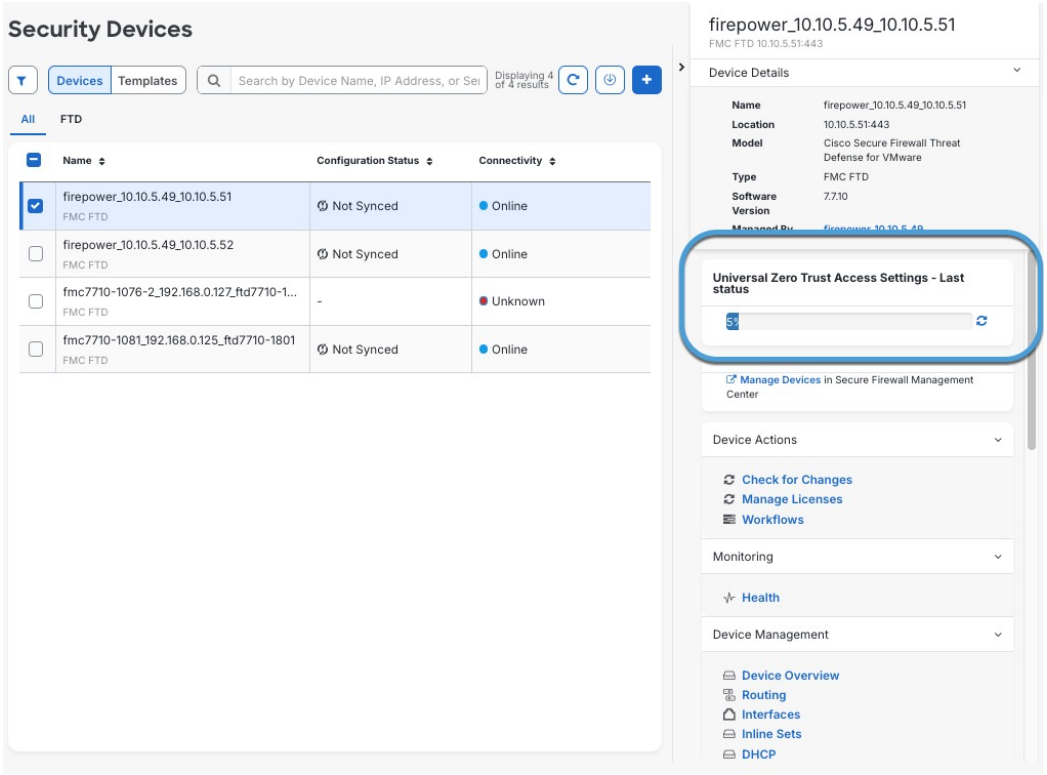
设备会重启以重新为 通用 ZTNA 组件分配系统资源。

注释
设备重启需要几分钟时间，在此期间，设备处理的所有流量都会中断。

如果您部署高可用性 (HA) 对设备，两台设备会同时重启。

步骤 11 在**安全设备**页面上，选中您刚刚部署 通用 ZTNA 配置的设备旁边的复选框。

右侧窗格显示部署状态，如下图所示。



有关详细信息，请在右侧窗格中点击**设备操作** > **工作流程**。

部署完成后，您可以在设备的**通用 Zero Trust 访问设置 - 最后状态**选项卡中查看完成状态。

已启用通用 ZTNA 的防火墙威胁防御设备已连接到安全访问。

下一步做什么

通过点击**安全云控制** > **安全访问** > **连接** > **网络连接** > **FTD**，检查安全访问下威胁防御设备的可用性。

Zero Trust 网络访问历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
通用 Zero Trust 网络访问（通用 ZTNA）。	7.7.10	7.7.10	通用 Zero Trust 网络访问（通用 ZTNA）是一种全面的解决方案，基于用户身份、信任和状态提供对内部网络资源的安全访问。它确保对一个应用的访问不会像远程访问 VPN 那样隐式授予对整个网络的访问权限。 新增/修改的屏幕： **策略** > **安全策略** > **Zero Trust 应用** 需要 Cisco 安全接入 和 Security Cloud Control。 部署限制：不支持集群设备、容器实例或透明模式。 支持的平台：Cisco Secure Firewall 1150、3100、4100、4200 和 Firewall Threat Defense Virtual。
Zero Trust 访问增强功能。	7.4.1	带有 Snort 3 的 7.4.1	防火墙管理中心 管理中心现在包括以下 Zero Trust 访问增强功能： • 现在，您可以为应用配置 NAT 的源网络。配置的网络对象或对象组用于将传入请求的公共网络源 IP 地址转换为应用网络内的可路由 IP 地址。 • 您可以使用诊断工具对 Zero Trust 配置问题进行故障排除。 新增/修改的屏幕： **策略** > **访问控制** > **Zero Trust 应用** 新增/修改的 CLI 命令：**show running-config zero-trust**、**show zero-trust statistics**

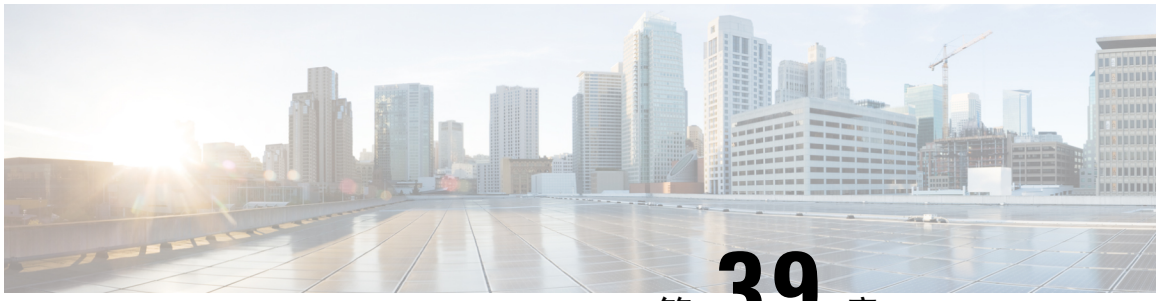
功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
无客户端 Zero Trust 访问。	7.4.0	带有 Snort 3 的 7.4.0	Zero Trust 访问允许使用外部 SAML 身份提供程序 (IdP) 策略对来自网络内部（本地）或外部（远程）的受保护基于 Web 的资源、应用或数据的访问进行身份验证和授权。 配置包括 Zero Trust 应用策略 (ZTAP)、应用组和应用。 新增/修改的菜单项： • **策略 (Policies)** > **Zero Trust 应用 (Zero Trust Application)** • **分析** > **连接** > **事件** • **概述 (Overview)** > **控制面板 (Dashboard)** > **Zero Trust** 新增/修改的 CLI 命令： • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics**



第 VIII 部分

访问控制策略基础

- 访问控制策略， 第 1701 页
- 安全智能， 第 1729 页
- 访问控制规则， 第 1743 页
- URL 过滤规则, on page 1785
- 入侵防御， 第 1813 页



第 39 章

访问控制策略

以下主题介绍如何使用访问控制策略：

- 关于访问控制策略， 第 1701 页
- 访问控制策略的要求和前提条件， 第 1706 页
- 管理访问控制策略， 第 1707 页
- 访问控制策略的历史记录， 第 1726 页

关于访问控制策略

访问控制是一种分层策略，可用于指定、检查和记录网络流量。您可以使用每个连接的特征来允许、信任、阻止或监控连接。

每个托管设备都可分配给一个访问控制策略。策略的已分配（也称为目标）设备收集有关网络流量的数据可用于根据以下内容过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目标、端口和协议等
- 流量的最新的上下文信息，包括诸如信誉、风险、业务相关性、使用的应用或访问的URL等特征
- 领域、用户、用户组或 ISE 属性
- 自定义安全组标记 (SGT)
- 加密流量的特性；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵尝试
- 时间和日期（在受支持的设备上）

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的阻止名单使用简单的源和目标数据，因此，可以在过程的早期阻止禁止的流量。相反，检测和阻止入侵和漏洞则是最后一道防线。

访问控制策略组件

以下是访问控制策略的主要元素。

名称和描述

每个访问控制策略必须拥有唯一的名称。说明是可选的。

沿用设置

通过策略继承，您可以创建访问控制策略的层次结构。父（或基本）策略定义和执行其后代的默认设置。

策略的继承设置允许您选择其基本策略。您还可以锁定当前策略中的设置以强制所有后代继承这些设置。后代策略可以覆盖未锁定的设置。

策略分配

每个访问控制策略可识别使用策略的设备。每台设备只能作为一个访问控制策略的目标。您还可以将策略分配给设备模板。

规则

访问控制规则提供了一种精细的网络流量处理方法。访问控制策略中的规则从1开始进行编号，包括从祖先策略继承的规则。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

通常，系统根据第一个访问控制规则（其中所有规则的条件都与流量匹配）处理网络流量。条件可以简单也可以复杂，条件的使用通常取决于某些许可证。

默认操作

默认操作确定系统如何处理和记录不是由任何其他访问控制配置处理的流量。默认操作可以阻止或信任所有流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

安全智能

安全智能是抵御恶意互联网内容的第一道防线。此功能允许您根据最新的IP地址、URL和域名信誉情报将阻止连接。要确保对重要资源的持续访问，您可以使用自定义不阻止列表条目来覆盖阻止列表条目。

HTTP 响应

在系统阻止用户的网站请求时，您可以显示系统提供的通用响应页面或自定义页面。也可以显示一个警告用户，同时允许他们继续访问初始请求站点的页面。

日志记录

通过访问控制策略日志记录的设置，您可以为当前的访问控制策略配置默认系统日志目标。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的解密、预过滤和入侵策略。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。通常，默认设置就非常适合。可修改的高级设置包括流预处理、解密、身份和各种性能选项。

访问控制策略默认操作

新创建的访问控制策略指示其分配的设备使用其默认操作处理所有流量。

在简单的访问控制策略中，默认操作指定设备如何处理所有流量。在更复杂的策略中，默认操作处理如下流量：

- 未被预过滤策略快速转发
- 不在安全智能阻止列表中
- 未被解密策略阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

访问控制策略默认操作可以阻止或信任流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。



注释 您不能对默认操作处理的流量执行文件或恶意软件检查。默认操作处理的连接的日志记录最初处于禁用状态，但是您可以启用该日志记录功能。

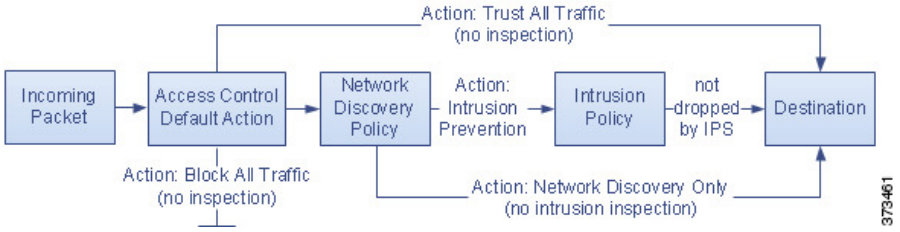
如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从其基本策略继承其默认操作，但您无法强制执行这一继承。

下表介绍了您可以对每个默认操作处理的流量执行的检查类型。

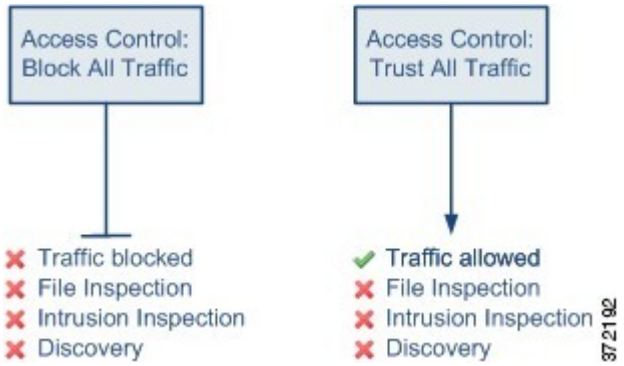
表 *101:* 访问控制策略默认操作

默认操作	对流量的影响	检查类型和策略
访问控制：阻止所有流量	直接阻止，不进行进一步检查。	无。
访问控制：信任所有流量	信任（允许流向其最终目标，而无需进一步检查）。	无。
入侵防御	允许，前提是其通过您指定的入侵策略检测。	入侵，使用指定的入侵策略和关联变量集。 发现，使用网络发现策略。
仅网络发现	允许。	仅发现，使用网络发现策略。
继承自基本策略	在基本策略中定义	在基本策略中定义

下图对该表进行了展示。



下图展示了**阻止所有流量 (Block All Traffic)** 和**信任所有流量 (Trust All Traffic)** 默认操作。



下图展示了**入侵防御 (Intrusion Prevention)** 和**仅网络发现 (Network Discovery Only)** 默认操作。



提示 **Network Discovery Only** 的目的是在仅发现部署中提高性能。如果您仅对入侵检测和防御感兴趣，则不同的配置可以禁用发现。

访问控制策略继承

您可以嵌套访问控制策略。在这种情况下，每个策略都会继承祖先（或基本）策略的规则和设置。您可以执行此继承，或允许较低级别的策略覆盖其祖先。

访问控制使用基于分层策略的实施。正如创建域层次结构一样，您也可以创建访问控制策略的相应层次结构。后代或子访问控制策略继承其直接父策略或基本策略的规则和设置。该基础策略可能有其子级的父级策略，它从父级策略沿用规则和设置等。

访问控制策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。这种实施执行来自祖先策略的强制规则，但也允许当前策略写入规则以抢先于来自祖先策略的默认规则。

您可以锁定以下设置，以便在所有后代策略中执行它们。后代策略可以覆盖未锁定的设置。

- 安全智能 — 根据 IP 地址、URL 和域名的最新信誉情报而被允许或阻止的连接。
- HTTP 响应页面 — 在阻止用户的网站请求时显示自定义或系统提供的响应页面。
- 高级设置 — 指定关联的子策略、网络分析设置、性能设置和其他常规选项。

如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

策略继承和多租户

访问控制的基于分层策略的实施完善了多租户策略。

在典型的多域部署中，访问控制策略的层次结构与域结构相对应，您将最低级别的访问控制策略应用于托管设备。这种实施支持在较高的域级别选择性地执行访问控制，而低层域管理员可以定制特定部署的具体设置。（要限制后代域中的管理员，您必须使用角色而不能只靠策略继承和实施。）

例如，作为组织的全局域管理员，您可以在全局级别创建访问控制策略。然后，您可以要求所有设备（按功能分为子域）使用该全局级策略作为基本策略。

当子域管理员登录 Secure Firewall Management Center配置访问控制时，他们可以按原样部署此全局级策略。或者，他们也可以在该全局级策略的界限之内创建和部署后代访问控制策略。

注释 虽然这种最有用的访问控制继承和执行的实施方法可以完善多租户策略，但您也可以在单个域中创建访问控制策略的层次结构。您还可以在任意级别分配和部署访问控制策略。

规则和其他策略警告

策略和规则编辑器使用图标来标记可能会对流量分析和流动有不利影响的配置。根据问题，系统可能会在您部署时向您发出警告或完全阻止您进行部署。

提示 将您的鼠标指针悬停在图标之上，即可读取警告、错误或信息文本。

表 *102:* 策略错误图标

图标	说明	示例
错误（）	如果规则或配置具有错误，则更正错误之前无法部署，即使禁用任何受影响规则也如此。	在分配没有URL过滤许可证的设备之前，执行基于类别和信誉的URL过滤的规则有效。此时，规则旁边会出现错误图标，您必须编辑或删除规则、取消分配设备或启用许可证才能部署。
警告（）	可以部署显示规则或其他警告的策略。然而，标记有警告的不当配置将不起作用。 如果您禁用包含警告的规则，则警告图标将消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。	已占用的规则或由于配置不当而无法与流量相匹配的规则不起作用。这包括使用空对象组的条件、与应用不匹配的应用过滤器、已排除的LDAP用户、无效端口等等。 但是，如果警告图标标记许可错误或型号不匹配，则在更正问题之前无法进行部署。
信息（）	信息图标传达有关可能影响流量流动的配置的有用信息。这些问题不会阻止您进行部署。	系统可能会跳过根据某些规则来匹配连接的前几个数据包，直至系统识别该连接中的应用或网络流量为止。这样，就可建立连接，以便识别应用和 HTTP 请求。
规则冲突（）	在启用规则冲突分析时，此图标会显示在具有冲突的规则的规则表中。	冲突包括冗余规则、冗余对象和影子规则。冗余和影子规则不匹配流量，因为以前的规则已与条件相匹配。冗余对象会使规则变得不必要地复杂。

访问控制策略的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员
- 您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。包含“修改

访问控制策略”权限的现有预定义用户角色支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。精细化权限包括：

- **策略** > **安全策略** > **访问控制** 并选择**访问控制策略** > **修改访问控制策略** > **修改威胁配置**允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。如果用户只有此选项，则不能修改策略或规则的其他部分。
- **修改剩余访问控制策略配置** 控制编辑策略所有其他方面的能力。

管理访问控制策略

您可以编辑系统提供的访问控制策略，并创建自定义访问控制策略。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

在页面顶部，有一些相关功能的便捷链接：对象管理、入侵策略、网络分析策略、DNS 策略和策略导入/导出。

步骤 2 管理访问控制策略：

- 分析策略 — 选择一个或多个策略然后点击 **分析策略** 评估冗余或影子规则等异常的访问控制策略，并采取措施修复已发现的异常。分析作业会发送到云，需要一些时间才能完成。请参阅使用策略分析器和优化器识别和修复异常，第 1720 页。

  “异常”列显示分析结果。点击 **% 可优化** 以查看异常，或点击 **重新分析** 以再次运行分析。“上次分析”列显示策略分析器和优化器上次运行的时间。

  完成分析和优化后，您可以通过从 **更多** (⋮) 菜单中选择以下选项来下载报告： **下载上次策略分析**、 **补救历史记录**。

  注释
  要使用策略分析功能，您必须使用 云交付的防火墙管理中心 或 连接到 Security Cloud Control (Security Cloud Control)。如果您的设置不符合要求，当您点击包含 **集成** 按钮的按钮时，系统会打开一个说明性对话框，可帮助您入门。策略分析器和优化器仅在云中运行。

- 创建 — 点击**创建策略**；请参阅创建基本访问控制策略，第 1708 页。
- 列 - 点击规则列表上方的 **显示/隐藏列 (Show/Hide Columns)** 图标，选择要在表中显示的信息。点击 **全部显示/全部隐藏 (Show All/Hide All)** 以快速添加或删除所有列出的列（名称和操作除外）。点击 **默认 (Default)** 以撤消所有自定义设置。
- 继承 — 垂直线表示策略之间的继承关系。
- 编辑 - 点击 **编辑** (✎)；请参阅编辑访问控制策略，第 1709 页

- 删除 - 点击 **删除** ()。您必须先删除任何设备分配，然后才能删除策略。

  要一次删除多个策略，请选中策略的复选框，然后选择表上方的 **删除策略** 。

- 复制-从 **更多** () 菜单中选择 **克隆** 。系统在副本保留设备分配。
- 报告 -从 **更多** () 菜单中选择**生成报告**。。报告将作为后台进程生成。转到消息/通知中心并查看任务列表。报告完成后，您可以从通知中下载。
- 查看审核日志 — 从 **更多** () 点击**查看审核日志**。
- 锁定或解锁策略 - 请参阅锁定访问控制策略 ， 第 1711 页。

创建基本访问控制策略

创建新的访问控制策略时，它包含默认操作和设置。创建策略后，您会立即进入编辑会话，以便您可以调整策略以满足您的要求。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击**创建策略**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 或者，选择基本策略。

如果已在您的域上执行访问控制策略，则此步骤不为可选步骤。必须选择已执行的策略或其后代之一作为基本策略。

如果您选择基本策略，则基本策略定义默认操作，您无法在此对话框中选择新的操作。日志记录连接由基础策略的默认操作处理。

步骤 5 不选择基本策略时，请指定初始**默认操作**：

- **Block all traffic** 通过 **Access Control: Block All Traffic** 默认操作创建策略。
- **入侵防御 (Intrusion Prevention)** 可以通过**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)** 默认操作创建策略，与默认入侵变量集相关联。
- **Network Discovery** 使用默认操作 **Network Discovery Only** 创建策略。

当您选择默认操作时，默认操作处理的连接的日志记录最初处于禁用状态。您可以稍后在编辑策略时启用它。

提示
如果要在默认情况下信任所有流量，或如果已选择基本策略但不想继承默认操作，则可以稍后更改默认操作。

步骤 6 或者，选择要分配给策略的设备。要减少显示的设备，请输入搜索字符串。该列表包括设备和设备模板。

如果要立即部署此策略，则必须执行此步骤。

步骤 7 点击**保存**。

新策略将打开以供编辑。您可以向其添加规则，并根据需要进行其他更改。请参阅编辑访问控制策略，第 1709 页。

编辑访问控制策略

编辑访问控制策略时，应将其锁定，以确保您的更改不会被同时编辑的其他人覆盖。

您只能编辑在当前域中创建的访问控制策略。此外，不能编辑由祖先访问控制策略锁定的设置。

为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

注释 当编辑某个策略但未将其锁定时，横幅消息可能会指示其他用户当前正在编辑该策略。当其中一个用户保存更改时，系统会提示您合并或放弃更改。您应该立即决定该怎么做。有关详细信息，请参阅并发编辑和合并更改，第 1712 页。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 编辑访问控制策略。

提示
您可以通过选中左列中的复选框，然后从搜索框旁边的**选择批量规则操作**下拉列表中选择要执行的操作，一次对多个规则进行操作。批量编辑可用于启用和禁用、复制、移动、删除和编辑规则，或查看命中计数或相关事件。您还可以删除所选规则中的对象重叠。

您可以更改以下设置或执行以下操作：

- 名称和说明 - 点击名称旁边的**编辑** (✎)，进行更改，然后点击**保存**。
- 默认操作和设置 - 从**默认操作**下拉列表中选择一个值，然后点击**齿轮**（⚙），对设置进行更改并点击**确定**。有关详细信息，请参阅设置访问控制默认操作，第 1714 页。

- 关联的策略 - 要编辑或更改数据包流中的策略，请点击策略名称下方数据包流表示中的策略类型。您可以选择 **预处理规则**、 **解密**、 **安全智能**和 **身份** 策略。必要时，点击**访问控制 (Access Control)** 以返回访问控制规则。
- 策略分配 - 要标识此策略的目标受管设备，或在子域中实施此策略，请点击**已分配：x 设备**链接。您可以将策略分配给设备或设备模板。
- 规则 - 要使用入侵和文件策略来管理访问控制规则，以及检查和阻止恶意流量，请点击**添加规则 (Add Rule)**，或右击现有规则并选择**编辑 (Edit)** 或其他响应操作。操作也可从每个规则的 **更多** (⋮) 按钮获取。请参阅创建和编辑访问控制规则，第 1764 页。
- 布局 - 使用规则列表上方的**网格/表视图 (Grid/Table View)** 图标更改布局。网格视图以易于查看的布局提供彩色编码的对象。表视图提供摘要列表，以便您可以同时查看更多规则。您可以在不影响规则的情况下自由切换视图。
- 列（仅限表视图）- 点击规则列表上方的**显示/隐藏列**图标，选择要在表中显示的信息。点击**显示/隐藏空列**以快速删除所有没有信息的列，即您不在任何规则中使用这些条件。点击**恢复为默认值 (Revert to Default)** 以撤消所有自定义设置。
- 分析规则逻辑 - 您可以从**分析**菜单中选择以下选项来检查规则的逻辑：
  - **管理规则命中计数** - 要查看每个规则的匹配连接数统计信息。请参阅查看规则命中计数，第 1721 页。
  - **启用/禁用规则冲突**-选择是否要查看有关规则是否相互干扰的信息。然后，您可以使用以下命令查看结果。请参阅分析规则冲突和警告，第 1723 页
    - **显示警告和错误** - 查看是否存在需要解决配置问题的规则。
    - **显示策略警告** - 查看策略是否存在配置问题。
    - **显示规则冲突**-查看是否有冗余或影子规则。这些冲突可能会阻止某些规则被连接匹配，这意味着您需要修复匹配条件、移动规则或直接删除规则。
- 其他设置 - 要更改策略的其他设置，请从数据包流末尾的**更多**下拉箭头中选择以下选项之一。
  - **加密可视性引擎** - 是否启用和配置加密可视性引擎。请参阅配置 EVE，第 1959 页。
  - **高级设置** - 要设置预处理、解密、身份、性能及其他高级选项。请参阅为访问控制策略配置高级设置，第 2456 页。
  - **HTTP 响应 (HTTP Responses)** - 要指定当系统阻止网站请求时用户在浏览器中看到的内容。请参阅选择 HTTP 响应页面，第 1803 页。
  - **继承设置 (Inheritance Settings)** - 更改此策略的基本访问控制策略，并在其后代策略中实施此策略的设置。请参阅选择基本访问控制策略，第 1715 页和锁定后代访问控制策略中的设置，第 1716 页。
  - **日志记录 (Logging)** - 设置策略的默认日志记录选项。

步骤 4 点击**保存**。

锁定访问控制策略

您可以锁定访问控制策略，以防止其他管理员对其进行编辑。锁定策略可确保在您保存更改之前，如果其他管理员编辑策略并保存更改，您的更改不会失效。如果您不锁定策略，但另一个用户同时编辑该策略并必须先保存更改，则您可能必须合并更改。有关详细信息，请参阅并发编辑和合并更改，第 1712 页。

该锁用于访问控制策略本身。锁定不适用于策略中所使用的对象。例如，另一个用户可以编辑锁定访问控制策略中所使用的网络对象。在明确解锁策略之前，您的锁定将保持不变，因此您可以稍后注销并返回到您的编辑。

策略被锁定时，其他管理员对该策略具有只读访问权限。但是，其他管理员可以将已锁定的策略分配给托管设备。

开始之前

有权修改访问控制策略的任何用户角色都有权锁定该策略，并且还可以解锁被其他用户锁定的策略。

但是，解锁被其他管理员锁定的策略的能力受以下权限控制：**策略** > **安全策略** > **访问控制** 选择访问控制 **(Access Control)访问控制策略 (Access Control Policy)** > **修改访问控制策略 (Modify Access Control Policy)** > **覆盖访问控制策略锁定 (Override Access Control Policy Lock)**。

如果您使用的是自定义角色，则您的组织可能会通过不分配此权限来限制您的解锁能力。如果没有此权限，则只有锁定策略的管理员才能解锁策略。

过程

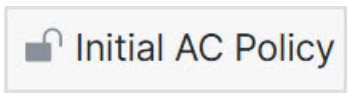
步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要锁定或解锁的访问控制策略旁边的 **编辑** ()。

在访问控制策略列表中：

- 策略名称旁的锁图标表示该策略已锁定。将鼠标悬停在该图标上即可查看哪个用户锁定了策略。
- 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。 否则，它已被其他用户锁定。

步骤 3 点击策略名称旁边的锁定图标可锁定或解锁策略。



如果策略从父策略继承了设置，则在点击锁定图标时必须选择以下选项之一。

- **锁定/解锁此策略** - 锁定或解锁仅适用于此策略。

- **锁定/解锁层次结构中的所有策略** - 锁定或解锁此策略和所有父策略。如果父策略已被其他管理员锁定，您将看到一条消息，并且无法锁定该父策略。解锁策略时，如果您具有“覆盖访问控制策略锁定”权限，则会解锁所有父策略，即使它们已被其他用户锁定。

并发编辑和合并更改

当允许多个用户编辑访问控制策略时，您有两种选择：

- 让用户在编辑策略时锁定策略。这可确保一次只能有一个用户进行更改。使用锁定，您永远不必担心更改丢失或冲突。但是，它会限制您快速响应意外事件的能力，尤其是在用户不在办公室时锁定策略的情况下。有关锁定策略的详细信息，请参阅锁定访问控制策略，第 1711 页。
- 允许用户同时编辑策略。如果多个用户在给定时间进行了未保存的编辑，则第一个保存策略的用户会得到其已保存的所有更改。其他用户会立即收到保存通知，然后必须合并其更改。本主题的其余部分介绍此方法。



注释 如果您使用变更管理（在故障单范围内进行编辑），故障单会锁定策略，无法进行并发编辑。

开始之前

要限制必须执行的合并量，请及早并经常保存策略。

过程

步骤 1 确定其他用户是否也在编辑策略。

编辑访问控制策略时，请查找页面顶部是否显示以下消息横幅：

```
User name is currently editing this policy.
```

此消息表明指定用户（可能有多个）当前已打开策略进行编辑。

步骤 2 留意其他用户已保存更改的通知并采取措施。

以下横幅消息表示另一用户已保存更改，您需要立即采取措施：

```
User name modified this policy and saved changes. Merge Discard.
```

点击以下任一链接：

- **合并**-打开一个合并窗口，您可以在其中决定保留或放弃哪些更改，并识别无法合并的更改。采用此选项时，请参阅下一步。

- **放弃**-立即放弃所有更改并重新开始。如果选择此选项，页面会刷新，以显示其他用户的最新更改。

步骤 3 合并更改。

当您点击**合并**选项时，系统将打开一个合并窗口，其中汇总了观察到的您的编辑与上次用户保存的编辑之间的差异总数。不包括其他用户的未保存编辑。观察结果包括直接冲突和信息性通知。

注释
您必须在关闭窗口之前完成所有合并决定。点击 **合并** 选项后，不能等到以后再进行合并。

a) 评估每个冲突并为每个冲突制定决策。

在评估更改列表时，请考虑以下事项：

- 最初，系统会显示所有观察结果，但您可以选择/取消选择 “**冲突**” 和 “**信息**” 的过滤选项，以限制显示的信息。当用户编辑相同的规则或设置时，会产生冲突。信息项目用于对不同规则或设置进行编辑。
- 如果不存在冲突，您的缓存将立即使用上次保存的更改进行更新，然后您可以继续。例如，如果您正在编辑规则 1，而另一个用户已保存对规则 2 的更改，则不可能存在任何冲突。
- 对于每个冲突（规则名称除外），窗口会显示其他用户保存的元素版本（**防火墙管理中心上的版本**）和您的更改（**修改后的版本**）。系统对新增的（例如，以前未定义的选项）、编辑的或删除的策略元素用更改进行颜色编码。您必须选择 “**放弃** 更改”或“ **接受我的更改**” 并覆盖其他用户的更改。放弃更改时，系统会使用其他用户的保存更改来刷新规则，并删除您的更改。
- 规则冲突是在规则级别考虑的，而不是规则中的每个元素考虑的。例如，如果您编辑目标网络，且保存的更改适用于源网络，则您的更改或其他用户的更改将保留，而不会同时保留。
- 如果冲突涉及规则名称，系统会尝试在名称中添加下划线和数字来创建唯一名称，例如 Rule_1。您也可以在提供的编辑框中输入新名称，然后点击 **保存**。如果点击 **丢弃 (Discard)**，将使用生成的规则名称。
- 您无法跳过任何冲突。对于每个冲突，您必须决定是放弃还是保留更改。
- 如果保存更改的用户删除了您编辑的规则，则规则将被删除，并且您无法选择保留该规则。
- 如果保存更改的用户更新了规则，而您的更改是为了删除该规则，则保留该规则：您无法合并删除。
- 对于以下选项，如果您的更改与已保存的更改冲突，您的更改会被丢弃，并且不会合并更改：
  - 其他策略分配：预过滤策略、安全智能策略、身份策略、解密策略
  - 更改高级设置、策略日志记录、EVE、HTTP 响应页面。
  - 策略默认操作。
  - 沿用设置。

b) 点击**关闭 (Close)**。

步骤 4 合并完成后，您可以立即保存策略或继续编辑策略。保存策略可能会降低未来合并的影响。

设置访问控制默认操作

访问控制策略的默认操作会应用于以下任意连接：

- 未被预过滤策略快速转发
- 不在安全智能阻止列表中
- 未被解密策略阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅编辑访问控制策略，第 1709 页。

步骤 2 选择规则列表底部的**默认操作**。

有关这些选项的详细信息，请参阅访问控制策略默认操作，第 1703 页。

步骤 3 点击**齿轮**（ ）以配置默认操作设置。

你可以配置以下选项。完成后点击**确定**。

- 日志记录选项 - 是否记录连接。您可以**在连接开始时记录**、**在连接结束时记录**，或两者都选。如果您选择阻止作为默认操作，则只能在连接开始时进行记录。
- **将连接事件发送至** - 如果选择一个日志记录选项，请选择是否将事件发送至以下任意组合：
  - **防火墙管理中心** - 将事件发送到管理器。
  - **系统日志服务器** - 将事件发送到为策略配置的默认系统日志服务器。您可以配置覆盖以指定不同的严重性级别或系统日志服务器目标。

  （Splunk 或 SIEM 系统日志服务器集成）如果您已将 防火墙管理中心 配置为 Splunk 配置中的连接事件源，请选择 **将连接事件发送至** 选项下的 **防火墙管理中心** 。如果您已将Firewall Threat Defense配置为连接事件源，请选择至少一个系统日志目标。有关 Splunk 或任何 SIEM 系统日志配置程序，请参阅 *Cisco Secure Firewall Management Center* 管理指南。
- **SNMP 陷阱** - 如果启用日志记录，则可以将 SNMP 陷阱发送到 SNMP 服务器。选择 SNMP 配置，或点击 + 配置新的配置。
- **默认操作变量集** - 如果选择了其中一种入侵防御默认操作，请选择应与所选入侵策略一起使用的变量集。

步骤 4 点击**保存**。

管理访问控制策略继承

继承与使用其他策略作为访问控制策略的基本策略相关。这允许您使用一个策略来定义可应用于多个策略的一些基准特征。要了解继承的工作原理，请参阅访问控制策略继承，第 1704 页。

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅编辑访问控制策略，第 1709 页。

步骤 2 管理策略继承：

- 更改基本策略 - 要更改基本访问控制策略，请从数据包流行末尾的**更多** 下拉箭头中选择**继承设置**，然后如选择基本访问控制策略，第 1715 页中所述继续操作。
- 锁定后代策略中的设置 - 要在此策略的所有后代策略中执行其设置，请从数据包流行末尾的**更多**下拉箭头中选择**继承设置**，然后如锁定后代访问控制策略中的设置，第 1716 页中所述继续操作。
- 从基本策略继承设置 - 要从基本访问控制策略继承设置，请按照继承基本策略的访问控制策略设置，第 1716 页中的指示进行操作。
- 要求在域中提供 - 要在子域中执行此策略，请点击**已分配：x 台设备**链接，然后如在域中要求访问控制策略，第 1717 页中所述继续操作。

选择基本访问控制策略

可以使用一个访问控制策略作为另一个访问控制策略的基础（父级）。默认情况下，子策略从其基本策略继承其设置，但是可以更改未锁定的设置。

当更改当前访问控制策略的基本策略时，系统会使用新基本策略中的任何已锁定的设置来更新当前策略。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **继承设置** 。

步骤 2 从**选择基本策略 (Select Base Policy)** 下拉列表中选择策略。

选择**无**以删除继承。

步骤 3 点击**确定**。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

锁定后代访问控制策略中的设置

锁定访问控制策略中的设置，以便在所有后代策略中执行该设置。后代策略可以覆盖未锁定的设置。

当您锁定设置时，系统会保存后代策略中已经做出的覆盖，以便在您再次解锁设置时可以恢复这些覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **继承设置** 。

步骤 2 在“子策略继承设置”(Child Policy Inheritance Settings) 区域中，选中要锁定的设置。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**确定** 保存设置。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

继承基本策略的访问控制策略设置

新的子策略继承其基本策略的许多设置。如果这些设置在基本策略中未锁定，您可以覆盖这些设置。

如果稍后重新继承基本策略的设置，系统会显示基本策略的设置且控件呈灰色。不过，系统会保存所做的覆盖，如果您再次禁用继承，则会恢复覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**安全智能**，或者从从数据包流行末尾的**更多**下拉箭头中选择 **HTTP 响应**、**日志记录**、**加密可视性引擎**或**高级设置**。

步骤 2 选中要继承的每个设置所对应的**继承自**（**基本策略**）复选框。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

在域中要求访问控制策略

您可以要求域中的每个设备都使用相同的基本访问控制策略或其后代策略之一。此程序仅适用于多域部署。

过程

步骤 1 在访问控制策略编辑器中，点击**已分配：x 台设备**链接。

步骤 2 点击 **在域中需要**。

步骤 3 构建域列表：

- 添加 - 选择要实施当前访问控制策略的域，然后点击**添加 (Add)** 或拖放到所选域列表中。
- 删除 - 点击枝叶域旁边的 **删除** ()，或者右键点击祖先域并选择 **删除所选项**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除** () 以清除搜索。

步骤 4 点击**确定** 以保存域实施设置。

步骤 5 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

将设备分配给访问控制策略

访问控制策略指定使用策略的设备。每个设备只能分配给一个访问控制策略。您还可以将策略分配给设备模板。模板包含在可用设备和选定设备列表中。

过程

步骤 1 在访问控制策略编辑器中，点击**已分配：x 台设备**链接。

步骤 2 制定目标联系人列表：

- 添加 - 选择一个或多个**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)** 或拖放到**所选设备 (Selected Devices)** 列表。
- 删除 - 点击单个设备旁边的**删除** ()，或选择多个设备，点击右键，然后选择**删除选择**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除** () 以清除搜索。

在**受影响的设备**下，系统会列出其分配的访问控制策略是当前策略子项的设备。对当前策略进行的任何更改都将影响这些设备。

步骤 3 点击**确定** 以保存目标设备设置。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

访问控制策略的日志记录设置

要配置访问控制策略的日志记录设置，请从数据包流行末尾的 **更多** 下拉箭头中选择 **日志记录** 。

您可以为访问控制策略配置默认系统日志目标和系统日志警报。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的解密、预过滤和入侵策略。

默认操作处理的连接的日志记录最初处于禁用状态。

只有在页面顶部选择通常用于发送系统日志消息的选项后，IPS 和文件和恶意软件设置才会生效。

默认系统日志设置

选择 **Syslog Server** 选项以便为策略配置默认系统日志服务器。然后，选择目标，如有需要，还需选择警报级别。您可以选择：

- **目标** > **特定系统日志警报对象** - 如果选择此选项，事件将根据*Cisco Secure Firewall Management Center* 管理指南中创建系统日志警报响应的说明配置的所选系统日志警报进行发送。您可以从列表中选择系统日志警报，或通过指定名称、记录主机、端口、设施和严重性来添加警报。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的入侵系统日志警报的设施和严重性。

  使用此选项时，系统会使用管理接口将系统日志消息发送到服务器。确保有从管理接口到系统日志服务器的路由，否则信息将无法到达服务器。

- **目标** > **使用 FTD 平台设置** - 如果选择此选项并指定**严重性**，系统会将具有该严重性的连接或入侵事件发送到“平台设置”中配置的系统日志收集器。使用此选项，您可以通过在“平台设置”中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。本部分中选择的严重性适用于所有连接和入侵事件。默认严重性为警报。

入侵设置

- **发送 IPS 事件的系统日志消息**-将 IPS 事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖** - 如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为 IPS 事件设置不同的系统日志服务器目标，并更改事件的严重性。

文件和恶意软件设置

- **发送文件和恶意软件事件的系统日志消息**-将文件和恶意软件事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖** - 如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为文件和恶意软件事件设置不同的系统日志服务器目标，并更改事件的严重性。

将其他策略与访问控制相关联

将主策略与访问控制策略相关联的最简单方法是点击访问控制策略主题中显示的数据包流中的策略链接。您可以快速选择关联的策略。或者，您可以使用策略的高级设置来关联策略，如本主题中所述。这些策略包括：

- 预过滤器策略 - 使用有限网络（第 4 层）外部报头条件执行早期流量处理。
- 解密 策略 - 用于监控、解密、阻止或允许使用安全套接字层 (SSL) 或传输层安全 (TLS) 加密的应用层协议流量。
- 身份策略 - 根据与流量关联的领域和确认方法执行用户身份验证。

开始之前

在将解密策略与访问控制策略关联之前，请查看TLS 服务器身份发现，第 2459 页中有关 TLS 服务器身份发现的信息。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 2 在相应的“策略设置”区域点击**编辑** ()。

如果显示**视图** ()，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 从下拉列表中选择策略。

如果选择用户创建的策略，则可以点击显示的编辑图标来编辑策略。

步骤 4 点击**确定**。

步骤 5 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

使用策略分析器和优化器识别和修复异常

您可以使用“策略分析和优化器”来评估访问控制策略中的异常情况，如冗余规则或阴影规则，并采取行动修复发现的异常情况。策略分析器和优化器托管在云中，与未与云集成的可用规则分析不同。与云集成后，非云策略分析不可用。

系统会每日定期自动执行策略分析（每24小时）。您也可以手动启动分析。最初启用该服务时，系统会开始分析所有现有访问控制策略。



注释 在优化策略之前，请创建策略的副本。如果您对优化结果不满意，可以轻松地将托管设备重新分配给副本，并将系统返回到其起始状态。

开始之前

- 您可以直接从带有 防火墙管理中心 7.2+ 的 Security Cloud Control 使用策略分析器和优化器，但只能从7.6开始交叉启动该功能。分配给访问控制策略的托管设备上运行的软件版本无关紧要。策略分析器和优化器仅托管在云中，因此无论您是从 防火墙管理中心 还是直接从Security Cloud Control 运行分析，都没有区别。
- 要使用该功能，您必须在**集成** > **安全云控制** 下选择**启用策略分析和优化**。
- 如果您已启用变更管理，则策略分析器和优化器会自动为更改创建通知单，并提交通知单。审批人必须先批准通知单，然后才能部署更改。
- 如果您使用的是域，则无法点击异常列中的链接来查看报告。请登录 Security Cloud Control 并从该应用程序中使用该功能。
- 策略分析器和优化器会在已更新、禁用或合并的规则上添加规则注释。您可以稍后搜索这些注释以查找优化的规则。
- 策略分析器和优化器实施的更改在审核日志中反映为默认名称 internaladmin 下的 API 调用。
- 启用策略分析器和优化器后，每次添加或编辑规则时，系统都会评估更改。如果应用规则编辑更改将导致冗余或影子规则等异常，用户会收到通知。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

如果您已运行分析，“异常”(Anomaly) 列会显示策略的问题数量和策略可以优化的百分比，以及策略分析的状态，例如“错误”(Error) 或“已完成”(Completed)。上次分析显示运行分析的日期/时间。

步骤 2 选择一个或多个策略，然后点击**分析策略 (Analyze Policy)**。

分析在云中作为后台进程运行。分析完成后，结果将显示在“异常”(Anomaly) 列中。

说明：

- 您还可以在编辑策略时通过选择**分析 (Analyze)** > **策略 (Policy)** 来开始分析。该菜单中的其他选项允许您显示命中计数和警告。
- 如果您尚未连接到云，当您点击此按钮时，系统会打开一个说明性对话框，其中包含可帮助您开始的**集成 (Integrate)** 按钮。策略分析器和优化器仅在云中运行。

步骤 3 分析完成后，点击“异常”(Anomaly) 列中的**可优化百分比 (% Optimizable)**，以在云中启动策略分析器和优化器。

完成要执行的所有操作后，点击**应用补救 (Apply Remediations)**（在云中）。系统将向您显示要执行的操作的确认。点击**继续 (Proceed)** 以实施更改。

如果初始分析以错误结束，您可以点击**重新分析 (Re-analyze)** 以重新启动该过程。

步骤 4 部署策略以完成更改。

如果您启用了变更管理，则审批者必须先批准包含补救措施的通知单，然后才能部署这些补救措施。

查看规则命中计数

命中计数表示策略规则或默认操作与连接匹配的次数。命中计数只会随匹配策略的连接的第一个数据包递增。您可以使用此信息来确定规则的有效性。只会为应用于 Firewall Threat Defense 设备的访问控制和预过滤规则提供命中计数信息。

注释

- 即便是重新启动和升级，计数也会仍然存在。
- 计数会按高可用性对或集群中的每台设备来维护。
- 当设备上正在进行部署或任务时，您将无法从设备获取命中计数信息。
- 您还可以使用 **show rule hits** 命令在设备 CLI 中查看规则命中计数信息。
- 如果已从“访问控制策略”(Access Control Policy) 页面访问“命中计数”(Hit Count) 页面，则无法查看或编辑预过滤器规则，反之亦然。
- 命中计数不适用于使用“监控”操作的规则。

开始之前

如果使用自定义用户角色，请确保角色包括以下权限：

- 查看设备，以查看命中计数。
- 修改设备，以刷新命中计数。

过程

步骤 1 在访问控制策略或预过滤策略编辑器中，点击页面右上角的**分析** > **管理规则命中计数**。

步骤 2 在“命中计数”页面上，从**选择设备**下拉列表中选择设备。

如果不是第一次为此设备生成命中计数，最后一次获取的命中计数信息将出现在下拉框旁边。此外，验证**最新部署**时间，以确认最新的策略更改。

选择**全部**以查看分配给该策略的所有设备的命中计数汇总。

步骤 3 如有必要，请点击 **刷新** (↻) 以便从所选设备获取当前命中计数数据。

在预过滤器策略中，您可能需要点击**获取当前命中计数 (Fetch Current Hit Count)**，获取初始命中计数数据。

您无法在部署到设备的过程中刷新命中计数。

步骤 4 查看和分析数据。

可以执行以下操作：

- 点击**预过滤器 (Prefilter)** 或**访问控制 (Access Control)**，以便在这些策略的命中计数之间切换。
- 通过在**过滤器**框中输入搜索字符串来搜索特定规则。
- 通过在**过滤条件 (Filter by)** 字段中选择这些选项，将列表广泛地限制为**命中规则 (Hit Rules)** 或**从不命中规则 (Never Hit Rules)**。在查看命中规则时，您可以通过在**最后时间 (In Last)** 字段中选择一个时间范围（例如，最近 1 天）来进一步限制列表。
- （在从访问控制策略查看时。）通过选中规则的复选框，然后点击 **清除命中计数**，清除一个或多个规则的命中计数。确认操作时，选择 **清除并重新加载** 以刷新命中计数数据。一次最多可以清除 500 条规则的命中计数。您无法撤消清除命中计数。

  注释
  点击表信头中的复选框以选择列表中的所有规则。要选择一系列规则，请选中第一个规则的复选框，然后按住 Shift 键并点击最后一个规则的复选框；中间的所有规则也会被选中。

- （在从访问控制策略查看时。）您可以对单个规则执行以下操作：
  - 通过点击 **更多** (⋮) 菜单中的 **编辑** 来编辑规则。
  - 通过点击 **更多** (⋮) 菜单中的 **删除** 来从策略中删除规则。
  - 通过点击 **更多** (⋮) 菜单中的 **启用/禁用规则** 来启用或禁用规则。
  - 通过点击 **更多** (⋮) 菜单中的 **清除命中计数** 来清除规则的命中计数（将其重置为零）。您无法撤销此操作。
- （从预过滤器策略查看时。）通过点击 **齿轮**（⚙） 并选择要显示的列来更改显示的列。

- （从预过滤器策略查看时。）点击规则名称以对其进行编辑，或点击最后一列中的**视图**()以查看规则详细信息。点击规则名称会在策略页面中突出显示它，您可以在该页面中对规则进行编辑。
- （从预过滤器策略查看时。）通过右键点击规则并选择**清除命中计数 (Clear Hit Count)**，清除规则的命中计数信息（将其重置为零）。您可以使用Ctrl+点击来选择多个规则。您无法撤销此操作。
- 通过点击页面左下角的**生成 CSV (Generate CSV)** 来生成页面详细信息的逗号分隔值报告。

步骤 5 点击**关闭**返回策略页面。

分析规则冲突和警告



注释 仅当未与思科安全云集成时，本主题中介绍的功能才可用。当您与云集成时，功能更强大的策略分析器和优化器将取代此功能。请参阅使用策略分析器和优化器识别和修复异常，第 1720 页。

您可以查看有关规则冲突的警告和信息，以便检查访问控制策略的逻辑并确定需要更改的规则。当规则重叠时，您可能会在策略中使用不必要的规则，而这些规则将永远不会与流量匹配。分析可以帮助您删除不必要的规则，或者确定应移动或修改的规则，以便实施所需的策略。

策略警告和错误会指出您应该了解并可能解决的问题，从而确保您的规则提供所需的服务。

规则冲突分析可识别以下类型的问题：

- 对象重叠 - 规则某字段中的元素是该规则同一字段中一个或多个元素的子集。例如，源字段可能包括 10.1.1.0/24 的网络对象以及主机 10.1.1.1 的另一个对象。由于 10.1.1.1 位于 10.1.1.0/24 覆盖的网络内，因此 10.1.1.1 的对象是冗余的且可被删除，从而简化规则并节省设备内存。
- 冗余规则 - 两个规则对同一类型的流量应用相同的操作，删除基础规则不会改变最终结果。例如，如果允许特定网络的 FTP 流量的规则后接允许该网络的 IP 流量的规则，并且在拒绝访问之间没有规则，则第一条规则是冗余的，您可以将其删除。
- 阴影规则 - 这与冗余规则相反。在这种情况下，一条规则将与另一条规则匹配相同的流量，因此第二条规则永远不会被应用于访问列表中稍后出现的任何流量。如果两个规则的操作相同，则您可以删除被屏蔽的规则。如果两个规则为流量制定了不同的操作，则您可能需要移动阴影规则或编辑两条规则之一，以便实施所需的策略。例如，对于给定的源或目标，基本规则可能会拒绝 IP 流量，而阴影规则可能会允许 FTP 流量。

开始之前

进行分析时：

- 仅识别给定规则的第一个冲突。在问题得到修复后，该规则可能会被识别为与表中的另一个规则存在冲突。但是，一个规则可能会有多个警告或错误。

- 规则冲突分析只会考虑源/目标安全区域、网络、VLAN和服务/端口匹配条件和操作。它不会考虑其他匹配条件，因此明显冗余的规则可能并非完全冗余。
- 无法分析 FQDN 网络对象是否存在冲突，因为无法在进行 DNS 查找之前知道 FQDN 的 IP 地址。
- 已禁用的规则会被忽略。
- 时间范围属性会被忽略。不同时间段的规则在时间范围内实际上不是冗余时，它们可能会被标记为冗余。
- 在启用该功能时，警告和错误以及规则冲突的图标会显示在规则表中。有关图标的参考，请参阅规则和其他策略警告，第 1705 页。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**，然后编辑该策略。

步骤 2 执行以下操作之一打开规则冲突和警告对话框：

- 要查看规则冲突，请点击**分析 (Analyze)** 下拉列表，然后点击**启用规则冲突 (Enable Rule Conflicts)**。分析完成后，您会在页面顶部看到冲突摘要。然后，从同一菜单中点击**显示规则冲突** 以查看具体结果。

  每次进行打开策略或更改并保存策略时，都必须重新启用规则冲突检测。
- 要查看规则警告和错误，请点击**分析** > **显示警告和错误**。

  对策略进行更改后，您可以通过点击分析按钮旁边的重新加载图标来刷新结果。
- 要查看策略警告，请点击 **分析** > **显示策略警告**。
- 如果您已查看完规则冲突，请点击**分析 (Analyze)** > **禁用规则冲突 (Disable Rule Conflicts)**.

步骤 3 在规则冲突和警告对话框中：

- 规则警告和错误会显示在与规则冲突分开的选项卡上。还有一个单独的选项卡用于显示策略警告。
- 每个选项卡都包含子选项卡，可让您检查各个类型的问题，例如冗余与阴影或警告与错误。此外，也可以搜索项目。
- 每个规则名称旁边的 **更多** (⋮) 提供编辑、禁用或删除规则的快捷方式。

步骤 4 完成后点击“**关闭**”。

搜索规则

您可以使用搜索功能来帮助自己查找规则，尤其是在有大量的规则时。

过程

步骤 1 编辑访问控制策略时，通过点击**搜索 (Search)** 框构建搜索字符串。

- 对于简单的文本字符串搜索，请键入字符串。搜索将返回在任何列中包含该字符串的规则。 不能将字符串搜索与标记搜索结合使用，例如将字符串搜索与源网络搜索结合使用。
- 要搜索特定的列，请开始键入列的名称，直到系统提示您输入全称，例如“源网络”，或选择可搜索字段的列表名称。在选择搜索标记后，即可输入该标记的搜索字符串。例如，**源网络 10.1.1.1**。
- 在源/目标列中搜索IP地址时（但不是作为简单的文本搜索），可以使用**搜索内部子网和范围**选项来控制是完全匹配IP地址（未选中）还是匹配包含搜索地址的任何子网或范围（选中）。例如，选中该选项后，搜索 10.1.1.1 将包含 10.1.1.0/24 的规则。
- 在端口字段中搜索仅会返回完全匹配项。
- 输入多个值时，请用逗号分隔这些值。
- 第一次搜索后，点击搜索框会提示您最近的搜索和标记。您可以通过选择快速重复搜索，或通过选择以前的搜索或标记并在其基础上来构建类似的搜索。
- 构建具有多个标记的搜索字符串时，请不要在标记之间包含空格。
- 在选择标记时，系统会提示您输入这些列中显示的值。选择您要搜索的值。
- 您可以根据一些常见功能快速进行筛选，方法是点击搜索框左侧的过滤器图标，然后选择显示具有以下任意组合的规则：允许、阻止、监视、入侵策略、时间范围、冲突、警告、错误、禁用规则、过期规则、、包含定义重叠的对象的规则。。
- 要查看适用于特定设备或一组设备的规则，请点击过滤器图标并选择设备。如果规则使用包含设备上至少一个接口的安全区域，或者它们不包含安全区域，则这些规则适用于设备。

步骤 2 将光标置于搜索框中搜索字符串的末尾，然后按 Enter 键。

满足搜索字符串的规则会被突出显示，而不匹配的规则会被隐藏。您可以取消选择**仅显示匹配规则 (Show Only Matching Rules)** 以查看整个表，以及该表中突出显示的规则。这让您能够查看周围的规则。

“仅显示匹配规则”(Show Only Matching Rules) 复选框旁边是与匹配搜索字符串的数量相比的策略中规则总数的摘要。

步骤 3 要关闭搜索并返回到未过滤和未突出显示的表，请点击搜索框右侧的 **X**。您还可以将光标放在搜索字符串的末尾，然后按 Esc 键。

访问控制策略的历史记录

表 *103:*

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
多个用户同时编辑访问控制策略。	10.0.0	任意	在以前的版本中，如果两个或多个用户同时编辑访问控制策略，第一个保存的用户将保留其更改，所有其他用户将立即丢失其所有编辑内容。现在，这些用户能够有选择地合并其更改，并且与第一个用户保存的更改不冲突的更改将自动被接受。这改进了用户之间的协作，并减少了在编辑期间锁定策略的需求。
对象组搜索性能增强。	7.6.0	7.6.0	对象组搜索现在速度更快，使用的 CPU 资源更少。 新的 CLI 命令：**clear asp table network-object**、**show asp table network-object**、**debug acl ogs** 修改的 CLI 注释（增强的输出）：**packet-tracer**、**show access-list**、**show object-group**
用于访问控制的策略分析器和优化器。	从管理中心：7.6.0 从 Security Cloud Control：7.2.0	任意	策略分析器和优化器评估冗余或影子规则等异常的访问控制策略，并采取措施修复已发现的异常。 您可以直接从版本 7.6 以上的防火墙管理中心启动访问控制策略分析与优化器；这需要思科安全云。对于版本 7.2-7.4 的防火墙管理中心，请使用Security Cloud Control。 新增/修改的屏幕： • 要启用：**集成 (Integration)** > **思科安全云 (Cisco Security Cloud)** > **启用策略分析器和优化器 (Enable Policy Analyzer & Optimizer)** • 要分析策略：**策略 (Policies)** > **访问控制 (Access Control)**，选择策略，点击**分析策略 (Analyze Policies)**。
用于修改访问控制策略和规则的精细权限。	7.4.0	任意	您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。 定义用户角色时，可以选择 **策略** > **访问控制** > **访问控制策略** > **修改访问控制策略** > **修改威胁配置** 选项，以允许在规则中选择入侵策略、变量集和文件策略，以及配置网络分析的高级选项和入侵策略、访问控制策略的安全智能策略配置以及策略默认操作中的入侵操作。您可以使用 **修改其余访问控制策略配置** 来控制编辑策略的所有其他方面的能力。包含“修改访问控制策略”权限的现有预定义用户角色继续支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
新的访问控制策略用户界面和规则冲突分析。	7.3.0	任意	7.2 中引入的访问控制策略用户界面现在为默认界面。您还可以启用规则冲突分析，以便帮助识别冗余规则和对象，以及识别由于策略中的先前规则而无法匹配的影子规则。
访问控制策略锁定。	7.2.0	任意	您可以锁定访问控制策略，以防止其他管理员对其进行编辑。锁定策略可确保在您保存更改之前，如果其他管理员编辑策略并保存更改，您的更改不会失效。任何有权修改访问控制策略的用户都有权锁定它。 我们在策略名称旁边添加了一个图标，用于在编辑策略时锁定或解锁策略。此外，还有一个允许用户解锁其他管理员锁定的策略的新权限：覆盖访问控制策略锁定。默认情况下，管理员、访问管理员和网络管理员角色启用此权限。
规则命中计数在重新启动后保持不变。	7.2.0	任意	重新启动托管设备不会再将访问控制规则命中计数重置为零。仅当您主动清除计数器时，才会重置命中计数。此外，高可用性对或集群中的每台设备单独维护计数。您可以使用 **show rule hits** 命令查看 HA 对或集群中的累计计数器，或查看每个节点的计数。 修改了以下设备 CLI 命令：**show rule hits**。
访问控制策略的可用性改进。	7.2.0	任意	有一个可用于访问控制策略的新用户界面。您可以继续使用旧版用户界面，也可以试用新的用户界面。新界面同时具有规则列表的表和网格视图、显示或隐藏列的功能、增强的搜索、无限滚动、与访问控制策略相关联的更清晰的数据包流视图，以及简化的用于创建规则的添加/编辑对话框。编辑访问控制策略时，可以在新旧用户界面之间自由切换。
DNS 过滤	7.0.0 6.7.0（实验性）	任意	如果启用并配置了 URL 过滤，则默认情况下会为每个新的访问控制策略启用一个新的选项，以用于增强类别和信誉过滤效率。 有关信息，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别，第 1798 页 和子主题。 访问控制策略的“高级”(Advanced) 选项卡在“常规设置”(General Settings) 下有一个新选项：**对 DNS 流量启用信誉实施 (Enable reputation enforcement on DNS traffic)**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
TLS 服务器身份发现	6.7.0	任意	在客户端连接到支持 TLS 1.3 的服务器时，启用访问控制策略以评估 URL 和应用条件。通过 TLS 服务器身份发现，无需解密流量即可对这些条件进行评估。 启用此功能可能会影响设备性能，但具体取决于型号。 访问控制策略的“高级”(Advanced) 选项卡页面具有新选项： • 警告会显示在“高级”(Advanced) 选项卡上；向右移动滑块可启用 TLS 服务器身份发现。 • “高级”(Advanced) 选项卡页面上的新选项：**TLS 服务器身份发现 (TLS Server Identity Discovery)**。
新的安全智能类别	-	任意	以下类别是在 6.6 版本时引入的，但并非特定于 6.6： • banking_fraud • high_risk • ioc • link_sharing • 广告的 • newly_seen • 间谍软件



第 40 章

安全智能

以下主题提供安全智能的概述，包括用于将流量和基本设置列入阻止名单和允许名单。

- 关于安全智能， 第 1729 页
- 安全智能许可证要求， 第 1730 页
- 安全智能的要求和前提条件， 第 1730 页
- 安全智能的最佳实践， 第 1730 页
- 安全情报准则和限制， 第 1731 页
- 安全智能来源， 第 1731 页
- 配置安全智能， 第 1732 页
- 安全智能监控， 第 1738 页
- 覆盖安全智能阻止， 第 1739 页
- 安全智能故障排除， 第 1740 页
- 安全智能阻止列表的历史记录， 第 1741 页

关于安全智能

作为防御恶意互联网内容的第一道防线，安全智能使用信誉智能快速阻止与IP地址、URL和域名的连接。这称为 列入安全智能阻止列表。

在系统执行需要更多资源的评估之前，安全智能是访问控制的第一阶段。使用阻止列表通过快速排除不需要检测的流量来提高性能。

注释 不能使用阻止列表阻止快速路径流量。预过滤器评估发生 在安全智能过滤之前。使用快速路径的流量会绕过所有的进一步评估，包括安全智能。

虽然您可以配置自定义阻止列表，但思科提供对定期更新的智能源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。

您可以使用“不阻止”列表和仅监控“阻止”阻止列表细化安全智能阻止列表。这些机制可以使流量免于列入阻止名单，但 **不会** 自动信任匹配流量或对其使用快速路径。 添加到 "不阻止 "列表中的流量或在安全智能阶段被监控的流量会被有意地与其他访问控制进行进一步分析。

相关主题

安全智能，第 2689 页

安全智能许可证要求

威胁防御 许可证

IPS

安全智能的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员



重要事项 您必须在设备上应用网络发现策略，才能成功应用 SI 策略。

安全智能的最佳实践

- 配置访问控制策略以阻止由思科提供的安全智能源所检测到的威胁。请参阅配置示例：安全智能阻止，第 1737 页。
- 如果要使用自定义威胁数据来补充思科提供的安全智能源，或手动阻止新出现的威胁：
  - 对于 IP 地址，请使用自定义安全智能列表和源，或者网络对象。要创建这些内容，请参阅安全智能，第 2689 页和网络，第 2658 页及其子主题。要将其用于安全智能，请参阅配置安全智能，第 1732 页。安全智能策略中使用的网络对象需要 IPS 许可证。

  - 对于 URL 和域，请使用自定义安全智能列表和源，而不是对象或组。请参阅手动 URL 过滤选项，第 1800 页中的详细信息
  - 您还可以将条目从事件添加到阻止列表。请参阅全局和域安全智能列表，第 2690 页。
- 要测试新源或被动部署，请将操作从阻止设为仅监控。请参阅安全智能监控，第 1738 页。
- 如果需要从安全智能阻止中排除特定站点或地址，请参阅覆盖安全智能阻止，第 1739 页。
- 如果您的 Cisco Secure Firewall 部署与思科安全云和思科 思科 XDR 集成，并且您使用自定义安全智能列表和提要，请确保使用这些列表和提要更新安全服务交换。有关详细信息，请参阅 安全服务交换 联机帮助中有关配置事件自动升级的说明。有关此集成的一般信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的与思科安全云集成 。
- 系统提供的安全智能类别可能会随着时间的推移而发生变化，恕不另行通知；您应该计划定期检查更改，并相应地修改策略。
- 您还应配置URL过滤，这是一项具有单独许可要求的单独功能，旨在进一步防御恶意站点。请参阅URL 过滤规则，第 1785 页。
- 要减少延迟和 CPU 开销，请避免在整个安全策略中引用单个大量 SI 源对象。相反，请利用自定义对象创建情报数据的较小型、有针对性的子集。
- 使用 URL/域源而不是 IP 阻止列表可以降低 CPU 开销，因为域过滤通常比管理大量 IP 阻止列表更高效且占用的资源更少。
- 通过将已知良好或重要合作伙伴 IP 地址添加到安全智能 (SI) 源中的“不阻止”列表中将受信任 IP 排除在外，有助于减少 CPU 开销，因为防火墙或安全设备会绕过对这些 IP 进行不必要的扫描和深度检查。

安全情报准则和限制

- 扫描 Firewall Threat Defense 故障排除文件时，包含检测签名或恶意软件 URL 的安全智能配置可能会导致错误的威胁警报。
- 如果从因信誉不佳而被阻止的 IP 地址发起 TCP 连接尝试，则会发送 TCP 重置 (RST) 数据包。这会导致连接立即终止，从而阻止 TCP 会话的建立并向发送方发出拒绝信号。

安全智能来源

- 系统-提供的源

  思科提供对定期更新的域名、URL 和 IP 地址的安全智能源的访问权限。有关详细信息，请参阅安全智能，第 2689 页。

  如果您看到名称中包含“TID”的源，则表明安全智能不会使用此源。相反，此源由威胁情报导向器，第 2411 页中所述的功能使用。

- 第三方源

  （可选）可以使用第三方信誉源（通常是 Secure Firewall Management Center定期从互联网下载的动态列表）补充思科提供的源。请参阅自定义安全智能源，第 2696 页。

- 自定义阻止列表或源（或对象）

  使用手动创建的列表或源来阻止特定 IP 地址、URL 或域名（对于 IP 地址，您还可以使用网络对象）。

  例如，如果您发现尚未被源阻止的恶意站点或地址，请将这些站点添加到自定义安全智能列表中，并将此自定义列表添加到访问控制策略的“安全智能”(Security Intelligence) 选项卡中的“阻止”列表。如自定义安全智能列表，第 2698 页和配置安全智能，第 1732 页中所述。

  对于IP地址，您可以选择使用网络对象而不是列表或源；有关信息，请参阅网络，第2658页。（对于 URL，强烈建议使用列表和源，而非其他方法。）

- 自定义不阻止列表或源

  优先于特定站点或地址的安全智能阻止。请参阅覆盖安全智能阻止，第 1739 页。

- 全局阻止列表（网络、URL 和 DNS 各一个）

  查看事件时，您可以立即将事件的IP地址、URL或域添加到适用的全局阻止列表，以便安全智能处理来自该源的未来流量。请参阅全局和域安全智能列表，第 2690 页。

- 全局不阻止列表（网络、URL 和 DNS 各一个）

  在查看事件时，如果您不希望安全智能阻止来自该源的未来流量，则可以立即将事件的 IP 地址、URL 或域添加到适用的全局不阻止列表。请参阅全局和域安全智能列表，第 2690 页。

配置安全智能

每个访问控制策略都具有安全智能选项。您可以将网络对象、URL 对象和列表以及安全智能源和列表列入阻止列表或不阻止列表，全部都可通过安全区域进行限制。您还可以将DNS策略与访问控制策略相关联，并将域名列入阻止列表或不阻止列表。

“不阻止列表”中的对象数加上“阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

开始之前

- 提示：有关最低配置建议的指南，另请参阅 配置示例：安全智能阻止，第 1737 页。
- 要确保所有选项可供选择，请向管理中心添加至少一个托管设备。
- 在被动部署中，或者如果要将安全智能过滤设置为仅监控，请启用日志记录；请参阅*Cisco Secure Firewall Management Center* 管理指南 中的使用安全智能记录连接。
- 配置 DNS 策略以对域执行安全智能操作。有关详细信息，请参阅安全情报 DNS 策略，第 2261 页。

过程

步骤 1 在访问控制策略编辑器中，点击**安全智能 (Security Intelligence)**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 您有以下选择：

- 点击 **网络** 以添加网络对象（IP 地址）。

  注释
  安全智能策略中使用的网络对象需要 IPS 许可证。

- 点击 **URL** 以添加 URL 对象。

步骤 3 查找要添加到“阻止”或“不阻止”列表的 **可用对象** 。您有以下选择：

- 通过在**按名称或值搜索 (Search by name or value)** 字段中输入内容，搜索可用对象。通过点击 **重新加载** (C) 或 **清除** (⊗) 来清除搜索字符串。
- 如果现有列表或源不满足需求，请点击 **添加** (+)，选择 **新建网络列表** 或 **新建 URL 列表**，然后继续操作，如 创建安全智能源，第 2697 页 或 将新的安全智能列表上传到 Secure Firewall Management Center，第 2698 页中所述。
- 如果现有对象不满足需求，请点击 **添加** (+)，选择 **新建网络对象** 或**新建 URL 对象**，然后继续操作，如 创建网络对象，第 2660 页中所述。

“安全智能”会忽略使用 `/0` 掩码的 IP 地址块。

步骤 4 在**可用对象**中选择一个或多个要添加的可用对象。

步骤 5 （可选）在**可用区域**中选择一个可用区域以按区域约束所选对象。

不能按区域限制系统提供的安全智能列表。

注释
SI的 **Any** 区域列表仅适用于属于安全区域的接口。但是，有一个例外是，如果设备没有与安全区域关联的任何接口，则 **Any** 区域将匹配任何接口。

例如，如果设备上有五个接口，但没有一个接口与安全区域相关联，则将根据设备上所有接口上的流量检查分配给 **Any** 区域的任何 SI 列表。如果将一个接口添加到该设备上的安全区域，它会有效地删除其他四个接口上的 SI 检查，其中 SI 列表的区域设置为 **Any** 。如果将其他四个接口添加到安全区域，它们将由附加到 **Any** 区域的 SI 列表进行评估。

步骤 6 点击 **添加到不阻止列表** 或 **添加到阻止列表**，或者点击所选对象并将其拖至任一列表。

要从阻止列表或不阻止列表中删除对象，请点击 **删除** (🗑) 。要删除多个对象，请选择这些对象并右键点击 **删除所选项**。

步骤 7 （可选）通过右键点击**阻止列表**下的对象，然后选择**仅监控**（**不阻止**），将列入阻止列表的对象设置为仅监控。

不能将系统提供的全域安全智能列表设置为仅监控。

步骤 8 从 **DNS 策略 (DNS Policy)** 下拉列表中选择 DNS 策略。

步骤 9 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

相关主题

安全智能，第 2689 页
Snort 重新启动场景，第 172 页

安全智能选项

使用访问控制策略编辑器中的“安全智能”(Security Intelligence) 选项卡配置网络（IP 地址）和 URL 安全智能，以及将访问控制策略与您在其中为域配置了安全智能的 DNS 策略相关联。

可用对象

可用对象包括：

- 由系统提供的源填充的安全智能类别。

  有关详细信息，请参阅安全智能类别，第 1736 页。

- 由系统提供的全局阻止和不阻止列表。

  有关说明，请参阅安全智能来源，第 1731 页。

- 在“对象”(Object) >“对象管理”(Object Management) >“安全智能”(Security Intelligence) 下创建的安全智能列表和源。

  有关说明，请参阅安全智能来源，第 1731 页。

- 在“对象”>“对象管理”下的相应页面上配置的网络和 URL 对象。这些对象与上一个项目符号中的安全智能对象有所不同。

  有关网络对象的详细信息，请参阅网络，第 2658 页。（对于 URL，请使用安全智能列表或源，而不是对象。）

  请注意，安全智能策略不支持范围和组网络对象类型。

可用区

除系统提供的全局列表之外，您可以按照区域限制安全智能过滤。

例如，为提高性能，您可能希望将实施目标限定在特定区域，而非所有接口。作为更具体的示例，您可以只阻止处理邮件流量的安全区域的垃圾邮件。

如要在多个区域上实施对象的安全智能过滤，对于每个区域，都必须将对象分别添加至阻止或不组织列表。

请注意，安全智能策略不支持范围和组网络对象类型。

DNS 策略

要使用安全智能来匹配 DNS 流量，您必须为安全智能配置选择 DNS 策略。

使用阻止或不阻止列表，或者根据 DNS 列表或源来监控流量还要求您：

- 配置 DNS 安全智能列表和源。请参阅安全智能，第 2689 页。
- 创建 DNS 策略。有关详细信息，请参阅创建基本 DNS 策略。
- 配置引用 DNS 列表或源的 DNS 规则。有关详细信息，请参阅创建和编辑 DNS 规则。
- 由于 DNS 策略部署为访问控制策略的一部分，因此必须将两个策略均进行关联。有关详细信息，请参阅DNS 策略部署。

不阻止列表

请参阅覆盖安全智能阻止，第 1739 页。

要选择列表中的所有对象，请右键点击对象。

阻止列表

请参阅 配置示例：安全智能阻止，第 1737 页 和本章中的其他主题。

有关阻止列表中的视觉指示的说明，请参阅阻止列表图标，第 1737 页。

要选择列表中的所有对象，请右键点击对象。

日志记录

启用安全智能日志记录（默认情况下处于启用状态）会记录由访问控制策略分配的设备处理的所有受阻和受监控的连接。然而，系统不会记录不阻止列表匹配项；对不阻止列表上的连接的日志记录取决于其最终性质。必须首先为阻止列表中的连接启用日志记录，然后才能将该列表中的对象设置为仅监控。

要启用、禁用或查看日志记录设置，请右键点击阻止列表中的对象。

相关主题

全局和域安全智能列表，第 2690 页
安全智能列表和多租户，第 2691 页

安全智能类别

安全智能类别由 安全智能，第 2689 页中所述的系统提供的源确定。

这些类别用于以下位置：

- 访问控制策略的“安全智能”选项卡上的“网络”子选项卡
- 访问控制策略的“安全智能”选项卡上“网络”选项卡旁边的 “URL” 子选项卡
- 在 DNS 策略配置页面的 DNS 选项卡上的 DNS 策略中
- 在流量与上述位置的阻止或监控配置匹配时生成的事件中

注释 如果您的组织使用 Cisco Secure Firewall 威胁智能导向器：查看事件时，您可能会看到指示 TID 已执行操作的类别，例如 `TID URL` 阻止。

类别由 Talos 从云更新，并且此列表可能会独立于 Firepower 版本进行更改。

表 *104:* 思科 *Talos* 智能小组 *(Talos)* 源类别

安全智能类别	说明
攻击者	出站恶意活动已知的活动扫描程序和主机
Banking_fraud	从事与电子银行相关的欺诈活动的网站
Bogon	Bogon 网络和未分配的 IP 地址
Bots	托管二进制恶意软件丢弃程序的站点
CnC	托管僵尸网络的命令和控制服务器的站点
加密货币挖矿活动	提供对用于挖掘加密货币的池和钱包的远程访问的主机
Dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法
Exploitkit	指定用于识别客户端中的软件漏洞的软件包
High_risk	根据来自安全图的 OpenDNS 预测安全算法进行匹配的域和主机名
IOC	观察到涉及危害表现 (IOC) 的主机
Link_sharing	未经许可共享版权文件的网站
恶意	表现出不一定属于另一种更精细的威胁类别的恶意行为的站点
恶意软件	托管恶意软件二进制或漏洞包的站点

安全智能类别	说明
Newly_seen	最近注册或尚未通过遥测发现的域。 **注意** 目前，此类别没有任何有效的源，已预留以供将来使用。
Open_proxy	允许匿名 Web 浏览的开放代理
Open_relay	已知用于垃圾邮件的开放邮件中继
网络钓鱼	托管网络钓鱼页面的站点
解决方案	主动参与恶意或可疑活动的 IP 地址和 URL
垃圾邮件	已知用于发送垃圾邮件的邮件主机
间谍软件	已知包含、提供或支持间谍软件和广告软件活动的网站
可疑	看似可疑并具有类似于已知恶意软件的特征的文件
Tor_exit_node	已知为 Tor Anonymizer 网络提供出口节点服务的主机

阻止列表图标

以下可视指示器可能会显示在访问控制策略的“安全智能”(Security Intelligence) 选项卡上的阻止列表中：

图标或可视指示灯	说明
阻止图标（）	对象被设为阻止。
监控（）	对象被设为仅监控。 请参阅 安全智能监控，第 1738 页
对象以删除线文本显示	同一对象也位于不阻止列表中，该列表将覆盖该阻止。

配置示例：安全智能阻止

配置访问控制策略以阻止系统定期更新的安全智能源可检测到的所有威胁。

“阻止列表”中的对象数加上“不阻止列表”中的数量不能超过 125 个 网络对象或 32767 个 URL 对象和列表。

开始之前

- 要确保所有选项可供选择，请向管理中心添加至少一个托管设备。

- 配置 DNS 策略以阻止域的所有安全智能威胁类别。有关详细信息，请参阅安全情报 DNS 策略，第 2261 页。
- 如果您拥有或将要拥有要阻止的实体的自定义列表，请创建每种类型（URL，DNS，网络）的安全智能对象。请参阅安全智能，第 2689 页。

过程

步骤 1 请点击 **策略** > **安全策略** > **访问控制**。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在访问控制策略编辑器中，点击**安全智能 (Security Intelligence)**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 点击**网络 (Networks)** 为 IP 地址添加阻止条件。

a) 在网络列表中向下滚动并选择全局列表下方列出的所有威胁类别。
b) 如果适用，请选择要阻止这些威胁的安全区域。
c) 点击 **添加到阻止列表 (Add to Block List)**。
d) 如果您创建的自定义列表或源具有要阻止的地址，请使用与上述相同的步骤将这些地址添加到阻止列表。

步骤 5 点击 **URL** 以添加 URL 的阻止条件，然后重复您对网络执行的步骤。

步骤 6 从 **DNS 策略**下拉列表中选择 DNS 策略；请参阅DNS 策略概述。

步骤 7 点击**保存**。

下一步做什么

- 为这些连接启用日志记录；请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的使用安全智能记录连接。
- 部署配置更改；请参阅 部署配置更改，第 180 页。
- 要获得额外保护，请配置 URL 过滤以阻止恶意 URL。请参阅URL 过滤规则，第 1785 页。

安全智能监控

监控会记录那些本应被安全智能阻止的流量的连接事件，但不会阻止流量。监控对于以下情况尤其有用：

- 在实施源之前对其进行测试。

考虑一下这样的情况，在使用第三方源实施阻止之前，想要先对该源进行测试。将源设置为仅监控时，系统允许已被阻止的连接，以便系统能对其进行进一步的分析，但是也会记录这些连接中的每一个连接，以供进行评估。

- 被动部署，以优化性能。

  被动部署的托管设备无法影响流量；与将系统配置为阻止流量相比，没有任何优势。此外，因为阻止的连接实际上在被动部署中并未被阻止，因此，系统可能针对每条已阻止连接报告多个连接开始事件。



注释 如已配置，Cisco Secure Firewall 威胁智能导向器 可能会影响所采取的行动（监控或阻止）。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 2433 页。

要配置安全智能监控：

按照配置示例：安全智能阻止，第 1737 页中的说明配置安全智能阻止后，右键点击阻止列表中的每个适用对象，然后选择**仅监控 (Monitor-only)**。 不能将系统提供的安全智能列表设置为仅监控。

覆盖安全智能阻止

或者，您可以使用“不阻止”列表来避免特定域、URL 或 IP 地址被安全智能列表或源阻止。

例如，您可以：

- 在信誉良好的安全智能源中覆盖偶尔的误报阻止
- 深入检查特定流量，而不是根据信誉来提前阻止流量
- 根据区域豁免其他受限事务的安全智能阻止

  例如，您可以将分类不当的URL加入“不阻止”列表中，但随后使用您的组织中需要访问这些 URL 的人员所使用的安全区域来限制“不阻止”列表对象。这样，只有有业务需要的人员才能访问“不阻止”列表中的 URL。



注释 “不阻止”列表中的条目只是阻止列表中的例外项。通过安全智能策略的任何连接都受访问控制规则的约束。因此，访问控制规则或入侵策略随后可以阻止“不阻止”列表中的条目。您的“不阻止”条目应始终是阻止列表的例外项。

过程

步骤 1 选项 1：将事件中的 IP 地址、URL 或域添加到“全局不阻止列表”。请参阅全局和域安全智能列表，第 2690 页。

步骤 2 选项 2：使用自定义安全智能列表或源。

a) 创建自定义安全智能列表或源。请参阅自定义安全智能列表，第 2698 页或创建安全智能源，第 2697 页。

b) 对于 IP 地址（网络）和 URL：编辑访问控制策略，点击“安全智能”(Security Intelligence)选项卡，然后点击“网络”(Networks) 或“URLs”子选项卡中的自定义列表或源，然后点击**添加到不阻止列表 (Add to Do Not Block List)**。

c) 保存更改。

d) 对于域 (DNS)：请参阅安全智能选项，第 1734 页主题中的“DNS 策略”部分。

e) 部署更改。

安全智能故障排除

请参阅以下有关安全智能故障排除的主题。

可用选项列表中缺少安全智能类别

症状：在访问控制策略的“安全智能”(Security Intelligence) 选项卡上，“可用选项”(Available Options) 下的“网络”(Networks) 选项卡中不会显示安全智能类别（例如 CnC 或漏洞攻击包）。

原因：

- 在管理中心至少添加一个托管设备之前，这些类别不会显示。您必须添加一个设备才能提取所有 TALOS 源。
- URL 过滤功能使用的类别集与安全智能功能有所不同；；您期望看到的类别可能是 URL 过滤类别。要查看 URL 过滤类别，请查看访问控制规则中的 **URLs** 选项卡。

安全智能阻止列表的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
新的安全智能类别	全部	任意	Talos 添加了以下新的安全智能类别： • banking_fraud • ioc • high_risk • link_sharing • 广告的 • newly_seen • 间谍软件 您应更新访问控制和DNS策略以应对新类别，并定期检查将来的更改。 新增/修改的页面：安全智能选项卡、网络和URL子选项卡； DNS策略中的 DNS 规则 支持的平台： 防火墙管理中心



第 41 章

访问控制规则

以下主题介绍如何配置访问控制规则。

- 关于访问控制规则， 第 1743 页
- 访问控制规则的要求和先决条件， 第 1754 页
- 访问控制规则的准则与限制， 第 1754 页
- 应用控制的最佳实践， 第 1755 页
- 访问控制规则的最佳实践， 第 1758 页
- 管理访问控制规则， 第 1763 页
- 访问控制规则的示例， 第 1777 页
- 访问控制规则的历史记录， 第 1781 页

关于访问控制规则

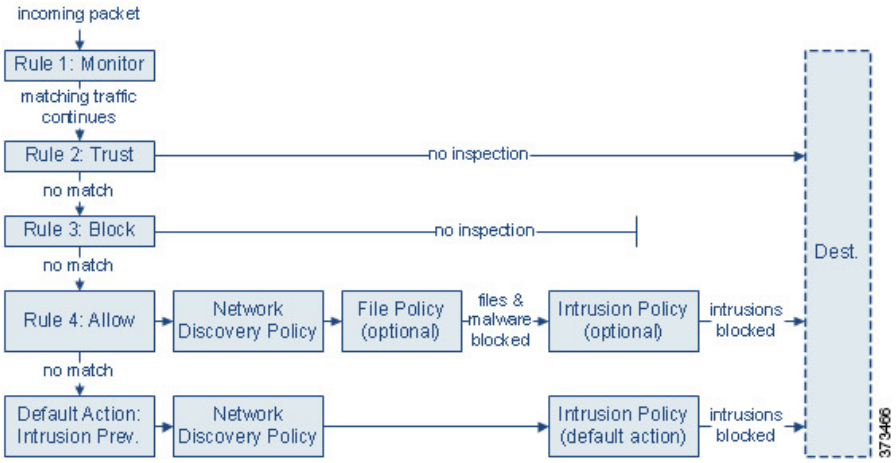
在访问控制策略中，访问控制规则提供在多台托管设备之间处理网络流量的精细方法。

注释 安全智能过滤、解密、用户标识以及某些解码和预处理发生在访问控制规则评估网络流量之前。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。

每个规则也有操作，确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在这种情况中，流量评估如下：

- **规则 1：监控** 首先评估流量。“监控”规则跟踪和记录网络流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。（但是，请参阅访问控制规则监控操作，第 1748 页中的重要例外情况和警告。）
- **规则 2：信任** 继续评估流量。系统允许匹配的流量传至目标，而无需进一步检查，但此类流量仍会受到身份要求和速率限制的制约。不匹配的流量继续根据下一规则进行评估。
- **规则 3：阻止** 第三步，评估流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据最终规则进行评估。
- **规则 4：允许**是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。系统允许其余未阻止的非恶意流量传至目标，但此类流量仍受到身份要求和速率限制的制约。您可以配置只执行文件检查、入侵检查或两类检查都不执行的“允许”(Allow) 规则。
- **默认操作**处理不匹配任何规则的所有流量。在此场景下，默认操作在允许非恶意流量通过之前执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。（您不能对默认操作处理的流量执行文件或恶意软件检测。）

无论是使用访问控制规则还是默认操作，您允许的流量都自动可用于根据网络发现策略检查主机、应用和用户数据。尽管可以增强或禁用发现功能，但不能明确启用该功能。但是，允许流量不会自动确保收集发现数据。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

请注意，当解密配置允许已加密流量通过或者您不配置解密时，访问控制规则处理已加密流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

访问控制规则管理

访问控制策略编辑器的规则表格让您可以添加、编辑、分类、搜索、过滤、移动、启用、禁用、删除或以其他方式管理当前策略中的访问控制规则。

正确创建和排序访问控制规则是一项复杂的任务，但重要的是构建有效部署。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。

使用搜索栏来过滤访问控制策略规则列表。您可以取消选择**仅显示匹配规则 (Show Only Matching Rules)** 选项以查看所有规则。匹配的规则会被突出显示。

对于每个访问控制规则，策略编辑器显示其名称、条件概述、规则操作以及传达规则检测选项或状态的图标。这些图标代表：

- 时间范围选项（）
- 入侵策略（）
- 文件策略（）
- 日志记录（）
- 警告（）
- 错误（）
- 规则冲突 （）

已禁用的规则在规则名称后面呈灰色显示并带有相应的标记“（已禁用）”(disabled)。

要创建或编辑规则，请参阅创建和编辑访问控制规则，第 1764 页。



提示 右键点击菜单提供很多规则管理选项的快捷方式，包括编辑、删除、移动、启用和禁用。

相关主题

访问控制规则组成部分，第 1745 页
访问控制规则的最佳实践，第 1758 页

访问控制规则组成部分

除唯一名称之外，每个访问控制规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

系统已对访问控制策略中的规则进行编号，从 1 开始。如果正在使用策略继承，则规则 1 是最外层策略的第一条规则。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

规则也可属于某个部分和某个类别，其仅有利于组织且不影响规则位置。规则位置跨越部分和类别。

部分和类别

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织访问控制规则，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。

如果正在使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。

条件

条件指定规则处理的特定流量。条件可以简单也可以复杂；条件的使用通常取决于许可证。

流量必须满足规则中指定的所有条件。例如，如果应用条件指定了 HTTP 而不是 HTTPS，则 URL 类别和信誉条件将不适用于 HTTPS 流量。

适用时间

您可以指定规则生效的日期和时间。

操作

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。系统不会对受信任、被阻止或加密的流量进行深度检查。

检查

深度检查选项管理系统如何检查和阻止您意外允许的恶意流量。通过规则允许流量时，可以指定系统先使用入侵或文件策略检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。一般来说，您可以在连接开始和/或结束时记录会话。您可以将连接记录到数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器。您可以按应用和协议记录会话，然后将这些日志转发到事件管理解决方案以进行进一步分析。

备注

每次保存对访问控制规则所做的更改时，都可以添加注释。

相关主题

访问控制规则的最佳实践，第 1758 页
访问控制规则管理，第 1745 页
创建和编辑访问控制规则，第 1764 页
访问控制规则操作，第 1748 页
访问控制规则条件，第 1766 页
使用文件和入侵策略的深度检测，第 1750 页
访问控制规则注释

访问控制规则顺序

系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。除监控规则，在流量匹配规则后系统不会根据其他优先级较低的规则继续评估流量。

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性”(Mandatory) 规则部分和“默认”(Default) 规则部分。要进一步组织，您可以在“强制性”(Mandatory) 和“默认”(Default) 部分中创建自定义规则类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

如果使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory) 规则部分与“默认”(Default) 规则部分之间。规则 1 是最外层策略（不是当前策略）中的第一条规则，系统跨策略、部分和类别分配规则编号。

允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动和修改访问控制规则。但是，可以创建自定义角色来限制用户移动和修改规则。允许修改访问控制策略的任意用户可以将规则添加到自定义类别，以及无限制的修改其中的规则。

注意 未能正确设置访问控制规则可能会导致意外结果，包括允许应阻止的流量。通常，应用控制规则应在访问控制列表中较低，因为与基于 IP 地址的规则相比，匹配这些规则所需的时间更长。

使用 特定 条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则 之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本准则，才可优化性能，同时满足您的需求。有关具体提示，请参阅规则排序的最佳实践，第 1759 页。

访问控制规则操作

每个访问控制规则都具有用于确定系统如何处理和记录匹配流量的操作：您可以监控、信任、阻止或允许（执行或无需执行进一步检查）匹配流量。

访问控制策略的 默认操作 会处理不符合任何非 Monitor 访问控制规则条件的流量。

访问控制规则监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。

如果连接与监控规则匹配，则该连接匹配的下一个非监控规则应确定流量处理和任何进一步检查。如果没有其他匹配的规则，系统应使用默认操作。

但存在一个例外。如果监控规则包含第 7 层条件（例如应用条件），则系统将允许早期数据包通过并建立连接（或完成 SSL 握手）。即使连接应被后续规则阻止，也会发生这种情况；这是因为这些早期数据包不会根据后续规则接受评估。为了使这些数据包不会未经检查就到达目的地，您可以在访问控制策略的高级设置中为此目的指定入侵策略；请参阅在识别流量之前检查通过的数据包。在系统完成其第 7 层识别后，它就会将相应的操作应用于剩余会话流量。

访问控制规则信任操作

信任 (Trust) 操作允许流量通过，无需深度检查或网络发现。受信任的流量仍会受到身份要求和速率限制的制约。

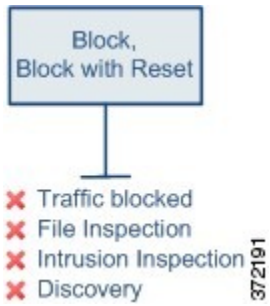


注释

- 某些协议（例如 FTP 和 SIP）会使用辅助信道，而系统会通过检测过程将其打开。在某些情况下，受信任的流量可以绕过所有检查，并且无法正确打开这些辅助通道。如果遇到此问题，请将信任规则更改为**允许 (Allow)**。
- 对于已禁用日志记录选项的信任规则，系统仍会生成流量结束事件。但是，在活动页面上看不到这些活动。
- 由于访问控制规则是在其他策略（如解密）之后进行评估的，因此信任一个连接并不一定意味着它可以快速通过而无需进行检查。例如，如果一个连接既符合需要解密的解密规则，又符合信任访问控制规则，那么在信任规则允许之前，就会对该连接进行必要的解密和检查。信任意味着不会进行额外的检查，如入侵检查。如果您打算允许连接不接受检查，则可以使用预过滤器策略来快速通过连接，或者确保没有其他策略对连接应用检查服务。

访问控制规则阻止操作

Block 和 **Block with reset** 操作拒绝流量，无需任何类型的进一步检测。



“阻止并重置”规则会重置连接，但 *HTTP* 响应页面遇到的 Web 请求除外。这是因为，如果立即重置连接，则配置为在系统阻止 Web 请求时显示的响应页面将无法显示。

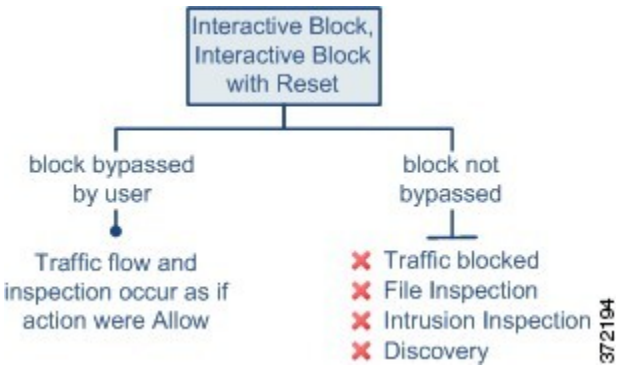
有关详细信息，请参阅配置 HTTP 响应页面，第 1801 页。

相关主题

配置 HTTP 响应页面，第 1801 页

访问控制规则交互式阻止操作

交互式阻止和**交互式阻止并重置**操作为 Web 用户提供继续访问其预期目的地的选项。



如果用户绕过阻止，该规则模拟“允许”规则。因此，您可以将交互式阻止规则与文件和入侵策略关联，并且匹配的流量也可用于网络发现。

如果用户未（或无法）绕过阻止，该规则模拟“阻止”规则。匹配流量会被拒绝，无需进一步检测。

请注意，如果启用交互式阻止，则无法重置所有被阻止的连接。这是因为，如果立即重置连接，响应页面将无法显示。使用**交互式阻止并重置**操作，以（通过非交互的方式）阻止并重置所有非 Web 流量，同时仍然为 Web 请求启用交互式阻止。

有关详细信息，请参阅配置 HTTP 响应页面，第 1801 页。

相关主题

基于规则的解密 规则阻止操作，第 1939 页

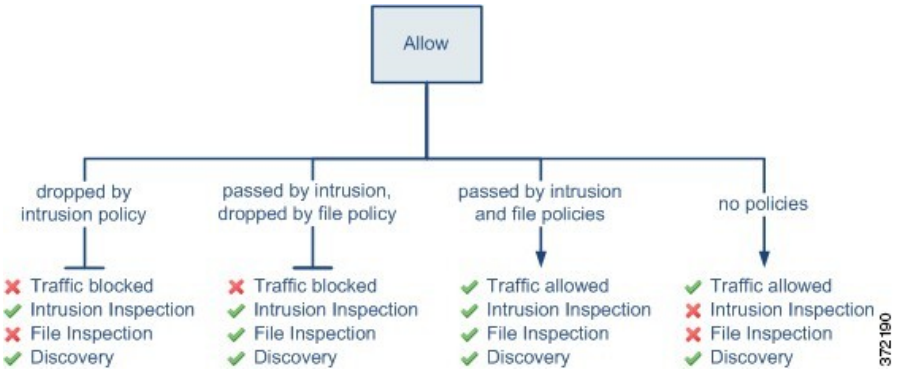
访问控制规则允许操作

允许 (Allow) 操作允许匹配的流量通过，但是仍会受到身份要求和速率限制的制约。

或者，您可以使用深度检查以在未加密或已解密流量到达目的地之前进一步对其进行检查和阻止：

- 您可以使用入侵策略，以便根据入侵检测和防御配置来分析网络流量，并根据配置丢弃恶意数据包。
- 您可使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。恶意软件防护 可检测文件中的恶意软件，并根据配置阻止检测到的恶意软件。

下图展示对满足“允许”(Allow) 规则（或用户绕过的“交互式阻止”[Interactive Block] 规则）条件的流量执行的检查类型。请注意，文件检测会在入侵检测之前发生；被阻止文件不会进行入侵相关漏洞检测。



为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，可以单独配置其中一个策略。如果没有文件策略，流量将由入侵策略确定；如果没有入侵策略，流量将由文件策略确定。

不管入侵或文件策略会检查还是丢弃流量，系统都可以使用网络发现功能进行检查。但是，允许流量不会自动确保发现检查。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

使用文件和入侵策略的深度检测

深度检测会将入侵策略和文件策略用作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。

  有关详细信息，请参阅关于入侵防御，第 1813 页。

- 文件策略监管系统的文件控制和恶意软件防护 功能。

  有关详细信息，请参阅网络恶意软件防护的文件策略，第 2283 页。

访问控制发生在深度检查之前；访问控制规则和访问控制默认操作确定哪些流量由入侵和文件策略检测。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。

注释 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

要将入侵策略和文件策略与访问控制规则相关联，请参阅：

- 访问控制规则：入侵策略选择，第 1820 页
- 配置访问控制规则以执行恶意软件保护，第 2291 页

文件和入侵检查顺序

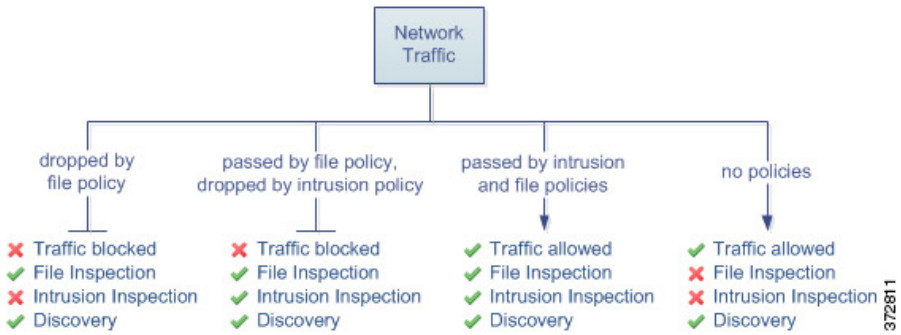
在您的访问控制策略中，您可以将多个 Allow 和 Interactive Block 规则与不同的入侵和文件策略相关联，以使检查配置文件匹配各种流量类型。

您不必在同一规则中同时执行文件和入侵检测。对于符合“允许”(Allow) 或“交互式阻止”(Interactive Block) 规则的连接：

- 没有文件策略，数据流取决于入侵策略
- 没有入侵策略，数据流取决于文件策略
- 若以上两者都没有，仅由网络发现检查允许的流量

提示 系统不会对受信任的流量执行任何种类的检测。虽然没有使用入侵或文件策略配置“允许”(Allow) 规则可以放行流量，就像“信任”(Trust) 规则那样，但“允许”(Allow) 规则让您可以对匹配的流量执行发现。

下图说明对符合“允许”(Allow) 或用户绕过的“交互式阻止”(Interactive Block) 访问控制规则的条件的流量执行的检查类型。为简单起见，该图显示入侵策略和/或文件策略与单个访问控制规则关联的情况的流量。



对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检测恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检测。

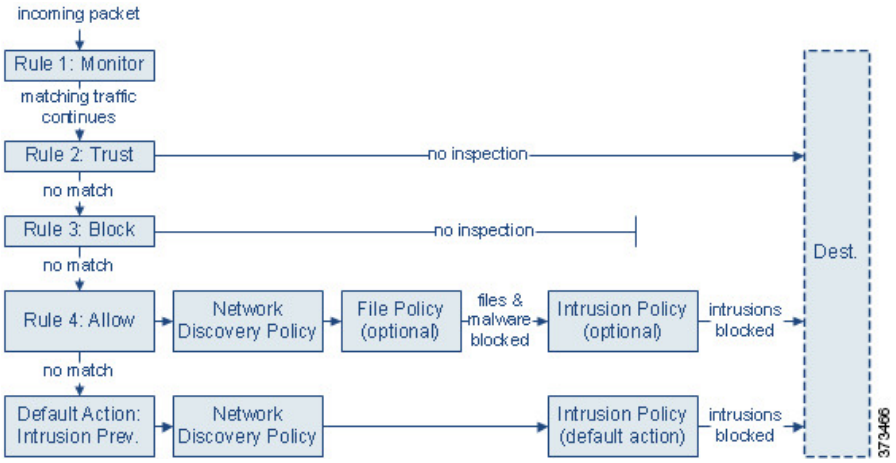
您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检测和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于会立即遭到阻止，因此这些文件既无法执行恶意软件检查也无法执行入侵检查。
- 接着，系统对下载到网络主机的 PDF 执行恶意软件云查找。具有恶意软件处置情况的任何 PDF 均被阻止，且不接受入侵检查。
- 最后，系统使用与访问控制规则关联的入侵策略检测任何剩余流量，包括文件策略未阻止的文件。

注释 在会话中的文件被检测并阻止之前，该会话的数据包可能会接受入侵检查。

使用入侵和文件策略的访问控制流量处理

下图显示一个内联入侵防御和恶意软件防护 部署中的流量，它受包含四种不同类型访问控制规则和默认操作的访问控制策略监管。



在上面的情景中，策略中的前三条访问控制规则 — Monitor、Trust 和 Block — 无法检查匹配的流量。Monitor 规则跟踪和记录但不检查网络流量，因此，系统继续将流量与其他规则进行匹配以确定是允许还是拒绝该流量。（但是，请参阅访问控制规则监控操作，第 1748 页中的重要例外情况和警告。）Trust 和 Block 规则处理匹配流量，无需任何何类型的进一步检查，不匹配的流量继续进入下一条访问控制规则。

策略中的第四个也是最后一条规则（Allow 规则）按照以下顺序调用各种其他策略以检查和处理匹配的流量：

- **发现：网络发现策略** - 首先，网络发现策略检查流量是否存在发现数据。发现是被动分析，并不影响流量的流动。尽管不显式启用发现，但您可以增强或禁用它。但是，允许流量不会自动确保收集发现数据。系统仅对涉及网络发现策略显式监控的 IP 地址的连接进行发现。
- **恶意软件防护 和文件控制：文件策略** - 通过发现功能检查流量后，系统可以检查其是否包含禁止文件和恶意软件。恶意软件防护 将检测并选择性地阻止多种文件中的恶意软件，包括 PDF、Microsoft Office 文档等。如果贵组织不仅要阻止传输恶意软件文件，还要阻止特定类型的所有文件（无论文件是否包含恶意软件），则 *file control* 可供您监控网络流量中特定文件类型的传输，然后阻止或允许文件。
- **入侵防御：入侵策略** - 在文件检查之后，系统可以检查流量中是否存在入侵和漏洞。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。
- **目标** - 通过上述所有检查的流量将传递到其目标。

“交互式阻止”(Interactive Block) 规则（未显示在图中）具有与“允许”(Allow) 规则相同的检查选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检测流量是否存在恶意内容。

在策略中不符合任何访问控制规则的流量，如果有监控以外的操作，则由默认操作来处理。在这种情况下，默认操作是入侵防御操作，只要流量由您指定的入侵策略进行传递，它就允许流量到达其最终目的地。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。请注意，系统可能检测默认操作允许的流量是否存在发现数据和入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注释 有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。然而，为了让这些数据包不会未经检查就到达目的地，您可以在访问控制策略的高级设置中指定一个入侵策略，以便检查这些数据包并生成入侵事件。

访问控制规则的要求和先决条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员
- 您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。包含“修改访问控制策略”权限的现有预定义用户角色支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。精细化权限包括：
  - **策略** > **安全策略** > **访问控制** 并选择**访问控制策略** > **修改访问控制策略** > **修改威胁配置**允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。如果用户只有此选项，则不能修改策略或规则的其他部分。
  - **修改剩余访问控制策略配置** 控制编辑策略所有其他方面的能力。

访问控制规则的准则与限制

- 当前页面一次最多可显示 1000 条规则。因此，如果您有大量规则，例如单个类别中有 3000 条规则，像选择类别中的所有规则并删除它们这样的操作不会删除所有规则。您可能需要再次选择/删除规则，以删除您要删除的所有规则。

- 如果编辑正在使用的访问控制规则，则更改不会在部署时应用于已建立的连接。此更新的规则用于根据未来的连接进行匹配。但是，如果系统正在主动检查连接（例如，使用入侵策略），则 会 将更改的匹配或操作条件应用于现有连接。

  对于 Firewall Threat Defense，您可以通过使用 Firewall Threat Defense **clear conn** CLI 命令结束已建立的连接，确保您的更改适用于所有当前连接。请注意，你应该只在结束这些连接是可以接受的情况下才这样做，前提是连接的来源将试图重新建立连接，从而与新规则进行适当的匹配。

- 访问规则中的 VLAN 标记仅适用于内联集；它们不能在应用于防火墙接口的访问规则中使用。
- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须在平台设置策略上配置适用于数据接口的 DNS。系统不使用管理 DNS 服务器设置查找访问控制规则中使用的 FQDN 对象。

  请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

  - 尽可能使用安全智能或 URL 过滤，而不是 FQDN 规则。
  - 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的 DNS 服务器。
  - 有些 FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

    建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备 DNS 缓存中已解析和可用地址的可能性很低。对于这些情况，请使用基于 URL 的规则，而不是 FQDN 网络对象规则。
  - 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的 DNS 服务器与您所配置的不同，基于 FQDN 的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
  - 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。
  - 如果超过 8 个 FQDN 解析为同一 IP 地址，则系统无法将流量可靠地匹配到这些 FQDN 的规则。每个 IP 地址最多可以处理 8 个 FQDN。

- 每个访问控制规则的每个匹配条件的最大对象数为 200。例如，单个访问控制规则中最多可以包含 200 个网络对象。

应用控制的最佳实践

以下主题讨论我们推荐的使用访问控制规则控制应用的最佳实践。

应用控制的建议

请牢记以下应用控制的准则与限制：

确保启用自适应分析

如果未启用（默认状态）自适应分析，访问控制规则将无法执行应用控制。

自动启用应用检测器

如果没有为要检测的应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

配置策略以检查在识别应用之前必须通过的数据包

在以下两种情况发生之前，系统无法执行应用控制：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。如果将访问控制规则配置为使用“应用默认端口”，则无需允许初始数据包通过即可实施应用规则。

如果早期流量与所有其他条件匹配，但应用识别未完成，系统会允许传递数据包，并允许建立连接（或允许 SSL 握手完成）。在系统完成其识别后，系统会将相应的操作应用于剩余会话流量。

要确保系统检查这些初始数据包，请在访问控制策略高级设置的**确定访问控制规则之前使用的入侵策略**选项中选择入侵策略。

了解识别应用的限制

服务器必须遵守应用的协议要求，这样系统才能识别该应用。例如，如果您有一台服务器在预期 ACK 时发送保持连接数据包而不是 ACK，则可能无法识别该应用，并且连接将不会匹配基于应用的规则。相反，它将由另一个匹配的规则或默认操作进行处理。这可能意味着您想要允许的连接会被拒绝。如果遇到此问题，并且无法修复服务器以遵循协议标准，则需要编写基于非应用的规则来覆盖该服务器的流量，例如，匹配 IP 地址和端口号。

为 URL 和应用过滤创建单独的规则

尽可能为 URL 和应用过滤创建单独的规则，因为组合应用和 URL 标准可能会导致非预期的结果，特别是对于加密的流量。

包括应用和 URL 标准的规则应位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。

将 URL 规则置于应用规则和其他规则之前

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

处理无负载的应用流量数据包

在执行访问控制时，对于在用于识别出应用的连接中没有负载的数据包，系统会应用默认策略操作。

处理关联应用流量

要处理由 Web 服务器所推荐的流量（如广告流量），请匹配被推荐应用（而非推荐应用）。

控制使用多个协议的应用流量（Skype、Zoho）

某些应用使用多个协议。要控制其流量，请确保访问控制策略能够涵盖所有相关选项。这些应用通常在每个可控制的环节中都包含应用名称。另请参阅特定于应用的说明和限制，第 1758 页。

控制规避应用流量

请参阅特定于应用的说明和限制，第 1758 页。

在应用匹配和端口匹配之间进行选择

在传统防火墙中，可以基于 OSI 第 3 层（协议）和第 4 层（传输层）（如 IP 或 TCP/80）匹配流量。然后，根据该规则的操作，允许或阻止给定端口（或整个协议）上的所有流量。

应用条件则对应 OSI 第 7 层。不同的应用可以使用同一个 TCP/UDP 端口。通过使用应用条件，您可以有选择地允许或阻止同一端口上的不同应用，而无需允许或阻止该端口上的所有应用。

在规则中使用基于端口的条件还是基于应用的条件，都会影响规则的性能。由于可以快速识别数据包中的 TCP/UDP 端口，系统可以在第一个数据包上匹配到正确的规则。使用应用层条件时，可能需要 3-5 个数据包才能识别特定应用（如果未同时指定端口）。

请考虑以下建议。

- 如果要对指定的接口和网络，以相同方式处理给定 TCP/UDP 端口上的所有流量，请使用基于端口的匹配。例如，要以相同方式处理所有 SSH 流量，请在“端口”选项卡上选择 SSH 端口 (TCP/22)。
- 如果要严格匹配与其他应用使用相同端口的特定应用，请在“应用”选项卡上选择该应用。这就是处理所有使用 TCP/80 或 443 端口的 Web 应用的方式，以便可以选择性地阻止或允许某些 Web 应用，而不影响所有 Web 应用。
- 如果要按用户组控制应用的使用，请在“用户”选项卡上选择用户组，然后在“应用”选项卡上选择应用。例如，您可以阻止承包商用户组成员使用游戏类应用。

  如果规则应适用于某一协议/端口的所有连接，也可以按用户组允许或阻止该协议/端口。
- 对于从不太安全的网络（如互联网）通往安全性较高的网络（如受保护的内部网络）的规则，请尽可能使用“端口”选项卡。例如，您可以允许或阻止从互联网到内部网络的 ICMP 流量。
- 避免在单个规则中同时指定“端口”选项卡和“应用”选项卡的参数。相反，选择某个应用时，应将“端口”选项卡留空，并在“应用”选项卡上将端口指定为**应用默认**端口。这样可将规则确定为正确的端口（每个应用），并加快将正确的应用与规则进行匹配的速度。

- 如果混合使用了基于端口和基于应用的规则，请将基于端口的规则在规则列表中靠前排列，以便首先将连接与这些规则进行匹配。识别协议和端口比识别应用更快。

特定于应用的说明和限制

- Office 365 管理门户 - 如果访问策略在连接开始和结束时均启用了日志记录，第一个数据包将被检测为 Office 365，而连接结束时将被检测为 Office 365 管理门户。这应当不会影响拦截。
- Skype - 要控制 Skype 流量，请从**应用过滤器**列表中选择 **Skype** 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- 为了完全检测 GoToMeeting，您的规则必须包含以下所有应用：
  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting 平台
  - LogMeIn
  - STUN
- Zoho - 要控制 Zoho 邮箱，请从“可用应用”列表中同时选择 **Zoho** 和 **Zoho 邮箱**。
- 对于规避类应用（如 Bittorrent、Tor、Psiphon 和 Ultrasurf），默认仅检测置信度最高的场景。如果需要对此流量（例如阻止或实施 QoS）采取措施，则可能需要配置效率更高、更为积极的检测。若要如此，请联系 TAC 审查您的配置，因为这些更改可能会导致误报。
- 如果您允许微信，则无法选择性地阻止微信媒体。
- 如果允许 RDP 应用但不允许文件传输，请确保 RDP 规则同时包含 TCP 和 UDP 端口 3389。RDP 文件传输会使用 UDP。

访问控制规则的最佳实践

正确配置和排序访问控制规则对于保护网络至关重要。以下主题总结了可最大限度提高规则性能和有效性的最佳实践。

注释 当部署配置更改时，系统会将所有规则共同进行评估，并创建分配的设备用于评估网络流量的扩展条件集。如果这些条件超过设备的资源（物理内存、处理器等），则您无法部署到该设备。

访问控制最佳实践

查看以下要求和一般最佳实践：

- 使用预过滤器策略为不需要的流量提供早期阻止，并为未受益于访问控制检查的流量提供快速路径。有关详细信息，请参阅快速路径预过滤器的最佳实践，第 2245 页。
- 虽然无需为部署提供许可也可配置系统，但许多功能要求您在部署之前，先启用适当的许可证。
- 访问控制规则在设备上部署为访问控制列表 (ACL)。为了最大限度地减少每个访问控制规则创建的访问控制条目数量，并提高整体性能，请为每台设备启用对象组搜索。对象组搜索是设备设置，而不是访问控制策略设置，因此您必须编辑每台设备以确保已启用该功能。有关详细信息，请参阅配置对象组搜索，第 919 页。
- 在部署访问控制策略时，其规则不会应用于现有连接。现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用策略规则，请清除现有连接会话，然后部署策略。
- 尽可能将多个网络对象合并为一个对象组。当您选择多个对象（分别用于源或目标）时，系统会自动创建对象组（在部署期间）。选择现有组可以避免对象组重复，并减少存在大量重复对象时对 CPU 使用率的潜在影响。
- 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向托管设备部署相关配置。

  有时，系统会阻止您将内联配置部署到被动部署的设备，包括分流模式下的内联设备。

  在其他情况下，策略可成功部署，但尝试使用被动部署的设备阻止或修改流量可能会出现意外结果。例如，由于受阻连接在被动部署中未被阻止，因此系统可为每个受阻连接报告多个连接开始事件。
- 某些功能（包括URL过滤、应用检测和速率限制）必须允许一些数据包通过，以便系统能够识别流量。
- 某些功能仅在特定设备型号上可用。警告图标和确认对话框会指出不支持的功能。
- 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。
- 访问控制规则的最佳实践，第1758页和子主题中详细介绍了创建、排序和实施访问控制规则的最佳实践。

规则排序的最佳实践

一般准则：

- 一般，将必须应用于所有流量的最优先规则靠近策略的顶部放置。
- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。

  否则，流量将首先匹配一般规则，而不会命中适用的特定规则。
- 仅基于第 3/4 层条件丢弃流量的规则（如 IP 地址、安全区和端口号）应尽早出现。基于这些条件的规则不需要通过检测来识别匹配的连接。

- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- URL 过滤、基于应用和基于地理位置的规则以及其他需要检查的规则应位于仅根据第 3/4 层条件（例如 IP 地址、安全区域和端口号）丢弃流量的规则之后，但在规则之前指定文件和入侵策略。
- 为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：
  - 它们包括应用条件。
  - 将对要检查的流量进行加密。
- 将 URL 过滤规则置于应用规则之上，并在应用规则之后加上微应用规则和通用工业协议 (CIP) 子分类应用过滤规则。
- 通常，包含应用条件的规则应位于访问控制列表的较下方，例如，与基于 IP 地址的规则相比，这些规则的匹配耗时更长。有关详细信息，请参阅在应用匹配和端口匹配之间进行选择，第 1757 页和应用控制的建议，第 1755 页。
- 指定文件策略和入侵策略的规则应位于规则顺序的底部。这些规则需要资源密集型深度检查，并且出于性能原因，您应首先使用强度较低的方法消除尽可能多的威胁，以便最大限度地减少需要深度检查的潜在威胁的数量。
- 始终应根据您的组织的需求对规则进行排序。

以下各节说明了上述准则的例外情况和补充内容。

应用程序规则顺序

通常，包含应用条件的规则应位于访问控制列表的较下方，例如，与基于 IP 地址的规则相比，这些规则的匹配耗时更长。

使用 特定 条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则 之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

有关详细信息，请参阅在应用匹配和端口匹配之间进行选择，第 1757 页和应用控制的建议，第 1755 页。

规则抢占

当一条规则由于评估中排序靠前的规则首先匹配流量而永远无法匹配流量时，会出现规则抢占问题。规则的条件控制其是否会抢占其他规则。在以下示例中，第二条规则无法阻止管理员流量，因为第一条规则会允许该流量：

访问控制规则 1：允许管理员用户
访问控制规则 2：阻止管理员用户

任何类型的规则条件均可以取代后续规则。第一条规则中的VLAN范围包含第二条规则中的VLAN，因此第一条规则抢占了第二条规则。要阻止 VLAN 27，您必须将该规则移到允许 VLAN 22-33 的规则上方。

访问控制规则 1：允许源网络 VLAN 22-33
访问控制规则 2：阻止源网络 VLAN 27

在以下示例中，规则 1 匹配所有 VLAN，因为没有配置 VLAN，因此规则 1 会取代尝试匹配 VLAN 2 的规则 2：

访问控制规则 1：允许源网络 10.4.0.0/16
访问控制规则 2：允许源网络 10.4.0.0/16，VLAN 2

规则还会抢占所有已配置条件均相同的相同后续规则：

访问控制规则 1：允许源网络 10.10.10.0/24 到 URL www.netflix.com
访问控制规则 2：允许源网络 10.10.10.0/24 到 URL www.netflix.com

如有任何条件不同，则后续规则不会被抢占：

访问控制规则 1：允许源网络 10.10.10.0/24 到 URL www.netflix.com
访问控制规则 2：允许源网络 10.10.11.0/24 到 URL www.netflix.com

规则操作和规则顺序

规则操作确定系统如何处理匹配的流量。通过将不执行也不确保进一步流量处理的规则置于会执行并确保进一步流量处理的资源密集型规则之前来提高性能。然后，系统可以转移可能已另外检查的流量。

以下示例显示在规则集中无任何规则更重要且抢占不是问题的情况下，可能如何在各种策略中对规则进行排序。

如果您的规则包括应用条件，另请参阅在应用匹配和端口匹配之间进行选择，第 1757 页。

访问控制规则的最佳顺序

入侵、文件和恶意软件检测需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更加如此。请将调用深度检查的访问控制规则放在最后。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。（但是，请参阅访问控制规则监控操作，第 1748 页中的重要例外情况和警告。）
2. 信任、阻止、阻止并重置 - 处理流量而不进一步检测的规则。
3. 允许，交互式阻止（无深度检查）- 不进一步检测流量，但是允许发现的规则。
4. 允许，交互式阻止（深度检查）- 与对禁止的文件、恶意软件和漏洞执行深度检查的文件或入侵策略关联的规则。

简化和集中规则的最佳实践

简化：不要过度配置

最小化单个规则条件。在规则条件中使用尽可能少的单独元素。例如，在网络条件中，使用 IP 地址块，而不是单独的 IP 地址。

如果一个条件足以匹配您想要处理的流量，请不要使用两个条件。使用冗余条件可能会大大扩展已部署的配置，这可能会导致设备性能问题以及集群和高可用性设备重新加入中的意外设备行为。例如：

- 请谨慎使用代表多个接口的安全区域。如果指定源和目标网络作为条件，并且这些条件足以匹配您的目标流量，则无需指定安全区域。
- 例如，如果要将一组内部接口与互联网上的任何目的地进行匹配，则只需使用包含内部接口的源安全区域。不需要网络或目标接口标准。

将元素组合到对象中**不**会提高性能。例如，使用包含 50 个 IP 地址的网络对象，与逐一将这些 IP 地址纳入条件中相比，只能给您带来组织优势，而不是性能优势。

有关应用检测的建议，请参阅在应用匹配和端口匹配之间进行选择，第 1757 页。

集中：更严格地限制资源密集型规则，尤其是按接口限制

尽可能使用规则条件以更严格定义资源密集型规则处理的流量。集中规则很重要的另一原因是，有着广泛条件的规则可能与许多不同类型的流量相匹配，并且可以抢占较为靠后、更为具体的规则。资源密集型规则的示例包括：

- 解密流量的TLS/SSL 规则 - 不仅解密，而且进一步分析已解密流量，也都需要资源。缩小集中范围，并尽可能阻止或选择不解密加密流量。

  某些 Firewall Threat Defense 模型在硬件中执行 TLS/SSL 加密和解密，这大大提高了性能。有关详细信息，请参阅TLS 加密加速，第 1849 页。

- 调用深度检查的访问控制规则 - 入侵、文件和恶意软件检查需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更是如此。确保只在必要时调用深度检查。
- 如果在规则中指定安全区域，该规则仅会部署到接口位于指定区域的设备上。因此，如果要将规则仅应用于分配给策略的某些设备，请确保选择适用于相应设备子集的安全区域。这可确保不会将不必要的规则部署到设备。

访问控制规则和入侵策略的最大数量

设备支持的访问控制规则或入侵策略的最大数量取决于许多因素，包括设备上的策略复杂度、物理内存以及处理器数量。

如果超出设备支持的最大值，您将无法部署访问控制策略，必须重新评估。

入侵策略的准则：

- 在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。
- 您可能希望整合入侵策略或变量集，从而能够将单个入侵策略/变量集对与多个访问控制规则相关联。在某些设备上，您可能会发现只能对所有入侵策略使用单个变量集，甚至对整个设备采用单个入侵策略-变量集对。

管理访问控制规则

以下主题介绍了如何管理访问控制规则。

添加访问控制规则类别

您可以将访问控制策略的“强制性”(Mandatory) 和“默认”(Default) 规则部分划分为自定义类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

过程

步骤 1 在访问控制策略编辑器中，点击**添加类别 (Add Category)**。

提示
如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键点击现有规则并选择 **Insert new category**。

步骤 2 输入 **Name**。

步骤 3 从**插入 (Insert)** 下拉列表中，选择要添加类别的位置：

- 要在某个部分中的所有现有类别下方插入类别，请选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 要在现有类别上方插入类别，请选择**类别上方 (above category)**，然后选择类别。
- 要在访问控制规则上方或下方插入类别，请选择**规则上方 (above rule)** 或**规则下方 (below rule)**，然后输入现有规则编号。

步骤 4 点击**应用 (Apply)**。

步骤 5 点击**保存**保存策略。

下一步做什么

现在，您可以：

- 将规则拖放到类别中或从类别中拖出。
- 创建规则时，请选择其所属的类别。
- 编辑规则时，请将规则重新定位到类别中，或者将其移出类别。

创建和编辑访问控制规则

使用访问控制规则将操作应用于特定流量类。规则允许您选择性地允许所需流量并丢弃不需要的流量。

开始之前

如果已启用策略分析器和优化器工具，系统会在您进行编辑时进行评估。如果检测到异常，则在编辑期间会收到通知，并在您点击“**应用**”保存规则时提示您进行更改。您可以查看异常（例如冗余和阴影规则），并选择编辑或删除规则。您还可以继续按原样保存规则，以便稍后处理问题。

过程

步骤 1 在访问控制策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击 **编辑** (✎)。
- 要从现有规则的副本开始，请从 **更多** (⋮) 菜单中选择以下命令之一。
  - **复制规则 (Copy Rule)**，将规则复制到剪贴板，以便可以使用 “**上方粘贴**”/“**下方粘贴**” 命令将其放置在同一策略中的任何位置。
  - **复制规则到其他策略** - 将该规则复制到另一个访问控制策略。系统将打开一个对话框，以便您选择目标策略并确定规则的放置位置。
  - **克隆规则**，以在复制规则的正下方创建副本。
- 要编辑多个规则，请使用复选框选择多个规则，然后从搜索框旁边的**选择操作/批量规则操作**列表中选择**编辑**或其他操作。
- 要执行内联编辑（更改规则条件中的对象配置），请右键点击该值并选择 **编辑**。您还可以使用右键点击菜单删除项目，将其添加到过滤器或复制文本或值。

如果规则旁显示**视图** (👁)，则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 如果这是新规则，请输入 **名称**。

步骤 3 配置规则组成部分。

如果批量编辑多个规则，则只有一部分选项可用。

- 位置：指定规则位置（新规则选择**插入**位置，现有规则使用规则名称旁的**重新定位**图标）；请参阅访问控制规则顺序，第 1747 页。
- **操作**：选择规则**操作**；请参阅访问控制规则操作，第 1748 页。
- **高级日志记录**：点击**高级日志记录**，为应用感知和协议感知事件日志选择协议。有关详细信息，请参阅关于应用 程序感知事件日志记录 *Cisco Secure Firewall Management Center* 管理指南 。

  注释
  当访问控制策略高级设置中启用了**高级日志记录**功能时，此选项可用。请参阅 启用应用感知事件日志记录，位于 *Cisco Secure Firewall Management Center* 管理指南 中。

- **日志记录**：点击**日志记录**，指定连接日志记录和 SNMP 陷阱的选项。相同的日志设置可以在默认 **操作配置 (Default Action Configuration)**配置 对话框（导航路径：编辑访问控制策略。在**“默认操作”(Default Action)** 区域中，点击 **默认日志记录和检测 (Default logging and inspection)** 图标 (**齿轮**（ ）) 。

  有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南 中的连接日志记录最佳实践。

  注释
  您可以集成 Splunk 或任何 SIEM 系统日志服务器，以直接从 防火墙管理中心 或其托管设备接收连接事件。如果您在 Splunk 配置中已将防火墙管理中心配置为连接事件源，请在**将连接事件发送至**下选择 **防火墙管理中心**。如果您已将Firewall Threat Defense配置为连接事件源，请选择至少一个目标地址。有关 Splunk 配置程序，请参阅 *Cisco Secure Firewall Management Center* 管理指南。

- **时间范围**：（可选。）对于 Firewall Threat Defense 设备，请选择规则适用的日期和时间。如果不选择选项，则规则始终处于活动状态。有关详细信息，请参阅创建时间范围对象，第2702 页。
- **启用规则**：规则是否处于活动状态。禁用的规则不会应用于连接。您可以禁用规则以暂时将其关闭（例如，在故障排除期间）。
- **安全保护**（深度检测）：（可选。）对于允许和交互阻止规则，选择 **入侵策略**， **变量集** 和 **文件策略** 选项。您可以单独应用入侵和文件策略；您不需要同时配置两者。
- 条件：选择要添加到源或目标的对象，然后点击**添加到源**或**添加到目标**以添加匹配的连接条件。您可以点击选项卡将可用对象列表限制为“网络”、“安全区域”、“应用”等。但是，无论您在哪个选项卡上，源和目标列始终显示所有选定的对象。有关详细信息，请参阅访问控制规则条件，第 1766 页。
- **注释**：打开对话框底部的注释列表，输入您的注释，然后点击**添加注释/发布**以添加注释。

步骤 4 点击**添加 (Add)** 或**应用 (Apply)** 保存规则。点击**应用并添加新规则 (Apply and Add New Rule)** 让对话框保持打开，以便创建新规则。

步骤 5 点击**保存** 保存策略。

下一步做什么

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅时区，第 1031 页。

部署配置更改；请参阅部署配置更改，第 180 页。

相关主题

访问控制规则的最佳实践，第 1758 页

访问控制规则条件

规则条件定义要使用每条规则作为目标的连接的特征。精确使用条件来微调规则，以应用于仅应由规则处理的流量。以下主题介绍可使用的匹配条件。

安全/隧道区域规则条件

可以使用安全区域和隧道区域为规则选择流量。

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。隧道区域允许您识别应作为隧道处理的隧道流量（例如 GRE），而不是将访问控制规则应用于隧道内的封装连接。

您可以使用安全区域按源接口和目标接口控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出，以匹配规则。正如安全区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

使用隧道区域时，请确保预过滤器策略中有匹配的规则，以将隧道流量与该区域相关联。然后，您可以选择隧道区域作为规则中的源区域；隧道区域不能是目的地。如果没有将隧道重新分区到隧道区域的预过滤器规则，则隧道的访问控制规则将永远不会应用于任何连接。您可以将目标安全区域指定为通过特定接口离开设备的目标隧道。

安全区域注意事项

在决定安全区域标准时，请考虑以下事项：

- 尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。
- 访问控制规则会在设备配置中生成 ACL 条目 (ACE)，以便尽可能提供早期处理和丢弃。如果在规则中指定安全区域，则会为区域中的每个接口创建 ACE，这会大大增加 ACL 的大小。从访问控制规则生成的过大 ACL 可能会影响系统性能。

网络规则条件

网络规则条件是定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请将条件添加到源列表。
- 要将流量匹配到某个 IP 地址或地理位置，请将条件添加到目标列表。

- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。

  尽可能将多个网络对象合并为一个对象组。当您选择多个对象（分别用于源或目标）时，系统会自动创建对象组（在部署期间）。选择现有组可以避免对象组重复，并减少存在大量重复对象时对 CPU 使用率的潜在影响。

  您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。然而，访问控制策略中的以下部分不支持 FQDN 对象：原始客户端网络、SGT/ISE 属性、网络分析和入侵策略、安全智能、威胁检测、大象流设置。

- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

网络条件中的原始客户端（过滤代理流量）

对于某些规则，可以根据始发客户端处理代理流量。使用源网络条件指定代理服务器，然后添加原始客户端限制以指定原始客户端 IP 地址。系统将使用数据包的 X-Forwarded-For (XFF)、真实客户端 IP 或自定义的 HTTP 标头报头字段来确定原始客户端 IP。

如果代理的 IP 地址与规则的源网络限制匹配，**并且**原始客户端的 IP 地址与规则的原始客户端限制匹配，则流量与规则匹配。例如，要允许来自特定原始客户端地址的流量，但仅允许其中使用特定代理的流量，请创建三条访问控制规则：

访问控制规则 1：阻止来自特定 IP 地址 (209.165.201.1) 的代理流量

源网络：209.165.201.1
原始客户端网络：无/任意
Action: Block

访问控制规则 2：允许来自同一 IP 地址的代理流量，但只允许其代理服务器为您所选的代理服务器（209.165.200.225 或 209.165.200.238）的流量

源网络：209.165.200.225 和 209.165.200.238
原始客户端网络：209.165.201.1
Action: Allow

访问控制规则 3：阻止来自同一 IP 地址但使用任何其他代理服务器的代理流量。

源网络：任意

原始客户端网络：209.165.201.1
Action: Block

VLAN 标记规则条件



注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

用户规则条件

根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

您只能为 Microsoft Active Directory 领域中的用户配置用户规则条件。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联，第 1719 页中所述。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅 应用检测器基础知识，第 2564 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *105:* 应用特征

特征	说明	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

配置应用条件和过滤器

要构建应用条件或过滤器，请从可用应用列表中选择要控制其流量的应用。或者，可以按照建议使用过滤器限制可用应用。在相同条件下可以使用过滤器和单独指定的应用。

开始之前

- 必须在访问控制策略的高级设置中启用自适应分析（其默认状态），访问控制规则才能执行应用程序控制。

过程

步骤 1 在访问策略规则编辑器中，点击**应用程序**。

步骤 2 从**可用应用 (Available Applications)** 列表查找并选择要添加的应用。

要限制**可用应用 (Available Applications)** 中显示的应用，请选择一个或多个**应用过滤器 (Application Filters)** 或搜索单个应用。

提示
点击应用旁边的 **信息**( ) 以显示摘要信息和互联网搜索链接。**锁**图标标记系统只能在已解密流量中识别的应用。

选择过滤器（单一或组合）时，“可用应用”(Available Applications) 列表会更新为仅显示符合条件的应用。您可以选择系统提供的组合形式的过滤器，但不能选择用户定义的过滤器。

- 针对同一特征选择多个过滤器（风险、业务关联性等）- 应用流量必须仅匹配其中一个过滤器。例如，如果选择中风险和高风险过滤器，则“可用应用”(Available Applications) 列表会显示所有中风险和高风险应用。
- 针对不同应用特征选择过滤器 - 应用流量必须与两个过滤器类型匹配。例如，如果您选择高风险和低业务关联性过滤器，则“可用应用”(Available Applications) 列表仅显示满足这两个条件的应用。

步骤 3 点击**添加应用 (Add Application)** 或**添加到规则 (Add to Rule)**，或进行拖放操作。

提示
在添加更多过滤器和应用之前，点击**清除过滤器/选择**以清除当前选择。

步骤 4 如果在“端口”选项卡上未指定目标端口，请为应用选择**端口**。

端口规格适用于列表中的所有应用；不适用于任何过滤器。无法为每个应用指定不同的“端口”选项。如果您已在“端口”选项卡上指定了目标端口，则该选择会反映在应用列表中，且无法进行以下选择。

如果尚未为规则指定目标端口，请选择以下选项之一：

- **应用默认** - 系统仅在评估流量以匹配应用时查看默认端口。点击信息按钮 (i)，查看每个应用的默认端口。

编辑规则时，如果规则已包含源端口，且您添加了具有不兼容端口的应用并选择“应用默认端口”，系统会发出警告。如果选择使用应用默认端口，不兼容的源端口会被删除。

- **任意** - 系统不根据连接中使用的端口来限制应用标识。如果“端口”选项卡上指定了源端口，则可能需要选择此选项才能保存规则。

无论选择哪个选项，如果后续在“端口”选项卡上配置了任何目标值，则“端口”选项卡上指定的端口会覆盖此处的选择，并将应用端口更改为“任意”。如果要将规则限制为非应用默认端口的一个、多个或一个范围的端口，请使用“端口”选项卡。

此选项不适用于自定义检测器。

注释
如果访问控制策略分配给运行 7.x 版本的设备，且规则中包含具有不同默认端口的应用，则规则的处理方式会有所不同。当您选择仅将规则应用于默认端口时，对于 7.7 系统，该规则会拆分为单独的规则，每个应用对应一条规则。对于运行 7.3-7.6 版本的系统，规则仍为单条规则，但“端口”页面会更新为每个默认端口。如果您管理的设备运行较低版本的软件，且希望使用默认端口匹配，建议将每条规则中的应用列表限制为具有相同默认端口的应用。

步骤 5 保存或继续编辑规则或配置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标记。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 Firewall Threat Defense设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- 解密 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅关于使用类别和信誉进行 URL 过滤，第 1786 页。

动态属性规则条件

动态属性包括：

- （源或目标。）动态对象（例如来自 dynamic attributes connector）

  dynamic attributes connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Secure Firewall Management Center 以便将它们用于访问控制规则中。

  有关dynamic attributes connector的详细信息，请参阅《关于 dynamic attributes connector，第 2325 页》。

- （仅源。）安全组标记 (SGT) 对象，包含手动定义或通过 ISE 定义的标记。有关更多信息，请参阅《源和目标安全组标记 (SGT) 匹配，第 2080 页》和《安全组标记，第 2649 页》。
- （仅源。）位置 IP 对象 由Cisco ISE定义
- （仅源。）设备类型对象，由（也称为终端配置文件）Cisco ISE定义。

动态属性可用作访问控制规则中的源条件和目标条件。使用以下准则：

- 不同类型的对象通过 AND 连接在一起
- 将相似类型的对象一起进行 ORd 运算

例如，如果选择源目标条件 SGT 1、SGT 2 和设备类型 1；如果在 SGT 1 或 SGT 2 上检测到设备类型 1，则规则匹配。例如，如果同时选择安全组标记和列出 IP 地址的动态对象，如果带有 标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

时间和日期规则条件

您可以指定连续时间范围或周期性时间段。

例如，规则只能在工作日工作时间或每个周末或节假关闭期间应用。

基于时间的规则基于处理流量的设备的本地时间应用。

基于时间的规则仅在 Firewall Threat Defense 设备上受支持。如果将具有基于时间的规则的策略分配给不同类型的设备，则在该设备上会忽略与该规则关联的时间限制。在这种情况下，您将看到警告。

启用和禁用访问控制规则

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。

您还可以使用规则编辑器启用或禁用访问控制规则。

过程

步骤 1 在访问控制策略编辑器中，右键点击规则并选择规则状态。

如果规则旁显示**视图** ( )，则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

从一项访问控制策略复制访问控制规则

您可以将访问控制规则从一个访问控制策略复制到另一个访问控制策略。您可以将规则复制到访问控制策略的**默认 (Default)** 部分或**强制 (Mandatory)** 部分。

已复制规则的所有设置（注释除外）都将保留在粘贴的版本中。

过程

步骤 1 执行以下操作之一：

- 要复制单个规则，右键点击规则并选择**将规则复制到不同策略**。
- 要复制多个规则，选中它们的复选框，然后从**选择批量操作**菜单中选择**将规则复制到不同策略**。

步骤 2 从**访问策略 (Access Policy)** 下拉列表中选择目标访问控制策略。

步骤 3 从**放置规则 (Place Rules)** 下拉列表中，选择要放置所复制规则的位置。您可以将它们放在“强制”或“默认”部分的顶部或 底部。

步骤 4 点击**复制 (Copy)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

将访问控制规则移至预过滤策略

您可以将访问控制规则从访问控制策略移至关联的非默认预过滤器策略。

您必须先将用户定义的预过滤器策略应用于访问控制策略。无法将访问控制规则移至默认的预过滤器策略，因为默认预过滤器策略不能包含规则。

开始之前

请在继续之前注意以下条件：

- 在将访问控制规则移至预过滤策略 时，无法移动访问控制规则中的第 7 层 (L7) 参数（例如应用程序或 URL 过滤）。L7 参数会在操作期间被丢弃。
- 在移动规则后，访问控制规则配置中的注释会丢失。但是，移动的规则中会添加一条新注释，其中提及了源访问控制策略。
- 您不能移动将**监控 (Monitor)** 设置为**操作 (Action)** 参数的访问控制规则。
- 移动时，访问控制规则中的**操作 (Action)** 参数将更改为预过滤器规则中的适当操作。要了解访问控制规则中的每个操作，请参阅下表：

访问控制规则中的操作	预过滤器规则中的操作
允许	分析
阻止	阻止
阻止并重置	阻止

访问控制规则中的操作	预过滤器规则中的操作
交互式阻止	阻止
交互式阻止并重置	阻止
信任	快速路径

- 同样，根据访问控制规则中配置的操作，在移动规则后，日志记录配置会被设置为适当的设置，如下表中所述。

访问控制规则中的操作	在预过滤器规则中启用日志记录配置
允许	未选中任何复选框。
阻止 阻止并重置 交互式阻止 交互式阻止并重置	• 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱
信任	• 在连接开始时记录 • 在连接结束时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱

- 从源策略移动规则时，如果其他用户修改了这些规则，您将看到一条消息。您可以在刷新页面后继续该过程。

过程

步骤 1 执行以下操作之一：

- 要移动单个规则，请右键点击该规则并选择**将规则移至预过滤策略**。
- 要移动多个规则，请选中其复选框，然后从**选择批量操作**菜单中选择**将规则移至预过滤策略**。

步骤 2 从**放置规则**下拉列表中，选择要放置移动规则的位置（**位于底部**或**位于顶部**）：

步骤 3 点击 **移动**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

定位访问控制规则

您可以移动访问控制策略中的现有规则，或在所需位置插入新的规则。将某条规则添加或移动到某个类别时，系统会将其置于该类别的末尾。

开始之前

查看访问控制规则的最佳实践，第 1758 页中的规则顺序准则。

过程

步骤 1 执行以下操作之一：

- 新规则 - 将鼠标悬停在现有规则之间的行上，然后点击**添加规则**即可插入新规则。在“添加规则”对话框的**插入**框中选择位置；您可以选择其他规则来调整位置。您还可以从右键点击菜单中选择**在上面添加规则 (Add Rule Above)** 或**在下面添加规则 (Add Rule below)**。
- 查看规则表时的现有规则 - 点击规则并将其拖动到新位置。此操作是最终的，系统不会提示您进行确认。
- 查看规则表时的现有规则 - 右键点击单个规则，然后选择**重新定位规则 (Reposition Rule)**。要将多个规则作为一个组移动，请选中其复选框，然后从**选择批量操作 (Select Bulk Action)** 菜单中选择**重新定位规则 (Reposition Rules)**。系统会提示您选择规则的目标位置。
- 编辑规则时的现有规则 - 点击规则名称旁边的**重新定位规则 (Reposition Rule)** 图标。

步骤 2 编辑或重新定位规则时，选择要移动或插入规则的位置，然后点击**移动**、**确认**或**重新定位**（具体取决于您在执行的操作）。

- 选择**插入强制性类别 (into Mandatory)** 或**插入默认类别 (into Default)**。
- 选择**插入强制性类别 (into Mandatory)**，然后选择类别。
- 选择**规则上方**或**规则下方**，然后选择规则。

步骤 3 如果正在编辑规则，请保存该规则。

步骤 4 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

将注释添加到访问控制规则

创建或编辑访问控制规则时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

保存规则时，自上次保存所做的所有注释都将变为只读。

要搜索访问控制规则注释，请使用规则列表页面上的“搜索规则”(Search Rules) 栏。

过程

步骤 1 在访问控制规则编辑器中，点击**注释 (Comments)**。

步骤 2 输入注释，然后点击**添加备注 (Add Comment)**。您可以在保存规则之前编辑或删除此注释。

步骤 3 保存规则。

访问控制规则的示例

以下主题提供了访问控制规则的示例。

如何使用安全区域来控制访问

假设在某个部署中，您希望主机对互联网具有不受限制的访问权限，但是仍然通过检测传入流量是否存在入侵和恶意软件来保护这些主机。

首先，创建两个安全区域：内部和外部。然后，将一个或多个设备上的接口对分配到这些区域，每个对中的一个接口位于内部区域，另一个接口位于外部区域。在内侧连接至网络的主机代表您的受保护资产。



注释 您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。

然后，配置访问控制规则，其中目标区域条件设置为“内部”(Internal)。此简单规则与从内部区域中的任何接口传出设备的流量相匹配。要检查匹配流量中是否存在入侵和恶意软件，请选择规则操作**允许 (Allow)**，然后将该规则与入侵和文件策略相关联。

如何控制应用的使用

Web 已成为企业交付应用（无论是基于浏览器的应用平台，还是使用 Web 协议传入和传出企业网络的富媒体应用）普遍使用的平台。

Firewall Threat Defense通过检查连接确定使用的应用。这样即可写入针对应用的访问控制规则，而不只是针对特定的 TCP/UDP 端口。因此，即使使用相同的端口，也可以选择性地阻止或允许基于 Web 的应用。

虽然可以选择要允许或阻止的特定应用，但也可以基于类型、类别、标记、风险或业务相关性写入规则。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

在此使用案例中，我们将阻止属于**匿名程序/代理**类别的任何应用。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**，然后编辑访问控制策略。

步骤 2 点击**添加规则**并配置应用控制规则。

a) 为该规则指定一个有意义的名称，例如 Block_Anonymizers。

b) 对于**操作 (Action)**，选择**阻止 (Block)**。



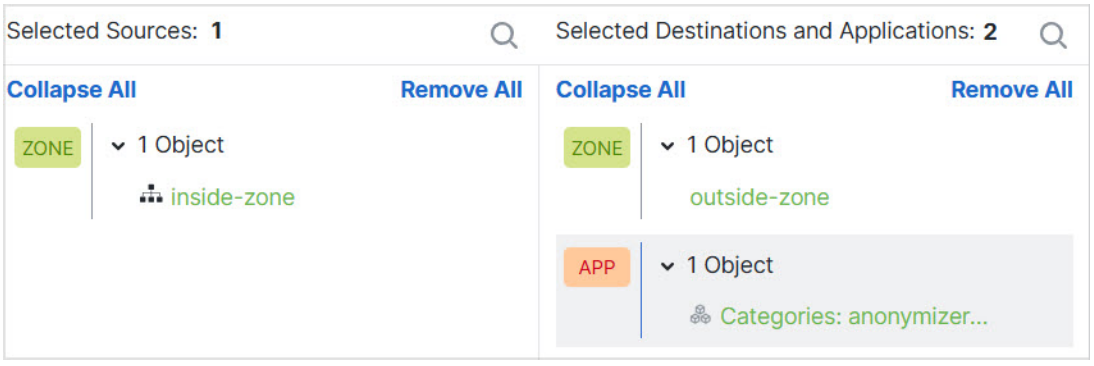
c) 假设您已配置区域，并希望将此规则应用于从内部到外部的流量，请选择**区域 (Zones)** 选项卡，然后选择内部区域作为源区域，选择外部区域作为目标区域。

d) 点击**应用 (Applications)** 选项卡，选择要匹配的应用，然后点击**添加应用 (Add Application)**。

在选择条件（例如类别和风险级别）时，条件右侧的列表会更新，从而准确显示哪些应用与条件匹配。您要编写的规则将应用到这些应用中。

仔细查看此列表。例如，您可能会希望阻止风险极高的所有应用。但是，截至本文撰写之时，TFPT 被归为风险极高类别。而大多数组织不想阻止该应用。请花些时间测试各种过滤条件，以查看哪些应用符合您的选择。请注意，这些列表可能随着每次 VDB 更新而变化。

在本例中，从“类别”(Categories) 列表中选择匿名程序/代理，并将其添加到“目标和应用”(Destinations and Applications)。匹配条件现在应如下图所示。



注释

对于**端口**，保留默认值应用默认值。这样可确保系统仅查看用于所选应用的默认端口，而不是所有端口。

e) 点击规则操作旁边的**日志记录 (Logging)**，并在连接开始时启用日志记录。如果您使用系统日志服务器，则可以选择一个。

您必须启用日志记录选项卡才能获取与此规则阻止的任何连接相关的信息。

步骤 3 移动规则，使其位于任何仅使用协议和端口条件的规则后面，但不允许应由应用规则阻止的流量。

匹配应用需要进行 Snort 检查。由于仅使用协议和端口的规则不需要 Snort 检查，因此可以将这些简单规则尽可能地分组到访问控制策略的顶部，从而提高系统性能。

步骤 4 部署更改。

您可以使用应用规则命中计数和分析控制面板来查看此规则的执行情况，以及用户尝试这些应用的频率。

如何阻止威胁

通过将入侵策略添加到访问控制规则中，可以实施下一代入侵防御系统 (IPS) 过滤。入侵策略可分析网络流量，根据已知威胁比较流量内容。如果某个连接与您正在监控的威胁匹配，系统将丢弃该连接，从而阻止攻击。

处理所有其他流量后，才会检验网络流量中是否存在入侵。通过将入侵策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略检测流量。

您只能对**允许**流量的规则配置入侵策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。此外，如果不想使用简单阻止，您可以将入侵策略配置为默认操作。

除了检查允许的流量是否存在潜在入侵之外，您还可以使用安全智能策略来预先阻止所有传送至或来自已知不良 IP 地址，或传送至已知不良 URL 的流量。

此示例添加了一个允许内部 192.168.1.0/24 网络进入外部的入侵策略，并且假设您已经具有阻止规则来选择性地消除不需要的连接，同时还添加了一个安全智能策略来执行预先阻止。

开始之前

您必须将 IPS 许可证应用于使用此规则的任何托管设备。

此示例假定您已经为内部和外部接口创建了安全区域，并且为内部网络创建了网络对象。

过程

步骤 1 创建应用入侵策略的访问控制规则。

a) 在编辑访问控制策略师，点击**添加规则**。

b) 为规则指定一个有意义的名称（例如 Inside_Outside），并确保规则操作为**允许 (Allow)**。



c) 对于**入侵策略 (Intrusion Policy)**，选择“平衡安全和连接”(Balanced Security and Connectivity)。您可以接受默认变量集，也可以选择自己的变量集（如果要对其进行自定义）。

对于大多数网络，合适的策略是**平衡安全和连接**策略。它提供良好的入侵防御，而不会过度激进，有可能会丢弃可能不想被丢弃的流量。如果您确定要丢弃很多流量，可以选择**连接优先于安全**以放宽策略。

如果您需要积极关注安全性，请尝试**安全优先于连接**策略。**最大检测**策略更加重视网络基础设施的安全性，有可能对操作造成更大的影响。

如果您要创建自己的自定义策略，则可以改为选择该策略。

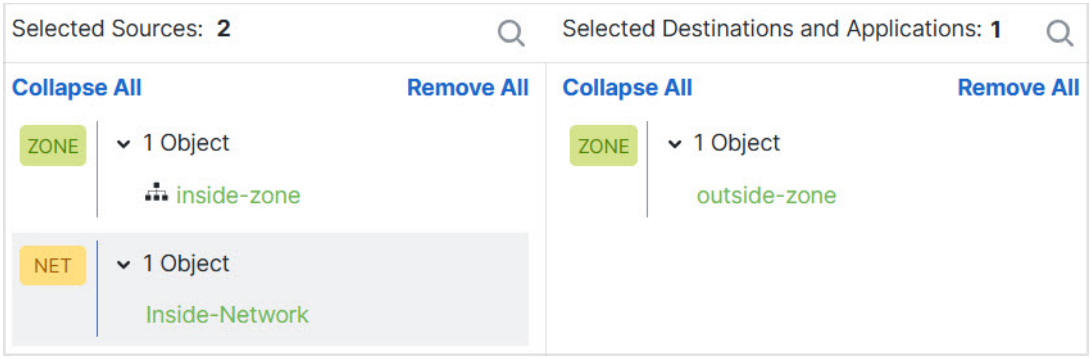
对变量集的讨论不在本示例的范围之内。有关变量集和自定义策略的详细信息，请阅读入侵策略章节。



d) 选择**区域 (Zones)** 选项卡，将内部安全区域添加到源条件，将外部区域添加到目标条件。

e) 选择**网络 (Networks)** 选项卡，并将定义内部网络的网络对象添加到源条件。

匹配条件应如下所示：



f) 点击**日志记录 (Logging)** 并根据需要在连接开始或结束时启用日志记录。

g) 点击**应用**保存规则，然后点击**保存**保存更新后的策略。

h) 将规则移至访问控制策略中的适当位置。

步骤 2 配置安全智能策略预先丢弃主机和站点已知不良的连接。

通过使用安全智能阻止连接属于已知威胁的主机或站点，为系统节省执行深度数据包检测，以识别每个连接中的威胁所需的时间。安全智能可提早阻止不必要的流量，为系统留出更多的时间来处理您真正关心的流量。

a) 在编辑访问控制策略时，点击数据包路径中的**安全智能 (Security Intelligence)** 链接。

该链接包括两个策略：顶部的 DNS 策略以及底部的安全智能（网络和 URL）。在本例中，我们将配置网络和 URL 列表。默认情况下，这些列表已包含全局阻止列表和不阻止列表，但在向其添加项目之前，这些列表都默认为空。

b) 选择**网络**并选择**任意**安全区域，在网络列表中向下滚动，直到您到达全局源和第一个安全智能类别（可能是攻击者）。点击“攻击者”(Attackers)，然后滚动到类别的末尾（可能是 Tor_exit_node），然后按住 Shift 键并点击以选择所有类别。点击**添加到阻止列表 (Add To Block List)**。

c) 选择 **URL** 选项卡和**任何**安全区域，然后使用 Shift +点击来选择相同类别的 URL 版本。点击**添加到阻止列表 (Add To Block List)**。

d) 点击**保存**保存策略。

e) 如有必要，您可以将网络和 URL 对象添加到阻止或不阻止列表。

不阻止列表不是真正的“允许”列表。它们是例外列表。如果例外列表中的地址或 URL 也出现在阻止列表中，系统允许该地址或 URL 的连接传递到访问控制策略。

通过这种方式，您可以阻止源，但如果您后期发现所需的地址或站点被阻止，可以使用例外列表来覆盖阻止，而不需要彻底删除源。

注意，这些连接随后由访问控制和入侵策略（如果已配置）评估。因此，如果任何连接包含威胁，这些连接将在入侵检查过程中被识别和阻止。

使用事件和控制面板来判断哪些流量实际上被策略丢弃，以及您是否需要在**不阻止**列表中添加地址或 URL。

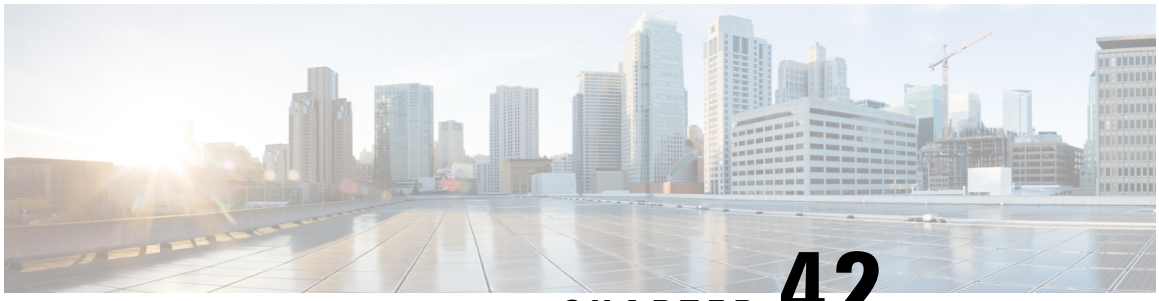
步骤 3 部署更改。

访问控制规则的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
基于应用的访问控制规则的默认端口规范。	10.0	10.0	向访问控制规则添加应用时，可以指定规则限于应用的默认端口。这与在“端口”选项卡上手动指定端口不同。也可以指定应用在任何端口上被识别，这是此增强功能之前系统的行为。 如果指定默认端口并且还在“端口”选项卡上进行指定，则“端口”选项卡会覆盖应用默认端口。您可以使用端口选项卡将规则限制为一个、多个或一系列端口。 升级后，现有的基于应用的规则继续应用于任何端口。如果要将这些规则限制为默认端口，必须编辑规则，清除“端口”选项卡上的所有规范，在“应用”选项卡上选择“应用默认端口”，然后保存规则。编辑所有要更改的规则后部署更改。 向访问控制规则添加应用时，添加了选择“应用默认”或“任何”端口的功能，只要“端口”选项卡上未配置任何内容。此选项不适用于任何类型的应用过滤器，也不适用于除访问控制规则之外的任何其他策略或对象。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
每个访问控制规则的每个匹配条件的最大对象数为 200。	7.3	任意	以前，单个访问控制规则中的每个匹配条件最多可以有 50 个对象。例如，单个访问控制规则中最多可以包含 50 个网络对象。现在，单个规则中的每个匹配条件的限制为 200 个对象。 我们更新了访问控制策略，以便允许添加对象限制。
搜索访问控制规则注释	6.7	任意	**搜索规则 (Search Rules)** 栏现在提供搜索注释的选项。 新增/修改的页面：访问控制规则页面、**搜索规则**文本输入字段。 支持的平台： 防火墙管理中心
在访问控制策略和预过滤器策略之间复制或移动规则。	6.7	任意	您可以将访问控制规则从一个访问控制策略复制到另一个访问控制策略。您还可以将访问控制规则从访问控制策略移至关联的预过滤器策略。 新增/修改的页面：访问控制策略页面；所选规则的右键点击菜单提供了用于复制和移动的其他选项。 支持的平台： 防火墙管理中心
批量编辑访问控制规则中的某些设置	6.6	任意	在策略中的规则列表中，按住 Shift 点击或按住 Control 点击可以选择多个规则，然后右键点击并选择一个选项。批量操作示例：您可以启用或禁用规则，选择规则操作，以及编辑大多数检测和日志记录设置。 新增/修改的页面：访问控制规则页面。 支持的平台： 防火墙管理中心
增强了对已配置规则的搜索	6.6	任意	增强了对已配置规则的搜索。 新增/修改的页面：访问控制规则页面。 支持的平台： 防火墙管理中心
规则应用的时间范围	6.6	任意	可以为要应用的规则指定绝对时间或循环时间或时间范围。规则会根据处理流量的设备的时区来应用。 新增/经修改的页面： • 访问控制“添加规则”(Add Rule) 页面上的新选项。 • **设备** > **平台设置** > **威胁防御**页面上的一个相关新选项，用于为托管设备指定时区。 支持的平台：仅限 Firewall Threat Defense 设备

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
从访问控制规则页面查看对象详细信息	pre-6.6	任意	要在规则列表中或从规则配置对话框中查看有关对象的信息，请右键点击该对象。 新/修改的页面：**策略** > **访问控制** > **访问控制**，以及**添加规则**页面。 支持的平台： 防火墙管理中心



CHAPTER 42

URL 过滤规则

您可以使用访问控制规则实施 URL 过滤。

- URL 过滤概述， 第 1785 页
- URL 过滤的最佳实践， 第 1787 页
- URL 过滤的许可证要求， 第 1793 页
- URL 过滤的要求和前提条件， 第 1793 页
- 如何使用类别和信誉配置 URL 过滤， 第 1793 页
- 手动 URL 过滤， 第 1799 页
- 配置 HTTP 响应页面， 第 1801 页
- 配置 URL 过滤运行状况监控器， 第 1805 页
- 争议 URL 类别和信誉， 第 1805 页
- 如果 URL 类别集发生更改，请执行操作， 第 1806 页
- URL 过滤故障排除， 第 1807 页
- URL 过滤的历史记录， 第 1810 页

URL 过滤概述

使用 URL 过滤功能控制网络上的用户可以访问的网站：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是建议选项。
- 手动 URL 过滤 - 通过任意许可证，可以手动指定单个 URL、URL 组以及 URL 列表和源，以实现对网络流量的精细、自定义控制。有关详细信息，请参阅手动 URL 过滤， 第 1799 页。

另请参阅安全智能， 第 1729 页，用于阻止恶意 URL、域和 IP 地址的类似但不同的功能。

URL 过滤功能仅适用于使用 Web 浏览器通过 HTTP/HTTPS 协议浏览网站的场景。对于其他应用，必须使用基于 FQDN 的访问控制规则，而非 URL 过滤。有关详细信息，请参阅访问控制规则。

关于使用类别和信誉进行 URL 过滤

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”类别，而 monster.com 属于“职位搜索”类别。

  URL 可以属于多个类别。

- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。信誉等级从未知风险（0 级）或不可信（1 级）到可信（5 级）。信誉根据完整的统一资源标识符 (URI) 确定，例如，www.cisco.com 上的不同页面可能具有不同的信誉。

基于类别和信誉的 URL 过滤的优势

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问控制来阻止黑客攻击类别中的高风险不可信的URL。或者，您可以使用 QoS 对来自流媒体视频流类别中站点的流量进行速率限制。也存在基于威胁类型的类别，例如间谍软件和广告软件类别。

使用类别和信誉数据可简化策略创建和管理。此方法可保证系统按预期控制网络流量。由于思科会不断更新有关新 URL 的威胁智能以及现有 URL 的新类别和新风险的信息，因此系统会使用最新信息来过滤所请求的 URL。代表安全威胁的站点或提供不良内容的站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下是一些系统如何适应的示例：

- 如果某个访问控制规则阻止所有游戏网站，在新域注册并分类为“游戏”时，系统则可以自动阻止这些站点。同样，如果 QoS 规则对所有流媒体视频流站点进行速率限制，则系统可自动限制流向新流媒体视频流站点的流量。
- 如果某个访问控制规则阻止所有恶意软件站点，而某个购物页面受到恶意软件感染，系统可以将来自该购物站点的 URL 重新分类为恶意软件站点，并阻止该站点。
- 如果访问控制规则阻止高风险不可信社交网站，但有人在其个人资料页面发布的链接中提供有指向恶意负载的链接，则系统便可以将该页面的信誉从良性站点可靠更改为高风险不可信，并阻止该网站。

解密策略 “不解密”规则中基于类别的过滤的限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅应用控制的建议，第 1755 页。

有关详细信息，请参阅在 URL 过滤中使用类别，第 1792 页。

URL 类别和信誉说明

类别说明

可从https://www.talosintelligence.com/categories中获取每个 URL 类别的说明。

要查看那些类别，请确保点击 **威胁类别** 。

信誉级别说明

转到 Web 信誉级别。

来自思科云的 URL 过滤数据

添加 URL 过滤许可证将自动启用启用 URL 过滤。允许根据网站的一般分类或 类别和风险级别或 信誉来进行流量过渡。

默认情况下，当用户浏览的URL的类别和信誉不在以前访问过的网站的本地缓存中时，系统会将其提交到云进行威胁情报评估，并将结果添加到缓存中。

或者，您可以使用类别和信誉的本地 URL 数据集，这可以加快 Web 浏览速度。当您启用（或重新启用）URL 过滤时， 防火墙管理中心 会自动向思科查询 URL 数据并将数据集推送到托管设备。然后，当用户浏览到某个URL时，系统会在将其提交到云进行威胁情报评估之前，检查本地数据集和缓存中的类别和信誉信息。要查看使用本地数据集的选项，包括如何完全禁用单个云查找，请参阅URL 过滤选项， 第 1795 页。

默认情况下，启用 URL 数据的自动更新；我们强烈建议您不要禁用这些更新。

注释 Cisco Secure Firewall Threat Defense 200 系列设备不在本地存储 URL 类别和信誉数据。它完全依赖浏览器缓存和基于云的查找来进行 URL 过滤和信誉评估。

URL 类别集可能会定期更改。当您收到更改通知时，请检查您的 URL 过滤配置，以确保按预期处理流量。有关详细信息，请参阅如果 URL 类别集发生更改，请执行操作， 第 1806 页。

URL 过滤的最佳实践

请记住以下的 URL 过滤的准则和限制：

按照类别和信誉过滤

请按照如何使用类别和信誉配置 URL 过滤， 第 1793 页 中的相关说明来操作。

配置策略以检查在可以识别 URL 之前必须通过的数据包

在满足以下情况之前，系统无法过滤 URL：

- 客户端与服务器之间建立受监控连接。

- 系统识别会话中的 DNS，HTTP 或 HTTPS 应用。
- 系统识别所请求的域或URL（对于加密会话，从一个非加密的域名、ClientHello 消息或服务器证书中获取）。

此识别应在 3 到 5 个数据包内发生，或者在 TLS/SSL 握手中的服务器证书交换（如果流量已加密）后发生。

重要提示！要确保您的系统检查否则会通过的这些初始数据包，请参阅在识别流量之前检查通过的数据包和子主题。

如果早期流量与所有其他规则条件都匹配，但是识别未完成，则系统允许数据包通过并建立连接（或完成 TLS/SSL 握手）。在系统完成其识别后，系统会将相应的规则操作应用于剩余会话流量。

阻止威胁类别

请确保您的策略专门处理威胁类别，以识别已知的恶意站点。除了阻止信誉不佳的站点之外，请执行此操作。

例如，要保护网络免受恶意站点的攻击，必须阻止所有威胁类别。此外，Talos 建议您仅阻止类别为“差”的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。

有关详细信息，请参阅URL 类别和信誉说明，第 1787 页中的 URL中的 **威胁类别** 。

URL 条件和规则顺序

- 将 URL 规则置于 必须 命中的所有其他规则之后。
- URL 可以属于多个类别。可以允许一个类别的网站并阻止另一个类别的网站，无论是明确地还是依赖于默认操作。在这种情况下，请确保创建 URL 规则并对其进行排序，从而获得预期效果，具体取决于允许还是阻止应优先。

有关规则的其他准则，请参阅以下主题：访问控制规则的最佳实践，第 1758 页。

未分类或无信誉的 URL

在构建 URL 规则时，首先应选择要匹配的类别。如果您明确选择 **未分类** URL，但不能通过信誉进一步限制。

具有“不受信任”信誉的未分类URL由 **恶意站点** 类别处理。如果要阻止具有任何其他信誉级别的未分类站点（例如“可疑”），则必须阻止所有未分类的站点。

选择类别和信誉级别后，可以选择 **应用到未知信誉**。例如，您可以创建应用于信誉不受信任，可疑和未知的站点的规则。

不能为 URL 手动分配类别和信誉，但在访问控制和 QoS 策略中，可以手动阻止特定 URL。请参阅手动 URL 过滤，第 1799 页。另请参阅争议 URL 类别和信誉，第 1805 页。

针对已加密 Web 网络流量的 URL 过滤

在对加密的 Web 网络流量执行 URL 过滤时，系统将：

- （如果已启用DNS过滤）检查系统之前是否已发现源域或该域在本地信誉数据库中，如果是，则根据域的信誉和类别执行操作。否则，即使已在访问控制策略的高级设置中启用**重试URL缓存缺失查找**，系统也会根据您的加密流量配置处理流量。
- 不考虑加密协议；如果规则包含URL条件，但不包含指定协议的应用条件，该规则将同时匹配HTTPS 和 HTTP 流量。
- 不使用 URL 列表。您必须改用 URL 对象和组。
- 根据用于加密流量的公钥证书中的使用者公用名匹配HTTPS流量，并评估事务期间随时提供的任何其他 URL（包括解密后的 HTTP URL）的信誉。
- 不考虑对象公用名内的子域。
- 不显示被访问控制规则（或任何其他配置）阻止的已加密连接的 HTTP 响应页面；请参阅对HTTP 响应页面的限制，第 1802 页。

URL 过滤和 TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和URL过滤条件，因此Firepower系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

访问控制策略高级设置提供用于 TLS 服务器身份发现的**增强的应用程序和 URL 检测**选项。

我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。解密策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。



注释

- TLS 服务器身份发现不能与以下任何一项配合使用：
  - STARTTLS 流量
  - HTTP CONNECT 方法
  - 已被网络上的其他设备解密的流量
- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由 Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。
- TLS 服务器身份发现也可在 TLS 1.2 会话上运行。

有关详细信息，请参阅TLS 服务器身份发现，第 2459 页。

HTPP/2

系统可从 TLS 证书提取 HTTP/2 URL，但无法从负载进行提取。

手动 URL 过滤

- 使用自定义安全智能列表或源对象指定 URL。请勿使用 URL 对象或直接在规则中输入 URL。有关详细信息，请参阅手动 URL 过滤选项，第 1800 页。
- 如果使用 URL 对象手动过滤特定 URL 或通过直接在规则中输入 URL，请仔细考虑可能会受到影响的其他流量。要确定网络流量是否与URL条件相匹配，系统执行简单的子字符串匹配。如果请求的 URL 与字符串的任何部分匹配，则认为该 URL 匹配。
- 如果使用手动URL过滤创建其他规则的例外情况，请将具有例外情况的特定规则置于本应适用的一般规则之上。

在 URL 中搜索查询参数

系统不使用 URL 中的搜索查询参数来匹配 URL 条件。例如，考虑这样一个场景：您阻止所有购物流量。在这种情况下，系统不会阻止使用网络搜索来搜索 amazon.com，但会阻止浏览至 amazon.com。

访问控制策略高级设置

除非有充分的理由进行更改，否则请在访问控制策略的“高级”选项卡上将以下设置保留为默认设置：

- **常规设置：**
  - **重试 URL 缓存缺失查询**
  - **对 DNS 流量启用信誉实施**

有关这些设置的说明，请参阅常规设置，第 2458 页。

减少不必要地使用连接表空间和 NAT 表插槽

考虑这样一个场景：启用 URL 过滤，并且阻止任何不符合 URL 过滤规则的流量。在这种情况下，Threat Defense 设备会分析流量中的初始数据包以提取 URL 信息。在分析后，如果流与任何 URL 过滤规则不匹配，则该流会被阻止。这意味着数据包将被 Threat Defense 设备丢弃。但是，关联连接仍保留在连接表中。此行为会导致不必要地使用连接表空间以及 NAT 表插槽（如果配置了 NAT），从而可能导致网络资源消耗增加。

有多种方法可以防止此类场景的发生。由于大多数流量为 TCP，因此您可以为 TCP 流量使用“阻止并重置”选项，而不是使用“阻止”。此方法可减少连接表空间和 NAT 表插槽的使用量。

高可用性部署中的 URL 过滤

有关使用高可用性中的 Firepower 管理中心进行 URL 过滤的准则，请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的 *URL* 过滤和安全智能。

所选设备型号的内存限制

- 内存较少的设备型号在本地存储较少的URL数据，因此系统可能会更频繁地检查云，以确定不在本地数据库中的站点的类别和信誉。

  内存较低的设备包括：

  - Firepower 1010
  - Firewall Threat Defense Virtual 配备 8 GB RAM

过滤 HTTPS 流量

要过滤加密流量，系统将根据TLS/SSL握手期间传递的信息确定请求的URL：用于加密流量的公钥证书中的使用者公用名。

HTTPS过滤与HTTP过滤不同，它不考虑使用者公用名称内的子域。在访问控制或QoS策略中手动过滤 HTTPS URL 时，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

提示 在 解密策略中，可以通过定义可分辨名称 解密策略 规则条件来处理和解密发送到特定 URL 的流量。证书的使用者可分辨名称中的公用名属性包含站点的 URL。通过解密 HTTPS 流量，访问控制规则可以评估解密的会话，从而改进 URL 过滤。

按加密协议控制流量

系统在访问控制或 QoS 策略中执行 URL 过滤时，不考虑加密协议（HTTP 与 HTTPS）。对于手动 URL 条件和基于信誉的 URL 条件均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com/
- https://example.com/

要配置仅与HTTP或HTTPS流量匹配的规则，请向该规则添加应用条件。例如，可以通过构造两个访问控制规则（每个规则具有应用和URL条件）来允许对某个站点进行HTTP访问，同时禁止HTTP访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
应用：HTTPS
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
应用：HTTP
URL：example.com

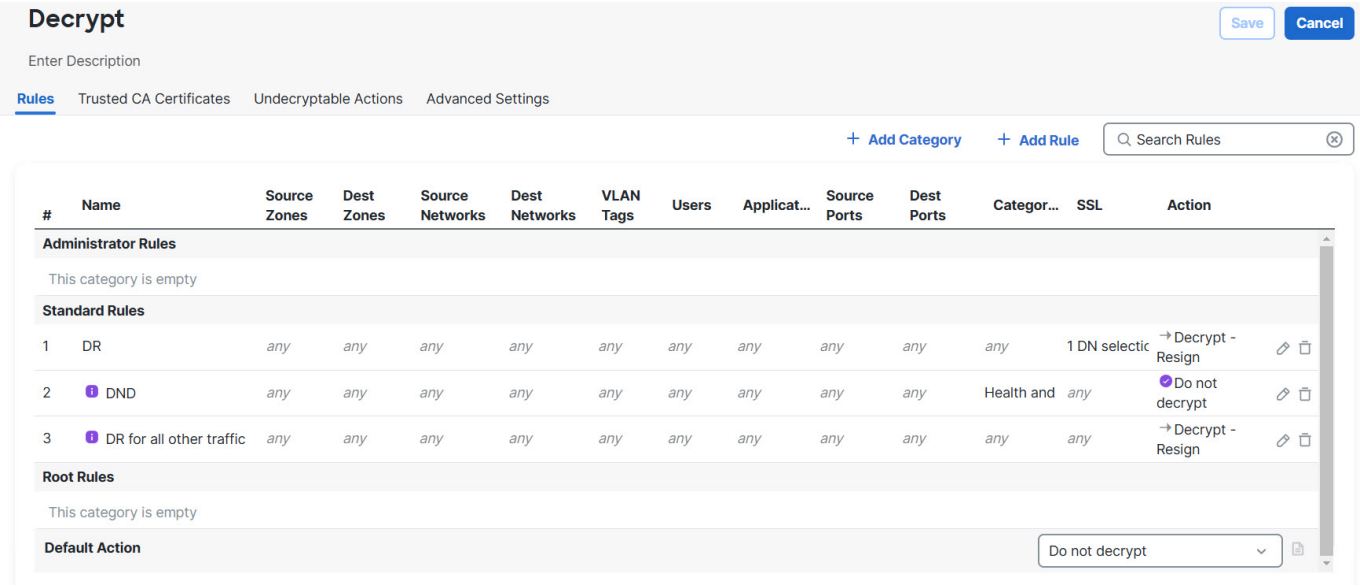
在 URL 过滤中使用类别

“不解密”规则中的类别限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用TLS/SSL解密的准则，第 1908 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅应用控制的建议，第 1755 页。

QUIC 指纹识别

Snort 可以根据 EVE 分析识别快速 UDP Internet 连接（QUIC 会话）中的客户端应用程序。有关详细信息，请参阅EVE 中的 QUIC 指纹识别，第 1959 页。

URL 过滤的许可证要求

威胁防御 许可证

- 类别和信誉过滤 - URL 过滤
- 手动过滤 - 无其他许可证。

威胁防御设备的 URL 过滤许可证

请参阅《Cisco Secure Firewall Management Center 管理指南》的 许可证一章中的 *URL* 许可证。

URL 过滤的要求和前提条件

型号支持

任意

Cisco Secure Firewall 200 不维护本地 URL 数据库。以下选项与此类设备无关，部署策略时会自动更改为“仅限云”查找：**启用自动更新**、**仅本地数据库**的URL查询源以及**本地数据库和思科云**选项。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

如何使用类别和信誉配置 URL 过滤

	相应操作	更多信息
步骤 1	确保拥有正确的许可证。	将 URL 过滤许可证分配给将过滤 URL 的每个托管设备。
步骤 2	确保防火墙管理中心可以与云通信以获取 URL 过滤数据。	*Cisco Secure Firewall Management Center* 管理指南中的互联网访问要求和通信端口要求。

	相应操作	更多信息
步骤 3	了解限制和准则并采取任何必要的措施。	URL 过滤的最佳实践， 第 1787 页
步骤 4	启用 URL 过滤功能。	使用类别和信誉启用 URL 过滤， 第 1794 页
步骤 5	配置规则以按类别和信誉过滤 URL。	配置 URL 条件， 第 1796 页 为了最好地防御恶意站点，您必须按信誉阻止站点，并阻止所有威胁类别中的 URL。 （选件）补充或选择性覆盖基于类别和信誉的 URL 过滤， 第 1801 页
步骤 6	（可选）允许用户能够通过点击忽略警告页面来绕过对网站的阻止。	配置 HTTP 响应页面， 第 1801 页
步骤 7	对规则进行排序，使流量首先命中关键规则。	URL 规则顺序， 第 1798 页
步骤 8	（可选）修改与URL过滤相关的高级选项。	通常，除非您有特定的原因需要更改默认值，否则请使用默认值。 有关高级选项的信息，包括以下内容，请参阅访问控制的高级设置， 第 2455 页。 • **要在连接事件中存储的最大 URL 字符数** • **允许交互式阻止绕过阻止的时长（秒）** • **重试 URL 缓存缺失查询** • **对 DNS 流量启用信誉实施**
步骤 9	部署更改。	部署配置更改， 第 180 页
步骤 10	确保系统按预期接收未来的URL数据更新	配置 URL 过滤运行状况监控器， 第 1805 页
步骤 11	确保您已启用其他功能来保护网络免受恶意站点的攻击	请参阅安全智能， 第 1729 页。

使用类别和信誉启用 URL 过滤

您必须是管理员用户才能执行此任务。

开始之前

按照 如何使用类别和信誉配置 URL 过滤， 第 1793 页中所述，完成所有前提条件。

过程

步骤 1 选择**集成** > **云服务**。

步骤 2 配置 URL 过滤选项，第 1795 页。

步骤 3 点击**保存**。

URL 过滤选项

添加 URL 过滤许可证将自动启用启用 URL 过滤。允许根据网站的一般分类或 类别和风险级别或 信誉来进行流量过渡。

虽然默认情况下系统配置为将所有URL提交到云以进行威胁情报评估，但使用类别和信誉数据的本地数据集可以提高 Web 浏览速度。当您启用（或重新启用）URL 过滤时， 防火墙管理中心 会自动向思科查询 URL 数据并将数据集推送到托管设备。此过程可能需要一些时间。

如果您使用 SSL 规则处理已加密的流量，则另请参阅 基于规则的解密规则准则和限制，第 1908 页。

启用自动更新

如果**启用自动更新**（默认），则 防火墙管理中心 每 30 分钟会检查一次云以获取更新。如果需要严格控制系统联系外部资源的时间，可以禁用自动更新，改为使用调度程序创建定期任务。请参阅在 *Cisco Secure Firewall Management Center* 管理指南中 使用已安排任务自动执行 *URL* 过滤更新 。

立刻更新

点击 **立即更新** 以执行一次性的按需 URL 数据更新。如果有更新正在进行，则不能启动按需更新。虽然每日更新通常是小量更新，但如果距离上一次更新超过五天，新的 URL 数据最多可能需要 20 分钟才能下载完，具体情况视带宽而定。然后，执行更新也可能最多需要 30 分钟。

URL 查询源

您可以选择系统如何为用户浏览的 URL 分配类别和信誉。您可以选择：

- **仅本地数据库**：仅使用本地数据集。如果您不想将未分类的 URL（类别和声誉不在本地数据集中）提交给思科，例如出于隐私原因，则可以使用此选项。但请注意，与未分类URL的连接不会与使用基于类别或信誉的URL条件的规则进行匹配。在这种情况下，您将无法手动对该URL指定类别或信誉。
- **本地数据库和思科云 (Local Database and Cisco Cloud)**：尽可能使用本地数据集，这样可以加快Web浏览速度。当用户浏览到类别和信誉不在本地数据集或之前访问过的网站缓存中的URL时，系统会将其提交到云端进行威胁智能评估，并将结果添加到缓存中。
- **仅思科云** （默认）：不使用本地数据集。当用户浏览到类别和信誉不在之前访问过的网站的本地缓存中的URL时，系统会将其提交到云端进行威胁智能评估，并将结果添加到缓存中。此选项可保证获得最新的类别和信誉信息。

此选项需要威胁防御版本 7.3。如果启用此选项，运行较早版本的设备将使用 **本地数据库和思科云** 选项。

已缓存的 URL 到期

如果您选择 **仅本地数据库** 作为 URL 查询源，则此设置不相关。

缓存类别和信誉数据使 Web 浏览速度更快。默认情况下，URL 的缓存数据永不过期，以获得最快的性能。

要尽量减少与过时数据匹配的 URL 实例，可以将缓存中的 URL 设置为过期。要获得更高的威胁数据准确性和通用性，请选择较短的到期时间。经过指定的时间之后，系统将在网络上的用户第一次访问缓存的 URL 后刷新缓存的 URL。第一个用户看不到刷新的结果，但访问此 URL 的下一个用户将会看到刷新的结果。

配置 URL 条件

通过根据 URL 类别和信誉控制对站点的访问来保护您的网络。

开始之前

注意 作为前提条件，请确保在访问控制策略的顶部至少创建一个包含类别或信誉参数的监控规则。这对于查看符合特定访问控制策略的任何 URL 的任何类别或信誉数据至关重要。

如果访问控制策略中没有配置类别或信誉参数的规则，则管理中心的“**连接事件**”页面不会显示任何命中访问控制策略的 URL 流量的类别或信誉数据。

过程

步骤 1 在规则编辑器中，点击 URL 条件的以下：

- 访问控制或 QoS-点击 **URLs**。
- SSL-点击 **类别**。

步骤 2 查找并选择要控制的 URL 类别：

在访问控制 或 QoS 规则中，点击 **类别**。

要有效保护网络免受恶意站点的攻击，必须阻止所有威胁类别 URL。此外，Talos 建议您仅阻止类别为“差”的站点。如果您具有积极的安全状态，可以阻止可疑的信誉，但这可能会导致更多的误报。有关威胁类别列表，请参阅URL 类别和信誉说明，第 1787 页。

请务必点击列表底部的箭头以查看所有可用类别。

步骤 3 （可选）通过选择**信誉 (Reputation)** 来限制 URL 类别。

请注意，如果您明确匹配**未分类**URL，但不能通过信誉进一步限制。选择信誉级别也会将比您选择的级别更高或更低的其他信誉包括在内，具体取决于规则操作：

- 如果规则允许或信任网络流量，则包括级别更低的信誉。例如，如果您将访问控制规则配置为允许良性（4 级），系统还会自动允许受信任（5 级）站点。
- 如果规则对网络流量进行速率限制、解密、阻止或监控，则包括级别更高的信誉。例如，如果将访问控制规则配置为阻止可疑站点（2 级），则系统还会阻止不受信任（1 级）站点。

如果更改规则操作，则系统会自动更改 URL 条件中的信誉级别。

或者，选择 **应用到未知信誉**。

步骤 4 点击 **添加 URL** 或 **添加到规则**，或进行拖放操作。

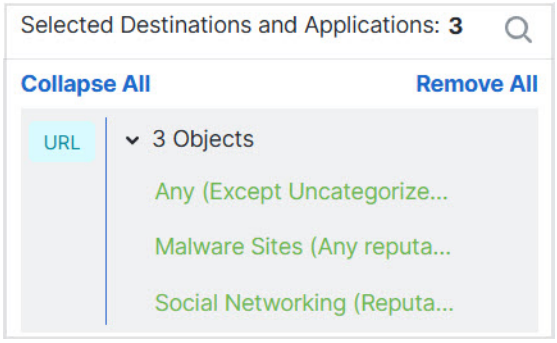
步骤 5 （可选）要在访问控制或 QoS 规则中选择预定义的 URL 对象或 URL 列表和源，请点击 **URL**，选择对象，然后将其添加到目标。

这些对象实施手动 URL 过滤，而不是基于类别的过滤。

步骤 6 保存或继续编辑规则。

示例：访问控制规则中的 URL 条件

下图显示用于阻止以下内容的访问控制规则的 URL 条件：所有具有中性或更差的信誉级别的恶意软件站点、所有不受信任站点以及所有社交站点。



下表总结如何构建该条件。

受阻 URL	类别	信誉
恶意软件站点，无论信誉如何	恶意软件网站	任意
任何不受信任的 URL（1 级）	任意	1 - 不受信任
具有声誉等级为中性或更差 （1 至 3 级）的社交站点	社交网络	3 - 中性

具有 URL 条件的规则

下表列出了支持 URL 条件的规则，以及每个规则类型支持的过滤类型。

规则类型	是否支持类别和信誉过滤？	支持手动过滤？
访问控制	支持	支持
解密策略	支持	否；使用可分辨名称条件
QoS	支持	支持

要在具有 **不解密** 规则条件的a解密策略 中使用URL过滤，请参阅在URL过滤中使用类别，第1792页。

URL 规则顺序

为了实现最有效的URL匹配，请将包括URL条件的规则放在其他规则前面，如果URL规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

如果为规则配置例外，请将例外置于另一条规则之上。

DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别

默认情况下，在每个新访问控制策略的**高级**选项卡上启用**启用对DNS流量的信誉实施**选项。此选项会轻微修改 URL 过滤行为，并且仅在启用和配置 URL 过滤时适用。

当此选项启用：

- 当浏览器查找域名以获取 IP 地址时，系统会在 URL 事务中尽早评估域类别和信誉
- 加密流量的类别和信誉通常无需解密即可确定

  如果 DNS 过滤无法确定加密流量的 URL，则使用您的加密流量配置处理该流量。

启用 DNS 过滤以在域查找期间识别 URL

默认情况下，在新的访问控制策略中启用DNS过滤。但是，可能需要其他配置才能使此设置生效。

开始之前

- 必须许可、启用和配置使用类别和信誉的 URL 过滤。

  （DNS 过滤不使用 URL 选项卡中的以下设置：URL 组、URL 对象、URL 列表和源，以及输入到“输入 URL”文本框中的 URL。）
- 请参阅DNS 过滤限制，第 1799 页中的限制。

过程

步骤 1 在访问控制策略的高级设置中，选择 **对 DNS 流量启用信誉实施**。

步骤 2 在同一策略中，对于配置了 URL 类别和信誉阻止的每个访问控制规则：

- 应用条件 - 如果应用条件不是**任何**（或为空），则将 **DNS** 添加到该列表。其他与 DNS 相关的选项与此目的无关。
- 端口条件 - 如果端口/协议条件不是**任何**（或为空），请添加 **DNS_over_TCP** 和 **DNS_over_UDP**。

步骤 3 保存更改。

下一步做什么

如果您已完成更改：部署配置更改，第 180 页

DNS 过滤限制

匹配具有**阻止并重置**、**交互式阻止**或**交互式阻止并重置**操作的规则的流量将被视为规则操作为**阻止**。

尝试访问阻止的URL的最终用户会遇到无法解释的无法连接到其页面的情况；连接将旋转，然后超时。

DNS 过滤和事件

由 DNS 过滤生成的连接事件使用以下特别需要关注的字段记录：DNS 查询、URL 类别、URL 信誉和目标端口。DNS 查询字段包含域名；对于 DNS 过滤匹配，URL 字段将为空。目的端口将是 53。

另外：

- 当访问控制规则操作为**允许**或**信任**时，将为同一流量生成两个连接事件，一个用于 DNS 过滤（填充 **DNS 查询 (DNS Query)** 字段），另一个用于 URL 过滤（填充 **URL** 字段）。
- 系统第一次遇到特定 URL 时，您将看到该单个会话的两个事件：一个事件显示 DNS 查询未分类/无信誉，一个事件显示 URL 的实际类别和信誉，这些是在 DNS 期间检索到的使用标准 URL 过滤进行处理时，将查询 和 应用于会话。

手动 URL 过滤

在访问控制和 QoS 规则中，您可以通过手动过滤单个 URL、URL 组 或 URL 列表和源，补充或选择性地覆盖基于类别和信誉的 URL 过滤。

示例：

- 您可使用访问控制阻止不适合您的组织的网站类别。但是，如果该类别包含合适的网站，并且您要为其提供访问权限，则您可以为该站点创建手动的“允许”(Allow)规则，然后将其置于该类别的“阻止”(Block) 规则之前。
- 如果不想使用基于类别的 URL 过滤，可以通过在访问控制策略中创建“允许”或“阻止”规则，手动允许或阻止一个 URL 或一组 URL。您可以在没有特殊许可证的情况下执行此类 URL 过滤。

SSL 规则不支持手动 URL 过滤；相反，使用可分辨名称条件。

⚠

注意 根据您实施手动 URL 过滤的方式，URL 匹配可能不是您想要的。请参阅手动 URL 过滤选项，第 1800 页。

手动 URL 过滤选项

有几种方法可以指定用于手动 URL 过滤的 URL：

选项	说明
（**最佳实践**） 使用自定义安全智能 URL 列表或源对象。	这是推荐的手动 URL 过滤方法。 您可以创建新列表或源，也可以在访问控制或 QoS 规则中选择现有列表或源。 有关信息，请参阅 自定义安全智能列表和源，第 2694 页 和子主题。
单独或作为组使用 URL 对象。有关 URL 对象的说明，请参阅 URL，第 2704 页。 或 将 URL 直接输入到访问控制规则中。（Web 界面中规则页面上的 **输入URL** 选项。）	如果不包含路径（即URL中无/字符），则匹配仅基于服务器主机名。如果包含一个或多个/字符，则整个URL字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项： • 字符串位于 URL 的开头。 • 字符串后面有一个点。 • 字符串开头包含一个点。 • 字符串后面跟有 :// 字符。 例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。 **注释** 我们建议您不要使用手动 URL 过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。 **输入 URL** 选项不支持通配符。

补充或选择性覆盖基于类别和信誉的 URL 过滤

在访问控制或 QoS 规则中，可以使用安全智能 URL 列表和源来补充或指定基于类别和信誉的 URL 过滤规则的例外情况。

重要提示！如果您在此过程中配置的列表或源包含基于类别或信誉的规则的例外情况，请按规则顺序将此规则置于这些规则之上。

在 SSL 规则中，使用可分辨名称条件配置并行行为。

开始之前

- 使用类别和信誉配置 URL 过滤请参阅配置 URL 条件，第 1796 页。
- 了解手动 URL 过滤的重要最佳实践。请参阅URL 过滤的最佳实践，第 1787 页和手动 URL 过滤选项，第 1800 页。
- 配置一个或多个包含要用于手动过滤的 URL 的安全智能对象（列表或源）。请参阅自定义安全智能列表和源，第 2694 页。

过程

步骤 1 导航至您将在其中定义规则的访问控制或 QoS 策略。

步骤 2 创建或编辑要在其中添加新条件的规则：

- 如果要补充基于类别或信誉的 URL 过滤规则，请编辑现有规则。
- 如果要覆盖或创建基于类别或信誉的 URL 过滤规则的例外，请创建新规则。

步骤 3 选择您创建的列表或源作为目标 URL 条件。

步骤 4 保存规则。

配置 HTTP 响应页面

作为访问控制的一部分，您可以使用访问控制规则或访问控制策略默认操作配置在系统阻止 Web 请求时要显示的 *HTTP* 响应页面。

所显示的响应页面取决于阻止会话的方式：

- **阻止响应页面**：覆盖用于说明拒绝已被连接的默认浏览器或服务器页面。
- **交互式阻止响应页面**：警告用户，并且还允许其点击按钮（或刷新页面）以加载最初请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

如果未选择响应页面，则系统将在没有交互或说明的情况下阻止会话。

对 HTTP 响应页面的限制

- 系统仅为被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的未加密连接或解密 HTTP/HTTPS 连接显示响应页面。对于被任何其他策略或机制阻止的连接，系统不会显示响应页面。
- 如果重置连接（发送 RST 数据包），系统将无法显示响应页面。如果启用响应页面，系统将优先处理此配置。即使选择**阻止并重置**或**交互式阻止并重置**作为规则操作，系统也会显示响应页面，但不会重置匹配的 Web 连接。要确保重置已阻止的 Web 连接，必须禁用响应页面。

  请注意，所有与此规则匹配的非 Web 流量都会被阻止并重置。
- 对于被访问控制规则（或其他任何配置）阻止的加密连接，系统不会显示响应页面。如果未配置 SSL 策略，或者 SSL 策略允许已加密流量通过，则访问控制规则会评估已加密连接。

  例如，系统无法解密 HTTP/2 或 SPDY 会话。如果使用以上协议之一加密的网络流量通过访问控制规则评估，则会话被阻止时系统不会显示响应页面。

  However, the system does display a response page for connections that are decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. 在这些情况下，系统会加密响应页面并在重新加密的 SSL 数据流最后发送该页面。
- 如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。
- 如果在未指定 “http” 或 “https” 的情况下输入 URL，并且浏览器在端口 80 上发起连接，并且用户点击响应页面，并且该连接随后重定向到端口 443，则用户不会看到第二个交互式响应页面，因为对此 URL 的响应已被缓存。
- 如果网络流量在系统识别请求的 URL 之前被阻止，则系统不会显示响应页面；请参阅URL 过滤的最佳实践，第 1787 页。
- 如果在允许应用规则之后配置了阻止 URL 访问控制规则，则系统不会显示响应页面。

HTTP 响应页面的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

选择 HTTP 响应页面

HTTP 响应页面能否稳定显示取决于页面的网络配置、流量负载和大小。较小的页面更有可能成功显示。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **HTTP 响应**。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 选择**阻止响应页面 (Block Response Page)** 和**交互式阻止响应页面 (Interactive Block Response Page)**：

- “系统提供”(System-provided) - 显示常规响应。点击 **视图** ( ) 可查看此页面的代码。
- “自定义”(Custom) - 创建自定义响应页面。屏幕上将显示一个弹出窗口，其中预先填充有系统提供的代码，您可以通过点击 **编辑** ( )来替换或修改此代码。计数器显示已使用的字符数量。
- “无”(None) - 在没有交互或说明的情况下禁用响应页面并阻止会话。要对整个访问控制策略快速禁用交互式阻止，请选择此选项。

步骤 3 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置对 HTTP 响应页面的交互式阻止

配置交互式阻止时，用户可在看到警告后加载原先请求的站点。用户在绕过响应页面后可能必须刷新才能加载未加载的页面元素。

提示 要对整个访问控制策略快速禁用交互式阻止，既不要显示系统提供的页面，也不要显示自定义页面。然后，系统会阻止所有连接而不交互。

如果用户不绕过交互式阻止，则会拒绝匹配流量而不进行进一步检查。如果用户绕过交互式阻止，则访问控制规则会允许流量，不过，流量仍然可能受到深度检查和阻止。

默认情况下，用户绕行的有效时间为 10 分钟（600 秒），而在在后续访问时不显示警告页面。可以将持续时间设置为长达一年，也可以强制用户每次都绕过阻止。此设置适用于策略中的每条“交互式阻止”规则。不能对每条规则都设置限制。

以交互方式阻止的流量的日志记录选项与允许的流量中的日志记录选项相同，但如果用户不绕过交互式阻止，则系统只能记录连接开始事件。在系统最初警告用户时，它会使用 `Interactive Block`

或 `Interactive Block with reset` 操作标记任何已记录的连接开始事件。如果用户绕过阻止，则为会话记录的其他连接事件具有操作 `Allow`。

配置交互式阻止

以下程序介绍了如何允许用户绕过 URL 过滤规则。

过程

步骤 1 作为访问控制的一部分，请配置与网络流量匹配的访问控制规则；请参阅创建和编辑访问控制规则，第 1764 页：

- 操作 - 将规则操作设置为**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**；请参阅访问控制规则交互式阻止操作，第 1749 页。
- 条件 - 使用 URL 条件指定要进行交互式阻止的网络流量；请参阅URL 条件（URL 过滤）。
- 日志记录 - 假设用户将绕过阻止并相应地选择日志记录选项；请参阅*Cisco Secure Firewall Management Center* 管理指南中的允许连接的日志记录 。
- 检测 - 假设用户将绕过阻止并相应地选择深度检查选项；请参阅关于访问控制策略，第 1701 页。

步骤 2 （可选）在访问控制策略 **HTTP 响应 (HTTP Responses)** 上，选择自定义交互式阻止 HTTP 响应页面；请参阅选择 HTTP 响应页面，第 1803 页。

步骤 3 （可选）在访问控制策略**高级 (Advanced)** 设置中，更改用户绕行超时；请参阅为受阻网站设置用户绕过超时，第 1804 页。

在用户绕过阻止后，系统允许用户浏览到该页面而不发出警告，直至经过超时期为止。

步骤 4 保存访问控制策略。

步骤 5 部署配置更改；请参阅部署配置更改，第 180 页。

为受阻网站设置用户绕过超时

以下程序介绍如何设置用户绕过URL过滤阻止后允许浏览的时间。超时到期后，用户必须再次绕过阻止。

过程

步骤 1 点击 **策略** > **安全策略** > **访问控制** 并编辑策略。

步骤 2 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 3 点击常规设置旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 4 在 **Allow an Interactive Block to bypass blocking for (seconds)** 字段中，键入用户绕过到期之前必须经过的秒数。

将此值设置为 0 表示交互式阻止响应显示一次，并且用户绕行永远不会过期。

步骤 5 点击**确定**。

步骤 6 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置 URL 过滤运行状况监控器

如果系统在获取或更新 URL 类别和信誉数据时出现问题，以下运行状况策略会发出警报。

- URL 过滤监视器
- 设备中威胁数据更新

要确保按照您希望的方式进行配置，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 运行状况模块 和 配置运行状况监控 。

争议 URL 类别和信誉

如果您不同意 Talos 指定的类别或信誉，可以提交重新评估请求。

开始之前

您将需要思科帐户凭证。

过程

步骤 1 在 防火墙管理中心 Web 界面中，执行以下操作之一：

争议选项的位置	争议选项的路径
云服务配置页面	a.导航到 **集成** > **云服务** 页面。 b. 选择**争议 URL 类别和信誉**。

争议选项的位置	争议选项的路径
手动 URL 查找页面	a. 导航到手动 URL 查找页面：**事件和日志** > **+ 显示更多** > **高级** > **URL 查找分析**。 b. 查找所有争议的 URL。 c. 要查看表格行末尾的 **争议**，请将鼠标悬停在结果列表中的相关条目上，然后点击争议。
URL 连接事件	a. 导航至**事件和日志** > **+ 显示更多** > **连接** > **事件**菜单下的任何页面，此页面包括一个包含 URL 的表。 b. 右键点击 **URL 类别**或 **URL 信誉**列（如有需要，请显示隐藏列）中的项目，然后选择一个选项。

Talos 网站将在单独的浏览器窗口中打开。

步骤 2 使用思科凭证登录 Talos 网站。

步骤 3 查看信息并遵循 Talos 页面上的说明。

步骤 4 在 Talos 网站上查找有关如何处理所提交的争议以及期望的响应（如有）的信息。

争议流程与 Firepower 产品无关。

如果 URL 类别集发生更改，请执行操作

URL 类别集可能会偶尔发生更改，以适应新的 Web 趋势和不断发展的使用模式。

这些更改会影响策略和事件。

在计划进行 URL 类别更改之前和之后不久，您将在受更改影响的任何访问控制，SSL 和 QoS 策略的规则列表中以及在您编辑。

在看到这些警报时，您应采取措施。

注释 本主题中描述的对 URL 类别集的更新与简单地在现有类别中添加新的 URL 或对错误分类的 URL 进行重新分类的变化不同。此主题不适用于单个 URL 的类别更改。

过程

步骤 1 如果您在访问控制策略中的规则旁边看到警报，请将鼠标悬停在警报上以查看详细信息。

步骤 2 如果警报提到 URL 类别更改，请编辑规则以查看更多详细信息。

步骤 3 将鼠标悬停在规则对话框中的 URL 或类别上，可查看有关更改类型的一般信息。

步骤 4 如果您在类别旁边看到警报，请点击警报以查看详细信息。

步骤 5 如果您在更改说明中看到“更多信息”链接，请点击该链接以在Talos网站上查看有关类别的信息。

或者，查看 URL 类别和信誉说明，第 1787 页 链接中的所有类别的列表和说明。

步骤 6 根据更改类型，采取适当的操作：

类别更改的类型	系统将执行的操作	您应该采取的措施
现有类别即将被弃用	还没有。您有几周的时间来更改受影响的规则。 如果您在此期间不执行操作，系统最终将无法重新部署策略。	从包含此类别的所有规则中删除此类别。如果有类似的新类别，请考虑改为使用该类别。
已添加新类别	默认情况下，系统不使用新添加的类别。	考虑为新类别创建新规则。
删除现有类别	类别将以加删除线文本的形式（即，在类别名称上划一条横线）显示在规则中。	您必须先从规则中删除过时类别，然后才能进行部署。

步骤 7 检查您的 SSL 规则（类别）是否存在这些更改，并根据需要执行操作。

步骤 8 检查您的 QoS 规则（URL）是否存在这些更改，并根据需要执行操作。

下一步做什么

部署配置更改；请参阅 部署配置更改，第 180 页。

URL 类别和信誉变更：对事件的影响

- 当URL类别发生更改时，系统在类别更改之前处理的事件将与其原始类别名称相关联，并标记为**旧版**。系统在类别更改之后处理的事件将与新类别相关联。

  随着时间的推移，较旧的旧版事件将逐渐退出系统。

- 如果在处理 URL 时其没有信誉，则事件查看器中的 URL 信誉列将为空。

URL 过滤故障排除

类别列表中缺少预期的 URL 类别

URL 过滤功能使用的类别集与安全智能功能不同；您期望看到的类别可能是安全智能类别。要查看这些类别，请查看访问控制策略中 **安全智能** 选项卡上的 **URL** 选项卡。

初始数据包不经检查通过

请参阅在识别流量之前检查通过的数据包以及子主题。

另请参阅DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别，第 1798 页。

运行状况警报：“URL 过滤注册失败”

验证您的 防火墙管理中心 和任何代理是否可以连接到思科云。您可能需要以下主题中有关 URL 过滤和 URL 类别的信息：*Cisco Secure Firewall Management Center* 管理指南中的互联网访问要求和通信端口要求，。

如何查找特定 URL 的类别和信誉？

进行手动查找。请参阅*Cisco Secure Firewall Management Center* 管理指南中的查找 *URL* 类别和信誉。

尝试手动查找时出错：“<URL> 云查找失败”

请确保已正确启用此功能。请参阅在 *Cisco Secure Firewall Management Center* 管理指南中 查找 *URL* 类别和信誉 中的前提条件。

似乎根据 URL 类别和信誉对 URL 进行了错误处理

问题：系统无法根据 URL 类别和信誉正确处理 URL。

解决方案：

- 验证与 URL 关联的 URL 类别和信誉是否如您所料。请参阅*Cisco Secure Firewall Management Center* 管理指南中的查找 *URL* 类别和信誉。
- 可以通过URL 过滤选项，第 1795 页（可以使用使用类别和信誉启用 URL 过滤，第 1794 页进行访问）中所述的设置来解决以下问题。
  - URL 缓存可以保存过时信息。请参阅URL 过滤选项，第 1795 页中有关**已缓存的 URL 到期**的信息。
  - 可能无法使用来自云的当前信息更新本地数据集。有关**启用自动更新**设置的信息，请参阅URL 过滤选项，第 1795 页。
  - 系统可以配置为不检查云以获取当前数据。请参阅 URL 过滤选项，第 1795 页中有关 **向思科云查询未知 URL** 设置的信息。
- 访问控制策略可以配置为将流量传递到 URL，而无需检查云。有关**重试 URL 缓存缺失查找**设置的信息，请参阅常规设置，第 2458 页。
- 另请参阅URL 过滤的最佳实践，第 1787 页。
- 如果使用 SSL 规则处理 URL，请参阅基于规则的解密规则准则和限制，第 1908 页和解密策略 规则顺序
- 验证是否正在使用您希望处理的访问控制规则处理 URL，并且此规则将执行您希望执行的操作。考虑规则顺序。

- 验证 防火墙管理中心上的本地 URL 类别和信誉数据库是否已从云中成功更新，且托管设备是否已从 防火墙管理中心成功更新。

  这些进程的状态将在运行状况监视器、**URL 过滤监视器**模块和**设备中威胁数据更新**模块中报告。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的 运行状况 /

如果要立即更新本地 URL 类别和信誉数据库，请转到 **集成** > **云服务**，然后在 **URL 筛选**区域中点击**立即更新**。有关详细信息，请参阅URL 过滤选项，第 1795 页。

URL 类别或信誉不正确

对于访问控制或 QoS 规则：使用手动过滤，注意规则顺序。请参阅手动 URL 过滤，第 1799 页和配置 URL 条件，第 1796 页。

对于 SSL 规则：不支持手动过滤。改为使用可分辨名称条件。

另请参阅争议 URL 类别和信誉，第 1805 页。

网页加载速度缓慢

可以在安全与性能之间权衡取舍。某些选项：

- 考虑修改**缓存 URL 到期**设置。选择**集成** > **云服务**。有关信息，请参阅URL 过滤选项，第 1795 页。
- 考虑在常规设置，第 2458 页中取消选择**重试 URL 缓存缺失查找**设置。

事件不包括 URL 类别和信誉

- 确保已在访问控制策略中包含适用的URL规则，规则处于活动状态，并且策略已部署到相关设备。
- 如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。
- 必须为 URL 类别和信誉配置处理连接的规则。
- 即使已在 SSL 规则的类别选项卡中配置 URL 类别，也必须在访问控制策略的规则中配置 URL 选项卡。

DNS 过滤不起作用

确保您已完成 启用 DNS 过滤以在域查找期间识别 URL ，第 1798 页中的所有前提条件和步骤。

最终用户尝试访问被阻止的 URL，而页面只是旋转和超时

当启用 DNS 过滤且最终用户访问被阻止的 URL 时，页面将旋转但不会加载。最终用户不会收到该页面被阻止的通知。这是当前启用 DNS 过滤时的限制。

请参阅DNS 过滤限制，第 1799 页。

事件包括 URL 类别和信誉，但 URL 字段为空

如果 DNS 查询字段已填充且 URL 字段为空，则在启用 DNS 过滤功能时会出现这种情况。

请参阅DNS 过滤和事件，第 1799 页。

为单个事务生成多个事件

单个 Web 事务有时会生成两个连接事件，一个用于 DNS 过滤，另一个用于 URL 过滤。当启用 DNS 过滤并且符合以下条件时，会出现这种情况：

- 流量的访问控制规则操作为“允许”或“信任”。
- 系统首次遇到 URL。

请参阅DNS 过滤和事件，第 1799 页。

URL 过滤的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
新的 URL 类别	版本 7.0 的新增内容，适用于所有版本	任意	新 URL 类别：专用 IP 地址 有关详细信息，请参阅 Talosintelligence.com
DNS 过滤	7.0 6.7（测试版）	任意	每个访问控制策略的高级设置中的新选项都允许按类别和信誉提前过滤网络流量。 该功能会在新安装中默认启用。 支持的平台：任何支持版本的 防火墙管理中心 和托管设备。
能够为未知信誉的站点指定处理方式	6.7	任意	您现在可以指定对未知信誉的 URL 的处理方式。 修改后的屏幕：访问控制策略和 QoS 策略中的 URL 规则以及 SSL 策略中的类别规则在信誉选择区域下方包括一个新复选框。 支持的平台：全部

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
新增和更改的 URL 类别 信誉级别的新名称	6.5	任意	以下更改适用于访问控制和 QoS 策略中的 URL 规则以及 SSL 策略中的类别规则： URL 类别集已更改。在您创建 URL 规则时，现在有两个类别“页面”可供选择。 与每个信誉级别关联的名称已更改。 有关新类别和信誉名称的说明，请参阅URL 类别和信誉说明，第 1787 页。 有关特定于升级的完整详细信息，另请参阅版本说明和版本 6.5 的升级说明。 如果将来类别集发生更改，您的规则将显示图标以提醒您。 修改的屏幕：访问控制策略、SSL 策略和 QoS 策略中的 URL 规则；与 URL 类别相关的事件数据。 支持的平台： 防火墙管理中心 和运行版本 6.5 的设备。
对传统设备许可的细微更改	6.5	任意	对于使用经典许可证的设备，在设备注册到 防火墙管理中心 并将 URL 过滤许可证分配给设备之前不会启用 URL 过滤。 支持的平台：NGIPSv 和 ASA 与 FirePOWER 服务设备。
用于从思科云检索URL数据的地址已更改	6.5	任意	请参阅*Cisco Secure Firewall Management Center* 管理指南中的互联网访问要求 。
有机会对指定的 URL 类别提出异议	6.5	任意	如果您不同意系统分配给 URL 的类别，您可以提交更改类别的请求。 新增/修改的屏幕： • 右键点击**分析**菜单下的连接事件表中的 URL 类别或信誉时的新菜单选项。 • URL 查找页面（**分析** > **高级** > **URL**）上的新按钮。（将鼠标指针悬停在 URL 上以显示此按钮。） • **系统** > **集成** > **云服务**页面上的新选项 支持的平台：所有
思科 CSI 选项卡已重命名为**云服务**	6.4	任意	修改的屏幕和导航：**系统** > **集成** > **Cisco CSI** 现在为**系统** > **集成** > **云服务** 支持的平台： 防火墙管理中心

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
将 URL 过滤信息从各个位置移动到新的“URL 过滤”章节	6.3	任意	将有关为 URL 过滤配置云通信的信息移动至新的“URL 过滤”章节。将某些其他 URL 过滤信息从其他位置移动至本章。在本章节中对思科 CSI 主题的结构进行了相关更改。
新选项：已缓存的URL到期	6.3	任意	使用此新控件来平衡 URL 类别和信誉数据的性能与新鲜度，以便尽量减少与过时数据匹配的 URL 实例。 修改的屏幕：**系统** > **集成** > **Cisco CSI**。 支持的平台：所有。
已更改菜单路径	6.3	任意	手动 URL 查找页面的路径已从**分析** > **查找** > **URL** 更改为**分析** > **高级** > **URL**。



第 43 章

入侵防御

Snort 检测引擎是 Firewall Threat Defense 中不可或缺的一部分。本章提供 Snort 3 网络分析和入侵策略概述。它可以让您深入了解系统提供的和自定义的网络分析和入侵策略。在大多数情况下，系统提供的策略就足够了。对于有特定需求的高级用户，您可以创建自定义规则。要配置自定义 Snort 3 规则，请参阅用于访问控制的 *Snort 3* 自定义入侵策略。

注释 。

要配置自定义 Snort 2 规则，请参阅用于访问控制的 *Snort 2* 自定义入侵策略。

- 关于入侵防御， 第 1813 页
- Snort 检测引擎， 第 1814 页
- 关于 Snort 3， 第 1815 页
- 网络分析和入侵策略的准则和限制， 第 1817 页
- 策略如何检查流量是否存在入侵， 第 1818 页
- 系统提供的与自定义的网络分析和入侵策略， 第 1824 页
- 网络分析和入侵策略的必备条件， 第 1829 页

关于入侵防御

网络分析和入侵策略作为入侵检测和防御功能的一部分，共同发挥作用。

- 术语入侵检测通常是指被动监控并分析网络流量以查找潜在入侵，并存储攻击数据以进行安全分析的过程。这有时称为“IDS”。
- 术语入侵防御包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。这有时称为“IPS”。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管如何解码和预处理流量，以便可进一步对其进行评估，尤其适用于可能表明入侵尝试的异常流量。

- **入侵策略**使用入侵和预处理程序规则（有时统称为入侵规则）根据模式检测已解码数据包是否存在攻击。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统随附若干以类似方式命名的网络分析和入侵策略（例如，平衡安全性和连接），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用思科 Talos 智能小组 (Talos) 的经验。对于这些策略， Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高托管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

有关其他支持和信息，请参阅视频：

- Snort 3 简明概述
- Snort 3 扩展概述

注意 **检测模式弃用**：从管理中心 7.4.0 版本开始，对于网络分析策略 (NAP)，**检测**检查模式已弃用，并将在后续版本中移除。

检测 模式旨在用作测试模式，以便您可以启用检测并查看它们在网络中的行为，然后再将其设置为丢弃流量，即显示将被丢弃的流量。

此行为已得到改进，其中所有检查器丢弃都由规则状态控制，并且您可以设置每个丢弃以生成事件。这样做是为了在配置规则状态以丢弃流量之前对其进行测试。由于我们现在可以对 Snort 3 中的流量丢弃进行精细控制，因此 **检测** 模式只会增加产品的复杂性，不需要，因此检测模式已弃用。

如果将**检测**模式下的 NAP 更改为**预防**，则处理入侵事件流量并具有结果 “会被丢弃”的 NAP 现在将为“已丢弃”，相应的流量将丢弃来自这些事件的流量。这适用于 GID 不是 1 或 3 的规则。GID 1 和 3 是文本/编译规则（通常由 Talos 提供或从您的自定义/导入规则中提供），所有其他 GID 都是异常检测。这些是在网络中触发的比较少见的规则。更改为 **预防** 模式不太可能对流量产生任何影响。您只需禁用适用于已丢弃流量的入侵规则，并将其设置为仅生成或禁用。

我们建议您选择 **预防** 作为检测模式，但如果您选择 **预防**，则无法恢复到 **检测** 模式。

Snort 检测引擎

Snort 检测引擎是 Cisco Secure Firewall Threat Defense （前称 Firepower 威胁防御）设备不可或缺的一部分。检测引擎实时分析流量，以提供深度数据包检测。网络分析和入侵策略共同利用 Snort 检测引擎的功能来检测和防御入侵。

关于 Snort 3

Snort 3 是最新版本的 Snort 检测引擎，与早期版本的 Snort 相比有很大改进。旧版 Snort 是 Snort 2，它不再受支持。Snort 3 更高效，可提供更好的性能和可扩展性。

与 Snort 2 相比，Snort 3 在架构上进行了重新设计，以使用相同的资源检查更多流量。Snort 3 提供简化且灵活的流量解析器插入。Snort 3 还提供了新的规则语法，使规则编写更加容易，并且共享对象规则等效项可见。

Snort 3 的其他重大变化包括：

- 与使用多个 Snort 实例的 Snort 2 不同，Snort 3 将多个线程与单个 Snort 实例相关联。这会使用更少的内存，缩短 Snort 重新加载时间，并支持更多入侵规则和更大的网络映射。Snort 线程的数量因平台而异，与每个平台的 Snort 2 实例数量相同。使用几乎是透明的。在 Secure Firewall 6160 和 6170 设备上，默认情况下，Snort 3 将多个线程与两个 Snort 进程关联。有关详细信息，请参阅 Snort 3 多进程支持 。
- Snort 版本 per防火墙威胁防御 - Snort 检测引擎是 防火墙威胁防御 特定的，而不是 Cisco Secure Firewall Management Center （前称 Firepower Management Center） 特定的。防火墙管理中心 可以管理多个 防火墙威胁防御，每个都使用任一版本的 Snort（Snort 2 和 Snort 3）。虽然 防火墙管理中心的入侵策略是唯一的，但系统会应用 Snort 2 或 Snort 3 版本的入侵策略，具体取决于设备所选的检测引擎。
- 解码器规则 - 仅在默认入侵策略中触发数据包解码器规则。系统会忽略您在其他策略中启用的解码器规则。
- 共享对象规则 - Snort 3 支持部分但不是全部共享对象 (SO) 入侵规则（生成器 ID (GID) 为 3 的规则）。不支持的已启用共享对象规则不会触发。
- 安全智能的多层检测 - Snort 3 会检测最内部的 IP 地址，而不考虑层。
- 平台支持 - Snort 3 需要 Firewall Threat Defense 7.0 或更高版本。ASA FirePOWER 或 NGIPSv 设备不支持此功能。
- 受管设备 - 版本 7.0 的 防火墙管理中心 可以同时支持版本 6.4、6.5、6.6、6.7 和 7.0 Snort 2 防火墙威胁防御以及版本 7.0 Snort 3 防火墙威胁防御。
- 切换 Snort 版本时的流量中断 - 切换 Snort 版本会中断流量检查，并且在部署期间可能会丢弃一些数据包。
- 统一策略 - 无论受管 防火墙威胁防御中启用的底层 Snort 引擎版本如何， 防火墙管理中心 中配置的访问控制策略、入侵策略、网络分析策略均可在应用策略时无缝地工作。 防火墙管理中心 版本 7.0 及更高版本中的所有入侵策略都有两个可用版本：Snort 2 版本和 Snort 3 版本。虽然入侵策略有两个版本（Snort 2 版本和 Snort 3 版本），但它具有统一的名称、基本策略和检测模式。Snort 2 和 Snort 3 版本的入侵策略在规则设置方面可能不同。但是，在设备上应用入侵策略时，系统会自动识别设备上启用的 Snort 版本，并应用为该版本配置的规则设置。
- 轻量级安全软件包 (LSP) - 替换适用于 Snort 3 下一代入侵规则的 Snort 规则更新 (SRU) 和配置更新的 SRU。下载更新会同时下载 Snort 3 LSP 和 Snort 2 SRU。

LSP 更新提供新的和更新后的入侵规则和检查器规则、现有规则的修改后状态以及 防火墙管理中心 和 防火墙威胁防御 版本 7.0 或更高的修改后的默认入侵策略设置。当您将 防火墙管理中心 从 6.7 或更低版本升级到 7.0 时，它同时支持 LSP 和 SRU。LSP 更新还可能删除系统提供的规则，提供新规则类别和默认变量，并修改默认变量值。有关 LSP 更新的详细信息，请参阅最新版本的 *Firepower* 管理中心配置指南 中的 更新入侵规则 主题。

- Snort 2 和 Snort 3 规则和预设的映射 - 映射 Snort 2 和 Snort 3 规则，并且映射由系统提供。但是，它不是一对一映射。系统提供的入侵基本策略是为 Snort 2 和 Snort 3 预配置的，它们提供相同的入侵防御，但规则集不同。系统为 Snort 2 和 Snort 3 提供的基本策略针对相同的入侵防御设置相互映射。
- 同步 Snort 2 和 Snort 3 规则覆盖 - 防火墙威胁防御 升级到 7.0 后，可以将 防火墙威胁防御 的检测引擎升级到 Snort 3 版本。防火墙管理中心 使用 Talos 提供的映射将 Snort 2 版本入侵策略的现有规则中的所有覆盖映射到相应的 Snort 3 规则。但是，如果在升级后执行了其他覆盖，或者如果您安装了版本为 7.0 的新 防火墙威胁防御 ，则必须手动进行同步。
- 自定义入侵规则 - 您可以在 Snort 3 中创建自定义入侵规则。您还可以将 Snort 2 的自定义入侵规则导入到 Snort 3。
- 规则组 - 防火墙管理中心 将所有 Snort 3 规则分组到规则组中。规则组是规则的逻辑组，提供简单的管理界面，以增强规则可访问性、规则导航以及对规则组安全级别的更好控制。

  从防火墙管理中心7.3.0，支持多个级别的规则组的规则导航，这为规则提供了更大的灵活性和逻辑分组。添加了 MITRE 框架，使您能够使用 MITRE 框架浏览规则。MITRE 只是另一个类别的规则组，是 Talos 规则组的一部分。

注释 有关 MITRE 的信息，请参阅 https://attack.mitre.org 。

一条规则可以是多个规则组的一部分，例如多个 MITRE ATT&CK 规则组、规则类别规则组、多个“资产类型”规则组、恶意软件活动等。入侵策略编辑器中列出了可用的规则组，可以选择这些规则组以增强策略。

使用多级分层规则组的结构，您现在可以向下遍历到最后一个元素，即“枝叶规则组”。这些规则组包含彼此相关的规则集，例如特定类型的漏洞、类似的目标系统或类似的威胁类别。规则组有四个与其关联的安全级别。您可以更改安全级别，添加或删除规则组，并且可以更改与网络上看到的流量匹配的规则的规则操作。这样做是为了在安全性、性能和防误报之间取得令人满意的平衡。

Snort 3 多进程支持

在运行 Cisco Secure Firewall 版本 10.0 的 Cisco Secure Firewall 6160 和 6170 设备上，默认情况下，Snort 3 将多个线程与两个 Snort 实例相关联。在部署过程中，每个 Snort 3 实例会根据需要自动配置线程。单独的 Snort 3 实例可以减少每个实例的内存负载，减少锁竞争，并缩短核心生成时间。这有助于提高恢复能力、性能和可扩展性。任何 Snort 实例故障都会导致流量影响，如果需要，还可以重新启动单个 Snort 进程。

Snort 线程分布在 NUMA 节点上，其中每个节点都被视为独立处理器。这可确保维护内存边界。例如，Snort 实例 0 使用节点 0 的内存，而实例 1 使用节点 1 的内存。

诸如 **show coredump** 和 **show perfstats** 等命令的 CLI 输出已经增强，可以显示两个 Snort 实例上的信息。在管理中心上，导航至“**故障排除**”**(Troubleshooting)**”“**监控**”**(Monitor)**”“**设备**”**(Devices)** 以查看 “**概述**”**(Overview)**“**关键进程**”**(Critical Processes)** 和“ **内存**”**(Memory)** 部分，以获取有关两个 Snort 实例的信息。如果存在任何规则分析错误，Snort 实例编号会随错误一起显示。

禁用 Snort 3 多进程支持

使用 **configure snort multi-process disable** 命令禁用 Snort 3 多进程支持。您还必须重新部署配置，以确保禁用 Snort 3 多进程支持。

```
> configure snort multi-process disable
----------------------------------------------------------------------
Caution: this command is intended for debugging purposes only.
A deployment is required after enabling/disabling multi-process and will cause a Snort
restart and temporary traffic interruption.
----------------------------------------------------------------------
Do you still want to continue?
Please enter 'YES' or 'NO': YES
Please perform a manual deployment to disable multi-process.
```



注释 此命令会导致 Snort 引擎重启，并且在下一次部署期间，当 Snort 从多进程状态更改为单进程状态时，还将导致流量中断。

网络分析和入侵策略的准则和限制

- 具有小数据包的流量百分比较高会导致Snort性能下降。即使禁用所有预处理器，也会观察到此行为。
- 当您尝试在内存不足的威胁防御设备上部署配置更改时，也会触发Snort部署。这会导致大量消耗RSS内存。如果在设备上部署大型配置（例如包含大量Snort IPS规则、网络对象和访问控制列表的多个IPS策略），Snort内存使用率也会受到影响。可以通过优化 配置来缓解此类内存问题。有关如何配置访问控制规则以优化配置的最佳实践，请参阅 访问控制规则的最佳实践。
- 如果增加Threat Defense Virtual实例的内存，必须重新部署配置，Snort 3才能利用额外的内存。



注释 增加 Threat Defense Virtual 实例的内存时，Snort 3 的内存分配不会自动调整。必须重新部署配置，以重新生成相关配置文件（例如 `memory_allocation.lua`），这些文件会将更新后的资源限制应用于 Snort 3。

- 如果 SIP 流之后跟随来自同一连接的 RTP 流，Snort 会检测用于建立连接的初始 SIP 通信，并允许 SIP 流量。默认情况下，SIP 通信之后的 RTP 流也会被信任，并绕过已配置的规则。要防止

此类情况，信任父 SIP 连接或将父 SIP 连接添加到预过滤器规则，可确保只有 SIP 流绕过 Snort 检测，并允许后续的 RTP 流分别根据相应规则进行评估。

- 如果管理中心中有多条具有相同动作的 Snort 规则匹配一个数据包，将为每条规则记录一个事件。但是，如果匹配的规则具有不同的动作，则仅具有最高优先级动作的规则会生成事件。动作优先级从高到低为：放行、重置、阻止、丢弃、警报、记录。
- 通过系统日志或 eStreamer 完全限定事件源转发入侵数据包事件时，由于可用于系统日志生成和 eStreamer 的缓冲区大小限制，数据包数据字段可能会被截断。在这种情况下，数据包长度将不匹配实际发送的数据包数据。
- 不能同时进行策略更改、切换 Snort 版本并部署这两类更改。必须先进行所需的策略更改并部署，或先切换 Snort 版本并部署。

防火墙管理中心管理的 防火墙威胁防御 的 Snort 3 的功能限制

下表列出了 防火墙管理中心管理的 防火墙威胁防御 设备的 Snort 2 支持但 Snort 3 不支持的功能。

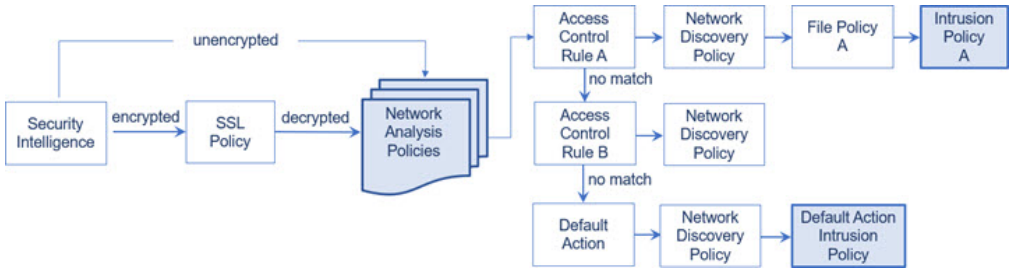
表 *106: Snort 3* 的功能限制

策略/区域	不支持的功能
访问控制策略	以下应用设置： • 安全搜索 • YouTube EDU
入侵策略	• 全局规则阈值 • 日志记录配置： • SNMP • SRU 规则更新，因为 Snort 3 仅支持 LSP 规则更新
其他功能	使用 FQDN 名称进行事件日志记录

策略如何检查流量是否存在入侵

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示网络部署的内联、入侵防御和 AMP 中的流量分析顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），系统可以在图示过程中的几乎任何步骤阻止流量而不进行进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略（被动检测数据包）无法影响流量的流动。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为入侵事件）指示数据包或其内容可能表示安全风险。

提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

解码、规范化和预处理：网络分析策略

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。网络分析策略在以下时机监管这些流量处理任务：

- 在流量由安全智能过滤**之后**
- 在加密流量由可选 SSL 策略解密**之后**
- 在流量可由文件或入侵策略检测**之前**

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由检查器并在以后由入侵规则轻松使用的格式。TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他检查器和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。

- 各种网络层和传输层检查器检测利用 IP 分段的攻击，执行校验和验证并执行 TCP 和 UDP 会话预处理。

  请注意，一些高级传输和网络检查器设置全局适用于由访问控制策略的目标设备处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置。

- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。

- Modbus、DNP3、CIP 和 s7commplus SCADA 检查器可检测流量异常并向入侵规则提供数据。监控与数据采集 (SCADA) 协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。

- 通过若干检查器，可以检测特定威胁，如 Back Orifice、端口扫描、SYN 泛洪和其他基于速率的攻击。

  请注意，您在入侵策略中配置敏感数据检查器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。

注释 禁用 TLS 服务器身份时，Snort 3 不会执行 SNI 不匹配检测。它仅评估客户端 Hello 数据包中的 SNI，并绕过服务器 Hello 数据包中证书的通用名称 (CN) 的验证。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的所有入侵策略的所有流量的预处理。最初，系统使用“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。

注释 对于规则操作为 **信任** 的访问控制策略和操作为 **快速路径** 的预过滤器规则并禁用日志记录选项，您将观察到仍在系统中生成流结束事件。这些事件在管理中心事件页面上不可见。

访问控制规则：入侵策略选择

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。



注释 所有数据包（**无论**哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。

策略如何检查流量是否存在入侵，第 1818 页 中的图显示流经内联的入侵防御和 AMP 网络部署中的设备的流量，如下所示：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由文件策略 A 检查是否存在受禁文件和恶意软件，最后由入侵策略 A 检查是否存在入侵。
- 访问控制规则 B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后该流量将依次由网络发现策略和入侵策略进行检查。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。

入侵检查：入侵策略、规则和变量集

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则以及如何配置它们。

入侵和检查器规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包括以下由 Cisoc Talos 智能组 (Talos) 创建的规则类型：

- 共享对象入侵规则，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- 标准文本入侵规则，可以保存并修改为规则的新自定义实例。
- 预处理器规则，是指与网络分析策略中的检查器和数据包解码器检测选项关联的规则。不能复制或编辑检查器规则。默认情况下，大多数检查器规则均已禁用；您必须将其启用才能使用检查器生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。

- 数据包异常搜索查找违反既定协议（而不是包含特定内容）的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。还可以遵从 Cisco Firepower 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。

注释 当没有足够的数据包根据阻止规则处理特定流量时，系统会继续根据其他规则评估剩余流量。如果任何剩余流量与设置为阻止的规则匹配，则会话将被阻止。但是，如果系统分析要传递的剩余流量，则流量状态在规则上显示为待处理，该规则因需要完整的数据包而被卡住。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。大多数系统提供的共享对象规则和标准文本规则均使用这些预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。

重要事项 如果要创建自定义变量集，请勿使用数字作为自定义变量集名称（例如，3Snort）中的第一个字符。当您将配置部署到 防火墙管理中心上的 Firewall Threat Defense 防火墙时，这将导致 Snort 3 验证失败。

入侵事件生成

当系统识别可能的入侵时，它会生成入侵或预处理程序事件（有时统称为入侵事件）。托管设备将其事件传输到防火墙管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，托管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成检查器事件。
- 如果 IP 分片重组检查器遇到一系列重叠的 IP 片段，则检查器会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成检查器事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

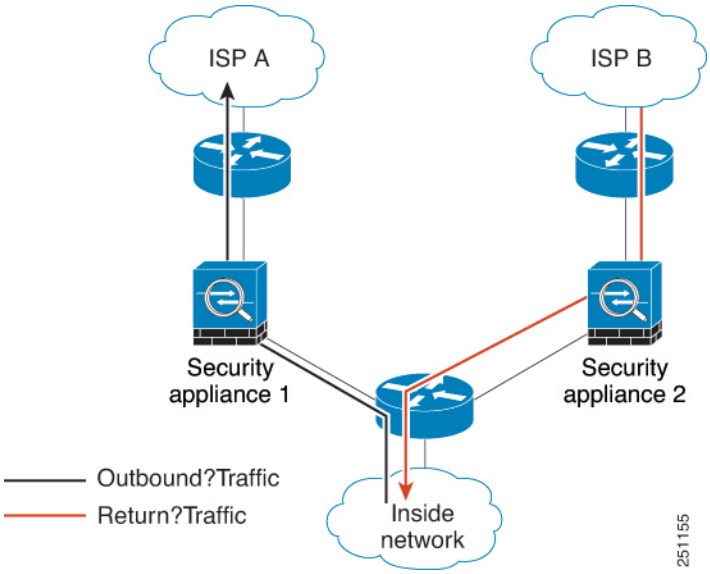
随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

Snort 中的不对称流检查

在使用不对称路由的内联部署中，由于 Snort 的单向流量可视性有限，因此会损害数据包规范化。Snort 无法从未知流方向考虑 TCP 握手参数，例如窗口缩放或最大分段大小 (MSS)，这些参数可能导致主机接收大量数据包。

在下图中，两台设备都在运行 Snort 引擎。但是，引擎都未观察到完整的流量。未完全捕获流的 TCP 三次握手，这限制了可以应用的规范化类型。但是，在对 Snort 引擎可见的流侧会执行其他有效的规范化。

图 *449:* 非对称路由



在具有非对称路由的环境中，Snort 可以无缝适应动态变化，而无需额外配置。它会根据流模式动态调整其操作。请注意，不对称流量可能会影响防火墙的有效性，可能不是最佳选择。但是，Snort 旨在在必要时为此类部署提供支持。

系统提供的与自定义的网络分析和入侵策略

创建新的访问控制策略是使用系统管理流量过程中的头几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 *Balanced Security and Connectivity* 网络分析策略是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity* 入侵策略确定的所有非恶意流量。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全智能选项（仅全局阻止列表和非阻止列表），不使用 SSL 解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略为作为默认值。Cisco 通过系统提供若干对策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的检查器选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

系统提供的网络分析和入侵策略

Cisco通过系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用 Cisco Talos 智能组 (Talos) 的经验。对于这些策略，Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

没有哪一个系统提供的策略能够涵盖所有的网络配置文件、流量组合或防御安全状况。但每个此类策略都涵盖常见情况和网络设置，为提供精细调整的防御策略奠定基础。虽然您可以按原样使用系统提供的策略，但思科强烈建议您将其作为自定义策略的基础，对其进行调整以适合您的网络。

提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少应修改默认变量集中的关键默认变量。

随着新的漏洞被发现，Talos 会发布入侵规则更新，又名 轻量安全安装包 (LSP)。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及检查器规则、

现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。您必须重新部署已更新的策略才能使其更改生效。

为方便起见，可以将规则更新配置为自动重新部署受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

为了确保获得最新的预处理设置，**必须**重新部署访问控制策略，该策略也会重新部署与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。

Cisco 通过系统提供以下网络分析和入侵策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用“平衡安全和连接”策略和设置作为默认值。

连接优先于安全网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全性比在“安全性优先于连接”(Security Over Connectivity) 策略中还要重要，有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

无活动规则入侵策略

在“无活动规则”入侵策略中，所有入侵规则和所有高级设置（除入侵规则阈值外）均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一中的已启用规则，可以尝试使用此策略。

注释 根据所选的系统提供的基本策略，该策略的设置有所不同。要查看策略设置，请点击策略旁边的**编辑**图标，然后点击**基本策略**链接。

自定义网络分析和入侵策略的优势

您可能会发现系统提供的网络分析和入侵策略中配置的检查器选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响部署，则 Web 界面将受影响策略标记为过期。

自定义网络分析策略的优势

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 Balanced Security and Connectivity 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。

可用的调整选项因检查器而异，但是可以调整检查器和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的检查器。例如，HTTP Inspect 检查器规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的检查器选项，从而减少系统处理开销。



注释 如果禁用自定义网络分析策略中的检查器，但系统稍后需要使用该检查器利用已启用的入侵或检查器规则对数据包进行评估，系统会自动启用并使用检查器，不过它在网络分析策略 Web 界面中保持禁用。

- 指定端口（如果适用）以关注某些检查器的活动。例如，可以确定要对DNS服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、HTTP 和 RPC 流量所在的端口

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）



注释 使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您**必须**注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。

自定义入侵策略的优势

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 Balanced Security and Connectivity 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 或用户。

入侵策略的主要功能是管理启用哪些入侵和检查器规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。您可以指定哪些规则应该丢弃或修改恶意数据包。
- 如果遵从Cisco的建议，则可将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 您可以修改现有规则并根据需要编写新的标准文本规则，以捕获新的漏洞或强制实施安全策略。

您可能对入侵策略进行的其他自定义包括：

- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他检查器。
- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志设施或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录设施的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

自定义策略的限制

由于预处理和入侵检测如此密切相关，因此，您**必须**小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预处理由托管设备使用单个访问控制策略处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请留意默认网络分析策略如何监管访问控制策略处理的所有流量的预处理。最初，系统提供的Balanced Security and Connectivity 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。但是，如果在自定义网络分析策略中禁用检查器，但系统需要根据已启用的入侵或检查器规则评估预处理的数据包，则系统会自动启用并使用该检查器，尽管其在网络分析策略 Web 界面中保持禁用。

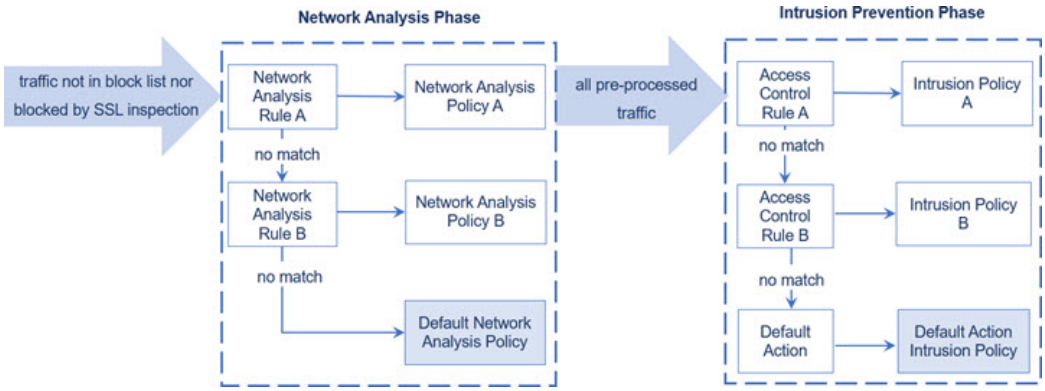
注释 要获取禁用检查器的性能优势，您 **必须** 确保自己的入侵策略均未启用需要该检查器的规则。

如果使用多个自定义网络分析策略，则会引起其他问题。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）为此，请向访问控制策略中添加自定义网络分析规则。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

提示 可以将网络分析规则配置为访问控制策略中的高级设置。与其他类型的规则不同，网络分析规则调用网络分析策略，而不是被其包含。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包**无论**由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包**不**保证将通过任何特殊入侵策略检测该数据包。您**必须**仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。

- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这**不**影响您在自定义网络分析策略中配置预处理的方式。

网络分析和入侵策略的必备条件

要允许 Snort 检测引擎处理流量以进行入侵和恶意软件分析，必须为 防火墙威胁防御 设备启用 IPS 许可证。

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。



第 IX 部分

访问控制的解密策略和加密可视性

- 流量解密概述， 第 1833 页
- 标准解密 策略， 第 1861 页
- 基于规则的解密 策略， 第 1885 页
- 基于规则的解密 规则， 第 1907 页
- 加密可视性引擎， 第 1957 页



第 44 章

流量解密概述

这些主题概述了传输层安全/安全套接字层 (TLS/SSL) 检查，讨论了 TLS/SSL 检查配置的先决条件，并详细介绍了部署场景。

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？等资源。

- 流量解密已说明， 第 1833 页
- TLS/SSL 握手处理， 第 1835 页
- 解密 规则和策略基础知识， 第 1840 页
- TLS 加密加速， 第 1849 页
- DTLS 加密加速， 第 1851 页
- 的历史记录解密策略， 第 1855 页

流量解密已说明

互联网上的大多数流量都是加密的，在大多数情况下，您可以选择不解密。您可以从加密流量中收集一些信息，也可以根据需要在网络中阻止该流量。

您的选择包括：

- 解密流量并对其进行完整的深度检查：
  - 高级恶意软件防护
  - 安全智能
  - 威胁情报导向器
  - 应用检测器
  - URL 和类别过滤

- 保持流量加密并设置访问控制和 解密策略 以查找并可能阻止：
  - 旧协议版本（例如安全套接字层）
  - 不安全的密码套件
  - 具有高风险和低业务关联性的应用
  - 不可信颁发者的可分辨名称

访问控制策略

访问控制策略是一种可调用子策略和其他配置（包括）的主配置。如果将 与访问控制相关联，则系统会在使用访问控制规则评估加密会话前使用该 解密策略对其进行处理。如果没有配置 TLS/SSL或设备不支持，则访问控制规则将处理所有加密流量。

当您的 TLS/SSL配置允许加密流量通过时，访问控制规则也会对其进行处理。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

在我们解密的协议中

我们解密的协议包括以下几种：

- TLS 版本 1.3 以下（如果已启用 Snort 3）
- 基于 HTTPS 的 DNS
- 基于 TLS 的 DNS (RFC 7858)
- FTPS、SMTPS、IMAPS、POP3S
- QUIC

注

解密规则 需要可能会影响性能的处理开销。在决定解密流量之前，请参阅何时解密流量以及何时不解密，第 1841 页。

只要托管设备启用了 Snort 3，系统就支持解密 TLS 1.3 流量。您可在 解密策略 的高级选项中启用 TLS 1.3 解密；有关详细信息，请参阅基于规则的解密策略高级选项，第 1902 页。

Firepower 系统不支持相互身份验证；也就是说，您无法将客户端证书上传到Secure Firewall Management Center并将其用于**解密 - 重新签名**、**解密 - 替换证书**，或**解密 - 已知密钥**解密规则操作。

如果使用 FlexConfig 设置 TCP 最大分段大小 (MSS) 的值，则观察到的 MSS 可能会小于您的设置。有关详细信息，请参阅关于 TCP MSS，第 816 页。

相关主题

TLS/SSL 握手处理，第 1835 页
解密 规则和策略基础知识，第 1840 页

TLS/SSL 握手处理

在本文档中，术语 *TLS/SSL* 握手表示启动 SSL 协议及其后续协议 TLS 中的加密会话的双向握手。

在内联部署中，系统处理可能会修改 ClientHello 消息并用作会话的 TCP 代理服务器的 TLS/SSL 握手。

下图显示了内联部署。



客户端确立与服务器的 TCP 连接后（成功完成 TCP 三向握手后），托管设备会监控 TCP 会话的任何启动加密会话的尝试。TLS/SSL 握手通过使用交换客户端与服务器之间的专门数据包来确立加密会话。在 SSL 和 TLS 协议中，这些专门数据包称为握手消息。握手消息传达客户端和服务器都支持的加密属性：

- ClientHello - 客户端为每个加密属性指定多个受支持的值。
- ServerHello - 服务器为每个加密属性指定一个受支持的值，而 ServerHello 响应会确定安全会话期间系统使用的加密方法。

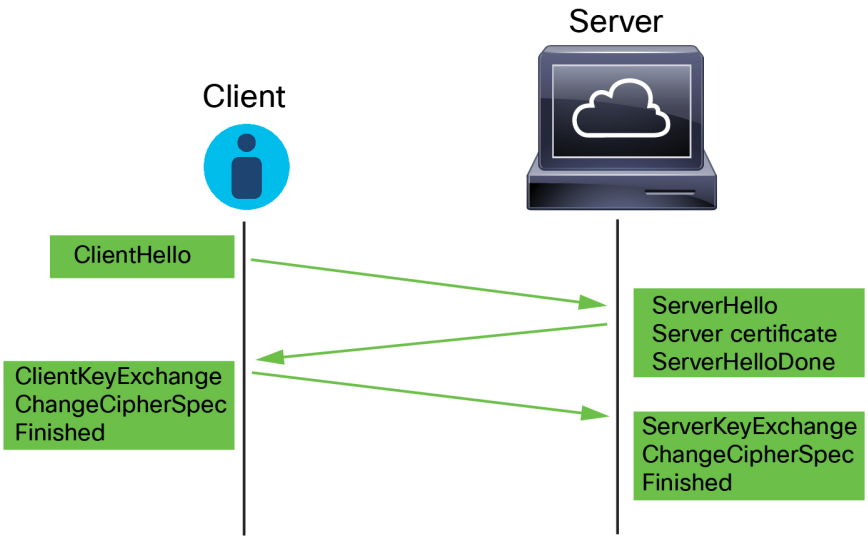
TLS/SSL 握手完成后，托管设备缓存加密会话数据，这允许在不需要完全握手的情况下进行会话恢复。托管设备还缓存服务器证书数据，这允许在使用相同证书的后续会话中更快速地处理握手。

ClientHello 消息的处理

客户端将 ClientHello 消息发送到一台服务器，如果可以建立安全连接，则该服务器将作为数据包的目标。客户端发送信息以启动 TLS/SSL 握手，或者用于响应目标服务器的 ServerHello 消息。

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以在 cloudflare.com 上查阅诸如 TLS 握手中发生的情况？等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

   ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当托管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称，第 2637 页。

3. 当托管设备收到这些消息时，会尝试将其与系统上配置的 解密规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 解密规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

数据交换

如果配置 TLS/SSL 解密，当托管设备收到 ClientHello 消息时，系统会尝试将该消息与具有**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**操作的解密规则进行匹配。该匹配依赖于来自 ClientHello 消息的数据，以及来自缓存服务器证书数据的数据。可能的数据包括：

表 *107:* 解密规则 条件的数据可用性

解密规则 条件	数据所在位置
区域	ClientHello
网络	ClientHello

解密规则 条件	数据所在位置
VLAN 标记	ClientHello
端口	ClientHello
用户	ClientHello
应用	ClientHello（服务器名称指示器扩展）
类别	ClientHello（服务器名称指示器扩展）
证书	服务器证书（可能已缓存）
可分辨名称	服务器证书（可能已缓存）
证书状态	服务器证书（可能已缓存）
密码套件	ServerHello
版本	ServerHello



重要事项 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。请勿将**密码套件**和**版本**用于**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**规则操作。在具有其他规则操作的规则中，这些条件可能会干扰系统的ClientHello处理，从而导致不可预测的性能。

ClientHello 修改

如果 ClientHello 消息与**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**规则匹配，系统会按如下方式修改 ClientHello 消息：

- （仅 TLS 1.2；TLS 1.3 不支持压缩。）压缩方法 - 删除 `compression_methods` 元素（其指定客户端所支持的压缩方法）。系统无法解密压缩的会话。
- 密码套件 - 如果系统不支持密码套件，则从 `cipher_suites` 元素中删除它们。如果系统不支持任何指定的密码套件，则系统将传输原始的未经修改的元素。此修改会减少无法解密的流量的“未知密码套件”(Unknown Cipher Suite) 和“不受支持的密码套件”(Unsupported Cipher Suite) 类型。
- 会话标识符 - 删除 `Session Identifier` 元素和 SessionTicket extension (RFC 5077, sec 3.2) 中任何与缓存会话数据不匹配的值。如果 ClientHello 值与缓存数据相匹配，则中断的会话无需客户端和服务器执行完整的 TLS/SSL 握手操作也可恢复。此修改会增加会话恢复的机会，并减少无法解密的流量的“不缓存会话”(Session Not Cached) 类型。
- 椭圆曲线 - 如果系统不支持椭圆曲线，则从受支持的椭圆曲线扩展中删除它们。如果系统不支持任何指定的椭圆曲线，则托管设备将删除扩展，并从 `cipher_suites` 元素中删除任何相关的密码套件。

- ALPN 扩展 - 删除应用层协议协商 (ALPN) 扩展中不受系统支持的任意值（例如，HTTP/2 协议）。
- 其他扩展 - 删除下次协议协商 (NPN) 和 TLS 通道 ID 扩展。

  目前，具有**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**操作的解密规则在 ClientHello 协商期间在本地支持扩展主密钥 (EMS) 扩展，从而实现更安全的通信。EMS 扩展由 RFC 7627 定义。

在系统修改 ClientHello 消息后，它会确定消息是否通过访问控制评估（可能包括深度检测）。如果消息通过评估，则系统会将其传输到目标服务器。

如果 ClientHello 消息与**解密 - 重新签名**、**解密 - 替换证书** 或**解密 - 已知密钥** 规则不匹配，则系统不会修改消息。然后，它会确定消息是否通过访问控制评估（可能包括深度检查）。如果消息通过检查，则系统会将其传输到目标服务器。

如果流量与**监控**规则条件匹配，则不会修改 ClientHello。

中间人

在 TLS/SSL 握手过程中，客户端和服务器之间无法再进行直接通信，因为在消息修改之后，由客户端和服务器计算的消息身份验证代码 (MAC) 不再匹配。对于所有后续的握手消息（和已建立的加密会话），托管设备将充当中间人。它创建两个 TLS/SSL 会话，一个是客户端与托管设备之间的会话，一个是托管设备与服务器之间的会话。因此，每个会话包含不同的加密会话详细信息。

注释 系统可以解密的密码套件会频繁更新，且其无法直接对应于您可以在解密规则条件中使用的密码套件。有关可解密密码套件的当前列表，请联系思科 TAC。

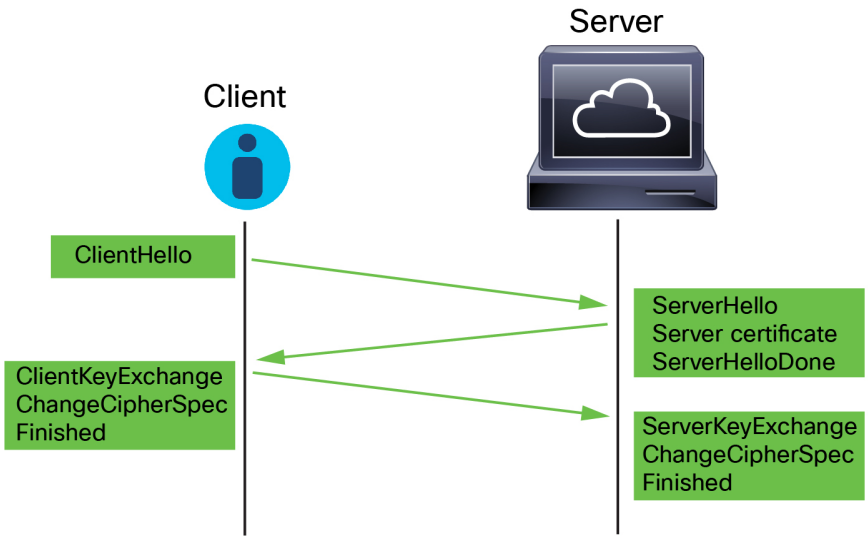
相关主题

无法解密流量的默认处理选项，第 1900 页
ServerHello 和服务器证书消息处理，第 1838 页

ServerHello 和服务器证书消息处理

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以在 cloudflare.com 上查阅诸如 TLS 握手中发生的情况？等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

   ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当托管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称，第 2637 页。

3. 当托管设备收到这些消息时，会尝试将其与系统上配置的 解密规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 解密规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

基于规则的解密 规则操作

如果消息与任何 解密规则 都不匹配，托管设备将执行 基于规则的解密策略默认操作，第 1899 页。

如果消息与属于与访问控制策略关联的 解密策略 的规则匹配，则托管设备会根据需要继续：

操作：“监控”(Monitor)
TLS/SSL 握手继续完成。托管设备会跟踪并记录流量，但不会对其进行解密。

操作：“阻止”(Block) 或“阻止并重置”(Block with reset)

托管设备会阻止 TLS/SSL 会话，并重置 TCP 连接（如已配置）。

操作：“不解密”(Do Not Decrypt)

TLS/SSL 握手继续完成。托管设备不解密 TLS/SSL 会话期间交换的应用数据。

操作：解密 - 替换证书

解密传入流量，并将证书替换为在解密规则中配置的内部证书对象。解密规则中配置的证书可以与内部服务器的证书相同，也可以不同；此外，您可以随时替换此证书。要更新证书，请使用 **对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)** 或 API。

操作：“解密 - 已知密钥”(Derypt - Known Key)

托管设备尝试将服务器证书数据与先前导入 Secure Firewall Management Center 的内部证书对象进行匹配。由于您无法生成内部证书对象，并且您必须拥有其私钥，因此假设您拥有在其上使用已知密钥解密的服务器。

如果此证书与已知证书匹配，则 TLS/SSL 握手将继续完成。托管设备使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

如果服务器在与客户端的初始连接和后续连接之间更改其证书，则必须在 Secure Firewall Management Center 中导入新服务器证书，以便用于将来解密连接。

操作：“解密 - 重新签名”(Decrypt - Resign)

托管设备将处理服务器证书消息并使用之前上传或生成的证书颁发机构 (CA) 证书重签服务器证书。TLS/SSL 握手继续完成。托管设备随手会使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

注释 Firepower 系统不支持相互身份验证；也就是说，您无法将客户端证书上传到Secure Firewall Management Center并将其用于**解密 - 重新签名**、**解密 - 替换证书**，或**解密 - 已知密钥**解密规则操作。

相关主题

ClientHello 消息的处理，第 1835 页

解密 规则和策略基础知识

本节讨论创建 解密策略 和规则时应牢记的信息。

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？等资源。

相关主题

解密案例，第 1841 页
何时解密流量以及何时不解密，第 1841 页
其他 解密规则 操作，第 1845 页
解密规则 组件，第 1845 页
解密规则基于规则的解密规则 顺序评估，第 1846 页

TLS 1.3 解密最佳实践，第 1904 页

解密案例

允许或阻止通过系统时加密的流量，但不能对其进行深度检查或全面的策略实施（例如入侵防御）。

所有已加密的连接：

- 通过 解密策略 发送，以确定是否应解密或阻止它们。

  您还可以配置 解密规则 以阻止您知道不想在网络上传输的类型的加密流量，例如使用非安全 SSL 协议的流量或具有过期或无效证书的流量。

- 如果未被阻止，无论是否解密，流量都要经过访问控制策略，以做出最终的允许或阻止决定。

只有已解密的流量才能利用系统的威胁防御和策略实施功能，包括：

- 高级恶意软件防护
- 安全智能
- 威胁情报导向器
- 应用检测器
- URL 和类别过滤
- QUIC

请记住，解密并重新加密流量会增加设备的处理负载，从而会降低整体系统性能。

总结：

- 可以通过策略允许或阻止已加密的流量；无法检查已加密的流量
- 已解密的流量受威胁防御和策略实施的约束；可以通过策略允许或阻止已解密的流量。

  检测使用 StartTLS（SMTPS、POPS、FTPS、TelnetS、IMAPS）的加密应用流量。还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的使用者专有名称来识别某些加密应用。

相关主题

使用文件和入侵策略的深度检测，第 1750 页

何时解密流量以及何时不解密

本节提供有关何时应解密流量以及何时应允许其通过加密防火墙的准则。

何时不解密流量

如果是以下情况，则不应对流量进行解密：

- 法律所禁止；例如，某些司法管辖区禁止解密财务信息

- 公司政策所禁止；例如，您的公司可能会禁止解密特权通信
- 隐私法规所禁止
- 使用证书固定（也称为*TLS/SSL*固定）的流量必须保持加密，以防止断开连接

（Snort 3。）对于任何符合访问控制规则的信任、阻止或阻止并重置的连接，除非流量被预先过滤，否则 解密策略 不会被绕过。加密流量会首先由 解密策略 进行评估，然后进入访问控制策略，在其中做出最终的允许或阻止决策。

加密流量可以在任何 解密规则 条件下被允许或阻止，包括但不限于：

- 证书状态（例如，证书已过期或无效）
- 协议（例如，非安全 SSL 协议）
- 网络（安全区域、IP 地址、VLAN 标记等）
- URL 类别和信誉
- 端口
- 用户组

解密规则 为您不想解密的流量提供**不解密**操作；有关详细信息，请参阅基于规则的解密 规则 不解密操作，第 1938 页。



注释 本主题末尾的相关信息链接解释了规则评估的某些方面是如何运作的。URL 和应用过滤等条件对加密流量存在限制。请确保您了解这些限制。

有关在 **不解密** 规则中使用URL过滤的详细信息，请参阅基于规则的解密 规则 不解密操作，第 1938 页。

何时解密流量

系统的威胁防护和策略实施功能必须在解密所有加密流量后才能发挥作用。如果您的托管设备有足够的内存和处理能力来解密流量，则应解密法律法规未禁止的流量。

如果您必须决定哪些流量要解密，请根据网络上允许流量的风险做出决定。系统提供了一个灵活框架，它会利用规则条件（包括 URL 信誉、密码套件、协议和许多其他因素）来对流量进行分类。

相关主题

解密和重新签名（传出流量），第 1844 页
基于规则的解密规则准则和限制，第 1908 页
解密策略 规则顺序
URL 条件（URL 过滤）
应用程序规则顺序，第 1760 页
TLS 1.3 解密最佳实践，第 1904 页

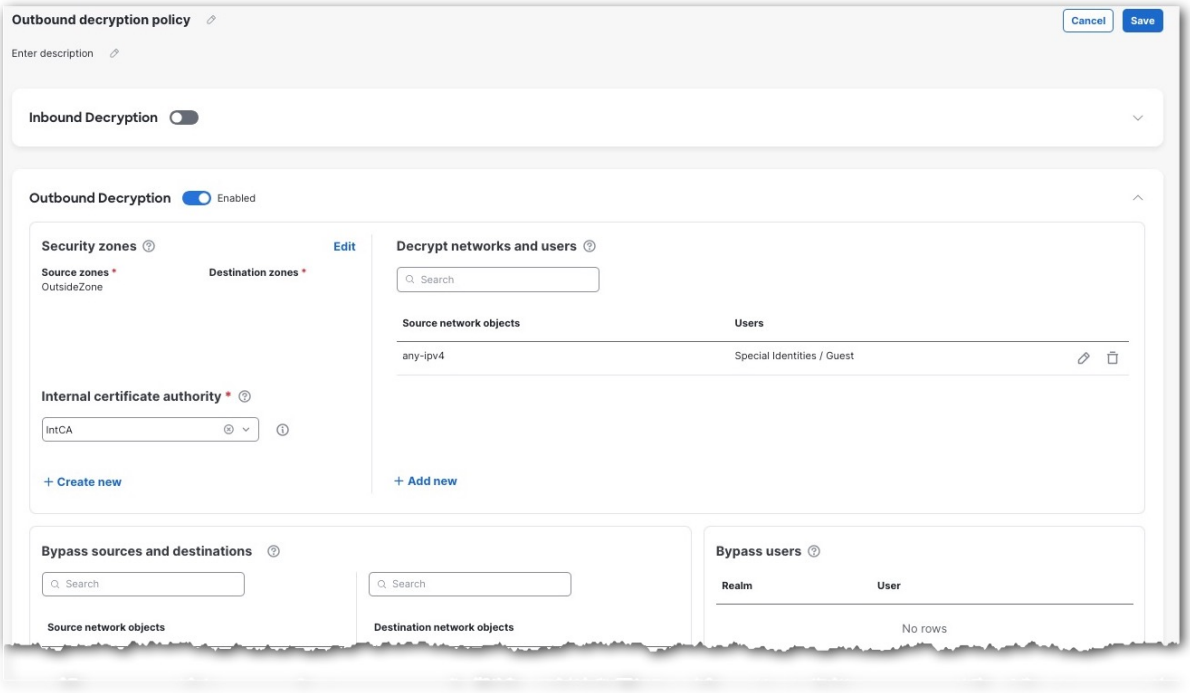
哪种类型的解密策略适合我？

本主题讨论 标准解密 策略和 基于规则的解密 策略。

标准解密策略

我们建议使用标准 解密策略类型，因为它具有向导式的外观，易于设置，使您能够轻松选择要在策略中使用的安全区、用户和网络以及其他对象。标准解密策略特别适合不熟悉解密策略细节的用户。

以下是设置标准解密策略的示例。



前述策略仅解密传出流量。来自任何 IPv4 网络上 OutsideZone 安全区域的所有流量均使用名为 `IntCA` 的内部 CA 解密。

请注意以下事项：

- 前面的规则是不完整的示例，还有更多可用选项
- 您可以配置入站条件和/或出站条件。
- 除了 对象，您还可以选择配置出站解密排除项，如：
  - 无法解密的应用（例如使用证书锁定的应用）。
  - URL 类别，例如医疗、贸易和财务。
- 您可以为证书状态和 TLS 版本配置出站阻止规则。
- 标准策略具有类似于旧版策略的高级策略选项。

基于规则的解密策略

使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。

基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。

解密和重新签名（传出流量）

此信息仅适用于 基于规则的解密 策略和规则。

解密 - 重新签名 (Decrypt - Resign) 解密规则 操作使系统能够充当中间人，拦截、解密以及（如果允许流量通过）检查和重新加密。**解密 - 重新签名 (Decrypt - Resign)** 规则操作用于传出流量；也就是说，目的服务器在受保护的网络之外。

Firewall Threat Defense 设备会使用规则中指定的内部证书颁发机构 (CA) 对象来与客户端协商，并在客户端和 Firewall Threat Defense 设备之间建立 TLS/SSL 隧道。同时，设备连接至目标网站，并在服务器和 Firewall Threat Defense 设备之间建立 TLS/SSL 隧道。

因此，客户端将看到配置用于 解密规则 的 CA 证书，而不是来自目标服务器的证书。客户端必须信任防火墙的证书才能完成连接。Firewall Threat Defense 设备随后会对客户端和目标服务器之间的流量执行双向解密/重新加密。

前提条件

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，您必须使用 CA 文件和配对的私钥文件创建内部 CA 对象。如果您还没有 CA 和私钥，则可以在系统中生成它们。

我们简化了配置**解密 - 重新签名 (Decrypt - Resign)** 规则的过程，方法是根据您对免于加密的流量类型（例如无法解密的应用）的选择，将**不解密 (Do Not Decrypt)** 规则自动添加到解密策略中。（通常情况下，这些应用使用证书锁定功能，因此解密连接会中断连接。）有关详细信息，请参阅创建具有出站连接保护的 基于规则的解密策略 ，第 1887 页。

注释 Firepower 系统不支持相互身份验证；也就是说，您无法将客户端证书上传到Secure Firewall Management Center并将其用于**解密 - 重新签名**、**解密 - 替换证书**，或**解密 - 已知密钥**解密规则操作。

相关主题

基于规则的解密 规则解密操作 ，第 1939 页
外部证书对象 ，第 2668 页

传入流量解密

此信息仅适用于 基于规则的解密 策略和规则。

使用已知密钥进行解密的主要目的是保护服务器免受外部攻击。

注释 Firepower 系统不支持相互身份验证；也就是说，您无法将客户端证书上传到Secure Firewall Management Center并将其用于**解密 - 重新签名**、**解密 - 替换证书**，或**解密 - 已知密钥**解密规则操作。

入站解密类型

有两种类型的入站解密：

- 替换证书（默认）：使用解密规则中定义的证书和密钥解密流量。此证书和密钥可以是内部服务器的证书，也可以是其他证书；此外，您可以随时更改证书和密钥。可以通过以下方式之一获取证书：
  - *Cisco Secure Firewall Threat Defense REST API* 指南中讨论的 API 。
  - 自动化证书管理环境 (ACME)
  - Secure Firewall Management Center中的**对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**

  我们建议您在模板中包含证书颁发机构链。
- 已知密钥 (Known Key)：使用内部服务器的证书解密传入流量。如果证书发生更改，您必须手动对其进行更新，从而中断解密，直到新证书在解密策略中和服务器上就位。

其他 解密规则 操作

此信息仅适用于 基于规则的解密 策略和规则。

这些主题讨论其他 解密规则 操作。

相关主题

基于规则的解密 规则阻止操作 ，第 1939 页
基于规则的解密 规则监控操作 ，第 1937 页

解密规则 组件

此信息仅适用于 基于规则的解密 策略和规则。

每个 解密规则 都有以下组件。

状态

规则可以具有两种状态之一：“已启用”或“已禁用”。默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

解密策略 中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。

条件

条件指定规则处理的特定流量。条件可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书使用者或颁发者、证书状态、密码套件或加密协议版本来匹配流量。使用条件取决于目标设备许可证。

操作

规则操作确定系统如何处理匹配的流量。您可以对加密的匹配流量执行监控、允许、阻止或解密操作。解密的流量会受到进一步检查。请注意，系统不对被阻止的加密流量执行检查。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。您可以在系统阻止加密会话或允许其未经解密便通过（取决于 解密策略中的设置）时记录连接。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。您可以将连接记录到Secure Firewall Management Center数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

有关日志记录的详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的连接日志记录最佳实践。

提示 正确创建解密规则并对其排序是一项复杂的任务。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，解密策略接口具有功能强大的规则警告和错误反馈系统。

我们建议您创建一个标准解密策略以避免这些复杂性。标准策略易于创建，并且可以避免我们的客户遇到的许多问题。有关详细信息，请参阅哪种类型的解密策略适合我？ ，第 1843 页

类别

有关使用 解密规则 类别（例如“应用”、“类别”和“证书状态”）的信息，请参阅 解密规则基于规则的解密规则 条件 ，第 1920 页。

解密规则基于规则的解密规则 顺序评估

此信息仅适用于 基于规则的解密 策略和规则。

在 基于规则的解密策略 中创建 基于规则的解密规则 时，您可以使用规则编辑器中的**插入**列表来指定其位置。 解密策略 中的 解密规则 会从 1 开始编号。系统按升序规则编号以自上而下的顺序将流量与 解密规则 相匹配。

在大多数情况下，系统根据第一个 解密规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 类别和信誉、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，它会通过访问控制来检查加密流量和无法解密的流量。但是，访问控制规则条件需要未加密流量，因此，已加密流量匹配的规则更少。

使用特定条件（例如网络和 IP 地址）的规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物

理、数据链路和网络）条件的规则应首先在规则中排序。稍后应在规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。



提示 适当的解密规则顺序可减少处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

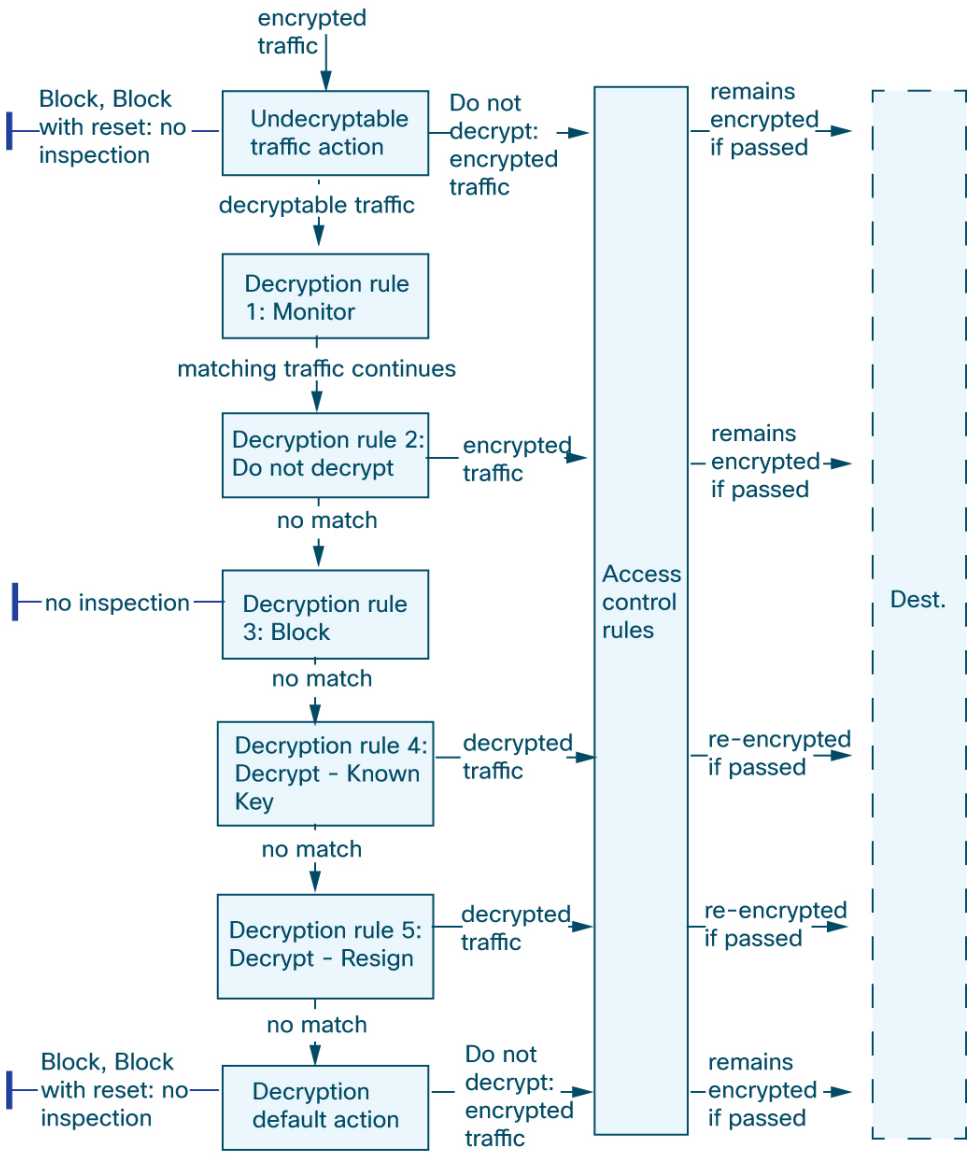
除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

相关主题

访问控制规则的最佳实践，第 1758 页
无法解密流量的默认处理选项，第 1900 页
解密策略 规则顺序

多规则示例

下述场景概括说明了 解密规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，**Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **解密规则 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **解密规则 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **解密规则 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。

- 第五，使用 **解密规则 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 解密规则 不匹配的流量会继续根据下一规则进行评估。
- **解密规则 5: Decrypt - Resign** 是最终规则。如果流量匹配，系统将使用上传的 CA 证书重新签名服务器证书并解密流量。然后，根据访问控制规则对解密流量进行评估，以同等对待已解密和未加密的流量。这项额外的检查可以让系统阻止交通。剩余的所有流量在发送到目标之前都会重新加密。与 解密规则 规则不匹配的流量将继续处理下一条规则。
- **解密策略 Default Action** 会处理与任何 解密规则 不匹配的所有流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

TLS 加密加速

TLS 加密加速 加快以下操作：

- TLS/SSL 加密和解密。
- VPN，包括TLS/SSL和 IPsec

支持的硬件

以下硬件型号支持 TLS 加密加速：

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持防火墙威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。



注释 有关 TLS 加密加速 和 4100/9300 的详细信息，请参阅 *FXOS* 配置指南。

以下方不支持的功能 TLS 加密加速

TLS 加密加速不支持的功能包括：

- 启用了 防火墙威胁防御 容器实例 的托管设备。
- 如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

  此行为受 **configure snort preserve-connection {enable | disable}** 命令控制。

TLS 加密加速准则和限制

如果托管设备启用了 TLS 加密加速，请记住以下几点。

仅 HTTP 性能

在不对流量进行解密的托管设备上使用 TLS 加密加速可能会影响性能。

联邦信息处理标准 (FIPS)

如果同时启用了 TLS 加密加速 和联邦信息处理标准 (FIPS)，则与以下选项的连接会失败：

- 大小小于 2048 字节的 RSA 密钥
- Rivest 密码 4 (RC4)
- 单一数据加密标准（单一 DES）
- Merkle – Damgard 5 (MD5)
- SSL v3

当您将 防火墙管理中心 和托管设备配置为以安全认证合规模式运行时，FIPS 会被启用。在这些模式下运行时，要允许连接，则可配置 Web 浏览器以接受更为安全的选项。

了解更多信息：

- FIPS 支持的密码：关于 SSL 设置，第 1007 页。
- 安全认证合规模式。
- 通用条件。

TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速的托管设备遇到使用 SSL 检测信号扩展的数据包时，托管设备将执行 解密策略 的**无法解密的操作**中**解密错误**的设置所指定的操作：

- 阻止
- 阻止并重置

有关详细信息，请参阅无法解密流量的默认处理选项，第 1900 页。

要确定应用是否正在使用 TLS 心跳，请参阅对 TLS 心跳进行故障排除，第 1948 页。

您可以在网络分析策略 (NAP) 中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。有关详细信息，请参阅SSL 预处理器。

TLS/SSL 超订用

TLS/SSL 超订用是托管设备过载 TLS/SSL 流量的状态。任何托管设备都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速的托管设备才提供可配置的方式对其进行处理。

启用了 TLS 加密加速 的托管设备在超订用时，托管设备接收的任何数据包都根据 解密策略 的**无法解密的操作**中**握手错误**设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 解密策略的 **无法解密的操作** 中 **握手错误** 的设置为 **不解密** ，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密 不会 发生。

如果出现大量超订用，有以下选项可供选择：

- 升级托管设备以提高 TLS/SSL 处理能力。
- 更改您的 解密策略，为不具有较高解密优先级的流量添加**不解密**规则。

查看 TLS 加密加速的状态

本主题讨论如何确定是否已启用 TLS 加密加速。

请执行 防火墙管理中心 中的下列任务。

过程

步骤 1 登录防火墙管理中心。

步骤 2 请点击 **设备** > **设备管理**。

步骤 3 点击 **编辑**（ ） 以编辑托管设备。

步骤 4 点击**设备 (Device)**页面。TLS 加密加速 状态显示在“常规”(General) 部分中。

DTLS 加密加速

Firewall Threat Defense 支持以下型号的数据报传输层安全 (*DTLS*) 加密加速：

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

Cisco Secure Firewall 4200 和 3100 系列设备在 FPGA 和 Nitrox V 加密加速器的帮助下支持 DTLS 加密加速。

在 Cisco Secure Firewall 6100 中，两个加密加速器取代了 Nitrox V：一个用于公共密钥基础设施 (PKI) 加速，另一个用于 IPsec 和 DTLS 分流。仅支持 AES-GCM 128 和 256 密码。

此功能可提高 DTLS 加密和 DTLS 解密流量的吞吐量。支持 IPv4 和 IPv6 流量。

Firewall Threat Defense还会对出口加密数据包执行优化，以改善延迟。数据路径经过优化，可增强单个隧道流的性能。

默认情况下，这两项功能均已启用，并且仅适用于 DTLS 1.2。

不支持这些功能：

- 流使用 DTLS 1.0 或数据包压缩
- 重新生成密钥的 DTLS 密钥
- 集群或多实例模式

您可以使用 FlexConfig 以及 **no flow-offload-dtls** 和 **no flow-offload-dtls egress-optimization** 命令禁用 DTLS 加密加速。

DTLS 加密加速的先决条件

支持的许可证

- 管理中心 Essentials（以前称为 Base）许可证必须允许导出控制功能。

  选择 **管理** > **许可证** > **智能许可证** 在管理中心验证此功能。

支持的版本

- 防火墙管理中心 的版本必须为 7.6.0 及更高版本。
- Cisco Secure Firewall 4200 和 3100 系列设备必须为版本 7.6.0 及更高版本。

支持的设备

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

监控 DTLS 加密加速

在威胁防御设备上使用以下 CLI 命令验证并监控出口加密数据包的 DTLS 加密加速和优化。

- 要验证 DTLS 加密加速和出口加密数据包优化的状态，请使用以下命令：

```
> show flow-offload-dtls info
  DTLS offload : Enabled
  Egress Optimization: Enabled
```

- 要查看 DTLS 加密加速统计信息，请使用以下命令：

```
> show flow-offload-dtls statistics
  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 975638666
  Tx Packet count : 975638666
  Error Packet count : 0
  Drop Packet count : 0

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 1145314723
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 0
  6-Tuple CAM Hit Count : 975638666
  6-Tuple CAM Miss Count : 169676057
   NOTE: The counters displayed are cumulative counters
   for all offload applications and indicates the total packets
  offloaded
```

- 要查看设备中用于 Cisco Secure Firewall 3100 和 4200 的 Nitrox V 加密加速器统计信息，请使用以下命令：

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
<snip>
[Offloaded SSL Input statistics, Pipe 0]
      Input packets: 290593023
      Input bytes: 147049729714
      Decrypted packets: 290593023
      Decrypted bytes: 147049729714
   [Offloaded SSL Output statistics, Pipe 0]
      Output packets: 254271808
      Output bytes: 136352952720
      Encrypted packets: 254271808
      Encrypted bytes: 136352952720
.
.
.
```

- 要查看 Cisco Secure Firewall 6100 的加密加速器统计信息，请使用以下命令：

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
<snip>
[Accelerator 0]
   Status: OK
```

```
   Software crypto engine
<snip>
[Accelerator 1]
   Status: OK
   Asymmetric Crypto Accelerator
<snip>
[Accelerator 4]
   Status: OK
   Asymmetric Crypto Accelerator
[Accelerator 5]
   Status: OK
   Offload Crypto Accelerator
      [Offloaded IPSec Input statistics, Pipe 0]
      [Offloaded IPSec Output statistics, Pipe 0]
<snip>
[Accelerator 8]
   Status: OK
   Offload Crypto Accelerator
      [Offloaded IPSec Input statistics, Pipe 3]
      [Offloaded IPSec Output statistics, Pipe 3]
```

- 要查看 Cisco Secure Firewall 6100 的加密加速计划版本，请使用以下命令：

```
> show version
<snip>
CSF6170 up 5 days 14 hours
Start-up time 12 secs
Hardware:   CSF-6170, 785423 MB RAM, CPU AMD Zen 5 2700 MHz, 2 CPUs (512 cores)
Encryption hardware device: Cisco Asymmetric Crypto Accelerator, hw version 0x00010001

                          : Cisco Asymmetric Crypto Accelerator, hw version 0x00010001

                          : Cisco Asymmetric Crypto Accelerator, hw version 0x00010001

                          : Cisco Asymmetric Crypto Accelerator, hw version 0x00010001

                          : Cisco Offload Crypto Accelerator, hw version 0x00000001
                          : Cisco Offload Crypto Accelerator, hw version 0x00000001
                          : Cisco Offload Crypto Accelerator, hw version 0x00000001
                          : Cisco Offload Crypto Accelerator, hw version 0x00000001

<snip>
```

的历史记录解密策略

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
	10.0.0	解密策略	您可以创建以下任何类型的解密策略： • 解密策略：也称为 标准解密 策略。我们建议使用标准解密策略类型，因为它具有向导式的外观，易于设置，使您能够轻松选择要在策略中使用的安全区、用户、网络以及其他对象。标准解密策略特别适合不熟悉解密策略细节的用户。 • 基于规则的解密 策略：使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。 **新增/修改的屏幕: 策略** > **解密** > **创建新** > **解密策略** **策略** > **解密** > **创建新** > **解密策略**（**基于规则**）
用于 Cisco Secure Firewall 3100/4200 的硬件 DTLS 1.2 加密加速。	7.6.0	7.6.0	Cisco Secure Firewall 3100/4200 现在支持 DTLS 1.2 加密加速和出口优化，从而提高了 DTLS 加密和解密流量的吞吐量。新设备和升级后的设备会自动启用该功能。要禁用，请使用 FlexConfig。 新增经修改的 FlexConfig 命令：**flow-offload-dtls**、**flow-offload-dtls egress-optimization**、**show flow-offload-dtls**
QUIC 解密。	10.0.0（Beta 版） 7.7.0（实验性） 7.6.0（实验性）	带有 Snort 3 的 7.6.0	您可以配置解密策略以应用于在 QUIC 协议上运行的会话。默认情况下，QUIC 解密处于禁用状态。您可以根据解密策略选择性地启用 QUIC 解密，并编写解密规则以应用于 QUIC 流量。通过解密 QUIC 连接，系统可以检查连接是否被入侵、是否有恶意软件或其他问题。您还可以根据访问控制策略中的特定条件来对已解密的 QUIC 连接应用精细控制和过滤。 我们修改了解密策略高级设置，以包含用于启用 QUIC 解密的选项。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
轻松绕过解密敏感和不可解密的流量。	7.6.0	7.6.0	现在，绕过敏感和不可解密流量的解密变得更加容易，从而保护了用户并提高了性能。 新的解密策略现在包括预定义规则，如果启用，可自动绕过敏感 URL 类别（如金融或医疗）、不可解密的区分名称和不可解密的应用的解密。可分辨名称和应用无法解密，这通常是因为它们使用 TLS/SSL 证书锁定，而证书锁定本身无法解密。 对于出站解密，可以在创建策略时启用/禁用这些规则。对于入站解密，规则默认为禁用。创建策略后，您可以编辑、重新排序或完全删除规则。 新增/修改的菜单项：**策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)** > **创建解密策略 (Create Decryption Policy)**
解密策略。	7.3.0	7.3.0	功能已重命名为解密策略，以更好地体现其功能。现在，您可以使用一个或多个**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Decrypt - Known Key)** 规则来配置解密策略。 新增/修改的菜单项： • **策略** > **访问控制标题** > **解密**（新建解密策略） • “创建机密策略”(Create Decryption Policy) 对话框现在有两个选项卡页面：**出站连接 (Outbound Connections)** 和**入站连接 (Inbound Connections)**。 使用**出站连接 (Outbound Connections)** 选项卡页面配置一个或多个具有**解密 - 重新签名 (Decrypt - Resign)** 规则操作的解密规则。（可以同时上传或生成证书颁发机构）。CA 与网络和端口的每种组合都会产生一个解密规则。 使用“入站连接”(Inbound Connections) 选项卡页面配置一个或多个具有“解密 - 已知密钥”(Decrypt - Known Key) 规则操作的解密规则。（您可以同时上传服务器的证书。）服务器证书与网络和端口的每个组合都会产生一个解密规则。 • **策略** > **访问控制标题** > **解密**（编辑解密规则）**高级设置**包含TLS 1.3 解密最佳实践，第 1904 页中讨论的新选项。 • **策略** > **访问控制标题** > **访问控制**（编辑访问控制策略），点击**解密**一词，将解密策略与访问控制策略相关联。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
TLS 1.3 解密。	7.2.0	7.2.0	现在，您可以在 SSL 策略的高级操作中启用 TLS 1.3 解密。TLS 1.3 解密需要托管设备运行 Snort 3。 同时还有其他选项；有关详细信息，请参阅TLS 1.3 解密最佳实践，第 1904 页。 新增/修改的屏幕：**SSL 策略 (SSL Policy)** > **高级设置 (Advanced Settings)**
SSL 策略高级设置。	7.2.0	7.1.0	SSL 策略高级设置 新增/修改的屏幕：**SSL 策略 (SSL Policy)** > **高级设置 (Advanced Settings)**
能够指定具有未知信誉的 URL 的处理方式。	6.7.0	6.7.0	有关详细信息，请参阅关于使用类别和信誉进行URL过滤，第1786页。
用于 **解密 - 已知** 密钥规则。	6.7.0	6.7.0	有关详细信息，请参阅ClientHello 消息的处理，第 1835 页。
能够提取 TLS 1.3 流量中的证书，以便让流量能够匹配访问控制规则中的 URL 和应用条件。	6.7.0	6.7.0	新增/修改的屏幕：**策略 (Policies)** > **访问控制 (Access Control)** > （**编辑访问控制策略**） > **高级 (Advanced)**链接。 有关详细信息，请参阅基于规则的解密策略高级选项，第 1902 页。
基于类别和信誉的URL过滤更改。	6.7.0	6.5.0	有关详细信息，请参阅关于使用类别和信誉进行URL过滤，第1786页。
TLS 加密加速 无法禁用。	6.4.0	6.4.0	TLS 加密加速 会在所有支持的设备上启用。 在具有本地接口的托管设备上，无法禁用 TLS 加密加速。 对 防火墙威胁防御 容器实例 上 TLS 加密加速 的支持是有限的，如此表的下一行所述。 删除的命令： • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持将 TLS 加密加速用于 Firepower 4100/9300 模块/安全引擎上的一个防火墙威胁防御 容器实例 。	6.4.0	6.4.0	您现在可以在模块/安全引擎上为一个 防火墙威胁防御 容器实例 启用 TLS 加密加速。TLS 加密加速 对其他容器实例禁用，但对本地实例启用。 新增/经修改的命令： • **config hwCrypto enable** • **show crypto accelerator status** 取代 **system support ssl-hw-status**）
TLS/SSL 硬件加速 现在称为 *TLS* 加密加速。	6.4.0	6.4.0	名称更改体现了可在更多设备上支持 TLS/SSL 加密和解密加速。根据设备的不同，加速可以在软件或硬件中执行。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **编辑 (Edit)** > **设备 (Device)** > **常规 (General)** > **TLS 加密加速 (TLS Crypto Acceleration)**
支持扩展主密钥扩展（请参阅 RFC 7627）。	6.3.0.1	6.3.0.1	SSL 策略支持 TLS 扩展主密钥扩展；具体而言，是指具有**解密 - 重新签名**或**解密 - 已知密钥**规则操作的策略。
不支持扩展主密钥扩展。	6.3.0	6.3.0	在 ClientHello 修改**解密 - 重新签名**规则期间删除此扩展。
TLS/SSL 硬件加速 默认为已启用。	6.3.0	6.3.0	TLS/SSL 硬件加速 默认为在所有支持的设备上启用，但是如有需要，可以禁用它。
支持扩展主密钥扩展（请参阅 RFC 7627）。	6.2.3.9	6.2.3.9	SSL 策略支持 TLS 扩展主密钥扩展；具体而言，是指具有**解密 - 重新签名**或**解密 - 已知密钥**规则操作的策略。
积极的 TLS 1.3 降级。	6.2.3.7	6.2.3.7	使用 **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI 命令，可以确定将 TLS 1.3 流量降级到 TLS 1.2 的行为。有关详细信息，请参阅 *Cisco Secure Firewall Threat Defense 命令参考*。
TLS/SSL 硬件加速 已引入。	6.2.3	6.2.3	某些托管设备型号会在硬件中执行 TLS/SSL 加密和解密，从而提高性能。默认情况下，此功能处于启用状态。 受影响的屏幕：要查看 TLS/SSL 硬件加速的状态，**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)**，常规 (General) 页面。
支持类别和信誉条件。	6.2.2	6.2.2	具有类别/信誉条件的访问控制规则或 SSL 规则。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
支持安全搜索。	6.1.0	6.1.0	系统可为先被SSL策略加密然后被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的HTTP响应页面。在这些情况下，系统会加密响应页面并在重新加密的SSL数据流最后发送该页面。 SafeSearch可过滤掉令人不快内容，并阻止用户搜索成人站点。
TLS/SSL策略。	6.0.0	6.0.0	引入的功能。



第 45 章

标准解密 策略

以下主题详细介绍了 标准解密 政策。

- 关于标准解密策略， 第 1861 页
- 创建新的 标准解密 策略， 第 1863 页
- 标准解密 策略高级选项， 第 1879 页
- 解密策略操作， 第 1882 页

关于标准解密策略

我们推荐使用 标准解密 策略类型，因为它设置更简单，且应能减少客户常遇到的问题。特别是，标准解密 策略可防止您在您的网络中解密过多流量。流量解密需要大量处理能力，解密过多流量会降低系统速度。

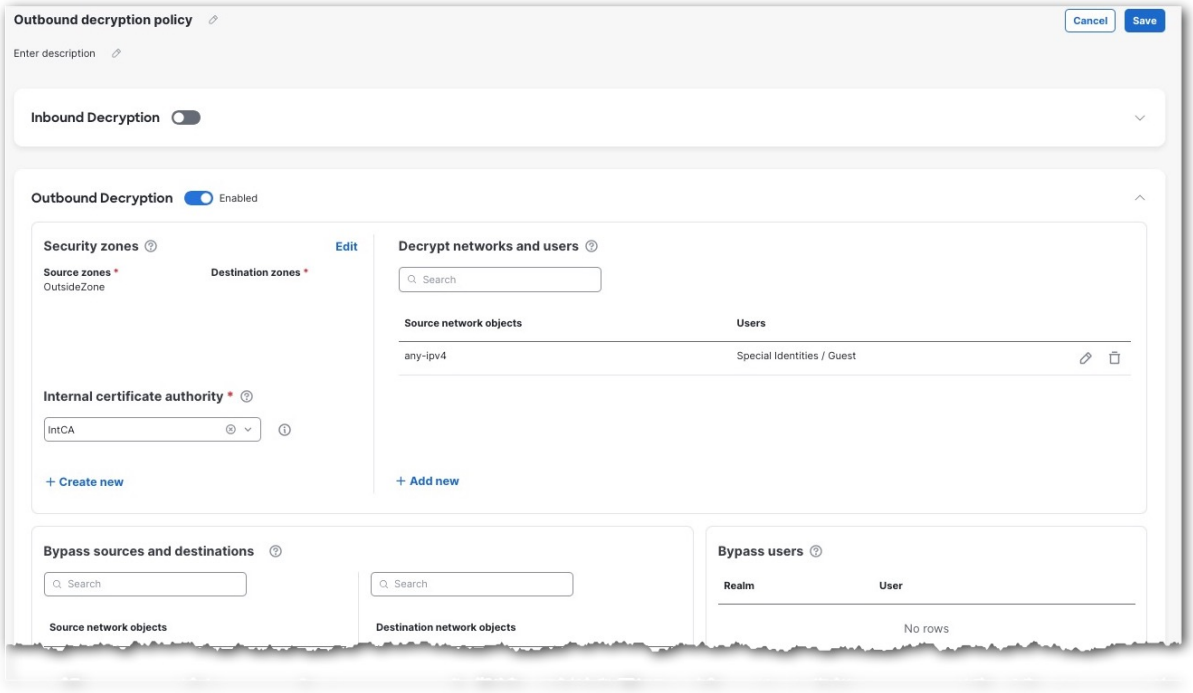
哪种类型的解密策略适合我？

本主题讨论 标准解密 策略和 基于规则的解密 策略。

标准解密策略

我们建议使用标准 解密策略类型，因为它具有向导式的外观，易于设置，使您能够轻松选择要在策略中使用的安全区、用户和网络以及其他对象。标准解密策略特别适合不熟悉解密策略细节的用户。

以下是设置标准解密策略的示例。



前述策略仅解密传出流量。来自任何 IPv4 网络上 OutsideZone 安全区域的所有流量均使用名为 `IntCA` 的内部 CA 解密。

请注意以下事项：

- 前面的规则是不完整的示例，还有更多可用选项
- 您可以配置入站条件和/或出站条件。
- 除了 对象，您还可以选择配置出站解密排除项，如：
  - 无法解密的应用（例如使用证书锁定的应用）。
  - URL 类别，例如医疗、贸易和财务。
- 您可以为证书状态和 TLS 版本配置出站阻止规则。
- 标准策略具有类似于旧版策略的高级策略选项。

基于规则的解密策略

使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。

基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。

10.0.0 之前版本的标准解密策略部署问题

如果将标准解密策略部署到运行 10.0.0 之前版本的设备，您可能会遇到以下问题：

- 如果配置任何入站解密规则，则规则操作会在这些设备上更改为**解密 - 已知密钥**。有关传入解密操作类型的详细信息，请参阅传入流量解密，第 1844 页。
- 高级策略选项**智能解密绕行**要求设备运行 7.7 或更高版本。默认情况下，此高级选项处于禁用状态，但如果启用此选项，并且设备运行的是 7.7 之前的版本，则策略部署会失败。

创建新的 标准解密 策略

您可以创建以下任何类型的解密策略：

- 保护入站流量的策略：解密传入您网络的网络流量。执行此操作通常是为了解密和检查定向到内部服务器的流量。
- 保护出站流量的策略：解密从网络流向外部服务器的网络流量。

有关详细信息，请参阅以下主题之一：

相关主题

创建具有入站保护的 标准解密 策略，第 1863 页
创建具有入站保护的 标准解密 策略，第 1867 页

创建具有入站保护的 标准解密 策略

以下任务讨论如何创建 标准解密 策略以解密 传入 网络的网络流量。执行此操作通常是为了解密和检查定向到内部服务器的流量。此页面上的所有选项均为必填项。

开始之前

在传入流量解密，第 1844 页中查看入站保护解密策略的含义。

要创建具有出站保护的解密策略，请参阅创建具有入站保护的 标准解密 策略，第 1867 页。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 **创建新的** > **解密策略**

步骤 4 在提供的字段中，输入**名称**和可选**说明**。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 5 点击**创建策略 (Create Policy)**。

步骤 6 将 “**入站解密**” 滑动到 “**启用**”，如下图所示。



步骤 7 将以下内容添加到解密策略中：

- 安全区，第 1864 页
- 内部服务器详细信息（入站解密），第 1866 页

安全区

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

了解更多信息：

- 入站解密：添加安全区域（入站解密），第 1864 页
- 出站解密：添加安全区域（出站解密），第 1868 页

添加安全区域（入站解密）

此任务讨论如何将安全区域添加到入站 标准解密 策略。安全区指定向内部服务器发送流量的Firewall Threat Defense设备接口。通常，对于入站保护，这是一个内部（或 *DMZ*）接口。

您必须同时选择源和和目标安全区域。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 1863 页中讨论的任务。

过程

步骤 1 点击安全区域旁边的**编辑区域**。

步骤 2 在安全区对话框中，执行以下任一操作：

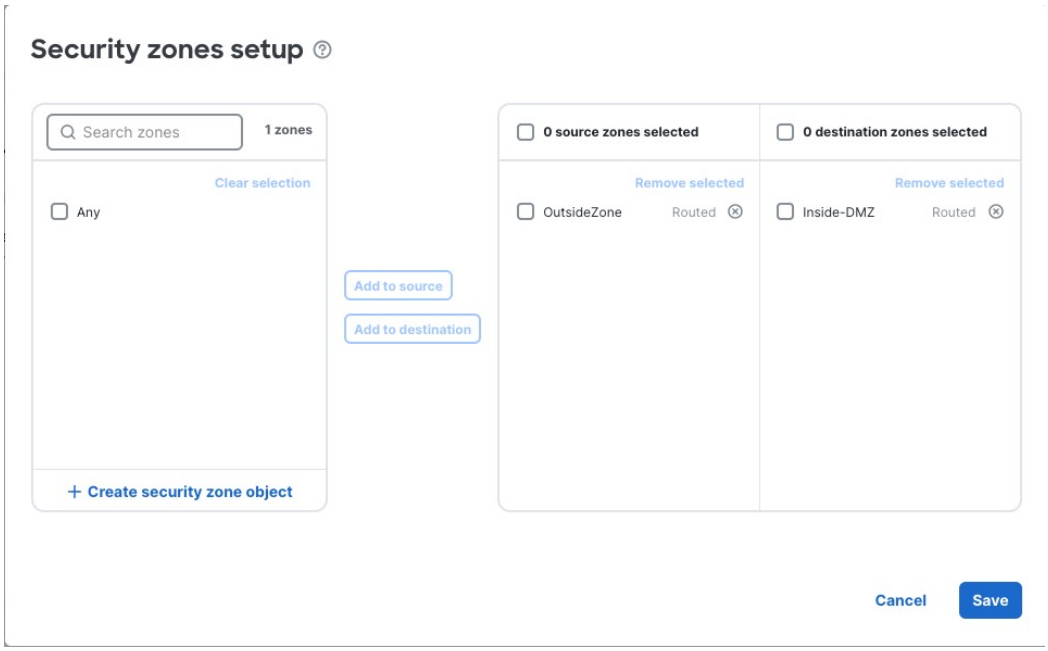
- 选中要添加到源或目标的安全区域旁边的复选框。
- 要创建新的安全区域，请点击 **创建安全区域对象 (Create security zone object)**。
- 在搜索区域字段中输入文本并按 Enter 键以搜索安全区。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

步骤 3 点击 **添加到源**以解密匹配源安全区域的流量，或点击**添加到目标**以解密匹配目标安全区域的流量。如果同时选择源网络和目标区域进行解密，则流量必须与两个区域匹配。

通常，您的内部服务器应是入站解密规则的目标。

下图显示了一个示例。



步骤 4 点击**保存**。

步骤 5 请参阅内部服务器详细信息（入站解密），第 1866 页。

内部服务器详细信息（入站解密）

通过解密和（可选）检查流向内部服务器的流量来添加要保护的内部服务器。您可以使用网络对象和可选端口指定这些服务器。

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

有关详细信息，请参阅添加内部服务器 ， 第 1866 页。

添加内部服务器

此任务讨论如何选择证书来解密到达要保护的内部服务器的流量。除了可以选择证书之外，还可以指定内部服务器所在的网络和端口，从而节省处理时间。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 1863 页中讨论的任务。

过程

步骤 1 点击内部服务器详情下的 **添加新的** 。

步骤 2 在内部服务器对话框中，执行以下任一操作：

- 在搜索字段中输入文本并按 Enter 键，从而搜索内部证书。
- 从 **内部证书对象** 列表中，选择现有证书，或点击 **新增 (Add New)** 以创建新证书。

  注释
  为流量提供服务的 Cisco Secure Firewall Threat Defense 设备必须信任您上传至规则的证书。如果上传自签名证书或不受证书颁发机构信任的证书，并且想要稍后替换证书，则必须通过以下任一方式更新策略的高级设置：

  - 将证书添加到**受信任 CA 证书**列表。
  - 选择**入站解密需要证书完全匹配**复选框。

  有关高级策略选项的详细信息，请参阅标准解密 策略高级选项 ， 第 1879 页。

  有关替换证书的详细信息，请参阅传入流量解密 ， 第 1844 页中有关替换证书的讨论。

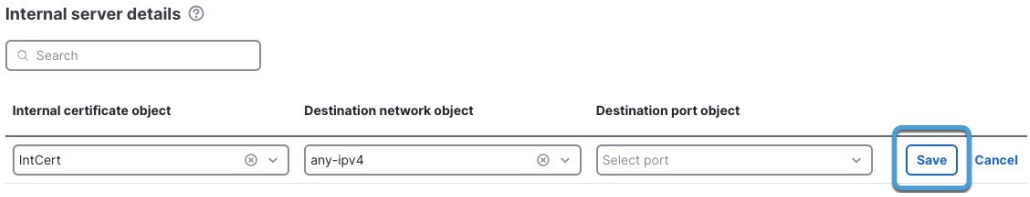
- 从**目标网络对象列表**中，点击内部服务器所在的网络，或点击**添加新网络**以创建新的网络。
- （可选。）从 **目标端口** 列表中，点击要应用解密规则的端口，或点击 **添加新的** 以创建新规则。

  有关详细信息，请参阅为入站保护上传内部证书 ， 第 1897 页。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

步骤 3 点击**保存**。

下图显示了一个示例。



步骤 4 通过点击页面顶部的 **保存** 来保存解密策略。

步骤 5 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

创建具有入站保护的 标准解密 策略

注释 有关将 标准解密 策略部署到运行 10.0.0 之前版本的设备时潜在问题的信息，请参阅10.0.0 之前版本的标准解密策略部署问题，第 1862 页。

以下任务讨论如何创建标准解密策略来保护内部网络外的服务器。要解密出站连接，除另有说明外，此页面上的所有选项均为必填项。要绕过或阻止某些出站连接，只需要安全区域以及绕过或阻止选项。

开始之前

在 解密和重新签名（传出流量），第 1844 页中查看出站保护解密策略的含义。

要改为创建具有入站保护的解密策略，请参阅创建具有入站保护的 标准解密 策略，第 1863 页。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 **创建新的** > **解密策略**

步骤 4 在提供的字段中，输入**名称**和可选**说明**。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 5 点击**创建策略 (Create Policy)**。

步骤 6 将**出站解密**滑动到**已启用**，如下图所示。



安全区

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

了解更多信息：

- 入站解密：添加安全区域（入站解密），第 1864 页
- 出站解密：添加安全区域（出站解密），第 1868 页

添加安全区域（出站解密）

此任务讨论如何将安全区域添加到出站 标准解密 策略。安全区指定向外部服务器发送流量的Firewall Threat Defense设备接口。

开始之前

完成 创建具有出站连接保护的 基于规则的解密策略 ，第 1887 页中讨论的任务。

过程

步骤 1 点击安全区域旁边的**编辑区域**。

步骤 2 在安全区对话框中，执行以下任一操作：

- 选中要添加到源或目标的安全区域旁边的复选框。

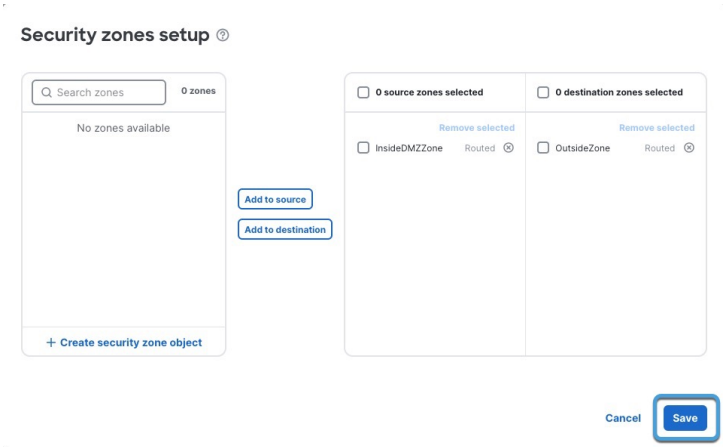
- 要创建新的安全区域，请点击 **创建安全区域对象 (Create security zone object)**。
- 在搜索区域字段中输入文本并按 Enter 键以搜索安全区。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

步骤 3 点击 **添加到源 (Add to Source)** 以解密匹配源网络的流量，或点击 **添加到目标 (Add to Destination)** 以解密匹配目标网络的流量。如果同时选择源网络和目标网络进行解密，则流量必须与两个安全区匹配。

通常，要为其解密流量的服务器应在目标区域中。

下图显示了一个示例。



步骤 4 点击**保存**。

步骤 5 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

解密网络和用户

通过此选项，您可以对特定网络对象以及 Microsoft AD、LDAP 或本地领域中的特定用户和组实施解密和深度检查。

网络对象

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象来构建网络条件。

用户和组

您可以选择解密来自身份领域中一部分用户和组的流量，也可以选择解密来自以下特殊身份的流量：

- 身份验证失败：强制网络门户身份验证失败的用户。

- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

相关详细信息

有关详细信息，请参阅添加网络和用户，第 1870 页。

添加网络和用户

此任务讨论如何对来自特定网络的出站流量强制解密；以及来自 Microsoft Active Directory、LDAP 或本地领域中的用户和组的流量。

只会解密与您选择的所有网络和用户都匹配的流量。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 1867 页中讨论的任务。

过程

步骤 1 完成 创建具有入站保护的 标准解密 策略，第 1867 页中讨论的任务。

步骤 2 点击“解密网络和用户”旁边的**新增**。

步骤 3 从**源网络对象**列表中，执行以下任一操作：

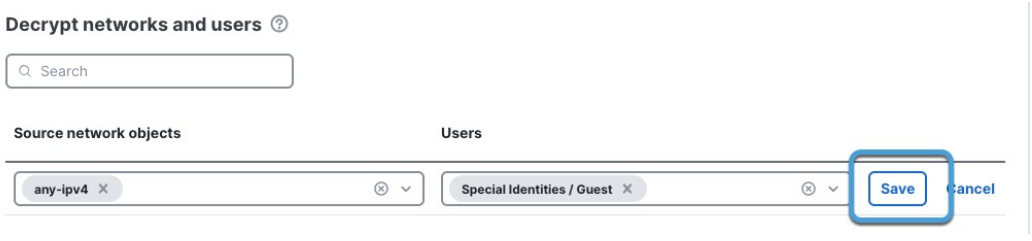
- 在提供的字段中，输入现有网络对象的全部或部分以过滤该对象。
- 选中要解密的网络旁边的复选框。要解密来自所有网络的流量，请点击**新增**和**保存**，而不选择任何网络。
- 点击**新增**以向列表中添加其他网络。

  有关详细信息，请参阅创建网络对象，第 2660 页。

步骤 4 从**用户**列表中，选中每个要解密的用户名或组名旁边的复选框。

要解密来自所有用户的流量，请点击**新增**和**保存**，而不选择任何用户。

下图显示选择要解密的网络和用户的示例。



步骤 5 点击**保存**。

步骤 6 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

内部证书颁发机构

本主题讨论如何将内部证书颁发机构 (CA) 添加到 标准解密 策略的出站部分。内部证书颁发机构用于在解密流量后对流量进行重新签名。内部 CA 必须受到网络上的用户的信任，以避免在其网络浏览器中看到不受信任的证书错误。

有关详细信息，请参阅为出站保护添加内部 CA，第 1871 页。

为出站保护添加内部 CA

此任务讨论如何添加内部 CA 以重新签发传出流量。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 1867 页中讨论的任务。

过程

在**内部证书颁发机构**列表中，执行以下任一操作：

- 点击内部 CA 的名称。
- 点击**新建**以创建新的内部 CA。

  点击**帮助**以获取更多信息。

  如果您还没有内部 CA，请参阅：

  - 为出站保护生成内部 CA，第 1871 页
  - 为出站保护上传内部 CA，第 1872 页

为出站保护生成内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地生成内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书，第 2664 页中所述的**对象**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象，第 2662 页中所述。

过程

步骤 1 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New)** > **生成 CA (Generate CA)**。

步骤 2 为内部 CA 提供一个**名称**，然后提供一个由两个字母组成的**国家/地区名称**。

步骤 3 点击**字签名 (Self-Signed)** 或**CSR**。

有关这些选项的详细信息，请参阅内部证书颁发机构对象，第 2662 页。

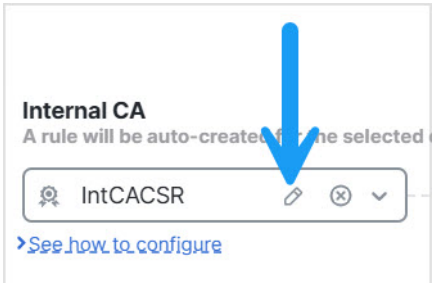
步骤 4 在提供的字段中输入请求的信息。

步骤 5 点击**保存**。

步骤 6 如果您选择了 **CSR**，则在签名请求完成后，点击**安装证书 (Install Certificate)**，如下所示：

a) 重复此程序中的上述步骤。

b) 从**内部 CA (Internal CA)** 列表编辑 CA，如下所示。



c) 点击 **Install Certificate**。

d) 按照屏幕提示完成任务。

步骤 7 按照创建具有出站连接保护的 基于规则的解密策略，第 1887 页中的说明继续创建策略。

为出站保护上传内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地上传内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书，第 2664 页中所述的**对象**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象，第 2662 页中所述。

过程

步骤 1 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New）** > **上传 CA (Upload CA)**。

步骤 2 为内部 CA 指定一个**名称**。

步骤 3 粘贴或在提供的字段中浏览找到证书及其私钥。

步骤 4 如果 CA 有密码，请选中**已加密 (Encrypted)** 复选框并在相邻字段中输入密码。

步骤 5 按照 创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页中的说明继续创建策略。

解密时绕过流量

本主题讨论您可以选择绕过解密流量的方法（即，流量通过设备加密）。您可以在此处查看对流量保持加密的一些原因：何时解密流量以及何时不解密，第 1841 页。绕过某些流量还有一个额外的优势，即解密流量时不会消耗系统资源。

我们提供以下方法在解密时绕过流量：

- 绕过源和目标网络：例如，无需解密来自您可信的内部/DMZ 网络上内部服务器的流量。
- 绕过用户：您可以为信任的用户和组绕过解密。
- 绕过无法解密的应用：（推荐。）绕过流向应用的传出流量的典型原因是此类流量可能使用无法解密的证书锁定。

  有关详细信息，请参阅关于 TLS/SSL 锁定 ， 第 1949 页。
- 绕过类别：（推荐。）由于以下原因，绕过解密站点的 URL 类别：
  - 类别代表可能非法解密和检查的应用（例如个人财务或健康）。
  - 思科确定为低风险的网站类别。
- 智能解密绕过：根据客户端的威胁置信度绕过服务器，该置信度由加密可见性引擎 (EVE) 和 URL 类别信誉确定。

  所有部署了启用此选项的 标准解密 策略的设备都必须运行 7.7 或更高版本；否则，策略部署会失败。

绕过源和目的地

（可选。）绕过来自源或目标网络对象的流量。例如，如果流量来自拥有受信任设备的内部网络，您可以选择不解密该流量。 网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。

有关详细信息，请参阅添加绕过源和目的地 ， 第 1873 页。

添加绕过源和目的地

以下任务讨论如何选择性地绕过来自源网络或前往目标网络的出站流量。通常，只有在您信任来自这些网络的流量时才执行此操作。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 1867 页中讨论的任务。

过程

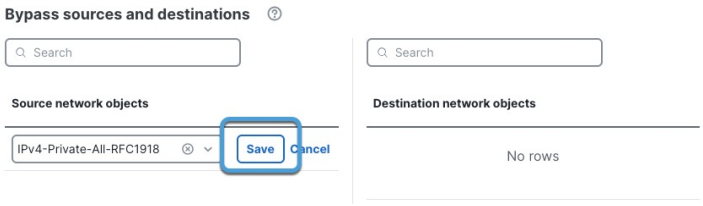
步骤 1 对于源网络对象或目标网络对象，点击“绕过源和目标”下的**新增**。

步骤 2 在显示的对话框中，执行以下任一操作：

- 在搜索字段中输入文本并按 Enter 键，即可搜索网络对象。
- 从**源网络对象**或**目标网络对象**列表中，选择现有的网络对象，或点击**新增**以创建一个新的网络对象。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

下图显示了一个示例。



步骤 3 点击**保存**。

步骤 4 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

绕过用户

（可选。）您可以在 Microsoft Active Directory、LDAP 和本地领域中为特定用户绕过解密；通常，这些是您信任的用户。

您可以选择绕过身份领域中的一部分用户和组，也可以选择从以下特殊身份绕过：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

有关详细信息，请参阅添加绕过用户，第 1874 页。

添加绕过用户

为选定的 Microsoft AD、LDAP 和本地领域中的用户和组绕过解密。

开始之前

完成 创建具有入站保护的 标准解密 策略， 第 1867 页中讨论的任务。

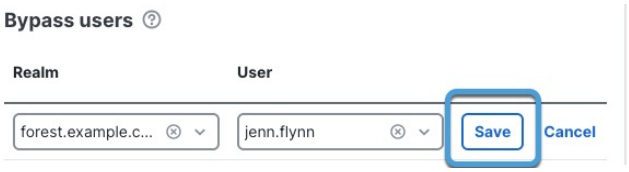
过程

步骤 1 点击绕过用户下的**新增**。

步骤 2 在显示的对话框中：

- 在**领域**列表中，点击领域名称。
- 从**用户**列表中，选中要绕过解密的一个或多个用户或组旁边的复选框。

下图显示了一个示例。



步骤 3 点击**保存**。

步骤 4 根据需要多次重复上述步骤，以绕过更多用户和组。

绕过应用

（可选。）选中此复选框可在重新签名证书可能导致连接失败时不解密流量。

通常，此行为与证书锁定相关，《TLS/SSL证书固定准则， 第 1914 页的证书锁定准则中对此进行了讨论。

无法解密的应用会在漏洞数据库 (VDB) 中自动更新。您可以在 Cisco Secure Firewall应用检测器 (Secure Firewall Application Detectors) 页面上找到所有应用的列表；**undecryptable** 标记会标识思科确定为无法解密的应用。

无法解密的应用列表由思科维护。

有关详细信息，请参阅添加绕过应用程序， 第 1875 页。

添加绕过应用程序

此任务讨论如何绕过应用程序的解密（通常是因为这些应用程序使用证书锁定，如关于 TLS/SSL 锁定， 第 1949 页中所述，无法解密）。

开始之前

完成 创建具有入站保护的 标准解密 策略， 第 1867 页中讨论的任务。

过程

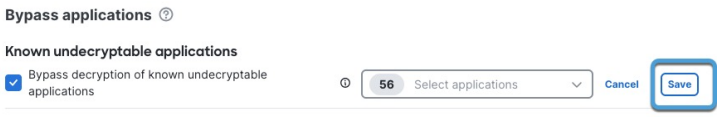
步骤 1 选中**绕过已知不可解密应用程序的解密**复选框。

步骤 2 点击**编辑应用程序**。

步骤 3 从列表中执行以下任一操作：

- 点击**全选**以选择思科确定的所有不可解密的应用程序。
- 选中要绕过解密的某个应用程序名称旁的复选框。
- 清除要解密连接的某个应用程序名称旁的复选框。

下图显示了一个示例。



步骤 4 在选定的应用程序和过滤器下，点击**新增**以添加要绕过的应用程序或应用程序过滤器。点击**帮助**以获取更多信息。

步骤 5 点击**保存**。

步骤 6 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

绕过 URL 类别和信誉

（可选。）选择不解密的类别和信誉，例如个人财务或健康信息。根据您所在地区的法律，解密此类流量可能被禁止。有关详细信息，请咨询您所在地区的权威机构。

URL 类别和信誉由 Cisco Talos 维护。

有关类别的详细信息，请参阅智能类别。

有关信誉的详细信息，请参阅 Web 信誉级别。

要将 URL 类别和信誉添加到您的解密策略，请参阅添加绕过 URL 类别和信誉，第 1876 页。

添加绕过 *URL* 类别和信誉

（可选。）此任务讨论如何根据 Cisco Talos 提供的评级绕过类别和信誉解密。

下图显示了我们建议的类别和信誉列表。



开始之前

完成 创建具有入站保护的 标准解密 策略， 第 1867 页中讨论的任务。

过程

步骤 1 在“绕过 URL 类别”部分中，执行以下任一操作：

- 要编辑现有的类别/信誉，请点击 **编辑** ()。
- 要删除现有类别/信誉，请点击 **删除** ()。
- 要添加新的类别/信誉，请点击**新增**。
- 要将类别和信誉列表返回到思科建议的类别和信誉列表，请点击**应用建议的设置**。

步骤 2 要添加或编辑类别/信誉，请从第一个列表中点击类别的名称。

有关类别的详细信息，请参阅智能类别。

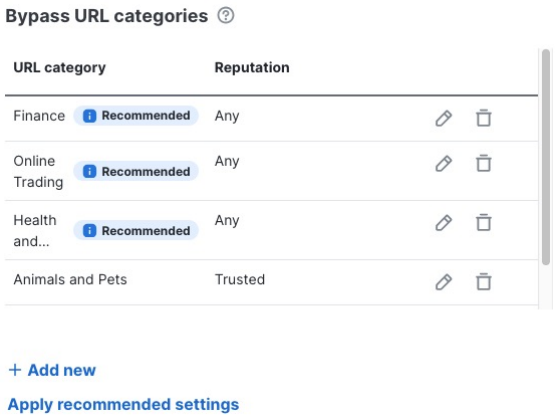
步骤 3 从第二个列表中，点击信誉的名称。

有关信誉的详细信息，请参阅 Web 信誉级别。

下图显示了使用思科的默认设置并添加信誉为“受信任”的“动物和宠物”类别的示例。

步骤 4 点击**保存**。

下图显示了一个示例。



步骤 5 如果您已完成策略配置，请参阅 解密策略操作，第 1882 页。

绕过智能解密

您可以将EVE设置为绕过解密前往受信任连接的流量。绕过行为广泛，涵盖许多一般浏览活动。例如，与 www.cnn.com 的连接不会被解密，但从 CNN 的内容交付网络 (CDN) 获取资产的其他连接如果未被分类为受信任，则可能会被解密。

客户端分类基于 EVE 的风险评估，该风险评估使用机器学习来识别流量风险级别。URL 分类基于 Talos URL 信誉。系统会绕过且不解密从风险极低的客户端到受信任 URL 的任何连接。所有其他连接（包括与不受信任的 URL 的连接或来自分类为较高风险级别的客户端的连接）均须遵守解密策略。

绕过受信任连接可减少不必要的解密处理，节省系统资源。这也尊重用户隐私，不会解密分类为低风险和受信任的流量。

要为出站解密规则设置智能解密绕过，请找到**智能解密绕过**并将其设置为**滑块已启用**()，以便根据加密可见性引擎 (EVE) 确定的客户端威胁置信度和URL类别信誉，不对连接到受信任服务器的极低风险客户端的流量进行解密。

要查看按信任级别分类的当前客户端列表，请转至 Cisco Secure Firewall 应用检测器。例如，cnn.com 被分类为“非常低”。确保您了解选择不解密的流量。

阻止连接

（可选。）此主题提供以下详细信息：如何在创建解密策略时阻止与 TLS 版本和服务器证书状态不安全的服务器连接。

您可以选择阻止以下任一项：

- SSL 和 TLS 版本，因为有些被视为不安全。
- 证书状态；例如，可以阻止流向证书过期的服务器的出站流量，因为该服务器可能不可信任。

有关详细信息，请参阅添加阻止连接，第 1879 页。

添加阻止连接

此任务讨论如何根据旧的 SSL 或 TLS 版本阻止连接；或基于服务器证书状态阻止连接。

注释 阻止会影响所有出站连接，并优先于您选择的所有其他绕过和解密条件。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 1867 页中讨论的任务。

过程

步骤 1 找到“阻止连接”部分。

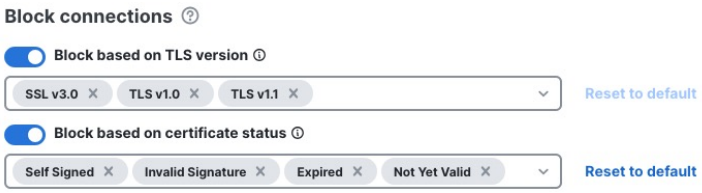
步骤 2 要根据 SSL 或 TLS 协议版本阻止出站流量，请将**基于 TLS 版本阻止**滑动到 **滑块已启用** ( )。

步骤 3 要根据服务器证书状态阻止出站流量，请将**基于证书状态阻止**滑动到 **滑块已启用** ( )。

步骤 4 您有以下选择：

- 从列表中选中选项旁边的复选框，以将该协议或状态添加到策略中。
- 点击项目旁边的 **x** 可将其从列表中移除。
- 点击**重置为默认值**，可将列表条目恢复为其原始值。

下图显示使用 TLS 版本和服务器证书状态阻止流量的示例。自签名已添加到要阻止的服务器证书列表。



步骤 5 如果您已完成策略配置，请参阅 解密策略操作 ， 第 1882 页。

标准解密 策略高级选项

（可选。）要设置高级解密策略选项，请创建或编辑一个标准解密 策略，然后展开**高级选项**。高级选项将在以下段落中讨论。

建议将所有高级选项设置为其默认值。

绕过思科旧版不可解密的站点

启用此选项可绕过对思科已确定无法解密的可分辨名称 (DN) 的网站进行解密。要查看 DN 列表，请转至 **对象** > **可分辨名称** > **对象组**。

入站解密需要证书完全匹配

启用此选项以要求在解密策略中使用内部服务器的证书（此选项称为已知密钥解密）。默认为使用其他证书，这样更便于在需要时替换策略的证书。有关详细信息，请参阅 传入流量解密操作，第 1940 页。

启用自适应 TLS 服务器身份探测

启用 TLS 1.3 解密时自动启用。 探测 是与服务器的部分 TLS 连接，其目的是获取服务器证书并将其缓存。（如果证书已缓存，则永远不会建立探测。）

如果在与解密策略关联的访问控制策略上禁用了 TLS 1.3 服务器身份发现，我们将尝试使用服务器名称指示 (SNI)，这并不可靠。

自适应 TLS 服务器身份探测发生在以下任何情况下，而不是在早期版本中的每个连接上发生：

- 证书颁发者 - 当解密规则的 DN 规则条件中的 **颁发者 DN** 值匹配时匹配。

  有关详细信息，请参阅可分辨名称 (DN) 规则条件，第 1926 页。

- 证书状态 - 当解密规则中的任何 **证书状态** 条件匹配时匹配。

  有关详细信息，请参阅证书状态 解密规则 条件，第 1932 页。

- 内部/外部证书 - 内部证书可以通过 **解密 - 已知密钥** 规则操作中使用的证书进行匹配；可以在 **证书** 规则条件中匹配外部证书。

  有关详细信息，请参阅已知密钥解密（传入流量）和证书规则条件，第 1926 页。

- 应用 ID - 可以通过访问控制策略或解密策略中的 **应用** 规则条件进行匹配。

  有关详细信息，请参阅应用规则条件，第 1420 页。

- URL 类别 - 可以通过访问控制策略中的 **URL** 规则条件进行匹配。

  有关详细信息，请参阅URL 规则条件，第 1423 页。



注释 任何部署到 AWS 的设备都不支持启用自适应 TLS 服务器发现模式。Secure Firewall Threat Defense Virtual如果您有任何由 Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。

解密事件日志记录选项

为了加快故障排除速度并了解解密策略的运行情况，建议您启用所有日志记录选项：绕过的流量、已解密的流量和被阻止的流量。

启用 QUIC 解密

是否将解密规则应用于通过 QUIC 协议使用 HTTP/3 的连接。解密 QUIC 连接时，系统可以检查会话内容是否存在入侵、恶意软件或其他问题。您还可以根据访问控制策略中的特定条件来对已解密的 QUIC 连接应用精细控制和过滤。QUIC 支持符合 RFC 9000、9001、9002、9114、9204 的要求。

实施 QUIC 解密时，请考虑以下事项：

- 在 高可用性或集群设备上，QUIC 解密只有在连接保持位于同一节点时才有效。如果对连接进行故障转移或将其转发到另一个节点，则连接会断开，必须重新建立。支持多实例而无限制。
- 适用于 QUIC 流量的规则将包括具有目的端口 443 的 UDP 协议。
- 适用于 QUIC 流量的访问控制规则将包括 HTTP/3 或 QUIC 协议（显式或隐式）。

以下限制适用于 QUIC 解密：

- QUIC 解密仅适用于 Firewall Threat Defense 7.6+。运行较低版本的设备无法解密 QUIC 连接。
- 无法为出站流量解密来自使用 Chromium 堆栈的浏览器（Google Chrome、Opera 和 Edge）的连接。但可以解密来自相同浏览器的入站流量。
- 不支持 RFC 9000 中所述的连接迁移。QUIC 中的连接 ID 概念允许终端在地址更改时保留相同的连接。
- 不支持密钥更新、会话恢复和 QUIC 版本 2。
- 不支持交互式阻止和交互式阻止并重置（在访问控制规则中）。这些操作将作为“阻止”和“阻止并重置”。
- 每个连接的活动连接 ID 限制为 5。如有必要，您可以使用设备 CLI 中的**system support quic-tuning** 和**system support quic-tuning-reset**命令修改这些限制。

启用 TLS 1.3 解密

是否将解密规则应用于 TLS 1.3 连接。如果不启用此选项，则解密规则仅适用于 TLS 1.2 或更低版本的流量。请参阅TLS 1.3 解密最佳实践，第 1904 页。

保存策略

在配置高级策略选项后，请参阅解密策略操作，第 1882 页。

添加受信任 CA 证书

（可选。）此任务讨论如何将受信任 CA 证书添加到解密策略。我们强烈建议为组织的证书添加颁发者 CA，以避免解密流量出现问题。

开始之前

完成以下讨论的任务：

- 创建具有入站保护的 标准解密 策略，第 1863 页

- 创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页

过程

步骤 1 在策略中，展开**高级选项**。

步骤 2 在**受信任的 CA 证书**列表中，执行以下任一操作：

- 点击列表中受信任 CA 证书的名称。
- 要从列表中删除所有证书，请点击 。
- 要将列表恢复为原始值，请点击**添加推荐**。

解密策略操作

以下主题讨论如何：

- 复制解密策略
- 将 标准解密 策略转换为 基于规则的解密 策略
- 生成有关解密策略的报告

相关主题

将 标准解密 策略转换为 基于规则的解密 策略 ， 第 1882 页
复制解密策略 ， 第 1883 页
生成解密策略报告 ， 第 1883 页

将 标准解密 策略转换为 基于规则的解密 策略

以下任务讨论如何将 标准解密 策略转换为 基于规则的解密 策略。转换为 基于规则的解密 策略后，您无法再转换回 标准解密 策略。此外，您无法将任何 基于规则的解密 策略转换为 标准解密 策略。

我们提供此功能，让您可以使用基于规则的解密策略中可用的其他自定义选项。有关详细信息，请参阅关于基于规则的解密策略 ， 第 1885 页。

开始之前

创建解密策略，如本指南中所述。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要转换的解密策略旁边，在操作列中，点击 更多图标 （ ··· ），然后点击**转换策略模式**。

步骤 4 您需要确认操作。

系统将创建一个备份策略，并在原始策略的名称后附加 **-backup**。原始策略保留其名称。

复制解密策略

以下任务讨论如何复制解密策略。复制策略会复制策略中的任何规则以及所有策略的设置。

开始之前

创建解密策略，如本指南中所述。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要复制的解密策略旁边的操作列中，点击 更多图标 （ ··· ），然后点击**复制策略**。

步骤 4 当出现提示时，请为策略提供名称。

步骤 5 点击**保存**。

生成解密策略报告

本主题讨论如何创建包含以下内容（以及其他内容）的解密策略报告：

- 规则列表
- 密码套件列表
- 策略的默认操作
- 受信任 CA 证书

开始之前

创建解密策略，如本指南中所述。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要创建报告的解密策略旁边，在操作列中，点击 更多图标 （ ··· ），然后点击**生成报告**。

系统会创建一个 PDF 报告，并使用默认的 PDF 应用程序将其打开。



第 46 章

基于规则的解密 策略

以下主题详细介绍了 基于规则的解密 政策。

- 关于基于规则的解密策略， 第 1885 页
- 创建一个 基于规则的解密策略 ， 第 1887 页
- 基于规则的解密策略默认操作， 第 1899 页
- 无法解密流量的默认处理选项， 第 1900 页
- 基于规则的解密策略高级选项， 第 1902 页

关于基于规则的解密策略

基于规则的解密策略

使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。

基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。

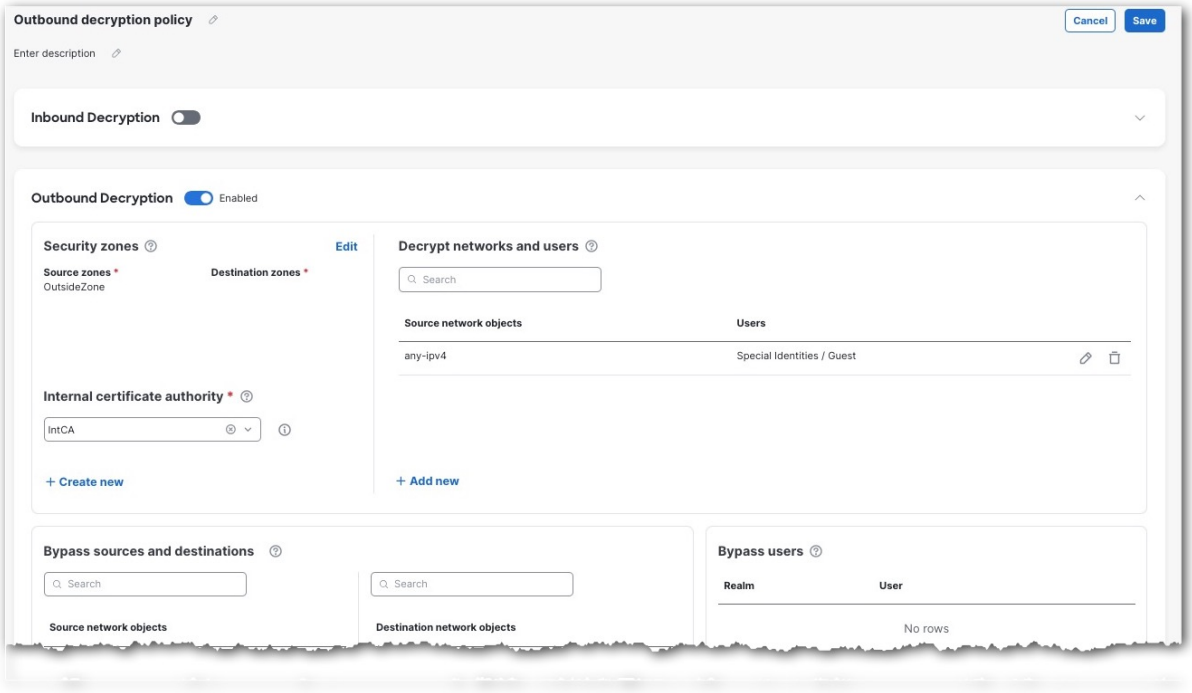
哪种类型的解密策略适合我？

本主题讨论 标准解密 策略和 基于规则的解密 策略。

标准解密策略

我们建议使用标准 解密策略类型，因为它具有向导式的外观，易于设置，使您能够轻松选择要在策略中使用的安全区、用户和网络以及其他对象。标准解密策略特别适合不熟悉解密策略细节的用户。

以下是设置标准解密策略的示例。



前述策略仅解密传出流量。来自任何 IPv4 网络上 OutsideZone 安全区域的所有流量均使用名为 `IntCA` 的内部 CA 解密。

请注意以下事项：

- 前面的规则是不完整的示例，还有更多可用选项
- 您可以配置入站条件和/或出站条件。
- 除了 对象，您还可以选择配置出站解密排除项，如：
  - 无法解密的应用（例如使用证书锁定的应用）。
  - URL 类别，例如医疗、贸易和财务。
- 您可以为证书状态和 TLS 版本配置出站阻止规则。
- 标准策略具有类似于旧版策略的高级策略选项。

基于规则的解密策略

使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。

基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。

创建一个 基于规则的解密策略

您可以创建以下任何类型的 基于规则的解密策略：

- 出站保护 策略具有保护出站连接的规则；也就是说，目标服务器位于受保护的网络外。此类规则具有 **解密 - 重新签名** 规则操作。我们还使用 **不解密**操作创建其他规则，排除您指定的流量（例如使用证书锁定的流量）。

  请参阅创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页

- 入站保护 策略具有保护入站连接的规则；也就是说，目标服务器位于受保护的网络内。此类规则具有**解密 - 已知密钥**或**解密 - 替换证书**规则操作。我们还使用“**不解密**”操作创建其他规则，排除您指定的流量（例如使用证书锁定的流量）。这些规则最初处于禁用状态，但您可以根据需要在以后修改和启用它们。

  请参阅创建具有入站连接保护的 基于规则的解密策略 ， 第 1889 页

- 其他操作（包括 “**不解密**”、“ **阻止**”和“ **阻止并重置**”）。

  请参阅创建一个带有其他规则操作的 基于规则的解密策略 ， 第 1898 页

创建具有出站连接保护的 基于规则的解密策略

此任务讨论如何使用保护出站连接的规则来创建解密策略；也就是说，目标服务器位于受保护的网络外。此类规则具有 **解密 - 重新签名** 规则操作。

创建解密策略时，您可以同时创建多条规则，包括多条**解密 - 已知密钥**规则、多条**解密 - 替换证书**规则和多条**解密 - 重新签名**规则。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理工单，第 162 页和支持变更管理的策略和对象 ， 第 157 页。

开始之前

您必须先上传或生成出站服务器的内部证书颁发机构 (CA)，然后才能创建保护出站连接的解密策略。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **PKI** > **内部 CA (Internal CAs)** 并引用 PKI ， 第 2661 页 来创建内部 CA 证书对象。
- 在创建此解密策略时。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

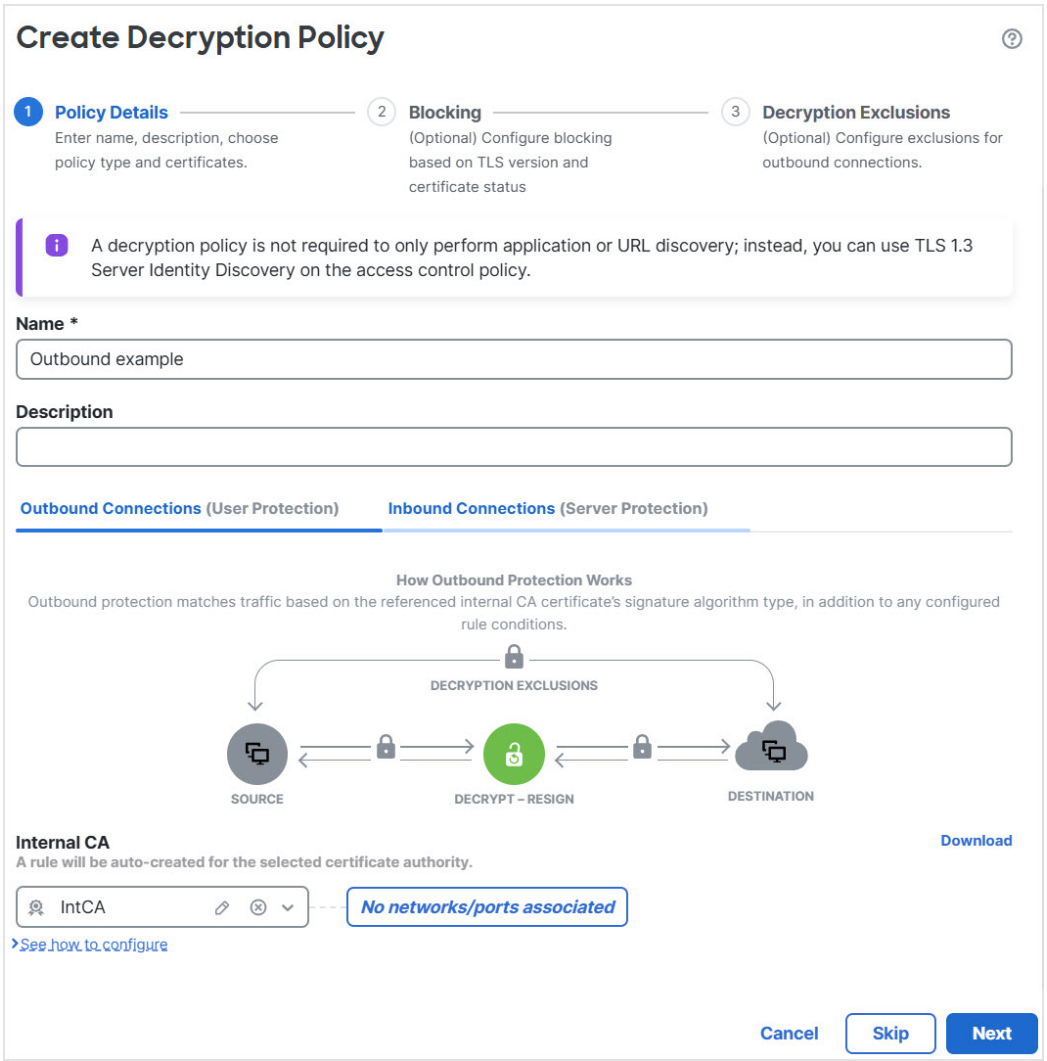
步骤 3 点击**新建** > **解密策略**（**基于规则**）。

步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。



步骤 6 从**内部 CA (Internal CA)** 列表中，上传或选择规则的证书。

有关内部证书的更多信息，请参阅 为出站保护生成内部 CA，第 1871 页 和 为出站保护上传内部 CA，第 1872 页。

步骤 7 （可选。）选择网络和端口。

了解更多信息：

- 网络规则条件， 第 1420 页
- 端口规则条件， 第 1421 页

步骤 8 点击**下一步 (Next)**。

步骤 9 继续执行基于规则的解密策略 阻止连接， 第 1891 页。

下一步做什么

- 添加规则条件： 解密规则基于规则的解密规则 条件， 第 1920 页
- 添加默认策略操作： 基于规则的解密策略默认操作， 第 1899 页
- 为默认操作配置日志记录选项，如*Cisco Secure Firewall Management Center* 管理指南 中的使用策略默认操作记录连接所述。
- 设置高级策略属性：基于规则的解密策略高级选项， 第 1902 页。
- 将 解密策略 与访问控制策略相关联，如将其他策略与访问控制相关联， 第 1719 页中所述。
- 部署配置更改；请参阅 部署配置更改， 第 180 页。

创建具有入站连接保护的 基于规则的解密策略

此任务讨论如何使用保护入站连接的规则来创建解密策略；也就是说，目标服务器位于受保护的网络内。此类规则具有**解密 - 已知密钥**或**解密 - 替换证书**规则操作。

创建解密策略时，您可以同时创建多条规则，包括多条“**解密 - 已知密钥**”或“**解密 - 替换证书**”规则和多条“**解密 - 重新签名**”规则。。

开始之前

您可以选择首先上传内部服务器的内部证书，然后才能创建保护入站连接的解密策略。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)** 并引用 PKI， 第 2661 页 来创建内部证书对象。
- 在创建此解密策略时。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理工单， 第 162 页和支持变更管理的策略和对象， 第 157 页。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击**新建** > **解密策略（基于规则）**。

步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

解密策略名称中不支持使用以下字符：

- `#,;,{,},=,$,<,>`

步骤 5 从**内部证书 (Internal Certificates)** 列表中，上传或选择规则的证书。

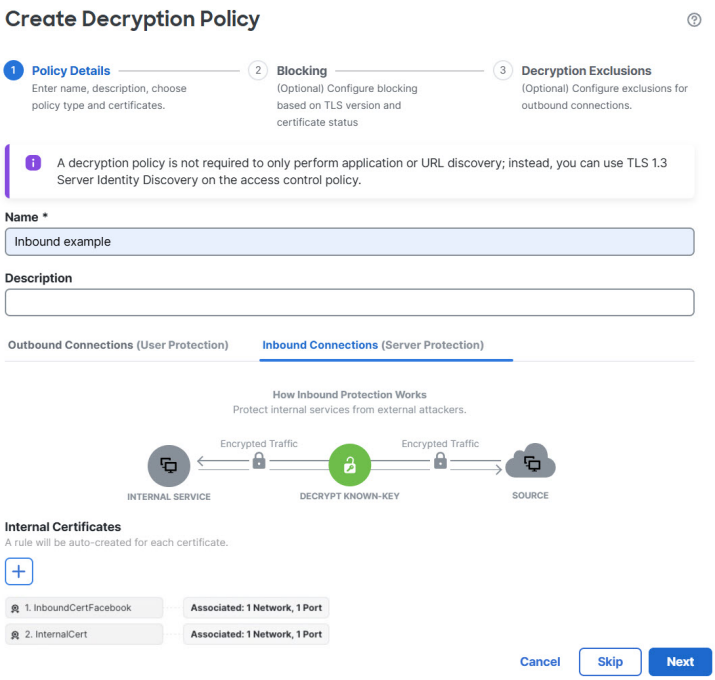
有关内部 CA 证书的详细信息，请参阅内部证书颁发机构对象，第 2662 页。

步骤 6 （可选。）选择网络和端口。

了解更多信息：

- 网络规则条件，第 1420 页
- 端口规则条件，第 1421 页

步骤 7 点击**入站连接 (Inbound Connections)** 选项卡。



步骤 8 点击**下一步 (Next)**。

步骤 9 继续执行 基于规则的解密策略 阻止连接，第 1891 页

步骤 10 继续执行基于规则的解密策略 排除项，第 1892 页。

下一步做什么

- 添加规则条件： 解密规则基于规则的解密规则 条件， 第 1920 页
- 添加默认策略操作： 基于规则的解密策略默认操作， 第 1899 页
- 为默认操作配置日志记录选项，如中的 使用策略默认操作记录连接*Cisco Secure Firewall Management Center* 管理指南所述。
- 设置高级策略属性：基于规则的解密策略高级选项， 第 1902 页。
- 将 解密策略 与访问控制策略相关联，如将其他策略与访问控制相关联， 第 1719 页中所述。
- 部署配置更改；请参阅 部署配置更改， 第 180 页。

基于规则的解密策略 阻止连接

本主题详细介绍在创建 基于规则的解密策略 时如何阻止连接到具有不安全 TLS 版本和服务器证书状态的服务器。您的解密策略中创建默认禁用的 **阻止并重置 (Block with Reset)** 规则。

过程

步骤 1 完成以下提到的任务：

- 创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页
- 创建具有入站连接保护的 基于规则的解密策略 ， 第 1889 页

步骤 2 **阻止 (Blocking)** 页面提供以下选项。默认情况下，会为解密策略操作禁用所有选项。

- **基于 TLS 版本阻止连接 (Block connections based on TLS version)** - 选中此复选框可阻止与使用不安全 TLS 版本的服务器的连接。默认情况下，系统会选择已知易受攻击的 **SSL v3.0**、**TLS v1.0** 和 **TLS v1.1**。您可以从下拉列表中选择其他版本。
- **基于服务器证书状态阻止连接 (Block connections based on server certificate status)** - 选中此复选框可阻止与服务器证书状态为不安全的服务器的连接。默认情况下，**无效签名 (Invalid Signature)**、**过期 (Expired)**、**尚未生效 (Not Yet Valid)** 和**无效证书 (Invalid Certificate)** 处于选中状态。您可以从下拉列表中选择其他状态。

点击 **删除** (✕) 以删除选择，或点击**重置为默认值 (Reset to default)** 恢复为默认选择。

步骤 3 点击**下一步 (Next)**。

下一步做什么

继续执行基于规则的解密策略 排除项， 第 1892 页。

基于规则的解密策略 排除项

此任务讨论如何将某些类型的流量排除在解密之外。虽然最初仅为出站解密策略（即，使用**解密 - 重新签名**策略操作的策略）启用这些规则，但我们会在解密策略中为这些策略创建**不解密**规则。

开始之前

您必须先上传出站服务器的内部证书颁发机构(CA)，然后才能创建保护出站连接的 基于规则的解密策略 。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **PKI** > **内部 CA (Internal CAs)** 并引用 PKI，第 2661 页 来创建内部 CA 证书对象。
- 在创建此解密策略时。

过程

步骤 1 完成以下讨论的任务：

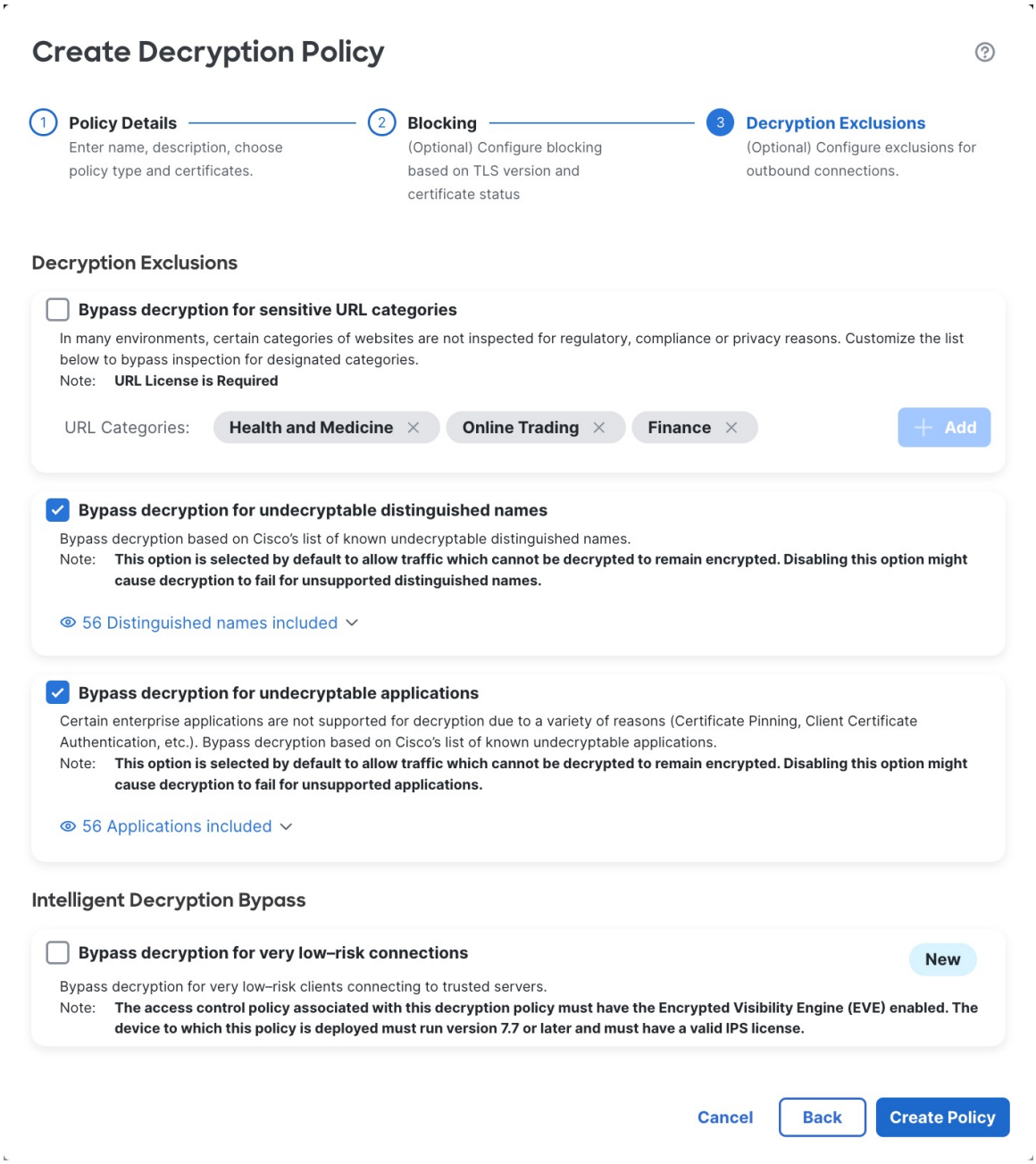
- 创建具有出站连接保护的 基于规则的解密策略 ，第 1887 页
- 有关详细信息，请参阅创建具有入站连接保护的 基于规则的解密策略 ，第 1889 页

步骤 2 排除项页面提供以下选项。为出站保护策略（**解密 - 重新签名**规则操作）启用 所有选项，并为所有其他解密策略操作禁用所有选项。

项目	说明
绕过解密敏感 URL 类别	选中此复选框可不解密来自指定类别的流量。根据您所在地区的法律，可能会禁止解密某些流量，例如与金融或健康相关的流量。有关详细信息，请咨询您所在地区的权威机构。 点击**添加 (Add)** 以添加更多类别。 点击 **删除** (✕) 以删除类别。
绕过对不可解密的可分辨名称的解密	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。通常，此行为与证书锁定相关，《TLS/SSL证书固定准则，第 1914 页的证书锁定准则中对此进行了讨论。 无法解密的可分辨名称列表由思科维护。

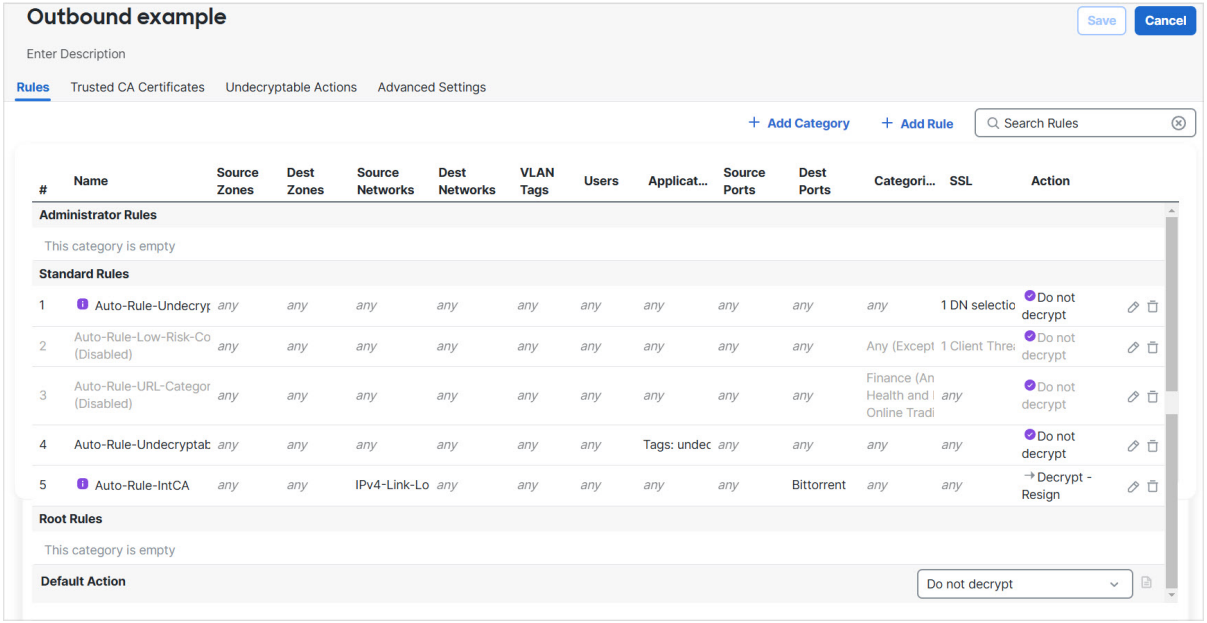
项目	说明
绕过解密无法解密的应用	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。 通常，此行为与证书锁定相关，《TLS/SSL证书固定准则，第1914页的证书锁定准则中对此进行了讨论。 无法解密的应用会在漏洞数据库 (VDB) 中自动更新。您可以在Cisco Secure Firewall应用检测器 (Secure Firewall Application Detectors) 页面上找到所有应用的列表；**undecryptable** 标记会标识思科确定为无法解密的应用。 无法解密的应用列表由思科维护。
对风险极低的连接绕过解密	选中此复选框，根据客户端的威胁置信度（由加密可见性引擎（EVE）和URL类别声誉决定），不解密连接到受信任服务器的极低风险客户端的流量。在新的解密策略中创建并启用了 **Auto-Rule-Low-Risk-Connections** 不解密规则。 要使用 **对风险极低的连接绕过解密** 选项，必须在对应地访问控制策略中启用加密可视性引擎 (EVE)，并且托管设备必须使用有效的 IPS 许可证运行版本 7.7 或更高版本。 要查看我们的当前应用风险和相关性分类列表，请转至Cisco Secure Firewall 应用检测器。

下图显示了默认选项。



步骤 3 点击创建策略 **(Create Policy)**。

下图显示了出站保护策略示例。



在前面的示例中，与您的规则排除项选择相对应的**不解密**规则会自动添加到**解密 - 重新签名**规则之前。敏感URL类别的规则已被禁用，因为默认情况下，该排除项已被禁用。如果您选中了**绕过敏感 URL 类别的解密 (Bypass decryption for sensitive URL categories)** 复选框，则该规则将被启用。

步骤 4 点击**创建策略 (Create Policy)**。

下一步做什么

- 添加规则条件： 解密规则基于规则的解密规则 条件 ， 第 1920 页
- 添加默认策略操作： 基于规则的解密策略默认操作 ， 第 1899 页
- 为默认操作配置日志记录选项，如*Cisco Secure Firewall Management Center* 管理指南 中的使用策略默认操作记录连接所述。
- 设置高级策略属性：基于规则的解密策略高级选项 ， 第 1902 页。
- 将 解密策略 与访问控制策略相关联，如将其他策略与访问控制相关联 ， 第 1719 页中所述。
- 部署配置更改；请参阅 部署配置更改 ， 第 180 页。

为出站保护生成内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地生成内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书 ， 第 2664 页中所述的**对象**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象 ， 第 2662 页中所述。

过程

步骤 1 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New)** > **生成 CA (Generate CA)**。

步骤 2 为内部 CA 提供一个**名称**，然后提供一个由两个字母组成的**国家/地区名称**。

步骤 3 点击**字签名 (Self-Signed)** 或**CSR**。

有关这些选项的详细信息，请参阅内部证书颁发机构对象，第 2662 页。

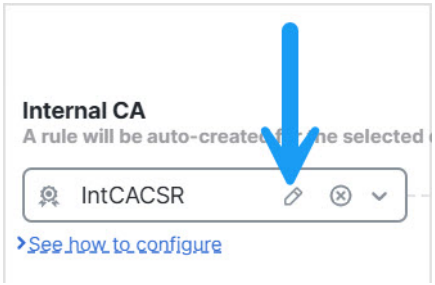
步骤 4 在提供的字段中输入请求的信息。

步骤 5 点击**保存**。

步骤 6 如果您选择了 **CSR**，则在签名请求完成后，点击**安装证书 (Install Certificate)**，如下所示：

a) 重复此程序中的上述步骤。

b) 从**内部 CA (Internal CA)** 列表编辑 CA，如下所示。



c) 点击 **Install Certificate**。

d) 按照屏幕提示完成任务。

步骤 7 按照创建具有出站连接保护的 基于规则的解密策略，第 1887 页中的说明继续创建策略。

为出站保护上传内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地上传内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书，第 2664 页中所述的**对象**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象，第 2662 页中所述。

过程

步骤 1 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New）** > **上传 CA (Upload CA)**。

步骤 2 为内部 CA 指定一个**名称**。

步骤 3 粘贴或在提供的字段中浏览找到证书及其私钥。

步骤 4 如果 CA 有密码，请选中**已加密 (Encrypted)** 复选框并在相邻字段中输入密码。

步骤 5 按照 创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页中的说明继续创建策略。

为入站保护上传内部证书

此任务讨论在创建保护入站连接的解密规则时如何上传内部证书。您还可以使用**对象**上传内部证书，如导入 CA 证书和私钥 ， 第 2663 页中所述。

开始之前

确保您具有中内部证书颁发机构对象 ， 第 2662 页所讨论的一种格式的内部证书。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在**名称 (Name)** 字段中输入策略的名称，在**说明 (Description)** 字段中输入可选的描述。

步骤 4 点击**入站连接 (Inbound Connections)** 选项卡。

步骤 5 从 **内部证书** 列表中，点击 **添加** (+)。

步骤 6 如果存在内部证书对象，请点击其名称。

步骤 7 否则，请点击**上传**。

步骤 8 输入所需信息。

请参阅添加内部证书对象 ， 第 2669 页。

步骤 9 按照 创建具有入站连接保护的 基于规则的解密策略 ， 第 1889 页中的说明继续创建解密策略。

在客户端计算机上安装内部 CA

为解密出站流量，Firewall Threat Defense 会充当中间人，首先解密流量（如果您选择，还可对其进行深度检查），然后使用不同的内部 CA 重新加密流量。当加密流量返回客户端时，客户端必须信任该 CA，否则用户会在其浏览器中看到错误。

例如，错误可能是：

```
www.example.com uses an invalid security certificate. The certificate is not trusted because

the issuer certificate is unknown
```

要避免这种情况，请在客户端计算机上导入内部CA（通常使用网络策略）。有关详细信息，请参考相关资源，例如：

- Windows：使用组策略向客户端计算机分发证书
- macOS：使用等同于 Windows 组策略对象 (GPO) 的第三方工具。有关详细信息，请参阅您的系统提供的文档。

创建一个带有其他规则操作的 基于规则的解密策略

要使用**不解密**、**阻止**、**阻止并重置**或**监控**规则操作来创建解密规则，请创建 基于规则的解密 并编辑该策略以添加该规则。

创建 基于规则的解密策略 时，您可以同时创建多条规则，包括多条**解密 - 已知密钥**规则、多条**解密 - 替换证书**规则和多条**解密 - 重新签名**规则。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理工单，第 162 页和支持变更管理的策略和对象，第 157 页。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 4 点击**下一步 (Next)**。

步骤 5 旁路页面仅供参考；您无法绕过其他类型解密（如**屏蔽**）的流量。

步骤 6 点击**创建策略 (Create Policy)**。

步骤 7 等待策略创建。

步骤 8 点击解密策略名称旁边的 **编辑** ()。

步骤 9 点击**添加规则**。

步骤 10 为规则 **命名**。

步骤 11 从**操作 (Action)** 列表中，点击规则操作，并参阅以下部分以了解详细信息：

- 基于规则的解密 规则 不解密操作，第 1938 页
- 基于规则的解密 规则阻止操作，第 1939 页
- 基于规则的解密 规则监控操作，第 1937 页

步骤 12 点击**保存**。

下一步做什么

- 添加规则条件： 解密规则基于规则的解密规则 条件， 第 1920 页
- 添加默认策略操作： 基于规则的解密策略默认操作， 第 1899 页
- 为默认操作配置日志记录选项， 如 *Cisco Secure Firewall Management Center* 管理指南 中的 使用策略默认操作记录连接 所述。
- 设置高级策略属性：基于规则的解密策略高级选项， 第 1902 页。
- 将 解密策略 与访问控制策略相关联，如将其他策略与访问控制相关联， 第 1719 页中所述。
- 部署配置更改；请参阅 部署配置更改， 第 180 页。

基于规则的解密策略默认操作

解密策略基于规则的解密策略的默认操作确定系统如何处理与策略中任何非监控规则都不匹配的可解密加密流量。当部署不包含任何解密规则的解密策略基于规则的解密策略时，默认操作将确定如何处理网络上所有可解密的流量。请注意，对于默认操作阻止的已加密流量，系统不会执行任何类型的检查。

要设置策略默认操作，请执行以下操作：

1. 如果尚未登录，请登录 Secure Firewall Management Center 。
2. 请点击 **策略** > **安全策略** > **解密**。
3. 点击 解密策略名称旁边的 **编辑** (✎) 。
4. 在“默认操作”行中，点击列表中的以下操作之一。

表 *108:* 解密策略 默认操作

默认操作	对已加密流量的影响
阻止	阻止 TLS/SSL 会话，无需进一步检查。
阻止并重置	阻止 TLS/SSL 会话并且无需进一步检查，然后重置 TCP 连接。如果流量使用的是像 UDP 一样的无连接协议，请选择此选项。在这种情况下，无连接协议将尝试重新建立连接，直到被重置。 执行此操作时，浏览器中还会显示连接重置错误，以便用户知道连接被阻止。
不解密	使用访问控制检查已加密的流量。

无法解密流量的默认处理选项

表 *109:* 无法解密的流量类型

类型	说明	默认操作	可用操作
压缩的会话	TLS/SSL 会话应用数据压缩方法。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
SSLv2 或 SSL v3 会话	此会话使用 SSL 版本 2或版本 3 加密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
未知密码套件	系统无法识别该密码套件。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
不支持的密码套件	系统不支持根据检测到的密码套件进行解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
会话无法缓存	TLS/SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
握手错误	TLS/SSL 握手协商期间出错。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作

类型	说明	默认操作	可用操作
解密错误	在流量解密时出错。	阻止	阻止 阻止并重置

首次创建 a 解密策略时，默认情况下将禁用记录默认操作所处理的连接。由于默认操作的日志记录设置也适用于无法解密的流量处理，默认情况下也将禁用记录无法解密的流量操作所处理的连接。

请注意，如果浏览器使用证书锁定验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。有关详细信息，请参阅基于规则的解密规则准则和限制，第 1908 页。

如果解密策略与使用 TCP 状态绕行的访问控制策略关联，则系统会根据策略为**握手错误**配置的**无法解密的操作**对匹配的流量执行操作。

例如，如果解密策略的**握手错误**被设置为**阻止 (Block)**，则匹配规则的流量会被阻止，并且连接事件的操作会报告为握手错误。

有关 TCP 状态绕行的详细信息，请参阅：

- 配置 TCP 状态绕行，第 2481 页
- 绕过非对称路由的 TCP 状态检查（TCP 状态绕行），第 2479 页

设置无法解密的流量的默认处理

您可以在解密策略基于规则的解密策略级别设置无法解密的流量操作以处理系统无法解密或检查的某些类型的已加密流量。部署不包含任何 解密规则 的 解密策略基于规则的解密策略 时，无法解密的流量操作确定如何处理网络上的所有无法解密的已加密流量。

视乎无法解密的流量类型，您可以选择：

- 阻止连接。
- 阻止连接，然后重置连接。对于UDP等一直尝试连接直到连接被阻止的无连接协议，最好选择此选项。
- 使用访问控制检查已加密的流量。
- 继承 解密策略基于规则的解密策略 的默认操作。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 解密策略名称旁边的 **编辑** (✎) 。

步骤 4 在 解密策略 编辑器中，点击**无法解密的操作 (Undecryptable Actions)**。

步骤 5 对于每个字段，请选择要对无法解密的流量类型执行的解密策略的默认操作或其他操作。有关详细信息，请参阅无法解密流量的默认处理选项，第 1900 页和基于规则的解密策略默认操作，第 1899 页。

步骤 6 点击**保存** 保存策略。

下一步做什么

- 为无法解密的流量操作所处理的连接配置默认日志记录；请参阅*Cisco Secure Firewall Management Center* 管理指南。
- 部署配置更改；请参阅 部署配置更改，第 180 页。

基于规则的解密策略高级选项

解密策略基于规则的解密策略的**高级设置**页面包含全局设置，这些设置适用于所有为 Snort 3 配置且应用了该策略的受管设备。

在运行以下命令的任何托管设备上，解密策略基于规则的解密策略高级设置都将被忽略：

- 早于 7.1 的版本
- Snort 2

阻止请求 ESNI 的流

加密服务器名称指示（ESNI [建议草案的链接]）是客户端告知 TLS 1.3 服务器其请求内容的一种方式。由于 SNI 会被加密，因此您可以选择阻止这些连接，因为系统无法确定服务器是什么。

禁用 HTTP/3 通告

此选项会从 TCP 连接中的 ClientHello 删除 HTTP/3 (RFC 9114)。HTTP/3 是 QUIC 传输协议的一部分，而不是 TCP 传输协议。阻止客户端通告 HTTP/3，可以防止可能隐藏在 QUIC 连接中的攻击和规避企图。

将不受信任的服务器证书传播到客户端

这仅适用于匹配**解密 - 重新签名 (Decrypt - Resign)** 规则操作的流量。

启用此选项可在服务器证书不受信任的情况下，使用托管设备上的证书颁发机构 (CA) 来替换服务器证书。不受信任的服务器证书是指未在 Secure Firewall Management Center 中列为受信任 CA 的证书。（**对象 (Objects)** > **PKI** > **受信任 CA (Trusted CAs)**）。

启用 TLS 1.3 解密

是否将解密规则应用于 TLS 1.3 连接。如果不启用此选项，则解密规则仅适用于 TLS 1.2 或更低版本的流量。请参阅TLS 1.3 解密最佳实践，第 1904 页。

启用自适应 TLS 服务器身份探测

启用 TLS 1.3 解密时自动启用。 探测 是与服务器的部分 TLS 连接，其目的是获取服务器证书并将其缓存。（如果证书已缓存，则永远不会建立探测。）

如果在与解密策略关联的访问控制策略上禁用了 TLS 1.3 服务器身份发现，我们将尝试使用服务器名称指示 (SNI)，这并不可靠。

自适应 TLS 服务器身份探测发生在以下任何情况下，而不是在早期版本中的每个连接上发生：

- 证书颁发者 - 当解密规则的 DN 规则条件中的 **颁发者 DN** 值匹配时匹配。

  有关详细信息，请参阅可分辨名称 (DN) 规则条件，第 1926 页。

- 证书状态 - 当解密规则中的任何 **证书状态** 条件匹配时匹配。

  有关详细信息，请参阅证书状态 解密规则 条件，第 1932 页。

- 内部/外部证书 - 内部证书可以通过 **解密 - 已知密钥** 规则操作中使用的证书进行匹配；可以在 **证书** 规则条件中匹配外部证书。

  有关详细信息，请参阅已知密钥解密（传入流量）和证书规则条件，第 1926 页。

- 应用 ID - 可以通过访问控制策略或解密策略中的 **应用** 规则条件进行匹配。

  有关详细信息，请参阅应用规则条件，第 1420 页。

- URL 类别 - 可以通过访问控制策略中的 **URL** 规则条件进行匹配。

  有关详细信息，请参阅URL 规则条件，第 1423 页。



注释 任何部署到 AWS 的设备都不支持启用自适应 TLS 服务器发现模式。Secure Firewall Threat Defense Virtual如果您有任何由 Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。

启用 QUIC 解密

是否将解密规则应用于通过 QUIC 协议使用 HTTP/3 的连接。解密 QUIC 连接时，系统可以检查会话内容是否存在入侵、恶意软件或其他问题。您还可以根据访问控制策略中的特定条件来对已解密的 QUIC 连接应用精细控制和过滤。QUIC 支持符合 RFC 9000、9001、9002、9114、9204 的要求。

实施 QUIC 解密时，请考虑以下事项：

- 在 高可用性或集群设备上，QUIC 解密只有在连接保持位于同一节点时才有效。如果对连接进行故障转移或将其转发到另一个节点，则连接会断开，必须重新建立。支持多实例而无限制。
- 适用于 QUIC 流量的规则将包括具有目的端口 443 的 UDP 协议。
- 适用于 QUIC 流量的访问控制规则将包括 HTTP/3 或 QUIC 协议（显式或隐式）。

以下限制适用于 QUIC 解密：

- QUIC 解密仅适用于 Firewall Threat Defense 7.6+。运行较低版本的设备无法解密 QUIC 连接。

- 无法为出站流量解密来自使用 Chromium 堆栈的浏览器（Google Chrome、Opera 和 Edge）的连接。但可以解密来自相同浏览器的入站流量。
- 不支持 RFC 9000 中所述的连接迁移。QUIC 中的连接 ID 概念允许终端在地址更改时保留相同的连接。
- 不支持密钥更新、会话恢复和 QUIC 版本 2。
- 不支持交互式阻止和交互式阻止并重置（在访问控制规则中）。这些操作将作为“阻止”和“阻止并重置”。
- 每个连接的活动连接 ID 限制为 5。如有必要，您可以使用设备 CLI 中的**system support quic-tuning**和**system support quic-tuning-reset**命令修改这些限制。

TLS 1.3 解密最佳实践

建议：何时启用高级选项

解密策略基于规则的解密策略 和访问控制策略都具有影响流量处理方式的高级选项，无论流量是否被解密。

高级选项包括：

- 解密策略：
  - TLS 1.3 解密
  - TLS 自适应服务器身份探测
- 访问控制策略：TLS 1.3 服务器身份发现

  访问控制策略设置优先于解密策略设置。

使用下表确定要启用的选项：

TLS 自适应服务器身份探测设置（解密策略）	TLS 1.3 服务器身份发现设置（访问控制策略）	结果	建议使用条件
已启用	已禁用	如果解密策略包含 基于规则的解密策略高级选项，第 1902 页中指定的任何规则条件 并且服务器证书未被缓存，则发送自适应探测。	• 您未在访问控制规则中使用应用或 URL 条件 • 您正在解密流量
已启用	已启用	如果服务器证书未缓存，则始终发送探测。	仅当访问控制规则具有 URL 或应用条件时使用
已禁用	已启用	如果服务器证书未缓存，则始终发送探测。	不推荐。

TLS 自适应服务器身份探测设置（解密策略）	TLS 1.3 服务器身份发现设置（访问控制策略）	结果	建议使用条件
Disabled	Disabled	从不发送探测。	用途非常有限；仅在不解密流量且不在访问控制规则中使用应用或 URL 条件时使用



注释 缓存的 TLS 服务器证书可用于特定 Firewall Threat Defense上的所有 Snort 实例。可以使用 CLI 命令清除缓存，并在设备重新启动时自动清除缓存。

参考

有关详细信息，请参阅 secure.cisco.com 上有关 TLS 服务器身份发现 的讨论。



第 47 章

基于规则的解密 规则

以下主题讨论如何管理 基于规则的解密 规则。

- 关于基于规则的解密， 第 1907 页
- 基于规则的解密规则 的要求和先决条件， 第 1907 页
- 基于规则的解密规则准则和限制， 第 1908 页
- 解密规则基于规则的解密规则 流量处理， 第 1916 页
- 解密规则基于规则的解密规则 条件， 第 1920 页
- 解密规则基于规则的解密规则 操作， 第 1937 页
- 监控 TLS/SSL 硬件加速， 第 1943 页
- 对基于规则的解密规则进行故障排除， 第 1945 页
- 使用加密归档进行故障排除， 第 1954 页

关于基于规则的解密

解密规则 提供一种精细的方法来跨多台托管设备处理加密流量：阻止流量而不进一步检查；不解密流量并通过访问控制对其进行检查；或者解密流量以进行访问控制分析。

此信息仅适用于 基于规则的解密 策略和规则。

基于规则的解密规则 的要求和先决条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

基于规则的解密规则准则和限制

在设置 基于规则的解密规则 时，请记住以下要点。正确配置 基于规则的解密规则 是一项复杂的任务，但是对于构建用于处理加密流量的有效部署至关重要。许多因素会影响您配置规则的方式，包括您无法控制的特定应用行为。

此外，规则可以互相抢占，需要其他许可证或包含无效配置。周全配置的 SSL 规则还可以减少处理网络流量所需的资源。创建过度复杂的规则和以错误方式对规则进行排序可能会对性能产生不利影响。

有关详细信息，请参阅访问控制规则的最佳实践，第 1758 页。

有关 TLS 加密加速的具体准则，请参阅TLS 加密加速，第 1849 页。

相关主题

规则和其他策略警告
访问控制规则的最佳实践，第 1758 页
使用TLS/SSL解密的准则，第 1908 页
基于规则的解密规则 不支持的功能，第 1909 页
TLS/SSL 不解密准则，第 1910 页
TLS/SSL 传入流量解密准则，第 1911 页
TLS/SSL 解密 - 重新签名准则，第 1912 页
TLS/SSL 阻止准则，第 1914 页
TLS/SSL证书固定准则，第 1914 页
TLS/SSL 心跳准则，第 1915 页
TLS/SSL 匿名密码套件限制，第 1915 页
TLS/SSL 标准化程序准则，第 1915 页
其他 解密规则基于规则的解密规则 准则，第 1915 页
解密策略 规则顺序

使用TLS/SSL解密的准则

一般准则

基于规则的解密规则 需要可能会影响性能的处理开销。在设置任何策略或规则之前，确定哪些流量必须解密并接受深度检测。

您无法解密使用以下任何一项的设备上的流量：

- 被动接口
- 内联或内联分路接口
- TCP 状态绕行

无法解密的流量准则

我们可以确定某些流量不可解密，要么是因为网站本身不可解密，要么是因为该网站使用了 TLS/SSL 锁定，这有效地阻止了用户访问其浏览器中没有错误的已解密网站。

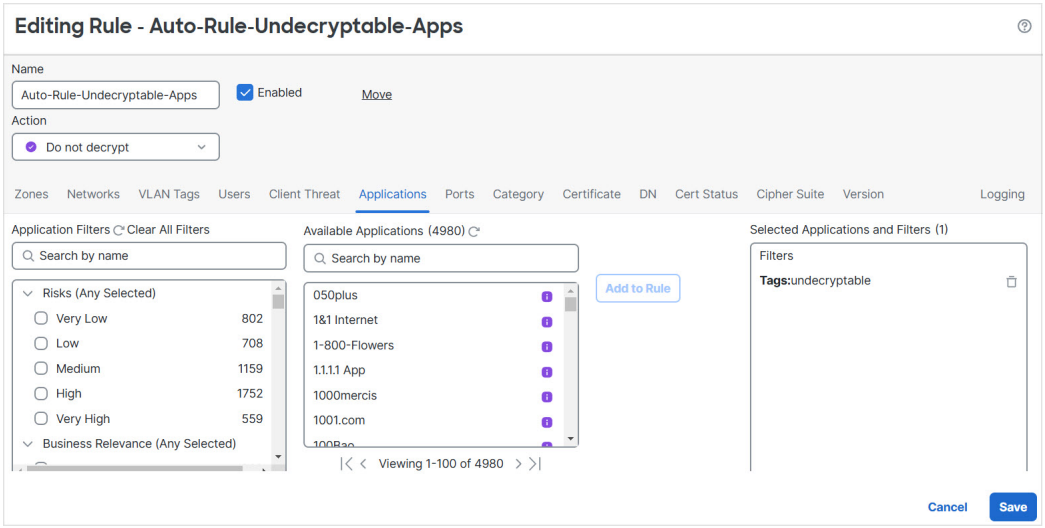
有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定，第 1949 页。

我们维护的这些站点的列表如下：

- 名为 **Cisco-Undecryptable-Sites** 的可分辨名称 (DN) 组
- **已固定证书**或**无法解密**应用过滤器

如果您正在解密流量，并且不希望用户在访问这些站点时在其浏览器中看到错误，我们建议您在 解密规则 底部设置**不解密规则**。

如果使用解密策略向导创建出站流量保护策略，系统会为您创建固定证书的**不解密**规则，如以下示例所示。



基于规则的解密规则 不支持的功能

不支持被动、内联分流模式以及 SPAN 接口

无法在被动、内联分流模式或 SPAN 接口上解密 TLS/SSL 流量。

不支持 DES 和 RC4 密码套件

已知 Rivest 密码 4（也称为 *RC4* 或 *ARC4*）和数据加密标准 (DES) 密码存在漏洞，被视为不安全。

在解密策略 策略的**无法解密的操作**页面中配置**不支持的密码套件**操作，以符合您组织的要求。有关详细信息，请参阅 无法解密流量的默认处理选项，第 1900 页。

TLS/SSL 不解密准则

如果是以下情况，则不应对流量进行解密：

- 法律所禁止；例如，某些司法管辖区禁止解密财务信息
- 公司政策所禁止；例如，您的公司可能会禁止解密特权通信
- 隐私法规所禁止
- 使用证书固定（也称为*TLS/SSL*固定）的流量必须保持加密，以防止断开连接

加密流量可以在任何 解密规则 条件下被允许或阻止，包括但不限于：

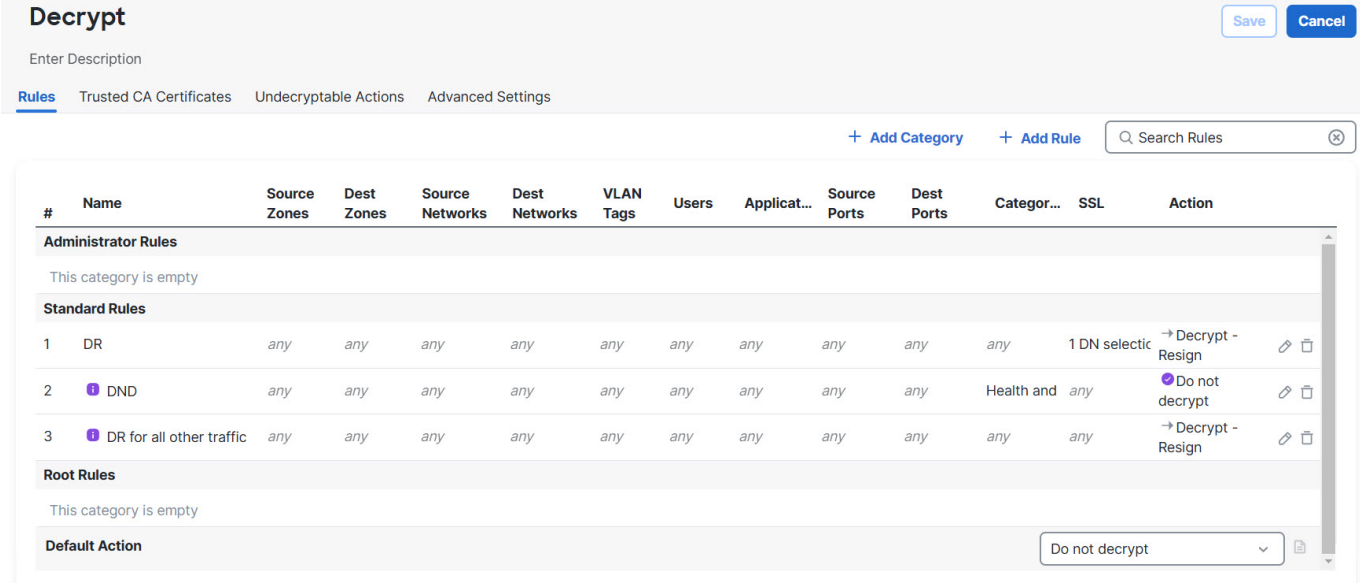
- 证书状态（例如，证书已过期或无效）
- 协议（例如，非安全 SSL 协议）
- 网络（安全区域、IP 地址、VLAN 标记等）
- URL 类别和信誉
- 端口
- 用户组

“不解密”规则中的类别限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用TLS/SSL解密的准则，第 1908 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅应用控制的建议，第 1755 页。

TLS/SSL 传入流量解密准则

解密 - 替换证书规则操作只能关联一个服务器证书和配对私钥。要解密 TLS 1.2 流量，规则中使用的公共密钥类型必须与内部服务器的公共密钥类型匹配。（例如，如果内部服务器使用 RSA 公共密钥类型，解密规则中使用的公共密钥类型也必须为 RSA。）此限制不适用于解密 TLS 1.3 流量。

解密 - 已知密钥规则操作可以关联一个或多个服务器证书和配对私钥。

如果流量与规则相匹配，并且用于加密流量的证书与操作的关联证书相匹配，则系统会使用相应的私钥获取会话加密和解密密钥。由于您必须有权访问私钥，此操作最适合于解密传入到组织控制的服务器的流量。

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

您不能在规则中使用**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**操作，因为匿名密码套件不用于身份验证。

无法匹配可分辨名称或证书

创建具有**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 解密规则 时，无法使用**可分辨名称 (Distinguished Name)** 或**证书 (Certificate)** 规则条件进行匹配。此限制基于这样一种假设：如果此规则与流量相匹配，则证书、使用者 DN 和颁发者 DN 已经与规则的关联证书相匹配。

请勿使用版本或密码套件规则条件



重要事项 切勿在具有**解密 - 重新签名**、**解密 - 替换证书**或**或解密 - 已知密钥**规则操作的规则中使用**密码套件**或**版本**规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

椭圆曲线数字签名算法 (*ECDSA*) 证书会导致流量被阻止。
（仅启用 TLS 1.3 解密。）如果将 ECDSA 证书与**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作配合使用，则会阻止匹配的流量。要避免这种情况，请将证书与其他类型的证书配合使用。

TLS/SSL 解密 - 重新签名准则

您可以将一个内部证书颁发机构 (CA) 证书和私钥与**解密 - 重新签名 (Decrypt - Resign)** 操作相关联。如果流量与此规则相匹配，则系统会使用 CA 证书对服务器证书重新签名，然后充当中间人。它创建两个 TLS/SSL 会话，一个是客户端与托管设备之间的会话，一个是托管设备与服务器之间的会话。每个会话包含不同的加密会话详细信息，并且允许系统解密并重新加密流量。

最佳实践

我们的建议如下：

- 对于解密传出流量，请使用**解密 - 重新签名**规则操作；对于传入流量，我们建议使用**解密 - 已知密钥** 或**解密 - 替换证书**规则操作。

  有关**解密 - 已知密钥** 或**解密 - 替换证书**的详细信息，请参阅TLS/SSL 传入流量解密准则，第 1911 页。

- 在设置**机密 - 重新签名 (Decrypt - Resign)** 规则操作时始终选中**仅更换密钥 (Replace Key Only)** 复选框。

  当用户浏览到使用自签名证书的网站时，他们会在 Web 浏览器中看到安全警告，并会意识到自己正在与不安全的站点通信。

  当用户浏览到使用受信任证书的网站时，他们不会看到安全警告。

详细信息

如果配置具有 **Decrypt - Resign** 操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您将一个 CA 证书与 **Decrypt - Resign** 操作相关联，因此无法创建用来解密使用不同签名算法加密的多种类型的传出流量的 解密规则。此外，添加到规则中的任何外部证书对象和密码套件都必须与关联的 CA 证书加密算法类型相匹配。

例如，仅当操作引用基于椭圆曲线 (EC) 的 CA 证书时，使用 EC 算法加密的传出流量才会与**解密 - 重新签名**规则相匹配；必须将基于 EC 的外部证书和密码套件添加到此规则，以创建证书和密码套件规则条件。

同样，引用基于 RSA 的 CA 证书的 **Decrypt - Resign** 规则仅与使用 RSA 算法加密的传出流量相匹配；使用EC算法加密的传出流量与该规则不匹配，即使所有其他已配置的规则条件都匹配也如此。

准则和限制

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

请勿使用版本或密码套件规则条件



重要事项 切勿在具有**解密 - 重新签名**、**解密 - 替换证书**或**或解密 - 已知密钥**规则操作的规则中使用**密码套件**或**版本**规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

“解密 - 重新签名”规则操作和证书签名请求

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，应创建证书签名请求 (CSR) 并由受信任的证书颁发机构签名。（您可以使用 FMC 创建 CSR： **对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**。）

要在解密 - 重新签名规则中使用，您的证书颁发机构 (CA) 必须至少具有以下扩展名之一：

- **CA: TRUE**

  有关详细信息，请参阅 RFC3280 第 4.2.1.10 节中对基本限制的讨论。

- **KeyUsage=CertSign**

  有关详细信息，请参阅 RFC 5280 第 4.2.1.3 节。

要验证您的 CSR 或 CA 是否至少具有上述扩展名之一，您可以按照 openssl 文档等参考资料中的说明来使用 **openssl** 命令。

这是必要的，因为要使**解密 - 重新签名 (Decrypt - Resign)** 检查工作，解密策略 中使用的证书会即时生成证书并对其进行签名，以便充当中间人并代理所有 TLS/SSL 连接。

证书固定

如果客户的浏览器使用证书锁定来验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。要允许此流量，请配置一个 解密规则，将**不解密**操作与服务器证书公用名或可分辨名称相匹配。

解密策略向导会为您创建此类规则；请参阅请参阅创建具有出站连接保护的 基于规则的解密策略 ， 第 1887 页。

不匹配的密码套件

如果尝试使用与证书不匹配的密码套件保存 解密规则，则会显示以下错误。要解决此问题，请参阅验证 TLS/SSL 密码套件 ， 第 1953 页。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

不受信任的证书颁发机构

如果客户端不信任用于对服务器证书重新签名的证书颁发机构(CA)，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

HTTP 代理限制

如果 HTTP 代理位于客户端和托管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 TLS/SSL 连接，则系统无法解密流量。**Handshake Errors** 无法解密操作将决定系统如何处理此流量。

上传签名的 CA

如果创建内部CA对象并选择生成证书签名请求(CSR)，那么在将签名证书上传到对象之前，会无法对 **Decrypt - Resign** 操作使用此 CA。

不匹配的签名算法

如果配置具有 **Decrypt - Resign** 操作的规则，并且不匹配一个或多个外部证书对象或密码套件的签名算法类型，则策略编辑器在该规则旁边显示 **信息**()。如果所有外部证书对象或所有密码套件的签名算法类型不匹配，则策略在该规则旁边显示警告图标 **警告**（），并且无法部署与解密策略相关联的访问控制策略。

TLS/SSL 阻止准则

如果您的解密规则与访问控制策略相关联，而该策略的规则具有**交互式阻止**或**交互式阻止并重置**，则系统会显示一个可定制的响应页面。

如果您在规则中启用了日志记录，则会显示两个连接事件（在 **事件和日志** > **+ 显示更多** > **连接** > **事件** 中）：一个事件用于交互式阻止，而另一个事件用于指示用户是否选择继续访问站点。

相关主题

配置 HTTP 响应页面 ， 第 1801 页

TLS/SSL证书固定准则

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 解密规则，则应用从托管设备收到重签的证书时，验证会失败且连接会中止。

由于 TLS/SSL 锁定用于避免中间人攻击，因此无法不能将其阻止或绕过。我们建议在**解密 - 重新签名**规则之前添加**不解密**规则，以便排除锁定流量进行解密。解密策略向导会为您执行此操作。

- 为排在**解密 - 重签**规则之前的应用创建**不解密**规则。
- 指示用户使用网络浏览器访问应用。

有关规则排序的详细信息，请参阅解密策略 规则顺序。

要确定应用是否正在使用 TLS/SSL 锁定，请参阅对 TLS/SSL 锁定进行故障排除 ， 第 1950 页。

TLS/SSL 心跳准则

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

您可以在网络分析策略 (NAP) 中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。有关详细信息，请参阅SSL 预处理器。

有关详细信息，请参阅关于 TLS 心跳 ， 第 1947 页。

TLS/SSL 匿名密码套件限制

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

您可以将匿名密码套件添加到解密规则的**密码套件**条件中，但系统会在 ClientHello 处理期间自动删除匿名密码套件。要让系统使用该规则，还必须配置 解密规则 的顺序以阻止 ClientHello 处理。有关详细信息，请参阅解密策略 规则顺序。

TLS/SSL 标准化程序准则

如果启用内联规范化预处理器中的**规范化多余负载**选项，则预处理器在规范化解密流量时，可能会丢弃数据包并将其替换为修整过的数据包。这不会结束 TLS/SSL 会话。如果允许流量，则修整过的数据包会作为 TLS/SSL 会话的一部分加密。

其他 解密规则基于规则的解密规则 准则

用户和组

如果向规则中添加用户或组，然后更改领域设置以排除该组或用户，规则将不会生效。（同样适用于禁用领域。）有关领域的更多信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录 ， 第 2019 页。

解密规则中的类别

如果您的 解密策略具有**解密 - 重新签名 (Decrypt - Resign)** 操作，但网站不会被解密，请检查与该策略相关的规则的**类别 (Category)** 页面。

在某些情况下，网站重定向到另一个站点进行身份验证或实现其他目的，而重定向的站点可能具有与您正在尝试解密的站点不同的 URL 分类。例如，`gmail.com`（**基于 Web 的电子邮件**类

别）将重定向到 accounts.gmail.com（**互联网门户**类别）进行身份验证。请务必在 SSL 规则中包含所有相关类别。



注释 为了根据URL类别完全处理流量，您还必须配置URL过滤。请参阅URL 过滤规则，第 1785 页一章。

查询不在本地数据库中的 URL

如果您创建了一个**解密 - 重签**规则，并且用户浏览到其类别和信誉不在本地数据库中的网站，则数据可能不会被解密。某些网站未分类在本地数据库中，如果未分类，默认情况下不会解密来自这些网站的数据。

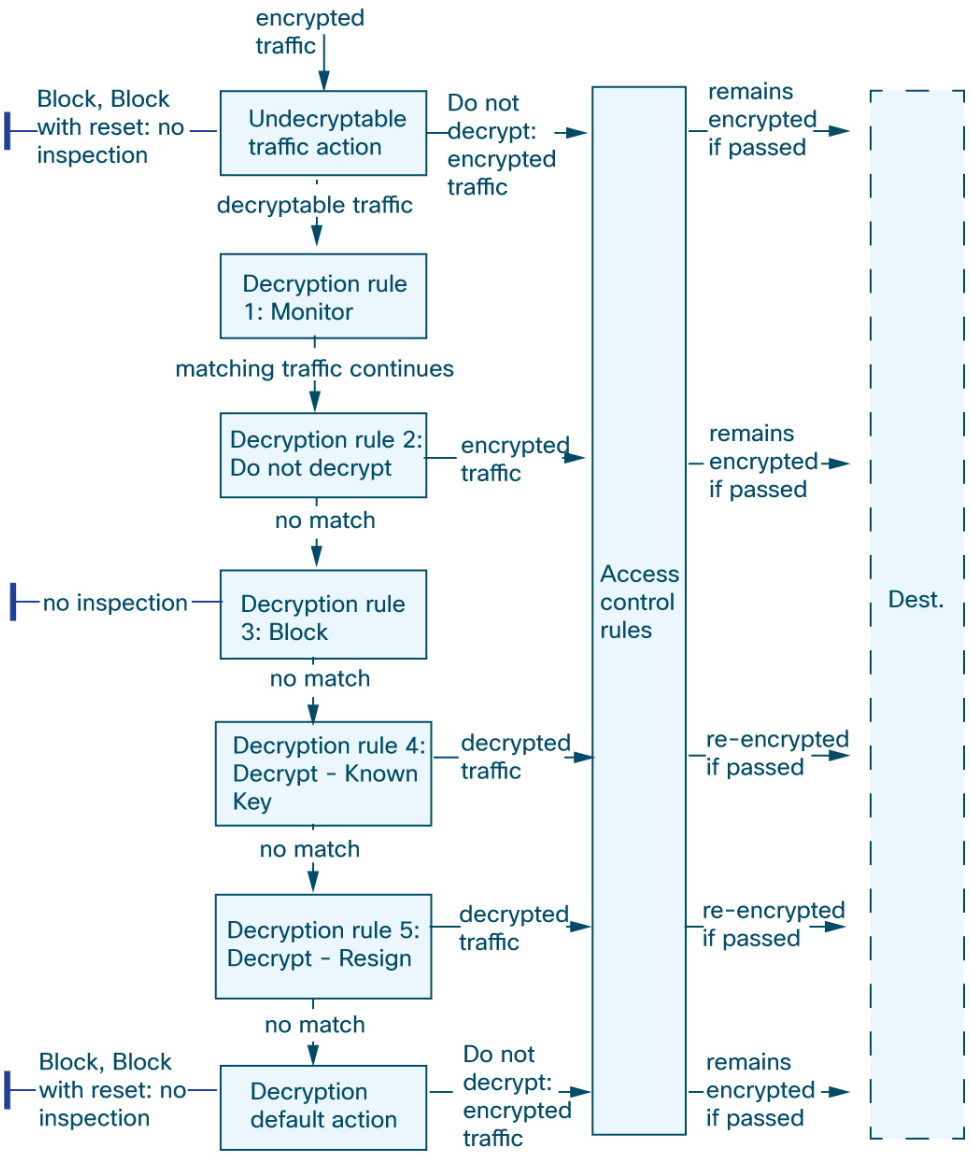
可通过**集成** > **云服务**中的**向思科云查询未知 URL** 设置来控制此行为。

解密规则基于规则的解密规则 流量处理

系统会按照您所指定的顺序将流量与基于规则的解密规则规则相匹配。在大多数情况下，系统会根据第一个 解密规则（使用规则的所有条件来匹配流量）来处理加密流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，而是会通过访问控制来检查加密流量和无法解密的流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。

下述场景概括说明了 解密规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，**Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **解密规则 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **解密规则 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **解密规则 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。

- 第五，使用 **解密规则 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 解密规则 不匹配的流量会继续根据下一规则进行评估。
- **解密规则 5: Decrypt - Resign** 是最终规则。如果流量匹配，系统将使用上传的 CA 证书重新签名服务器证书并解密流量。然后，根据访问控制规则对解密流量进行评估，以同等对待已解密和未加密的流量。这项额外的检查可以让系统阻止交通。剩余的所有流量在发送到目标之前都会重新加密。与 解密规则 规则不匹配的流量将继续处理下一条规则。
- **解密策略 Default Action** 会处理与任何 解密规则 不匹配的所有流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

加密流量检查配置

您必须创建可重用公共密钥基础设施 (PKI) 对象才能基于加密会话特性控制加密流量并解密加密流量。可以在将受信任证书颁发机构 (CA) 证书上传到 a 解密策略 并创建 解密规则，以及在此过程中创建关联对象时即时添加此信息。不过，提前配置这些对象可降低不正确创建对象的几率。

使用证书和配对密钥解密加密流量

如果通过上传用于会话加密的服务器证书和私钥来配置内部证书对象，则系统可以解密传入的加密流量。如果在包含**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 a 解密策略 规则中引用该对象并且流量与该规则相匹配，则系统会使用上传的私钥来解密会话。

如果通过上传 CA 证书和私钥来配置内部 CA 对象，则系统还可以解密传出流量。如果在包含**解密 - 重新签名 (Decrypt - Resign)** 操作的 解密规则 规则中引用该对象并且流量与该规则相匹配，则系统会对传递到客户端浏览器的服务器证书重新签名，然后充当中间人来解密会话。 您可以选择只替换自签名证书密钥，而不是整个证书，在这种情况下，用户可在浏览器中看到自签名证书密钥通知。

根据加密会话特性控制流量

系统可以根据用于协商会话的密码套件或服务器证书来控制加密流量。您可以从多个不同的可重用对象中选择一个进行配置，并在解密规则条件中参照该对象来匹配流量。下表介绍可以配置的不同类型的可重用对象：

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含一个或多个密码套件的密码套件列表	用于协商加密会话的密码套件与密码套件列表中的密码套件相匹配
受信任 CA 对象（通过上传组织信任的 CA 证书）	受信任 CA 根据以下情况来确定是否信任用于加密会话的服务器证书： • CA 直接颁发证书 • CA 向颁发服务器证书的中间 CA 颁发证书
外部证书对象（通过上传服务器证书）	用于加密会话的服务器证书与上传的服务器证书相匹配

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含证书使用者或颁发者可分辨名称的可分辨名称对象	用于加密会话的证书上的主题或颁发者通用名称、国家/地区、组织或组织单位与已配置的可分辨名称相匹配

相关主题

密码套件列表，第 2634 页
可分辨名称，第 2637 页
PKI，第 2661 页

解密规则基于规则的解密规则 顺序评估

此信息仅适用于 基于规则的解密 策略和规则。

在 基于规则的解密策略 中创建 基于规则的解密规则 时，您可以使用规则编辑器中的**插入**列表来指定其位置。 解密策略 中的 解密规则 会从 1 开始编号。系统按升序规则编号以自上而下的顺序将流量与 解密规则 相匹配。

在大多数情况下，系统根据第一个 解密规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 类别和信誉、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，它会通过访问控制来检查加密流量和无法解密的流量。但是，访问控制规则条件需要未加密流量，因此，已加密流量匹配的规则更少。

使用特定条件（例如网络和 IP 地址）的规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在规则中排序。稍后应在规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的解密规则顺序可减少处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

相关主题

访问控制规则的最佳实践，第 1758 页
无法解密流量的默认处理选项，第 1900 页
解密策略 规则顺序

解密规则基于规则的解密规则 条件

基于规则的解密规则 的条件识别此规则处理的加密流量的类型。条件可以简单也可以复杂，并且可以指定每个规则有多个条件类型。仅当流量满足规则中的所有条件时，该规则才适用于此流量。

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话 SSL 或 TLS 版本如何，具有证书条件但不具有版本条件的规则根据用于协商会话的服务器证书来评估流量。

每个 基于规则的解密策略 都具有对匹配的加密流量确定以下处理的关联操作：

- 处理：最重要的是，规则操作管理系统是监控、信任、阻止还是解密与规则条件匹配的加密流量
- 日志记录：规则操作确定何时及如何记录有关匹配的加密流量的详细信息。

您的 TLS/SSL 检查配置会处理、检查并记录解密流量：

- 解密策略 的无法解密的操作处理系统无法解密的流量。
- 策略的默认操作处理不满足任何非监控器 解密规则 的条件的流量。

当系统阻止或信任加密会话时，可以记录连接事件。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。已加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。您可以仅记录连接结束事件，但是：

- 对于受阻连接（“阻止”、“阻止并重置”），系统会立即结束会话并生成事件
- 对于“不解密”连接，系统在会话结束时生成事件

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

⚠

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 a 解密策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

相关主题

安全区域规则条件，第 1921 页
网络规则条件，第 1420 页
VLAN 标记规则条件，第 1768 页
用户规则条件，第 1420 页
应用规则条件，第 1420 页
端口规则条件，第 1421 页

类别规则条件，第 1925 页
基于服务器证书的规则条件，第 1925 页

安全区域规则条件

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

VLAN 标记规则条件



注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

用户规则条件

根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

您只能为 Microsoft Active Directory 领域中的用户配置用户规则条件。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联 ，第 1719 页中所述。

客户端威胁规则条件

客户端进程的威胁置信度由加密可视性引擎 (EVE) 确定，代表传入流量是恶意流量的可能性。客户威胁置信度级别从很低到很高不等，这些级别可指定为解密策略规则的规则条件。当配置了客户端威胁置信度和服务器URL类别信誉后，它们就会成为解密策略中的强大组合。强烈建议您为指定客户端威胁规则条件的规则指定URL类别信誉规则条件。如果同时为解密策略规则指定了客户端威胁和URL类别信誉条件，则客户端和服务器的信誉都会被利用，从而做出更准确的解密策略决策。在未指定URL类别信誉规则条件的情况下，建议不要单独指定客户端威胁规则条件，因为此规则配置仅作用于有关客户端的信息，会缺少有关服务器的信息。

配置客户端威胁规则条件的前提条件

- 必须在相应的访问控制策略中启用 EVE。
- 管理中心和威胁防御设备的版本必须为 7.7。
- 必须在设备上启用 Snort 3。
- 托管设备上必须安装有效的 IPS 和 URL 过滤许可证。

我们建议您根据 EVE 和 URL 类别信誉确定的客户端威胁，对连接到可信服务器的极低风险客户端绕过解密。为此，请使用以下配置创建新的解密策略规则或编辑现有规则：

1. 选择**不解密 (Do not decrypt)** 作为解密策略规则操作。
2. 在**客户端威胁 (Client Threat)** 选项卡中，选择客户端威胁级别为**非常低 (Very Low)**。
3. 在**类别 (Category)** 选项卡中，将类别选择为**所有 (All)**，将信誉选择为**受信任 (Trusted)**。

应用规则条件

系统分析IP流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅应用检测器基础知识，第 2564 页。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *110:* 应用特征

特征	说明	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

对于会动态打开独立通道以区分控制流和数据流的应用（如 Firewall Threat Defense），也建议使用应用过滤。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

类别规则条件

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。

有关详细信息，请参阅URL 过滤概述，第 1785 页。

如果在具有 **不解密** 规则操作的规则的 解密策略 中使用类别规则条件，请参阅 基于规则的解密 规则不解密操作，第 1938 页。

基于服务器证书的规则条件

解密规则可以根据服务器证书特征来处理和解密已加密的流量。您可以根据以下服务器证书属性配置 解密规则：

- 通过可分辨名称，您可以根据颁发服务器证书的 CA 或证书使用者来处理和检查加密流量。根据颁发者可分辨名称，可以根据颁发站点服务器证书的 CA 处理流量。
- 通过 解密规则中的证书条件，可以根据用于对加密流量进行加密的服务器证书来处理和检查该流量。可以配置具有一个或多个证书的条件；如果证书与该条件的任何证书相匹配，则流量与规则相匹配。
- 通过 解密规则中的证书状态条件，可以根据用于对流量加密的服务器证书的状态（包括证书是否有效、已被吊销、已过期、尚未生效、自签署、由可信 CA 签署、证书吊销列表 (CRL) 是否有效；证书中的服务器名称指示 (SNI) 是否与请求中的服务器相匹配）处理和检查加密流量。
- 通过 解密规则中的密码套件条件，可以根据用于协商加密会话的密码套件来处理和检查加密流量。
- 通过 解密规则中的会话条件，可以根据用于加密流量的 SSL 或 TLS 版本来检查加密流量。

要检测规则、证书颁发者或证书持有者中的多个密码套件，可以创建可重用密码套件列表和可分辨名称对象并将其添加到规则中。要检测服务器证书和某些证书状态，必须为规则创建外部证书和外部 CA 对象。

相关主题

证书规则条件，第 1926 页
证书状态 解密规则 条件，第 1932 页
信任外部证书颁发机构，第 1930 页

按证书状态匹配流量
密码套件规则条件，第 1934 页
加密协议版本规则条件，第 1937 页

证书规则条件

构建基于证书的 解密规则条件时，可以上传服务器证书；将证书另存为外部证书对象，该对象可重用并会将名称与服务器证书相关联。或者，可以使用现有外部证书对象和对象组来配置证书条件。

可以根据以下证书可分辨名称特性在外部证书对象或对象组所基于的规则条件中搜索**可用证书 (Available Certificates)** 字段：

- 使用者或颁发者公用名 (CN)，或者 URL 包含在证书的使用者可选名称 (SAN) 中

  用户在浏览器中输入的 URL 与通用名称 (CN) 匹配
- 使用者或颁发者组织 (O)
- 使用者或颁发者组织单位 (OU)

您可以选择根据单个证书规则条件中的多个证书进行匹配；如果用于加密流量的证书与上传的任何证书相匹配，则加密流量与规则相匹配。

在单个证书条件中，可以向**所选证书 (Selected Certificates)** 添加最多 50 个外部证书对象和外部证书对象组。

请注意以下事项：

- 如果还选择**解密 - 已知密钥 (Decrypt - Known Key)** 操作，则无法配置证书条件。由于该操作要求选择服务器证书来解密流量，因此结果是证书已经与流量相匹配。
- 如果使用外部证书对象配置证书条件，则添加到密码套件条件中的任何密码套件或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与外部证书的签名算法类型相匹配。例如，如果规则的证书条件引用基于 EC 的服务器证书，则添加的任何密码套件或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告。
- 系统首次检测新服务器的加密会话时，证书数据不可用于 ClientHello 处理，因为这会导致首个会话不解密。在初始会话后，托管设备会缓存服务器证书消息中的数据。对于来自同一个客户端的后续连接，系统可将 ClientHello 消息与使用证书条件的规则进行决定性匹配，并处理消息以最大限度提高解密的可能性。

可分辨名称 (DN) 规则条件

本主题讨论如何在 解密规则 中使用可分辨名称条件。如果您不确定，可以使用 Web 浏览器查找证书的使用者可选名称 (SAN) 和公用名，然后可以将这些值作为可分辨名称条件添加到 解密规则。

有关 SAN 的详细信息，请参阅 RFC 528 第 4.2.1.6 节。

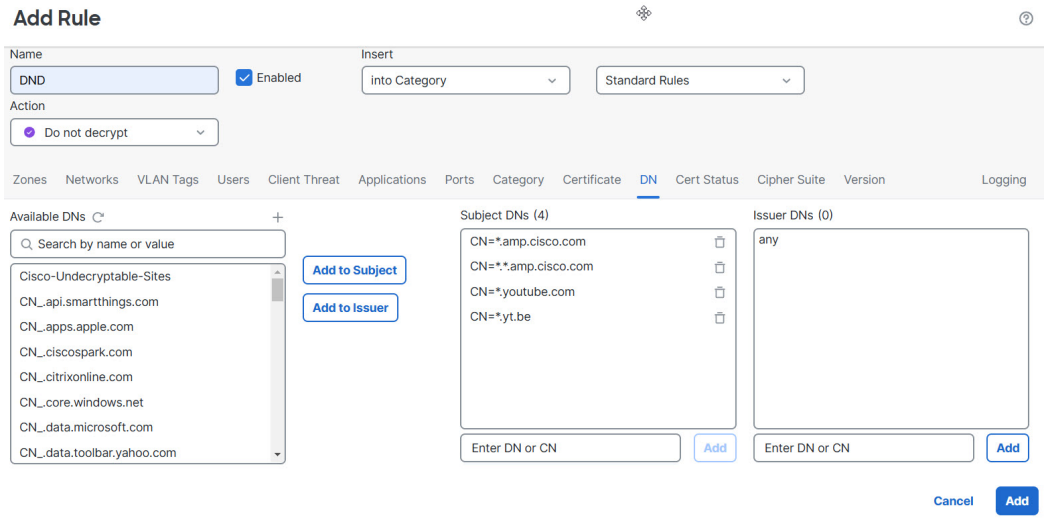
以下各部分讨论：

- DN 规则匹配示例

- 系统如何使用 SNI 和 SAN
- 如何查找证书的通用名称和使用者可选名称
- 如何添加 DN 规则条件

DN 规则匹配示例

以下是不解密规则中 DN 规则条件的示例。假设您希望确保不解密流向 `amp.cisco.com` 或 YouTube 的流量。那么您可以按如下方式来设置 DN 条件：



前面的 DN 规则条件将与以下 URL 匹配，因此先前被规则阻止的流量会被解密：

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

前面的 DN 规则条件与以下任何 URL 都不匹配，因此，流量将不匹配“不解密”(Do Not Decrypt) 规则，但可能匹配同一 解密策略 中的任何其他 解密规则。

- amp.cisco.com
- youtube.com
- yt.be

要匹配上述任何主机名，请向规则中添加更多 CN（例如，添加 `CN=yt.be` 就会匹配该 URL。）

系统如何使用 SNI 和 SAN

客户端请求中 URL 的主机名部分是服务器名称指示 (SNI)。客户端会使用 TLS 握手中的 SNI 扩展名来指定要连接的主机名（例如，`auth.amp.cisco.com`）。然后，服务器会选择在单个 IP 地址上托管所有证书时建立连接所需的相应私钥及证书链。

如果证书中的 SNI 与 CN 或 SAN 匹配，则我们会在与规则中列出的 DN 进行比较时使用 SNI。如果没有 SNI 或它与证书不匹配，则我们将在与规则中列出的 DN 进行比较时使用证书的 CN。

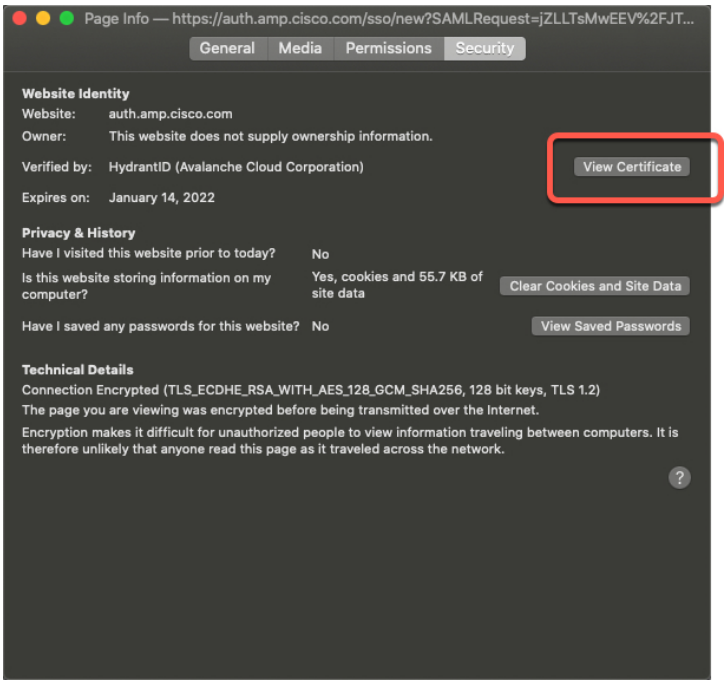
如何查找证书的通用名称和使用者可选名称

要查找任何证书的通用名称，请执行以下步骤。您甚至可以使用这些步骤来查找自签名证书的通用名称和 SAN。

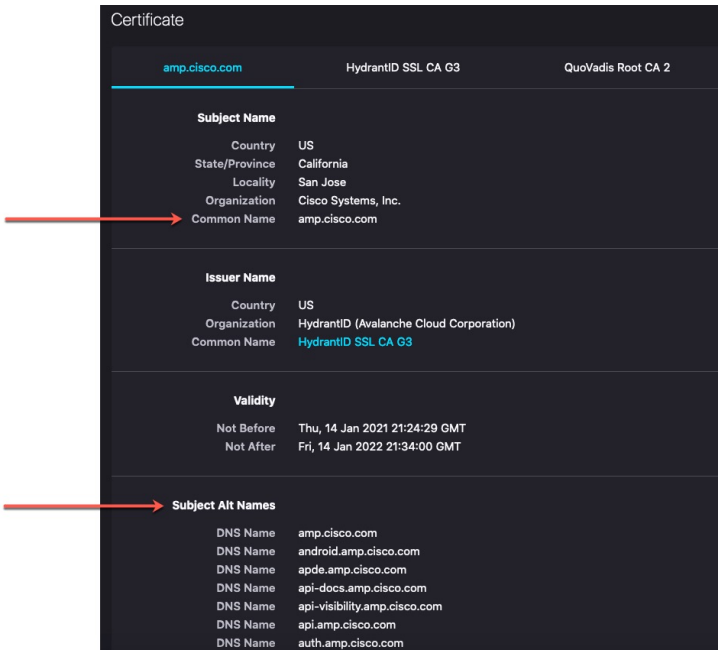
这些步骤适用于 Firefox，但其他浏览器也与之类似。以下程序以 `amp.cisco.com` 为例。

1. 在 Firefox 中浏览到 `amp.cisco.com`。
2. 在浏览器的地址栏中，点击 URL 左侧的 。
3. 点击**连接安全 (Connection secure)** > **更多信息 (More Information)**。

   （对于非安全或自签名证书，请点击**连接不安全 (Connection not secure)** > **详细信息 (More Information)**。）
4. 在页面信息对话框中，点击**查看证书 (View Certificate)**。



5. 下一页显示了证书详细信息。



请注意以下事项：

- `CN=auth.amp.cisco.com`，如果用作 DN 规则条件，则仅与该主机名（即 SNI）匹配。SNI `amp.cisco.com` 不匹配。
- 要匹配尽可能多的域名字段，请使用通配符。

  例如，要匹配 `auth.amp.cisco.com`，请使用 `CN=*.amp.cisco.com`。要匹配 `auth.us.amp.cisco.com`，请使用 `CN=*.*.amp.cisco.com`。

  像 `CN=*.example.com` 这样的 DN 与 `www.example.com` 匹配，但与 `example.com` 不匹配。要匹配两个 SNI，请在规则条件中使用两个 DN。
- 但不要过多使用通配符。例如，DN 对象（例如 `CN=*.google.com`）与大量的 SAN 匹配。使用 DN 对象（例如 `CN=*.youtube.com`）而不是 `CN=*.google.com`，使其与 `www.youtube.com` 等名称匹配。

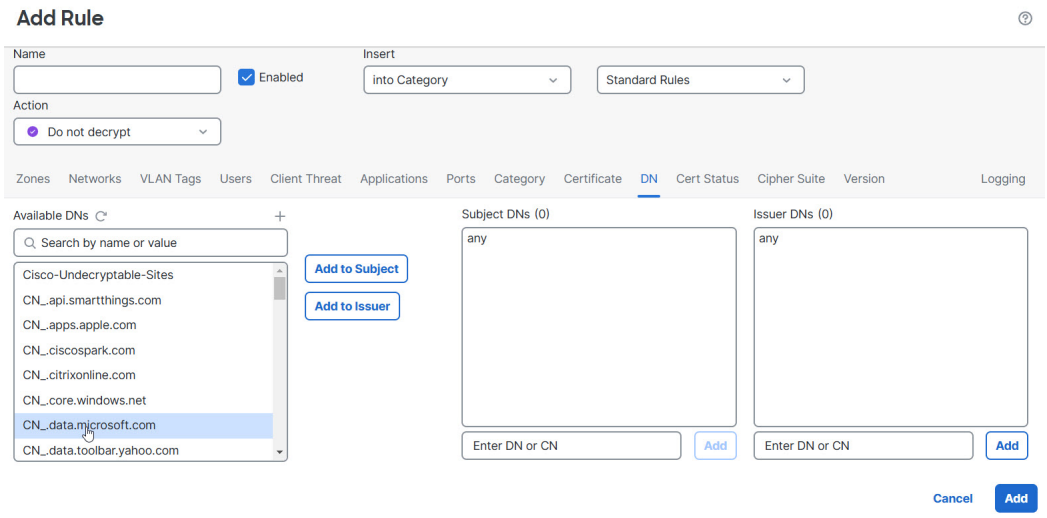
  您还可以使用与 SAN 匹配的 SNI 变体，例如 `CN=*.youtube.com`、`CN=youtu.be`、`CN=*.yt.be` 等。
- 自签名证书应以相同的方式工作。您可以通过颁发者 DN 与使用者 DN 是否相同来确认它是否为自签名证书。

如何添加 DN 规则条件

在知道要匹配的 CN 后，请通过以下方式之一编辑 解密规则：

- 使用现有 DN。

  点击 DN 的名称，然后点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。（**添加到使用者 (Add to Subject)** 更为常用。）要查看 DN 对象的值，请将鼠标指针悬停在它上面。）

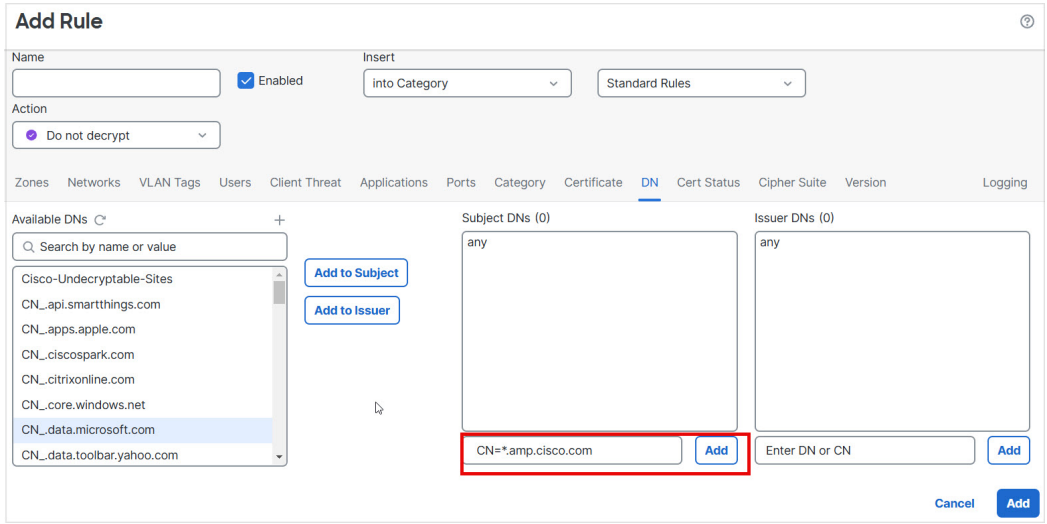


- 创建新的 DN 对象。

  点击可用 DN 右侧的 **添加** (+)。DN 对象必须包含名称和值。

- 直接添加 DN。

  在**使用者 DN (Subject DNs)** 字段或**颁发者 DN (Issuer DNs)** 字段底部的字段中输入 DN。（**使用者 DN (Subject DNs)** 更为常用。）输入 DN 后，点击**添加 (Add)**。



相关主题

可分辨名称，第 2637 页

信任外部证书颁发机构

您可以通过向 解密策略中添加根 CA 证书和中间 CA 证书来信任 CA，然后使用这些受信任 CA 验证用于加密流量的服务器证书。

如果受信任 CA 证书包含上传的证书撤销列表 (CRL)，则还可以验证受信任 CA 是否已撤销加密证书。

提示 将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。此外，如果将证书状态条件配置为根据根颁发者 CA 来信任流量，则可以允许而不解密受信任 CA 的信任链中的所有流量，而不是不必要地将其解密。

有关详细信息，请参阅受信任的 CA 对象 ，第 2666 页。

注释 创建 a 解密策略时，策略的 **受信任 CA 证书** 选项卡页面将填充多个受信任 CA 证书，包括添加到 **选择受信任 CA** 列表中的 **Cisco-Trusted-Authorities** 组。

过程

步骤 1 如果尚未登录，请登录防火墙管理中心。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 解密策略 旁边的 **编辑** (✎) 进行编辑。

步骤 4 点击**添加规则**以添加新的 解密规则，或者点击 **编辑** (✎) 以编辑现有的规则。

步骤 5 点击**证书 (Certificates)** 选项卡。

步骤 6 从**可用证书 (Available Certificates)** 中查找要添加的受信任 CA，如下所示：

- 要即时添加可随后添加到条件中的受信任 CA 对象，请点击**可用证书 (Available Certificates)** 列表上方的 **添加** (+)。
- 要搜索将添加的受信任 CA 对象和组，请点击 **可用证书** 列表上方的 **按名称或值搜索** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 7 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后是 **全选**。

步骤 8 点击 **Add to Rule**（添加至规则）。

提示
您也可以拖放选定对象。

步骤 9 添加或继续编辑规则。

下一步做什么

- 将证书状态 解密规则条件添加到 SSL 规则。有关详细信息，请参阅按证书状态匹配流量。

- 部署配置更改；请参阅 部署配置更改，第 180 页。

证书状态 解密规则 条件

对于配置的每个证书状态 解密规则，您可以根据给定状态存在还是缺失来匹配流量。可以在一个规则条件中选择若干状态，如果证书与任何所选状态相匹配，则规则与流量相匹配。

可以选择根据单个证书状态规则条件中多个证书状态的存在或缺失进行匹配；证书只需匹配其中一个条件即可与规则相匹配。

设置此参数时，应考虑是配置解密规则还是阻止规则。通常情况下，应对阻止规则点击**是**，对解密规则点击**否**。示例：

- 如果要配置**解密 - 重新签名**规则，则默认行为是使用过期的证书解密流量。要更改此行为，请对**过期**点击**否**，以确保不会解密并重签具有过期证书的流量。
- 如果要配置**阻止**规则，则默认行为是允许具有过期证书的流量。要更改此行为，请对**过期**点击**是**，以阻止具有过期证书的流量。

下表介绍系统如何根据加密服务器证书的状态评估加密流量。

表 *111:* 证书状态规则条件标准

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
已撤销	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书包含用于撤销服务器证书的 CRL。	策略信任颁发服务器证书的 CA，并且上 略的 CA 证书不包含用于撤销证书的 CI
自签名	检测到的服务器证书包含相同的使用者和颁发者可分辨名称。	检测到的服务器证书包含不同的使用者 可分辨名称。
有效	以下所有情况都成立： • 策略信任颁发证书的 CA。 • 签名则是有效的。 • 颁发者有效。 • 策略的受信任 CA 未撤销证书 • 当前日期介于证书的有效期开始日期和有效期结束日期之间。	至少以下情况之一成立： • 策略不信任颁发证书的 CA。 • 签名无效。 • 颁发者无效。 • 策略中的受信任 CA 已撤销证书。 • 当前日期在证书的有效期开始日期 • 当前日期在证书的有效期结束日期
无效签名	无法根据证书的内容正确验证证书的签名。	根据证书的内容正确验证证书的签名。
无效颁发者	颁发者 CA 证书未存储在策略的受信任 CA 证书列表中。	颁发者 CA 证书存储在策略的受信任 CA 表中。
到期	当前日期在证书的有效期结束日期之后。	当前日期在证书的有效期结束日期之前

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
尚未生效	当前日期在证书的有效期开始日期之前。	当前日期在证书的 Valid From 日期之
无效的证书	证书无效。至少以下情况之一成立： • 证书扩展名无效或不一致；即，证书扩展名具有无效值（例如，编码不正确）或某些值与其他扩展名不一致。 • 证书无法用于指定用途。 • 已超出基本约束路径长度参数。 有关详细信息，请参阅 RFC 5280 第 4.2.1.9 节。 • 证书的“有效起始日期”或“有效终止日期”值无效。这些日期可以编码为 UTC 时间或通用时间 有关详细信息，请参阅 RFC 5280 第 4.1.2.5 节。 • 无法识别名称限制的格式；例如 RFC 5280 第 4.2.1.10 节中未提及表单的邮件地址格式。这可能是由于扩展名不正确或当前不支持的某些新功能导致的。 遇到了不受支持的名称限制类型。OpenSSL 目前仅支持目录名称、DNS 名称、邮件和 URI 类型。 • 根证书颁发机构不受信任，不可用于指定用途。 • 根证书颁发机构拒绝指定的用途。	证书有效。以下所有情况都成立： • 验证证书扩展名。 • 证书可用于指定用途。 • 基本约束路径长度有效。 • “有效起始日期”和“有效终止 有效。 • 名称限制有效。 • 根证书受信任，可用于指定用途 • 根证书接受指定的用途。

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
无效 CRL	证书撤销列表 (CRL) 的数字签名无效。至少以下情况之一成立： • CRL 的“下次更新”或“上次更新”字段的值无效。 • CRL 尚未生效。 • CRL 已过期。 • 尝试验证 CRL 路径时出错。仅在启用扩展 CRL 检查时才会发生此错误。 • 找不到 CRL。 • 唯一可以找到的CRL与证书的范围不匹配。	CRL 有效。以下所有情况都成立： • “下次更新”和“上次更新”字段 • CRL 日期有效。 • 路径有效。 • 已找到 CRL。 • CRL 与证书的范围相匹配。
服务器不匹配	服务器名称与服务器的服务器名称指示 (SNI) 名称不匹配，这可能表示尝试欺骗服务器名称。	服务器名称与客户端请求访问的服务器名称匹配。

请注意，即使证书可能匹配多个状态，但是该规则导致仅对流量执行一次操作。

检查颁发或撤销证书的 CA 是否要求将根 CA 证书和中间 CA 证书以及关联的 CRL 作为对象进行上传。然后，将这些受信任 CA 对象添加到 解密策略 的受信任 CA 证书列表。

密码套件规则条件

系统提供了预定义的密码套件，您可以将“阻断”或“具有重置规则动作的阻断”添加到密码套件规则条件中。您还可以添加包含多个密码套件的密码套件列表对象。

重要事项 密码套件规则条件只可以阻止流量，而不能用于解密流量。

注释 不能添加新的密码套件。不能修改和删除预定义密码套件。

在单个密码套件条件中，可以向**所选密码套件 (Selected Cipher Suites)** 添加最多 50 个密码套件和密码套件列表。系统支持向密码套件条件添加以下密码套件：

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

请注意以下提示：

- 如果添加部署不支持的密码套件，则无法部署配置。例如，被动部署不支持使用任何短 Diffie-Hellman (DHE) 或短椭圆曲线 Diffie-Hellman (ECDHE) 密码套件来解密流量。使用这些密码套件创建规则将会阻止部署访问控制策略。
- 您可以将匿名密码套件添加到 解密策略 中的 **密码套件** 条件以使用该规则，还必须按阻止 ClientHello 处理的顺序配置 。有关详细信息，请参阅解密策略 规则顺序。
- 指定密码套件作为规则条件时，应该考虑使用 ServerHello 消息中协商的密码套件进行匹配的规则，而不是使用 ClientHello 消息中指定的整个密码套件列表进行匹配的规则。在 ClientHello 处理期间，托管设备从 ClientHello 消息中删除不受支持的密码套件。但如果这会导致所有指定的密码套件被删除，系统会保留原始列表。如果系统保留不受支持的密码套件，后续评估会导致会话不解密。

加密协议版本规则条件

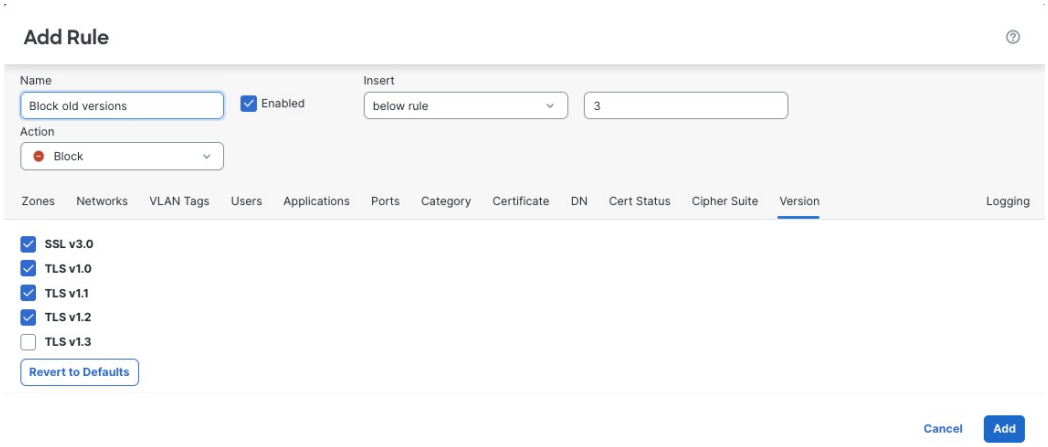
可以选择根据使用 SSL V3.0 或 TLS V1.0、V1.1 或 V1.2 加密的流量进行匹配。默认情况下，在创建规则时会选择所有协议版本；如果选择多个版本，则与任何所选版本相匹配的加密流量都与该规则相匹配。保存规则条件时，必须至少选择一个协议版本。

您可以在“不解密”、“阻止”或“阻止并重置”规则操作中使用 SSL 3.0。

您 无法 在版本规则条件中选择 SSL V2.0；系统不支持解密使用 SSL V2.0 加密的流量。可以配置无法解密的操作来允许或阻止此流量而不进一步检查。有关详细信息，请参阅设置无法解密的流量的默认处理，第 1901 页。

重要事项 协议版本规则条件只可以阻止流量，而不能用于解密流量。

例如，要阻止所有 SSL v3.0、TLS v1.0、TLS v1.1 和 TLS v1.2 流量，请按如下所示设置选项：



解密规则基于规则的解密规则 操作

以下各部分讨论 基于规则的解密规则 可用的操作。

基于规则的解密 规则监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。如果流量与**监控**规则条件匹配，则不会修改 ClientHello 消息。

系统随后会根据其他规则（如果有）来匹配流量，以确定信任、阻止还是解密该流量。所匹配的第一个非“监控”(Monitor) 规则确定流量和任何进一步的检测。如果没有其他匹配的规则，系统使用默认操作。

由于“监控”规则的主要目的是跟踪网络流量，因此系统会自动将受监控流量的连接结束事件记录到 Secure Firewall Management Center数据库，而无论稍后处理该连接的规则或默认操作的日志记录配置如何。

基于规则的解密 规则 不解密操作

不解密操作会让加密流量通过，以通过访问控制策略的规则和默认操作进行评估。由于某些访问控制规则条件需要未加密的流量，因此该流量可能与较少的规则相匹配。系统无法对加密流量执行深入检查，例如入侵或文件检查。

不解密规则操作的常见原因包括：

- 法律禁止解密 TLS/SSL 流量。
- 确定可以信任的站点。
- 通过检查流量（如 Windows Update）可以中断的站点。
- 使用连接事件查看 TLS/SSL 字段的值。（您无需解密流量即可查看连接事件字段。）有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的填充连接事件字段的要求。

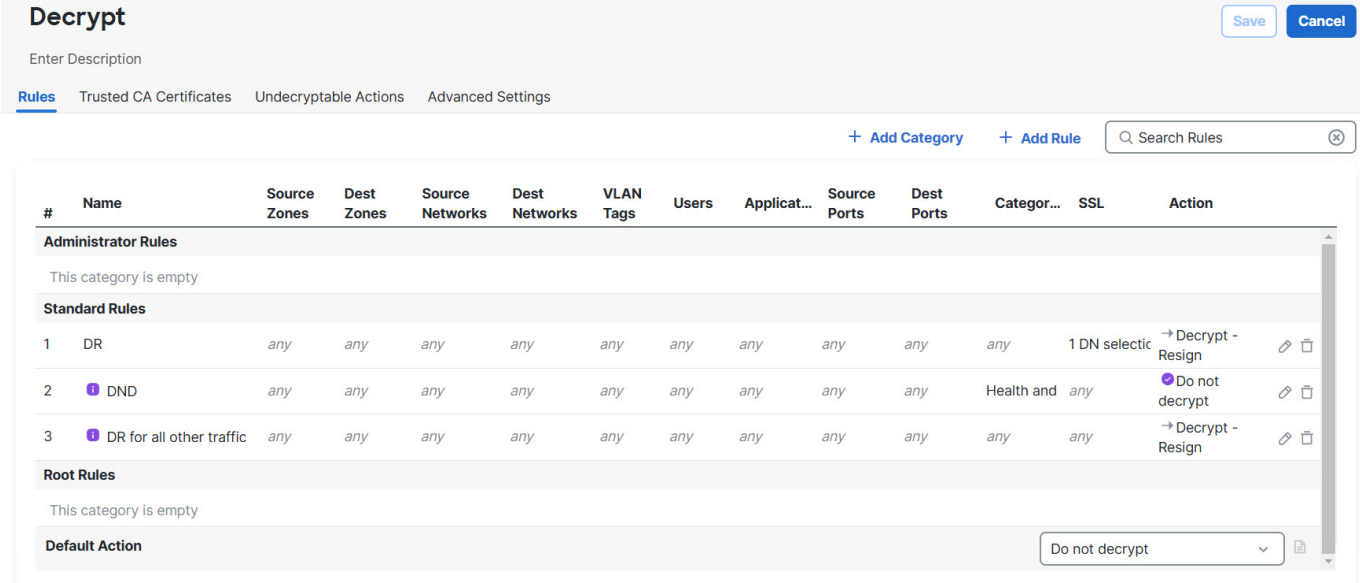
有关详细信息，请参阅无法解密流量的默认处理选项， 第 1900 页

“不解密”规则中的类别限制

您可以选择在 解密策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 智能组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用TLS/SSL解密的准则， 第 1908 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅应用控制的建议，第 1755 页。

基于规则的解密 规则阻止操作

系统为您不希望通过系统的流量提供以下 解密规则 操作：

- **阻止 (Block)**，此操作可终止连接，从而导致客户端浏览器出错。

  错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

- **阻止并重置 (Block with reset)**，此操作可终止并重置连接，从而导致客户端浏览器出错。

  该错误会指明连接已重置，但未指明具体原因。

提示 在被动或内联（触点模式）部署中不能使用 **阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作，因为设备不会直接检查流量。如果创建具有**阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作的规则，该规则在安全区域条件内包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告 (⚠)。

基于规则的解密 规则解密操作

解密 - 替换证书、**解密 - 已知密钥**和**解密 - 重新签名**操作会解密加密流量。系统通过访问控制来检查解密流量。访问控制规则以相同方式处理已解密和未加密的流量，您可以检查该流量来获得发现

数据，并检测和阻止入侵、禁止的文件及恶意软件。系统在将允许的流量传递到其目标之前会将其重新加密。

建议使用来自受信任证书颁发机构 (CA) 的证书来解密流量。这可以防止**Invalid Issuer**显示在连接事件的“SSL 证书状态”列中。

有关添加受信任对象的详细信息，请参阅受信任证书颁发机构对象，第 2666 页。

相关主题：TLS 1.3 解密最佳实践，第 1904 页。

相关主题

TLS 1.3 解密最佳实践，第 1904 页

传入流量解密操作

通过**解密 - 替换证书**和**解密 - 已知密钥**解密操作，您可以解密流向要保护其免受恶意攻击的服务器的传入流量。

出于以下原因，我们提供**解密 - 替换证书**解密操作作为**解密 - 已知密钥**的替代操作：

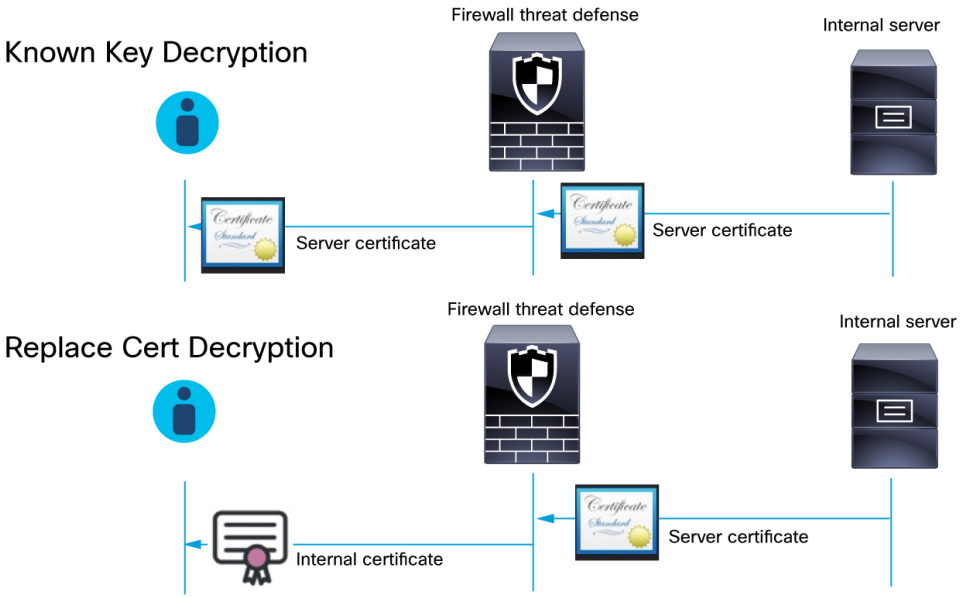
- 证书可能随时过期或需要更换。

  如果选择**解密 - 已知密钥 (Decrypt - Known Key)** 操作，则当证书因任何原因被替换时，解密可能会停止，并且规则可能会停止运行。

- 使用**解密 - 替换证书**，连接匹配和流量被解密，即使在设备上延迟数小时或数天部署证书也无妨。

- 通过**解密 - 替换证书**，您可以灵活地拥有单独的内部和外部证书。例如，您可以使用 `payroll.example.local` 作为内部服务器主机名，而使用 `payroll.example.com` 作为面向外部的主机名。您也可以为内部服务器使用企业 PKI 证书，但外部证书请使用 DigiCert 或其他公共证书颁发机构。

下图显示**解密 - 替换证书**和**解密 - 已知密钥** 解密操作之间的差异。



下表提供了更多信息。

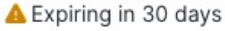
	已知密钥	替换证书
必须与内部服务器或资源上安装的证书匹配	支持	否
设备必须信任内部证书（即该证书必须在解密策略中与受信任 CA 列表建立证书链）	否	否
设备安装的证书与内部服务器上的证书，其证书主机名可以不同	不，证书必须完全相同。（尽管证书上可以有多个 SAN 来支持不同的内部和外部主机名。）	是的，证书和证书主机名可以完全不同，只要内部证书被用户设备信任即可。
如果内部服务器证书已过期，则有效	是的 - 只要它与设备上安装的证书匹配即可。	不 - 过期的证书会导致信任中断，从而引发不匹配。

替换内部证书（仅限解密 - 替换证书）

此任务讨论如何使用 Secure Firewall Management Center (**对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**) 替换传入解密规则中的内部证书。

您还可以使用 API 来替换证书，如*Cisco Secure Firewall Threat Defense REST API* 指南中所述。

当今天的日期在内部证书的到期日期的30天内时，系统指示内部证书将要到期。下图显示了一个示例。



开始之前

您必须通过以下任何一种方式选择**解密 - 替换证书**解密规则操作：

- 在 基于规则的解密 策略中，通过点击规则的**操作**列表中的操作来实现。
- 创建始终使用**解密 - 替换证书**规则操作的 标准解密 策略。

过程

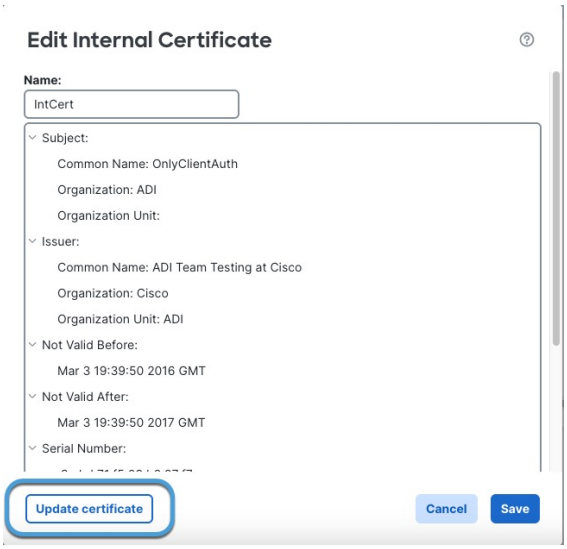
步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**。

步骤 3 找到已过期或即将到期的内部证书（例如，已过期的证书显示为 Expired ）。

步骤 4 请点击 **编辑** ()。

步骤 5 点击**更新证书**，如下图所示。



步骤 6 输入请求的信息；有关详细信息，请参阅为入站保护上传内部证书，第 1897 页。

步骤 7 按照屏幕提示完成操作。

解密 - 重新签名规则操作

您可以使用**解密 - 重新签名**规则操作解密传出流量，以便可以对流量进行深度检查。

选择内部证书对象

开始之前

要使用**解密-已知密钥**操作创建解密规则，必须使服务器添加内部证书以解密流量。有关详细信息，请参阅 内部证书对象，第 2668 页。

有关重要准则，请参阅TLS/SSL 传入流量解密准则，第 1911 页。

过程

步骤 1 点击解密规则**操作 (Action)** 旁边字段中的 **编辑** ()。

步骤 2 在“选择内部证书对象”(Select Internal Certificate Objects) 对话框中，执行以下操作：
可用证书 (Available Certificates) 列表：点击证书的名称，然后点击**添加到规则 (Add to Rule)** 以在此规则中使用此证书。您可以将一个或多个证书添加到规则。

所选证书 (Selected Certificates) 列表：显示规则中使用的内部证书。要删除证书，请点击 **删除**（）。

步骤 3 要保存这些更改，请点击**确定**。

监控 TLS/SSL 硬件加速

以下主题讨论如何监控 TLS/SSL 硬件加速状态

信息计数器

如果负载的系统运行良好，您应会看到以下计数器的计数较大。由于跟踪器进程的每个连接有 2 端，所以您会看到每个连接的这些计数器呈 2 倍增长。PRIV_KEY_RECV 和 SECU_PARAM_RECV 计数器最为重要，并会突出显示。CONTEXT_CREATED 和 CONTEXT_DESTROYED 计数器与加密芯片内存的分配相关。

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
```

```
TLS_TRK      DECRYPTED_APPLICATION          33568976   Summary
TLS_TRK      ALERT_RX_CNT                     258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            258222   Summary
TCP_PRX      OPEN_SESSION                     516450   Summary
TCP_PRX      FREE_SESSION                     516450   Summary
TCP_PRX      UPSTREAM_CLOSE                   516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                 516450   Summary
TCP_PRX      FREE_CONN                        258222   Summary
TCP_PRX      SERVER_CLEAN_UP                  258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                  258222   Summary
```

警报计数器

我们按照 TLS 1.2 规范实施了以下计数器。FATAL 或 BAD 警报可能表明存在问题；但是，ALERT_RX_CLOSE_NOTIFY 表明正常。

有关详细信息，请参阅 RFC 5246 第 7.2 节。

```
TLS_TRK      ALERT_RX_CNT                       311   Summary
TLS_TRK      ALERT_TX_CNT                         2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT            2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT             308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                 3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                 2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY              308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC              2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE             1   Summary
```

错误计数器

这些计数器指示系统错误。这些计数在运行状况正常的系统上应较低。BY_PASS 计数器指示不经解密便直接传递到检测引擎 (Snort) 进程（在软件中运行）或从其传递的数据包。以下示例中列出了一些错误计数器。

值为 0 的计数器不会显示。要查看计数器的完整列表，请使用命令 **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR           123   Summary
TLS_TRK      DECRYPT_FAIL                     43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                   127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                 127   Summary
```

严重错误计数器

重大错误计数器表示严重的错误。这些计数器在正常运行的系统中应达到或接近于 0。以下示例列出了重大错误计数器。

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

RING_FULL 计数器不是重大错误计数器，但表明系统中加密芯片过载的频率。ACCELERATOR_RESET 计数器指示 TLS 加密加速进程意外失败的次数，该进程意外失败也导致挂起的操作失败，即您在 ACCELERATOR_CORE_TIMEOUT 和 RSA_PRIVATE_DECRYPT_FAILED 中看到的数字。

如果问题仍未解决，请禁用 TLS 加密加速（ 或 **config hwCrypto disable**）并配合思科 TAC 来解决问题。

注释 您可以使用 **show snort tls-offload** 和 **debug snort tls-offload** 命令进行其他的故障排除。使用 **clear snort tls-offload** 命令可将 **show snort tls-offload** 命令中显示的计数器重置为零。

对基于规则的解密规则进行故障排除

以下主题讨论如何对 基于规则的解密规则 进行故障排除。

关于 TLS/SSL 超订用

TLS/SSL 超订用是托管设备过载 TLS/SSL 流量的状态。任何托管设备都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速的托管设备才提供可配置的方式对其进行处理。

启用了 TLS 加密加速 的托管设备在超订用时，托管设备接收的任何数据包都根据 解密策略 的**无法解密的操作**中**握手错误**设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 解密策略的 **无法解密的操作** 中 **握手错误** 的设置为 **不解密** ，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密 不会 发生。

对 TLS/SSL 超订用进行故障排除

如果您的托管设备已启用 TLS 加密加速，您可以查看连接事件，以确定设备是否遇到了 SSL 超订用。您必须至少将 **SSL 流标志**事件添加到连接事件的表视图。

开始之前

- 配置一个 a 解密策略，其中包含一项针对**无法解密的操作 (Undecryptable Actions)** 页面上的**握手错误 (Handshake Errors)** 的设置。

  有关详细信息，请参阅设置无法解密的流量的默认处理，第 1901 页。

- 为 SSL 规则启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 解密规则 中记录可解密连接的部分所述。

过程

步骤 1 如果尚未登录，请登录 防火墙管理中心。

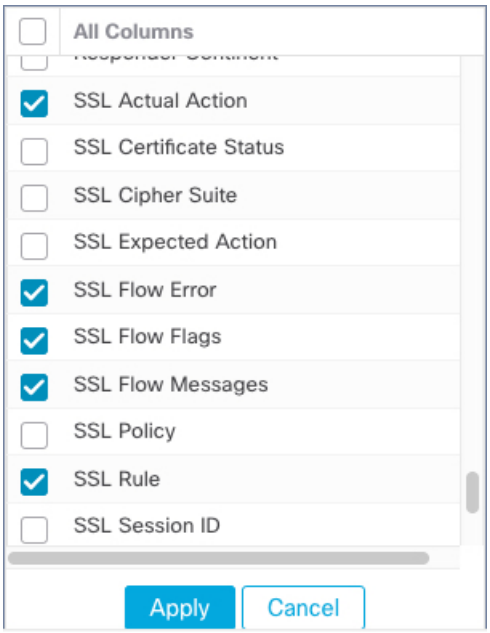
步骤 2 请点击 **事件和日志** > **+ 显示更多** > **连接** > **事件**。

步骤 3 点击**连接事件的表视图 (Table View of Connection Events)**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。



以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。（查看对话框的“禁用列”部分。）



列按 *Cisco Secure Firewall Management Center* 管理指南 中的 连接和安全智能事件字段 中讨论的顺序添加。

步骤 5 点击**应用 (Apply)**。

TLS/SSL 超订用通过 **SSL 流标志**列中的 `ERROR_EVENT_TRIGGERED` 和 `OVER_SUBSCRIBED` 的值指示。

步骤 6 如果出现 TLS/SSL 超订用，请登录到托管设备并输入以下命令之一：

命令	结果
show counters	如果 **TCP_PRX BYPASS_NOT_ENOUGH_MEM** 的值较大，请考虑将设备升级到容量更大的可以容纳 SSL 流量的设备，或使用**不解密**规则以获得优先级较低的加密流量。
show snort tls-offload	如果 **BYPASS_NOT_ENOUGH_MEM** 的值较大，请考虑将设备升级到容量更大的可以容纳 SSL 流量的设备，或使用**不解密**规则以获得优先级较低的加密流量。

关于 TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速的托管设备遇到使用 SSL 检测信号扩展的数据包时，托管设备将执行 解密策略 的**无法解密的操作**中**解密错误**的设置所指定的操作：

- 阻止
- 阻止并重置

相关主题

对 TLS 心跳进行故障排除 ， 第 1948 页

对 TLS 心跳进行故障排除

如果您的托管设备已启用 TLS 加密加速，则您可以查看连接事件，以确定设备是否看到了具有 SSL 心跳扩展的流量。您必须至少将 **SSL 流消息**事件添加到连接事件的表视图。

开始之前

SSL 心跳由连接事件的表视图中 **SSL 流消息**列内的心跳值来指示。要确定您的网络中的应用是否会使用 SSL 心跳，请先执行以下任务：

- 配置一个 解密策略，其中包含一项针对**无法解密的操作 (Undecryptable Actions)** 选项卡页面上的**解密错误 (Decryption Errors)** 的设置。

  有关详细信息，请参阅设置无法解密的流量的默认处理 ， 第 1901 页。

- 为 SSL 规则启用日志记录，如Cisco Secure Firewall Management Center 和威胁防御管理网络管理中所述。

过程

步骤 1 如果尚未登录，请登录 防火墙管理中心。

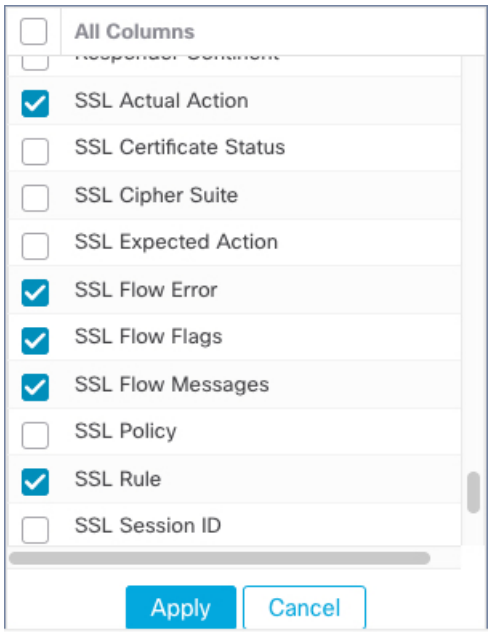
步骤 2 请点击 **事件和日志** > **+ 显示更多** > **连接** > **事件**。

步骤 3 点击**连接事件的表视图 (Table View of Connection Events)**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。



以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



列按 *Cisco Secure Firewall Management Center* 管理指南 中的 连接和安全智能事件字段 中讨论的顺序添加。

步骤 5 点击**应用 (Apply)**。

TLS 心跳由 **SSL 流消息**列中的心跳值来指示。

步骤 6 如果您网络中的应用使用SSL心跳检测信号，请参阅基于规则的解密规则准则和限制，第 1908 页。

关于 TLS/SSL 锁定

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 解密规则，则应用从托管设备收到重签的证书时，验证会失败且连接会中止。

要确认是否出现TLS/SSL锁定，请尝试登录到Facebook等移动应用。如果显示网络连接错误，则使用网络浏览器进行登录。（例如，您无法登录到 Facebook 移动应用，但可以使用 Safari 或 Chrome 登录到 Facebook。）您可以使用 Firepower 管理中心连接事件来进一步证明 TLS/SSL 锁定

注释 TLS/SSL 锁定不限于移动应用。

如果您网络中的应用使用 SSL 锁定，请参阅TLS/SSL证书固定准则，第 1914 页。

相关主题

对 TLS/SSL 锁定进行故障排除，第 1950 页

对 TLS/SSL 锁定进行故障排除

通过查看连接事件，可以确定设备是否遇到 TLS/SSL 锁定。您必须至少向连接事件的表视图中添加 **SSL 流标志**和 **SSL 流消息**列。

开始之前

- 为 解密规则 启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 解密规则中记录可解密连接的部分所述。
- 登录 Facebook 等移动应用；如果显示网络连接错误，请使用 Chrome 或 Safari 登录 Facebook。如果您可以使用网络浏览器登录，但无法使用原生应用登录，则可能发生了 TLS/SSL 锁定。

过程

步骤 1 如果尚未登录，请登录 防火墙管理中心。

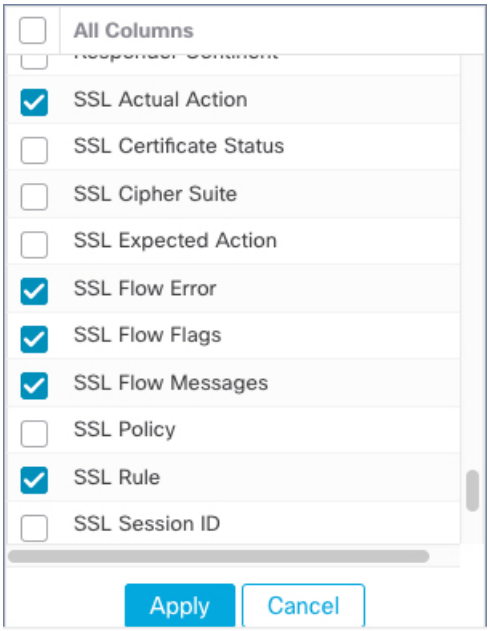
步骤 2 请点击 **事件和日志** > **+ 显示更多** > **连接** > **事件**。

步骤 3 点击**连接事件的表视图 (Table View of Connection Events)**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。



以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



这些列将按 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中的连接和安全智能事件字段中讨论的顺序进行添加。

步骤 5 点击**应用 (Apply)**。

步骤 6 以下内容介绍如何识别 SSL 锁定行为。

步骤 7 如果您确定网络中的应用使用 SSL 锁定，请参阅基于规则的解密规则准则和限制，第 1908 页。

下一步做什么

您可以使用 TLS/SSL 连接事件，通过查找以下任何项目来确认发生 TLS/SSL 锁定：

- 在客户端收到来自服务器的 SERVER_HELLO，SERVER_CERTIFICATE、SERVER_HELLO_DONE 消息后立即发送 SSL ALERT 消息并后跟 TCP 重置的应用会出现以下症状。（使用数据包捕获可查看警报：`Unknown CA (48)`。）
  - “SSL 流标志”列显示 `ALERT_SEEN`，但不显示 `APP_DATA_C2S` 或 `APP_DATA_S2C`。
  - 如果托管设备已启用 SSL 硬件加速，则“SSL 流消息”列通常显示：`CLIENT_ALERT`、`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`。
  - 如果托管的设备不支持SSL硬件加速或该功能被禁用，则“SSL流消息”(SSL Flow Messages)列通常会显示：`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`。
  - “SSL 流错误”列将显示 `Success`。
- 在执行 SSL 握手后不是发送警报而是“TCP 重置”的应用会出现以下症状：
  - “SSL 流标志”列不显示 `ALERT_SEEN`、`APP_DATA_C2S` 或 `APP_DATA_S2C`。
  - 如果托管设备已启用 SSL 硬件加速，则“SSL 流消息”列通常显示：`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`、`CLIENT_KEY_EXCHANGE`、`CLIENT_CHANGE_CIPHER_SPEC`、`CLIENT_FINISHED`、`SERVER_CHANGE_CIPHER_SPEC`、`SERVER_FINISHED`。
  - 如果托管的设备不支持SSL硬件加速或该功能被禁用，则“SSL流消息”(SSL Flow Messages)列通常会显示：`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`、`CLIENT_KEY_EXCHANGE`、`CLIENT_CHANGE_CIPHER_SPEC`、`CLIENT_FINISHED,SERVER_CHANGE_CIPHER_SPEC`、`SERVER_FINISHED`。
  - “SSL 流错误”列将显示 `Success`。

相关主题

对未知或错误的证书或证书颁发机构进行故障排除，第 1952 页

对未知或错误的证书或证书颁发机构进行故障排除

您可以查看连接事件，以确定设备是否遇到未知证书颁发机构、错误证书或未知证书。如果已固定 TLS/SSL 证书，则也可以使用此程序。您必须至少向连接事件的表视图中添加 **SSL 流标志**和 **SSL 流消息**列。

开始之前

- 设置一个 解密规则。
- 为 解密规则 启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 解密规则中记录可解密连接的部分所述。

过程

步骤 1 如果尚未登录，请登录 防火墙管理中心。

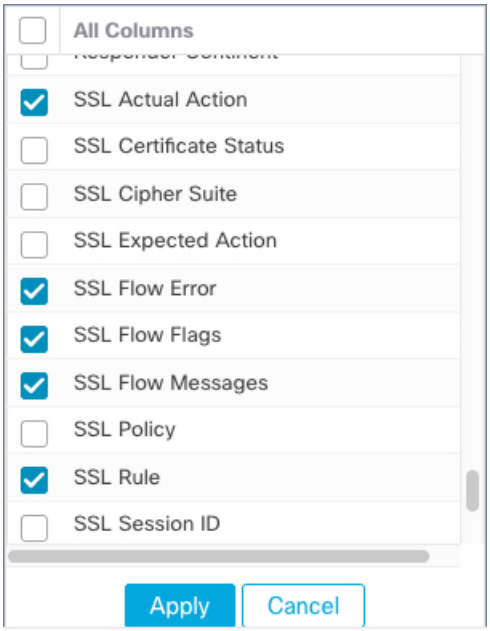
步骤 2 请点击 **事件和日志** > **+ 显示更多** > **连接** > **事件**。

步骤 3 点击**连接事件的表视图 (Table View of Connection Events)**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。



以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



这些列将按 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中的连接和安全智能事件字段中讨论的顺序进行添加。

步骤 5 点击**应用 (Apply)**。

步骤 6 下表讨论如何确定证书或证书颁发机构是否出错或缺失。

SSL 流量标志	含义
CLIENT_ALERT_SEEN_UNKNOWN_CA	表示 SSL 客户端应用收到了有效的证书链或部分证书链，但由于无法找到CA 证书或者无法与已知的受信任CA 匹配，因此该证书未被接受。此消息始终表示不可恢复的错误。
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	证书已损坏、包含未正确验证的签名或存在其他问题。
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	处理证书时出现了一些其他（未指定的）问题，使得其无法被接受。

验证 TLS/SSL 密码套件

开始之前

本主题讨论在保存具有密码套件条件的 解密规则时看到以下错误时必须执行的操作：

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that matches the resigning CA's signature algorithm
```

此错误表示您为解密规则条件选择的一个或多个密码套件与此解密规则中使用的证书不兼容。要解决此问题，必须有权访问正在使用的证书。

注释 本主题中的任务假定了解 TLS/SSL 加密的工作原理。

过程

步骤 1 当您尝试保存包含**解密 - 重新签名**、**解密 - 替换证书**或**解密 - 已知密钥**（且指定了密码套件）的 解密规则 规则时，会显示以下错误：

示例：

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

步骤 2 找到将用于解密流量的证书，并在必要时将证书复制到可以运行 openssl 命令的系统。

步骤 3 运行以下命令，以显示证书使用的签名算法：

openssl x509 -in *CertificateName* **-text -noout**

输出的前几行显示内容类似于以下各项：

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

步骤 4 **Signature algorithm** 显示以下内容：

- 所使用的加密函数（在上述示例中，**ECDSA** 表示椭圆曲线数字签名算法）。
- 用于创建加密消息摘要的散列函数（上述示例中为 **SHA256**）。

步骤 5 搜索与这些值匹配的密码套件资源（如犹他大学的 *OpenSSL*）。密码套件必须采用 RFC 格式。您还可以搜索各种其他站点，例如 Mozilla Wiki 上的服务器端 TLS 或 RFC 5246 的附录 C。Microsoft 文档格式的 TLS/SSL (Schannel SSP) 中的密码套件对密码套件进行了详细说明。

步骤 6 如有必要，请将 OpenSSL 名称转换为 Firepower 管理系统使用的 RFC 名称。请参阅 `https://testssl.sh` 站点上的 RFC 映射列表。

步骤 7 上述示例 **ecdsa-with-SHA256** 可以在 Mozilla Wiki 上的现代兼容性列表中找到。

a) 仅选择名称中包含 **ECDSA** 和 **SHA-256** 的密码套件。这些密码套件遵循以下原则：

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) 在 RFC 映射列表中找到相应的 RFC 密码套件。这些密码套件遵循以下原则：

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

步骤 8 将上述密码套件添加到 解密规则中。

使用加密归档进行故障排除

关于加密存档

加密问题难以分类。而加密存档可帮助您解决这些问题。加密存档包含有关加密请求的加密会话信息、对等体信息、发送加密请求的组件以及超时的加密会话信息。威胁防御不会保存会话的密钥和初始化向量 (IV)。对于 SSL 和 IPsec，您还可以查看以下信息：

- 对于 SSL：会话 SSL 版本、源、目的 IP 地址和端口。
- 对于 IPsec：IPsec 安全关联信息。

一个环可以容纳2000个加密命令条目。威胁防御会在其中一个环中推送crypto命令，并在完成加密请求后提取结果。加密存档文件现在包含超时加密请求的环和条目索引。环及其条目索引有助于对有问题的加密命令进行故障排除。

加密存档有两种格式：文本文件和二进制文件。您可以使用 **debug menu ctm 103** 命令来解码二进制文件。加密存档文件位于 disk0:/crypto_archive。

例如：

```
FTD# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443
```

在上例中，突出显示的信息显示了超时环、崩溃时间（超时条目）和SSL会话信息。

加密存档支持的设备

以下配备 Nitrox V 加密加速器的设备可支持加密存档：

- Cisco Firepower 3105、3110、3120、3130、3140
- Cisco Firepower 4112、4115、4125、4145
- Cisco Firepower 9300 SM-40、SM-48 和 SM-56
- Cisco Secure Firewall 4200



第 48 章

加密可视性引擎

加密可视性引擎 (EVE) 用于识别使用 TLS 加密的客户端应用和进程。它支持可视性，并允许管理员在其环境中采取行动并实施策略。EVE 技术还可用于识别和阻止恶意软件。

- 加密可视性引擎概述， 第 1957 页
- EVE 工作原理， 第 1958 页
- 危害事件表现， 第 1959 页
- EVE 中的 QUIC 指纹识别， 第 1959 页
- 配置 EVE， 第 1959 页
- 配置 EVE 例外规则， 第 1962 页
- 事件扩充， 第 1965 页
- EVE 示例， 第 1965 页

加密可视性引擎概述

加密可视性引擎 (EVE)用于提供对加密会话的更多可视性，而无需对其进行解密。对 TLS 连接的见解源自思科的开源库，该库包含在思科的漏洞数据库 (VDB) 中。库指纹并分析传入的加密会话，并将其与一组已知指纹进行匹配。已知指纹的数据库在思科 VDB 中也可用。

注释 只有运行 Snort 3 的 防火墙管理中心管理的设备才支持加密可视性引擎功能。Snort 2 设备和防火墙设备管理器受管设备不支持此功能。

EVE 的一些重要功能如下：

- 您可以使用从 EVE 派生的信息对流量执行访问控制策略操作。
- Cisco Secure Firewall 中包含的 VDB 能够以高置信度值将应用分配给 EVE 检测到的某些进程。或者，您可以创建自定义应用检测器，以便：
  - 将 EVE 检测到的进程映射到用户定义的新应用。
  - 覆盖用于将应用分配给 EVE 检测到的进程的进程置信度的内置值。

请参阅 Cisco Secure Firewall Management Center 设备配置指南的**应用检测**一章中的**配置自定义应用检测器**和**指定 EVE 进程分配**部分。

- EVE 可以检测在加密流量中创建客户端 Hello 数据包的客户端的操作系统类型和版本。
- EVE 也支持快速 UDP 互联网连接 (QUIC) 流量的指纹识别和分析。来自客户端 Hello 数据包的服务器名称显示在 **连接事件** 页面的 URL 字段中。

注意 要在 防火墙管理中心上使用 EVE，您的设备上必须具有有效的 IPS 许可证。在没有 IPS 许可证的情况下，策略会显示警告，并且不允许部署。

注释

- EVE 可以检测 SSL 会话的操作系统类型和版本。操作系统的正常使用（例如运行应用、软件包管理软件等）可以触发操作系统检测。要查看客户端操作系统检测，除了启用 EVE 切换按钮，您还必须在 **策略 (Policies)** > **网络发现 (Network Discovery)** 下启用 **主机 (Hosts)** 。要查看主机 IP 地址上可能的操作系统的列表，请点击 **事件和日志** > **主机** > **网络映射**，然后选择所需的主机。
- 为访问控制策略启用 EVE 后，确保已为该策略中的访问控制规则开启日志记录，以便在满足任何特定规则条件时，能在 EVE 控制面板上显示预期结果。有关如何开启日志记录的详细信息，请参阅创建和编辑访问控制规则。
- 从 Cisco Secure Firewall 版本 10.0.0 开始，支持用于 Mercury 检测的 GRE 封装。

EVE 工作原理

加密可视性引擎 (EVE) 检查 TLS 握手的客户端 Hello 部分，以识别客户端进程。客户端 Hello 是发送到服务器的初始数据包。这可以很好地指示主机上的客户端进程。此指纹与其他数据（例如目的 IP 地址）相结合，为 EVE 的应用识别提供基础。通过识别 TLS 会话建立中的特定应用指纹，系统可以识别客户端进程并采取适当的操作（允许/阻止）。

EVE 可以识别 5,000 多个客户端进程。系统将许多此类进程映射到客户端应用，以用作访问控制规则中的条件。这使得系统能够在不启用 TLS 解密的情况下识别和控制这些应用。通过使用已知恶意进程的指纹，EVE 技术还可用于识别和阻止加密的恶意流量，而无需出站解密。

通过机器学习 (ML) 技术，思科每天要处理超过 10 亿个 TLS 指纹和超过 10000 个恶意软件样本，以创建和更新 EVE 指纹。然后，使用思科漏洞数据库 (VDB) 软件包将这些更新交付给客户。

如果 EVE 无法识别某个指纹，它会识别客户端应用，并使用目标详细信息（例如 IP 地址、端口和服务器名称）估算第一个数据流的威胁评分。此时，指纹的状态已随机化，可以在调试日志中查看状态。对于具有相同指纹的后续流，EVE 会跳过重新分析并将指纹状态标记为未标记。

危害事件表现

用于加密可视性引擎检测的主机危害表现 (IoC) 事件允许您检查恶意软件置信度非常高的连接事件，如 EVE 所报告的那样。使用恶意客户端从主机生成的加密会话会触发 IoC 事件。您可以查看恶意主机的 IP 地址、MAC 地址和操作系统信息等信息，以及可疑活动的时间戳。

如连接事件中所示，加密可视性威胁置信度评分为“非常高”的会话将 IoC 事件类型化。您必须从**策略** > **+ 显示更多** > **内容关联** > **网络发现**启用 **主机** 。在 防火墙管理中心中，您可以从以下位置查看 IoC 事件的存在情况：

- **分析** > **危害表现**。**事件和日志** > **+ 显示更多** > **主机** > **危害指标**
- **事件和日志** > **主机** > **网络映射** >选择必须检查的主机。

  您可以在**连接事件 (Connection Events)** 页面查看产生该 IoC 的会话的进程信息。点击**事件和日志** > **+ 显示更多** > **连接** > **事件**以访问**统一事件**页面。请注意，您必须从“**连接事件表视图**”选项卡中手动选择“加密可见性”字段和“IoC”字段。

  安全相关连接事件 (Security-Related Connection Events) 页面显示 EVE 阻止的连接，以及具有中、高和极高威胁置信度级别的恶意连接。点击 **事件和日志** > **+ 显示更多** > **连接** > **安全相关事件** 访问 “**安全相关的连接事件**” 页面。

EVE 中的 QUIC 指纹识别

Snort 可以根据 EVE 分析识别快速 UDP Internet 连接（QUIC 会话）中的客户端应用程序。QUIC 指纹识别可以：

- 通过 QUIC 检测应用而不启用解密。
- 在不启用解密的情况下识别恶意软件。
- 检测服务应用。您可以根据通过 QUIC 协议检测到的服务分配访问控制规则。

配置 EVE

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

步骤 3 从数据包流行末尾的**更多**下拉箭头中选择**加密可视性引擎**。

步骤 4 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，启用**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮。

步骤 5 选择**监控**模式或**保护**模式。

- 选择**监控**模式以检测客户端应用并监控加密流量。
- 选择**保护**模式可根据客户端进程的威胁置信度级别监控和阻止加密流量。您可以使用此模式在两个威胁置信度级别监控和阻止恶意连接：
  - **高**：使用此级别可阻止威胁置信度级别从高到极高的连接。
  - **非常高**：使用此级别可阻止威胁置信度级别归类为非常高的连接。

步骤 6 点击**保存**，然后部署访问控制策略。

注释
有关管理例外的信息，请参阅配置 EVE 例外规则， 第 1962 页。

下一步做什么

部署配置更改。

查看 加密可视性引擎事件

启用**加密可视性引擎 (Encrypted Visibility Engine)** 并部署访问控制策略后，您可以开始通过系统发送实时流量。您可以在**统一事件**页面中查看记录的连接事件。

执行此过程以访问防火墙管理中心中的连接事件。

过程

步骤 1 请点击 **事件和日志** > **分析** > **统一事件**。

您也可以在**连接事件**页面中查看连接事件。点击**事件和日志** > **+ 显示更多** > **连接** > **事件**以访问**统一事件**页面。

此外，您可以使用**与安全相关的连接事件**页面（**分析** > **连接标题** > **安全相关的事件**）查看被 加密可视性引擎阻止的连接，以及具有中、高和非常高威胁置信度级别的恶意连接。

加密可视性引擎可以识别发起连接的客户端进程和客户端中的操作系统，并指示该进程是否包含恶意软件。

步骤 2 在**统一事件**页面上，显式启用为 加密可视性引擎添加的这些列：

- **EVE 指纹**
- **EVE 进程名称**
- **EVE 进程信心分数**

- **EVE 威胁信心**
- **EVE 威胁信心分数**
- **检测类型**

有关这些字段的信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的 连接和安全相关的连接事件字段。

注释
在**连接事件**页面上，如果进程被分配了应用程序，**检测类型**列会显示**加密可视性引擎**，表明客户端应用程序是由 加密可视性引擎识别的。如果没有为进程名称分配应用，**检测类型**列会显示**AppID**，表示识别客户端应用的引擎是 AppID。

查看 EVE 控制面板

您可以在以下控制面板中查看 EVE 分析信息：

开始之前

- 在访问控制策略中，必须在 **高级设置** 下启用 **加密可视性引擎（EVE）**。
- 要查看**检测到进程名称的连接**和**恶意进程**小组件，您的设备必须运行 Firewall Threat Defense 版本 7.7 或更高版本。
- 要查看**恶意进程响应器 IP**、**恶意进程联系的域**和**已阻止连接**数据，您的设备必须运行 Firewall Threat Defense 版本 10.0 或更高版本。

过程

步骤 1 转至**洞察和报告** > **控制面板**。

步骤 2 在 **摘要控制面板** 窗口中，点击 **加密可视性引擎 (Encrypted Visibility Engine)** 选项卡。

步骤 3 您可以查看以下控制面板：

- **发现的进程**：显示网络中使用的排名靠前的客户端进程和连接数。您可以点击表中的进程名称，查看 **连接事件** 页面的过滤视图，该视图按进程名称进行过滤。
- **威胁置信度**：按置信度（非常高、非常低等）显示连接。您可以点击表中的 威胁 置信度级别，查看 ”**连接事件**“ 页面的过滤视图，该视图按置信度级别进行过滤。
- **与检测到的进程的连接**：显示 EVE 在其中识别出客户端进程的连接总数。
- **恶意进程**：显示 EVE 识别的威胁置信度为高和极高的恶意客户端进程的计数。

- **恶意响应方 IP**：显示EVE识别为恶意的排名靠前的目标IP地址，按高或极高威胁置信度分类。点击构件中的任何响应方 IP 地址可导航至**连接事件**页面，该页面已按所选响应方 IP 地址进行过滤。
- **恶意域**：显示被EVE识别为恶意并归类为高或极高威胁置信度的域名的计数。点击构件中的任何域名可导航至按所选域名过滤的 **连接事件** 页面。
- **阻止的连接**：显示被 EVE 阻止的连接计数。

注释

- 如果管理中心使用的是 Cisco Secure Firewall 版本 10.0.0，并且没有运行 10.0.0 版本的设备，则不会填充 **恶意进程响应方 IP**、 **恶意进程联系的域**和 **受阻连接** 构件中的数据。
- 如果管理中心使用的是 Cisco Secure Firewall 版本 10.0.0，并且只有一台设备运行版本 10.0.0，则 **恶意进程响应方 IP**、 **恶意进程联系的域**和 **阻止的连接** 构件将仅从该设备填充。其他构件将显示使用较旧版本的设备的数据。

配置 EVE 例外规则

您可以创建加密可视性引擎 (EVE) 例外规则来绕过 EVE 的阻止操作，从而确保可信连接和服务的连续性。您可以将进程名称、源和目标IP地址/FQDN以及动态对象等属性添加到异常规则中。例如，您可能希望绕过受信任网络的EVE阻止判定。根据威胁置信度，绕过网络中的所有连接都免于执行 EVE 阻止判定。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

步骤 3 从数据包流行末尾的**更多**下拉箭头中选择**加密可视性引擎**。

步骤 4 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，启用**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮。

步骤 5 选择**保护**模式可根据客户端进程的威胁置信度级别监控和阻止加密流量。您可以使用此模式在两个威胁置信度级别监控和阻止恶意连接：

- **高**：使用此级别可阻止威胁置信度级别从高到极高的连接。
- **非常高**：使用此级别可阻止威胁置信度级别归类为非常高的连接。

步骤 6 点击**管理例外**以查看和添加例外规则。

步骤 7 在**加密可视性引擎（EVE）例外列表**窗口中，点击 **+添加例外规则**，并添加所需属性。

注释

只能在全局域中配置 EVE 例外规则。在子域中，您只能查看 EVE 例外规则详细信息。您无法在子域中添加、编辑或删除 EVE 例外规则。

a) 在**进程名称**选项卡下，输入 EVE 识别的进程名称，然后点击窗口右侧的 **+添加**。

可以将多个进程名称添加到同一例外规则。基于进程名称的 EVE 例外列表仅适用于 EVE 识别的进程名称，这些进程名称区分大小写和空格。

b) 在**网络对象 (Network Objects)** 选项卡下，执行以下操作之一：

- 从**可用网络**列表中选择一个或多个网络对象，并将其添加到**选定源网络**或**选定目标网络**列表中。
- 在**选定源网络 (Selected Source Network)** 或**选定目标网络 (Selected Destination Network)** 下，手动输入 IP 地址，然后点击 **添加** (+) 图标以将其添加到所选网络列表中。
- 要创建新的网络对象，请点击 **+创建网络对象**。

  1. 输入**名称**和可选的**说明**。
  2. 选择所需的网络类型 - **主机**、**范围**、**网络**或 **FQDN**。如果选择**主机**、**范围**或**网络**，请输入相关的 IP 地址。如果选择 **FQDN**，请输入完全限定域名 (**FQDN**)，并从**查找**下拉列表中选择所需选项。
  3. 如果要允许配置覆盖，请选中**允许覆盖**复选框。
  4. 点击**添加 (Add)**。

c) 在**动态属性**选项卡下，从**可用动态属性**列表中选择所需的动态属性，并使用 > 按钮将其添加到**选定目标动态属性**列表中。

有关创建动态对象或使用动态对象的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的首次创建动态对象或使用动态对象部分。

d) 要创建新的动态属性，请点击 **+创建动态属性**。

1. 输入**名称**和可选的**说明**。
2. 点击**添加 (Add)**。可以使用思科安全动态属性连接器 (CSDAC) 或管理中心 API 配置此对象。

e) （可选）在所有选项卡的**注释**字段中，可以输入将所需网络对象和动态属性添加到 EVE 例外规则的原因。

步骤 8 点击**保存**，然后部署访问控制策略。

注释 当连接匹配例外规则时，它会绕过 EVE 的阻止判定。您可以在**连接事件**或**统一事件**页面中查看 EVE 的操作。**原因 (Reason)** 列标题显示 **EVE 已豁免 (EVE Exempted)**，用于识别此类绕过 EVE 的流量。

从统一事件添加例外规则

使用**统一事件**页面为被EVE阻止的连接添加例外规则。防火墙管理中心会将例外规则添加到**加密可视性引擎(EVE)例外列表**对象。请注意，添加到此列表的例外规则适用于所有启用了EVE的访问控制策略。

开始之前

仅 Threat Defense 版本 7.6.0 及更高版本支持例外列表。

过程

步骤 1 请点击 **事件和日志** > **分析** > **统一事件**。

步骤 2 在**原因**为“**加密可见性块**”的原因列中，点击单元格内的**省略号**( )图标。

步骤 3 从下拉列表中选择**添加 EVE 例外规则 (Add EVE Exception Rule)**。

注释
只能在全局域中配置 EVE 例外规则。在子域中，您只能查看 EVE 例外规则详细信息。您无法在子域中添加、编辑或删除 EVE 例外规则。

步骤 4 在显示的**加密可视性引擎 (Encrypted Visibility Engine)** 窗口中，规则会自动添加到例外列表的底部。您可以在保存和部署配置之前查看并更改添加的规则。

升级 EVE 例外规则

在 Cisco Secure Firewall 7.7 及更早版本上，为每个策略单独配置 EVE 例外规则。从 Cisco Secure Firewall版本10.0.0开始，EVE例外列表是全局域的一部分。因此，EVE例外规则在全局域中配置，并应用于启用 EVE 以阻止流量的所有策略。

当您将管理中心从版本 7.7 升级到 10.0.0 时，系统会识别并存储包含枝叶域网络对象的枝叶域的所有 EVE 例外规则。升级完成后：

- 全局域策略中的所有 EVE 例外规则，以及叶域策略中引用全局域对象或内联 IP 地址的规则，都会整合到单个全局 EVE 例外列表中。因此，某些策略现在可能包括升级前不存在的 EVE 例外规则。
- 包含 EVE 例外规则的所有策略都将被标记为过期。

如果枝叶域的例外规则包含枝叶域网络或动态对象，则在升级过程中这些规则将被删除。升级脚本日志文件包含所有合并和删除的例外规则的日志，以及每个规则源自的相应访问控制策略和域。日志文件位于 */var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade10.0.0/800_post/1114_eve_rules.pl.log*。

当您在升级后首次部署配置时，管理中心上的警告消息会列出所有已删除的EVE例外规则。警告消息还指出，如果未在全局EVE例外列表中重新配置规则，则可能会产生流量影响。请注意，只有在升级完成后首次部署配置时，才会显示警告消息。

对于映射到运行 10.0.0 版本的管理中心的运行 7.7 及更早版本的 Cisco Secure Firewall 设备，只有“**非常高**”威胁置信度连接事件才会发送到“**安全相关连接事件**”表。对于运行版本 10.0.0 的 Cisco Secure Firewall 设备，EVE **阻止** 和 **中+** EVE 威胁置信度连接事件将发送到 **安全相关连接事件** 表。

EVE 升级期间的更改管理支持

当您将管理中心升级到 10.0.0 版本时，包含启用了 EVE 的访问控制策略的所有活动更改管理故障单的 EVE 例外规则将自动与全局 EVE 例外列表合并。

无论通知单处于何种审批状态，EVE 例外规则都会与全局 EVE 例外列表合并。这可确保在升级期间不会丢失例外规则。

EVE 故障单预览生成行为

如果变更管理故障单包含锁定的策略，并且其中仅包含与 EVE 相关的修改（例如 EVE 设置或例外规则），则在升级后不会自动重新生成 EVE 故障单预览。如果除了与 EVE 相关的修改外，通知单还包含其他策略修改，则 EVE 通知单预览将正常生成。

事件扩充

Talos 分类法和加密可视性引擎 (EVE) 可丰富 MITRE ATT&CK 的情景。Talos 和 EVE 扩充都使用 Talos 分类法进行传达。启用 EVE 时，EVE 扩充有效。有关启用 EVE 的详细信息，请参阅配置 EVE，第 1959 页。

在**连接事件 (Connection Events)** 页面上，可以查看作为扩充事件内容的一部分添加的以下列标题。您必须明确启用这些列。

- **MITRE ATT&CK**
- **其他扩充**

有关这些字段的信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的“连接和 中的“安全相关连接 事 件字段” 。

EVE 示例

关于加密可视性引擎

您可以使用加密可视性引擎 (EVE) 来识别使用传输层安全 (TLS) 加密的客户端应用和进程。EVE 无需解密即可提供对加密会话的更多可视性。根据 EVE 的调查结果，管理员可以对其环境中的流量实施策略操作。您还可以使用 EVE 识别和阻止恶意软件。

优势

管理员可以利用和调整EVE的威胁评分来阻止恶意加密流量。如果传入流量是恶意的，则可以根据威胁评分将 EVE 配置为阻止连接。

示例业务情景

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，采用强大的网络安全措施是必要且重要的。安全团队使用加密可视性引擎 (EVE) 来增强加密流量检查，而无需实施完整的中间人(MITM)解密。EVE技术使用已知恶意进程的指纹来识别和阻止恶意软件。网络管理员必须能够灵活地配置EVE的阻止流量阈值，以阻止基于其配置的阻止阈值的潜在恶意连接。

前提条件

- 您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。
- 确保您拥有有效的入侵防御系统 (IPS) 许可证，并且 Snort 3 是检测引擎。

高级工作流程

1. EVE 分析传入流量，并判定传入流量是否为恶意软件的可能性。
2. 如果 EVE 以一定的置信度检测到传入流量为恶意软件，则可以将 EVE 配置为阻止该流量。
3. 首先检查数据包的恶意软件概率或威胁评分，然后将威胁评分与您设置的阻止阈值进行比较。
4. 如果威胁评分高于配置的阈值，EVE 将阻止流量。
5. 如果威胁评分低于配置的阈值，EVE 不采取任何措施。

在 EVE 中配置阻止阈值

此程序显示如何根据 90% 或更高的 EVE 威胁置信度分数阻止潜在的恶意流量。

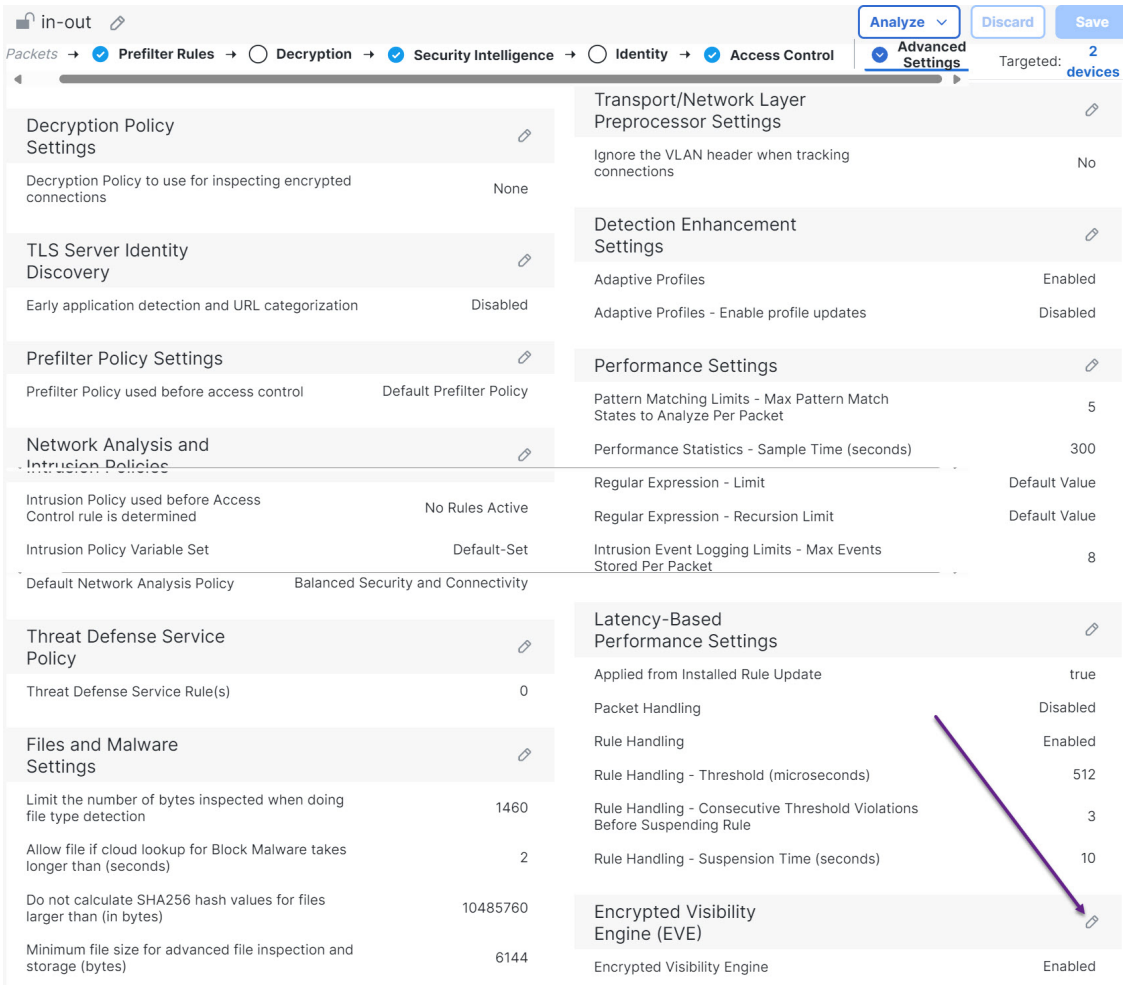
过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

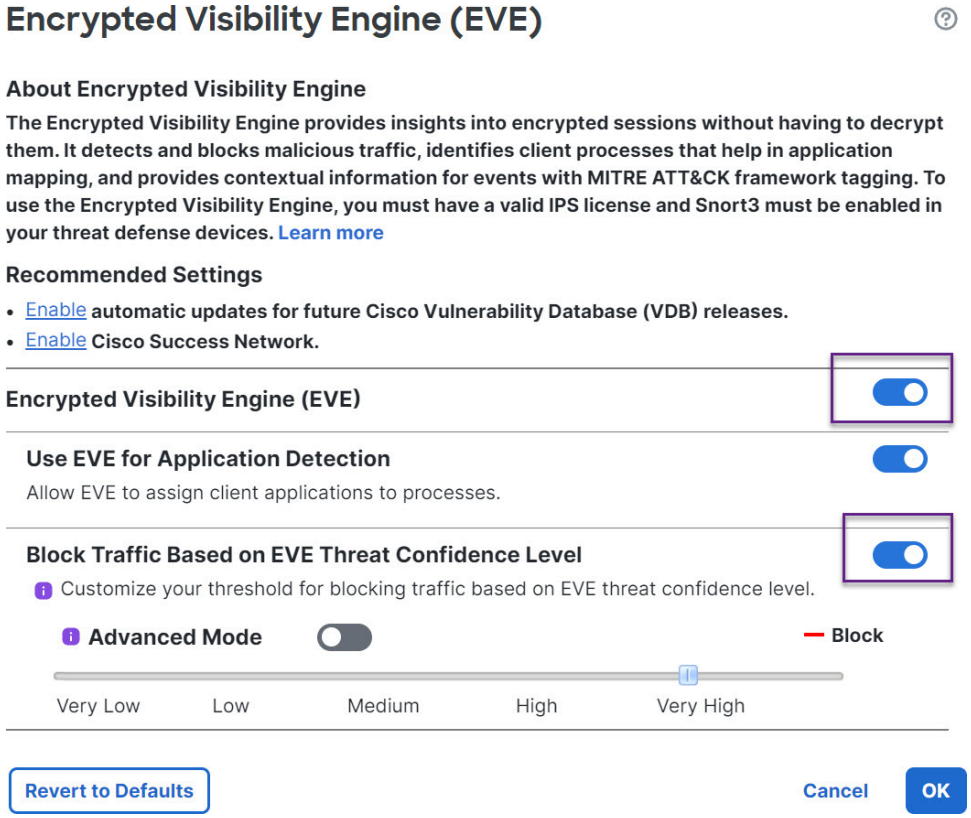
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**加密可视性引擎 (Encrypted Visibility Engine)** 旁边的 **编辑** (✎)。



步骤 5 在 **加密可视性引擎** 页面中，启用 **加密可视性引擎 (EVE)** 切换按钮。

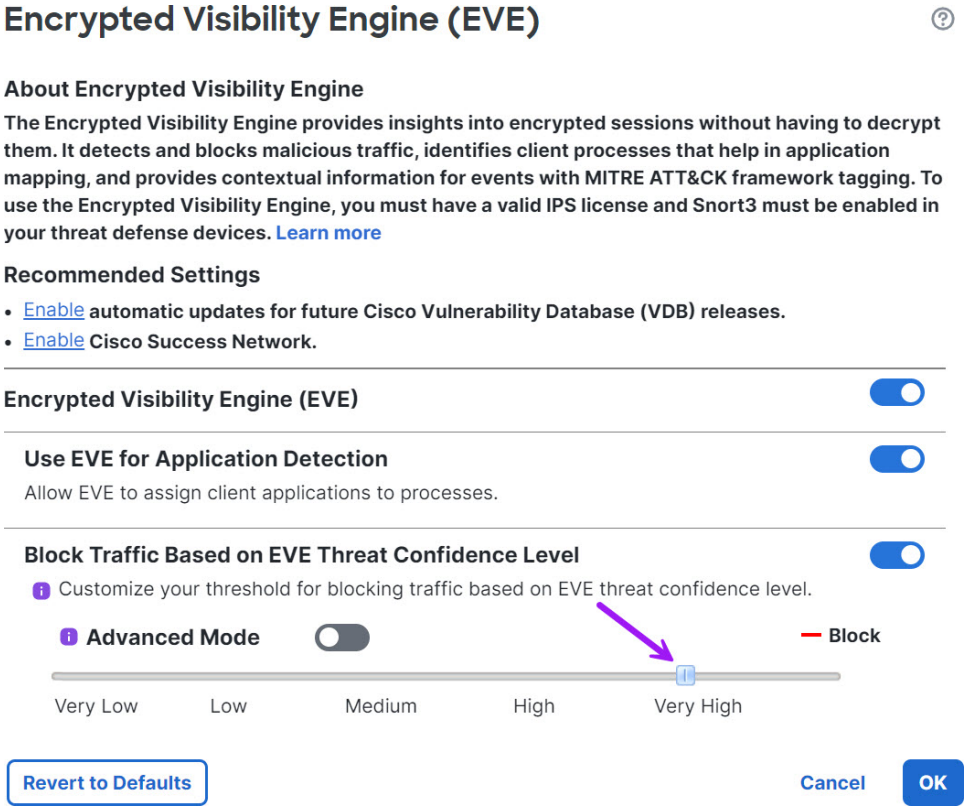
步骤 6 启用 **基于 EVE 分数阻止流量** 切换按钮。默认情况下，任何可能构成威胁的传入流量都会被阻止。



注释
默认情况下，阻止恶意软件的阈值为 99%，这意味着：

- 如果 EVE 检测到流量为恶意软件且置信度为 99% 或更高，则 EVE 会被阻止流量。
- 如果 EVE 检测到流量为恶意软件且其置信度低于 99%，则 EVE 不会采取任何措施。

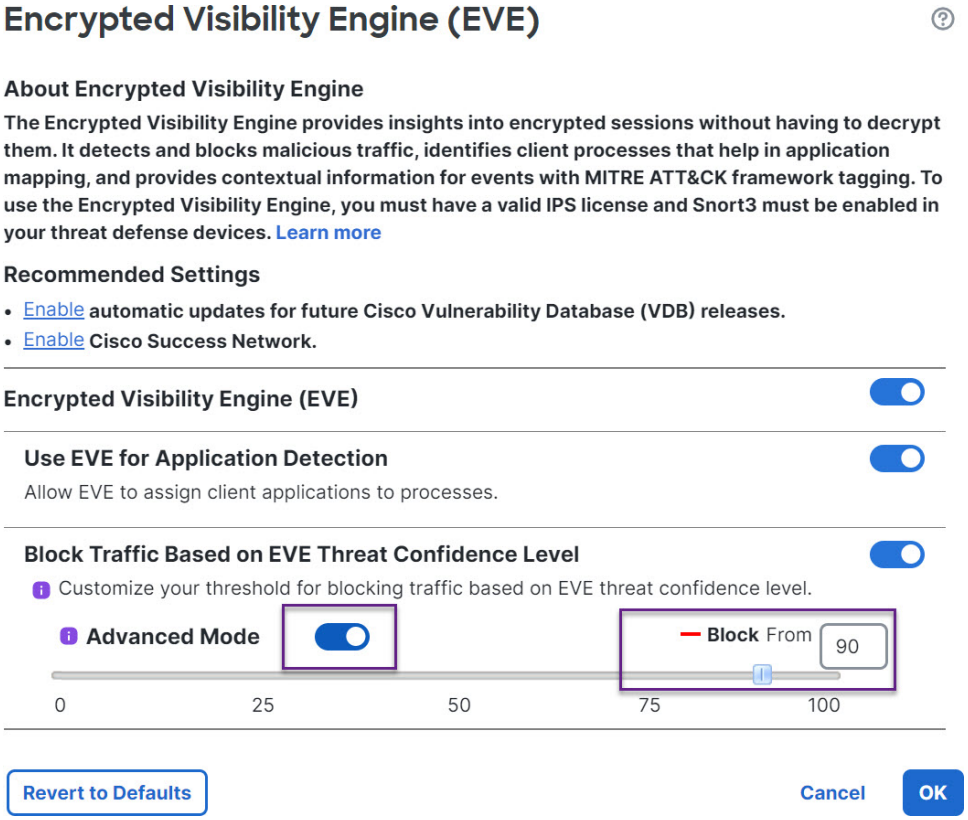
步骤 7 使用滑块根据 EVE 威胁置信度调整阻止阈值。范围从 **非常低** 到 **非常高**。在本例中，滑块设置为 **非常高**。



步骤 8 要进行进一步精细控制，请启用**高级模式 (Advanced Mode)** 切换按钮。现在，您可以为阻止流量分配特定的 EVE 威胁置信度评分。默认阈值为 99%。

步骤 9 在本例中，将阻止阈值更改为 **90**%。

注意
作为最佳实践，我们建议您不要将阻止阈值设置为低于 50%，以确保最佳性能。



步骤 10 点击**确定**。

步骤 11 点击**保存**。

下一步做什么

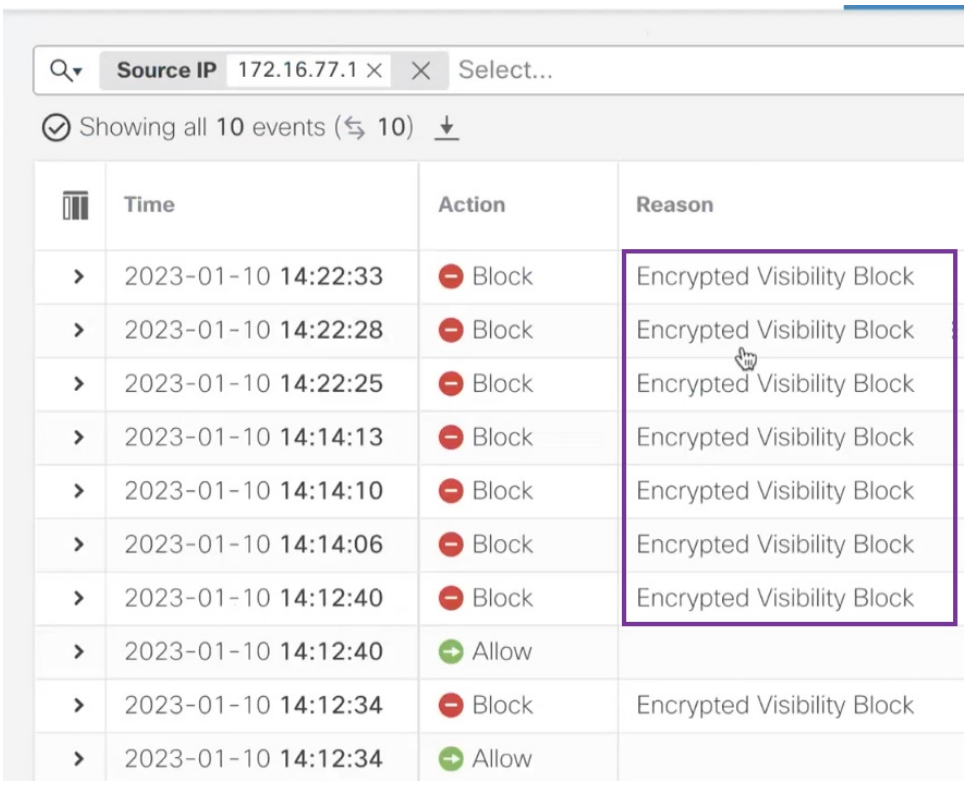
部署配置更改。

查看 EVE 事件

过程

步骤 1 要验证阻止操作，请选择 **事件和日志** > **+ 显示更多** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 如果您已将 EVE 配置为阻止流量，则 **原因** 字段将显示 **加密可视性阻止**。



步骤 3 以下是 **加密可视性进程名称** 为 **test_malware**、 **加密可视性威胁置信度** 为 **非常高**、 **加密可视性威胁置信度** 为 **90** % 的示例。



其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 加密可视性引擎”一章或以下链接中的内容：

加密可视性引擎



第 X 部分

访问控制的身份策略

- 身份概述， 第 1975 页
- 领域， 第 1993 页
- 身份源：强制网络门户， 第 2059 页
- 身份源：ISE/ISE-PIC， 第 2079 页
- 身份源：被动身份代理， 第 2107 页
- 身份源：pxGrid Cloud 身份（ISE 3.3 及更低版本）， 第 2141 页
- 身份源：pxGrid Cloud 身份（ISE 3.4 及更高版本）， 第 2173 页
- 身份源：远程访问 VPN， 第 2203 页
- 身份源：TS 代理， 第 2207 页
- 身份策略， 第 2211 页



第 49 章

身份概述

以下主题讨论用户身份：

- 关于用户身份，第 1975 页
- 主机和用户限制，第 1986 页
- 身份领域限制，第 1991 页
- Microsoft Azure Active Directory 领域的用户限制，第 1991 页

关于用户身份

用户身份信息可以帮助识别政策违规、攻击或网络漏洞的来源，并跟踪它们到具体用户。例如，您可以确定：

- 谁拥有作为影响程度为“易受攻击”（级别 1：红色）的入侵事件的目标的主机。
- 谁发起了内部攻击或端口扫描。
- 谁正在尝试对指定主机进行未经授权的访问。
- 谁正在耗用异常大量的带宽。
- 谁尚未应用关键操作系统更新。
- 谁正在违反公司政策使用即时消息软件或点对点文件共享应用。
- 谁与您网络中的每个危害表现相关。

借助这些信息，您可以使用系统的其他功能降低风险，执行访问控制以及采取措施防止中断他人的活动。这些功能还可以大大改善审核控制并提高合规性。

在配置用户身份源以收集用户数据后，您可以执行用户感知和用户控制。

有关身份源的详细信息，请参阅 关于用户身份源，第 1976 页。

相关主题

身份术语，第 1976 页
关于用户身份源，第 1976 页
身份部署，第 1980 页

如何设置身份策略，第 1982 页

身份术语

本主题讨论用户身份和用户控制的常用术语。

用户感知

使用身份源（如、TS 代理或Cisco ISE）标识网络中的用户。通过用户感知，您可以从授权（例如 Active Directory）和非授权（基于应用）源中识别用户。要使用 Active Directory 作为身份源，必须配置领域和目录。有关详细信息，请参阅关于用户身份源，第 1976 页。

用户控制

配置与访问控制策略关联的身份策略。（然后，身份策略将作为访问控制子策略引用。）身份策略指定身份源以及（可选）属于该源的用户和组。

通过将身份策略与访问控制策略相关联，可以确定在网络中是监控、信任、阻止还是允许流量中的用户或用户活动。有关详细信息，请参阅访问控制策略，第 1701 页。

授权身份源

验证了用户登录的受信任服务器（例如，Active Directory）。您可以使用从授权登录获取的数据执行用户感知和用户控制。授权用户登录是从被动和主动身份验证中获取：

- 被动身份验证发生在用户利用 Cisco ISE 进行身份验证时。
- 主动身份验证发生在用户通过预先配置的托管设备进行身份验证时。强制网络门户又称为主动身份验证。主动身份验证通常使用与被动身份验证相同的用户存储库（ISE/ISE-PIC TS 代理和 被动身份代理例外，它们仅是被动身份验证）。

非授权身份源

未知或不受信任的服务器已验证用户登录。基于流量的检测是系统唯一支持的未授权身份源。您可以使用从非授权登录获取的数据执行用户感知。

关于用户身份源

下表提供系统支持的用户身份源的简要概述。每个身份源都提供一个用户存储库以获取用户感知。然后，可以使用身份和访问控制策略来控制这些用户。

用户身份源	服务器要求	登录类型	身份验证类型	用户控制	有关详细信息，请参阅...
强制网络门户	OpenLDAP Microsoft Active Directory Microsoft Azure Active Directory	权威	主用	支持	强制网络门户身份源，第 2059 页 创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户），第 2014 页
被动身份验证	OpenLDAP Microsoft Active Directory	非授权	主用	支持	创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页
被动身份验证	Microsoft Azure Active Directory	被动	无源	支持	为被动身份验证配置 Microsoft Entra ID，第 1997 页
使用 被动身份代理 进行被动身份验证	Microsoft Active Directory	非授权	无源	支持	被动身份代理身份源，第 2107 页
使用 TS 代理进行被动身份验证	Microsoft Windows 终端服务器	权威	无源	支持	终端服务 (TS) 代理身份源，第2207页
远程访问 VPN	OpenLDAP 或 Microsoft Active 目录	权威	主用	支持	远程访问 VPN 身份源，第 2203 页
	RADIUS	权威	主用	否，仅感知	
ISE/ISE-PIC	Microsoft Active Directory	权威	无源	支持	The ISE/ISE-PIC 身份源，第2079页
基于流量的检测 （在网络发现策略中配置。）	-	非授权	-	否，仅感知	基于流量的检测身份源，第 2592 页

当选择要部署的身份源时，请考虑以下事项：

- 必须使用基于流量的检测来检测非 LDAP 用户登录。
- 必须使用基于流量的检测或强制网络门户来记录失败的登录或身份验证活动。如果登录或身份验证尝试失败，则不会将新用户添加到数据库的用户列表中。

- 强制网络门户身份源需要具有路由接口的托管设备。您不能使用具有强制网络门户的内联（也称为分路模式）接口。

这些身份源的数据存储在 Secure Firewall Management Center的用户数据库和用户活动数据库中。您可以配置 Secure Firewall Management Center服务器用户下载，以将新用户数据定期自动下载到您的数据库中。

在使用所需的身份源配置身份规则之后，必须将每个规则与访问控制策略相关联，并将策略部署到托管设备，策略才能产生效果。有关访问控制策略和部署的详细信息，请参阅将其他策略与访问控制相关联，第 1719 页。

有关用户身份的常规信息，请参阅关于用户身份，第 1975 页。

用户身份的最佳实践

我们建议您在设置身份策略之前查看以下信息。

- 了解用户限制
- 运行状况监控
- 使用最新版本的 ISE/ISE-PIC，两种类型的补救
- 6.7 中的用户代理支持丢弃
- 强制网络门户需要路由接口，多个单独的任务

Microsoft Active Directory 和 LDAP

系统支持 Active Directory、LDAP 和其他用户存储库，以实现用户感知和控制。Active Directory 或 LDAP 存储库与 Secure Firewall Management Center 之间的关联被称为领域。您应为每个 LDAP 服务器或 Active Directory 域创建一个领域。有关支持版本的详细信息，请参阅领域支持的服务器，第 2027 页。

LDAP 支持的唯一用户身份源是强制网络门户。要使用其他身份源（ISE/ISE-PIC 除外），您必须使用 Active Directory。

仅适用于 Active Directory：

- 为每个域控制器创建一个目录。

  有关详细信息，请参阅 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页

- 如果将所有 Active Directory 域和域控制器分别添加为领域和目录，则支持两个域之间存在信任关系的用户和组。

  有关详细信息，请参阅领域和受信任的域，第 2023 页。

被动身份代理 身份源

被动身份代理 软件可以监控多个 Microsoft Active Directory 服务器和域控制器，并向 Secure Firewall Management Center 发送用户名和 IP 地址信息。

有关详细信息，请参阅被动身份代理身份源，第 2107 页。

运行状况监控

Secure Firewall Management Center 运行状况监控器提供有关各种 Secure Firewall Management Center 功能状态的重要信息，包括：

- 用户/领域不匹配
- Snort 内存使用情况
- ISE 连接状态

有关运行状况模块的详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的运行状况模块。

要设置策略以监控运行状况模块，请参阅*Cisco Secure Firewall Management Center* 管理指南中的创建运行状况策略。

设备特定的用户限制

每个物理或虚拟防火墙管理中心设备对可下载的用户数量都存在限制。如果达到用户限制，防火墙管理中心 可能会耗尽内存，并因此无法可靠地运行。

Microsoft Active Directory 的用户限制，第 1988 页中讨论了用户限制。

如果使用 ISE/ISE-PIC 身份源，则可以选择使用身份映射过滤器限制 防火墙管理中心 监控的子网，如创建身份策略，第 2213 页中所述。

使用最新版本的 ISE/ISE-PIC

如果您希望使用 ISE/ISE-PIC 身份源，则强烈建议您始终使用最新版本，以确保获得最新的功能和漏洞修复。

pxGrid 2.0（版本 2.6 补丁 6 或更高版本使用；或 2.7 补丁 2 或更高版本）还将 ISE/ISE-PIC 使用的补救从终端保护服务 (EPS) 更改为自适应网络控制 (ANC)。如果升级 ISE/ISE-PIC，您必须将中介策略从 EPS 迁移到 ANC。

有关使用 ISE/ISE-PIC 的更多信息，请参阅ISE/ISE-PIC 准则和限制，第 2081 页。

要设置 ISE/ISE-PIC 身份源，请参阅如何为用户控制配置 ISE/ISE-PIC，第 2084 页。

强制网络门户信息

您可以通过以下任何一种方式使用强制网络门户主动身份验证：

- LDAP

  有关详细信息，请参阅 强制网络门户身份源，第 2059 页。

- Microsoft AD

  有关详细信息，请参阅 强制网络门户身份源，第 2059 页。

- Microsoft Azure AD (SAML)

  有关详细信息，请参阅 创建Microsoft Azure AD (SAML)领域，第 1994 页。

有关强制网络门户身份源的详细信息，请参阅强制网络门户身份源，第 2059 页。

TS 代理信息

需要 TS 代理用户身份源来识别 Windows 终端服务器上的用户会话。TS 代理软件必须安装在终端服务器计算机上，如《思科终端服务 *(TS)* 代理指南》中所述。此外，您必须将 TS 代理服务器上的时间与 Secure Firewall Management Center上的时间进行同步。

TS代理数据显示在“用户”、“用户活动”和“连接事件”表中，并可用于用户感知和用户控制。

有关详细信息，请参阅TS 代理准则，第 2208 页。

将身份策略与访问控制策略相关联

在配置领域、目录和用户身份源后，您必须在身份策略中设置身份规则。要让策略生效，您必须将身份策略与访问控制策略相关联。

有关创建身份策略的详细信息，请参阅创建身份策略，第 2213 页。

有关创建身份规则的详细信息，请参阅创建身份规则，第 2221 页。

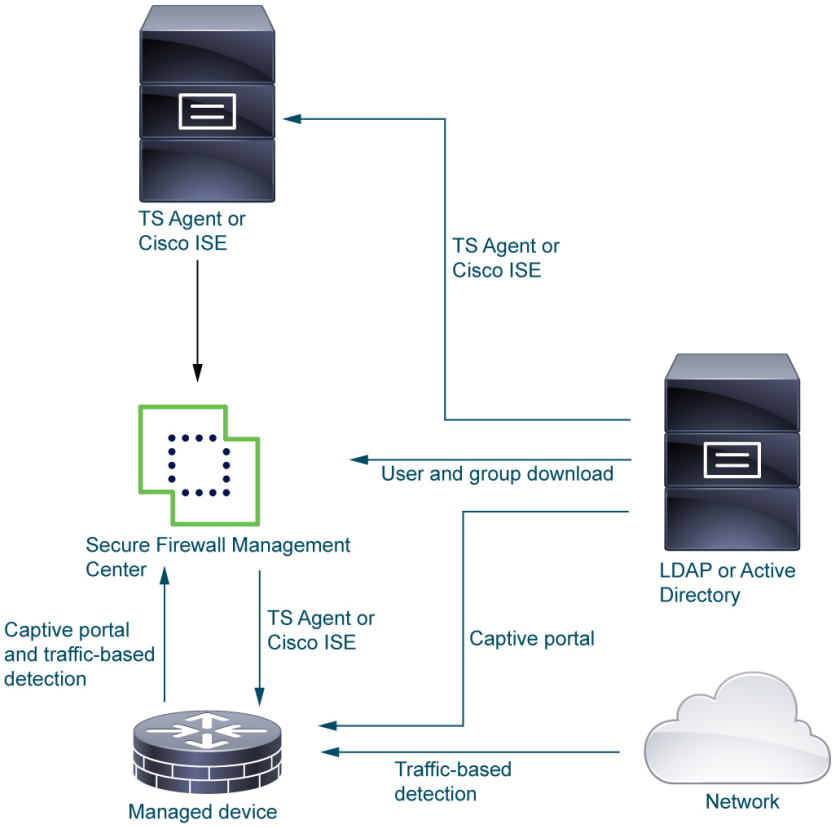
要将身份策略与访问控制策略相关联，请参阅将其他策略与访问控制相关联，第 1719 页。

身份部署

系统从任何身份源检测到用户登录的用户数据时，会将登录用户与 Secure Firewall Management Center 用户数据库中的用户列表进行比对。如果登录用户与现有用户匹配，则登录数据将会分配给该用户。如果登录信息与现有用户不匹配，则会创建新用户，除非登录信息位于 SMTP 流量中。SMTP 流量中不匹配的登录信息将被丢弃。

一旦用户被 Secure Firewall Management Center 发现，用户所属的组就会与用户关联。

下图展示了系统如何收集和存储用户数据。



简单身份部署

在上图中，Secure Firewall Management Center 和一个托管设备会被部署到 AWS，而其他设备位于本地。这些设备可以是物理设备，也可以是虚拟设备；它们只需要能够相互通信。

只有 TS 代理和强制网络门户需要 LDAP 或 Active Directory，如以下段落所述。

有关设置此类系统的详细信息，请参阅如何设置身份策略，第 1982 页。

ISE/ISE-PIC 身份源

当您部署 ISE/ISE-PIC 身份源时，ISE/ISE-PIC 服务器会将用户、组和订用发送到 Secure Firewall Management Center。

您可以选择在 ISE/ISE-PIC 部署中使用 LDAP 服务器，但由于它是可选的，因此并未在下图中显示。

有关 ISE / ISE-PIC 的详细信息，请参阅The ISE/ISE-PIC 身份源，第 2079 页。

被动身份代理 身份源

用于监控一个或多个 Microsoft AD 域控制器，并将用户名和 IP 地址信息发送到 Secure Firewall Management Center 的软件。

有关详细信息，请参阅被动身份代理身份源，第 2107 页。

TS 代理身份源

终端服务 (TS) 代理软件可在 Microsoft 服务器上运行，并会根据用户登录服务器所用的端口范围来发送 Secure Firewall Management Center 用户信息。TS 代理会从 LDAP 或 Active Directory 获取用户身份信息，然后将它们发送到 Secure Firewall Management Center。

有关 TS 代理身份源的详细信息，请参阅终端服务 (TS) 代理身份源，第 2207 页。

强制网络门户

您可以通过以下任何一种方式使用强制网络门户主动身份验证：

- LDAP

  有关详细信息，请参阅 强制网络门户身份源，第 2059 页。

- Microsoft AD

  有关详细信息，请参阅 强制网络门户身份源，第 2059 页。

- Microsoft Azure AD (SAML)

  有关详细信息，请参阅 创建Microsoft Azure AD (SAML)领域，第 1994 页。

有关强制网络门户身份源的详细信息，请参阅强制网络门户身份源，第 2059 页。

如何设置身份策略

本主题提供了使用任何可用的用户身份源（TS 代理、ISE/ISE-PIC、Microsoft Azure AD (SAML)、强制网络门户）设置身份策略的高级概述。

过程

	命令或操作	目的
步骤 1	选择身份源。	• 要使用 Microsoft Active Directory 或 LDAP，请继续执行下一步。 • 要使用 Microsoft Azure AD (SAML) 领域，请参阅创建Microsoft Azure AD (SAML)领域，第 1994 页。 • 要使用 Cisco ISE 身份源，请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页。 • 要使用 被动身份代理 身份源，请参阅被动身份代理身份源，第 2107 页。
步骤 2	（可选。）创建领域和目录，林中包含要在用户控制中使用的用户的每个域都要创建一个领域。还为每个域控制器创建一个目录。	如果满足以下任一条件，则创建领域、领域目录为可选：

	命令或操作	目的
	只有具有相应 防火墙管理中心 领域和目录的用户和组才能用于身份策略中。	• 您使用的 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件。 • 您仅使用身份策略来过滤网络流量。 领域是受信任的用户和组存储区，通常是 Microsoft Active Directory 存储库。防火墙管理中心 会按您指定的间隔时间下载用户和组。您可以包括或排除用户和组来进行下载。 请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。有关创建领域的选项的详细信息，请参阅领域字段，第 2029 页。 目录是一个 Active Directory 域控制器，它组织有关计算机网络的用户和网络共享的信息。Active Directory 控制器将为该领域提供目录服务。Active Directory 将跨域控制器分发用户和组对象，这些控制器是通过使用目录服务传播相互之间的本地更改的对等体。有关详细信息，请参阅 MSDN 上的 Active Directory 技术规范术语表。 您可以为某个领域指定多个目录，在这种情况下，每个域控制器都按该领域的**目录**选项卡页面上列出的顺序进行查询，以匹配进行用户控制的用户和组凭证。 **注释** 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件，则可自行决定是否配置领域或领域序列。
步骤 3	从领域同步用户和组。	要想能够控制用户和组，您必须将它们与防火墙管理中心 同步。您可以随时将其与用户和组同步，也可以将系统配置为按指定的时间间隔进行同步。 同步用户和组时，可以指定例外；例如，您可以从该领域的所有用户控制中排除“工程”组，也可以从应用于“工程”组的用户控制中排除用户 **`joe.smith`**。

	命令或操作	目的
		请参阅 同步用户和组， 第 2037 页
步骤 4	（可选。）创建领域序列。	领域序列是一个有序的领域列表，如果用于身份策略中，则会导致系统按指定顺序搜索领域，以查找与规则匹配的用户。请参阅创建领域序列， 第 2039 页。
步骤 5	创建检索用户和组数据的方法（身份源）。	设置一个具有其独特配置的身份源，以便能够使用存储在该领域中的数据控制用户和组。身份源包括 TS 代理、网络强制门户或远程 VPN。请参见以下选项之一： • 如何为用户控制配置强制网络门户， 第 2063 页 • 配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页 • 配置用户控制 RA VPN， 第 2204 页
步骤 6	创建身份策略。	身份策略包含一个或多个身份规则，可选择按类别对其进行组织。请参阅创建身份策略， 第 2213 页。 **注释** 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置领域或领域序列。
步骤 7	创建一个或多个身份规则。	身份规则使您能够指定许多匹配条件，包括身份验证类型、网络区域、网络或地理位置、领域、领域序列等。请参阅创建身份规则， 第 2221 页。
步骤 8	请将您身份策略与访问控制策略关联起来。	访问控制策略将会过滤并（可选）检查流量。身份策略必须与访问控制策略相关联方可生效。请参阅将其他策略与访问控制相关联， 第 1719 页。
步骤 9	将访问控制策略部署到至少一个托管设备。	要使用策略控制用户活动，必须将该策略部署到客户端所连接到的托管设备。请参阅部署配置更改， 第 180 页。
步骤 10	监控用户活动	查看由用户身份源收集的活动会话列表或由用户身份源收集的用户信息列表。请参阅

	命令或操作	目的
		Cisco Secure Firewall Management Center 管理指南 中的使用工作流程。 如果满足以下所有条件，则不需要身份策略： • 您使用 ISE/ISE-PIC 身份源。 • 您未在访问控制策略中使用用户或组。 • 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

相关主题

配置基于流量的用户检测 ， 第 2593 页

用户活动数据库

Secure Firewall Management Center上的用户活动数据库包含已配置的所有身份源检测或报告的网络上的用户活动记录。系统会在以下情况下记录事件：

- 检测到单独的登录或注销时。
- 检测到新用户时。
- 系统管理员手动删除用户时。
- 系统检测到不在数据库中的用户，但因已达到用户限制而无法添加该用户时。
- 您解决与用户关联的危害表现，或者为用户启用或禁用危害表现规则时。



注释 如果 TS 代理监控与其他被动身份验证身份源（如 ISE/ISE-PIC）相同的用户，则 防火墙管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 防火墙管理中心。

可以使用 Secure Firewall Management Center查看系统检测到的用户活动。（**事件和日志** > **用户** > **用户活动**。）

用户数据库

Secure Firewall Management Center中的用户数据库包含所有已配置身份源检测或报告的每个用户的记录。您可以使用从授权源获取的数据进行用户控制。

有关受支持的非授权和授权身份源的详细信息，请参阅关于用户身份源 ， 第 1976 页。

如 Microsoft Active Directory 的用户限制，第 1988 页所述， Secure Firewall Management Center 可以存储的用户总数取决于 Secure Firewall Management Center 型号。达到此用户限制后，系统将基于其身份源对以前未检测到的用户数据划分优先级，如下所示：

- 如果新用户来自非授权身份源，则系统不会将该用户添加到数据库。要允许添加新用户，您必须手动或使用数据库清除删除用户。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新用户添加到数据库。

如果身份源配置为排除特定用户名，则这些用户名的用户活动数据将不会报告给 Secure Firewall Management Center。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。有关系统存储的数据类型的详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的用户数据。

如果已配置 防火墙管理中心高可用性且主连接失败，则在故障转移停机期间无法识别强制网络门户、ISE/ISE-PIC、TS 代理、远程接入 VPN 报告的所有登录，即便以前查看过这些用户并已将他们下载到 防火墙管理中心也是如此。无法识别的用户在 防火墙管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

注释 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 防火墙管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 防火墙管理中心。

系统检测到新用户会话时，用户会话数据会保留在用户数据库中，直至出现以下其中一种情形：

- 防火墙管理中心 的用户将手动删除用户会话。
- 某个身份源报告该用户会话的注销操作。
- 某个领域结束其**用户会话超时：通过验证的用户**、**用户会话超时：未通过验证的用户**或**用户会话超时：访客用户**设置指定的用户会话。

主机和用户限制

您的 Secure Firewall Management Center型号确定您可以通过部署监控的单独主机数量，以及可以您可以监控和用于执行用户控制的用户数。

主机限制

当在监控网络中检测到与 IP 地址相关联的活动时，系统会将主机添加到网络映射，如网络发现策略中所定义。Secure Firewall Management Center可以监控因而存储在网络映射中的主机数取决于其型号。

表 *112:* 按 ***Secure Firewall Management Center***型号列出的主机限制

防火墙管理中心 型号	主机数
MC1000	50,000
MC1600	50,000
MC1700	50,000
MC1800	60,000
MC2500	150,000
MC2600	150,000
MC2700	150,000
MC2800	180,000
MC4500	600,000
MC4600	600,000
MC4700	600,000
MC4800	1,500,000 *
虚拟	50,000

您无法查看不在网络映射中的主机的情景数据。但是，您可以执行访问控制。例如，您可以对不在网络映射中的主机接收和发出的流量进行应用控制，即使您无法使用合规 allow 名单监控主机的网络合规性。



注释 系统分别从 IP 地址和 MAC 地址识别的主机对仅 MAC 主机进行计数。与一台主机关联的所有 IP 地址均视为一台主机共同计数。

达到主机限制并删除主机

网络发现策略控制在达到主机限制后检测到新主机时的处理方式。您可以丢弃新主机，或替换不活动时间最长的主机。您也可以设置系统在主机处于非活动状态多长时间后将其从网络映射中删除的时间段。虽然您可以从网络映射中手动删除主机、整个子网或所有主机，但如果系统检测到与已删除主机相关的活动，它会重新添加该主机。

相关主题

网络发现数据存储设置，第 2599 页

Microsoft Active Directory 的用户限制

关于用户限制

防火墙管理中心型号确定可监控的个人用户数量。用户会在以下情况时被添加到防火墙管理中心用户数据库：

- 从领域下载用户。
- 强制网络门户或 RA-VPN 用户登录。
- 从任何身份源 （例如，TS 代理）检测到用户。

仅授权用户才能使用访问控制策略进行用户控制。

请注意以下事项：

- 下载用户的最大数目取决于您的 防火墙管理中心 型号。
- 并发用户会话（即登录）的最大数量取决于您的托管设备型号。一个用户可以拥有来自不同的唯一 IP 地址的多个会话。

注释 系统将所有用户会话下载到所有 Firewall Threat Defense 设备。如果您的设备具有不同的用户并发用户会话限制，则具有最小限制的 Firewall Threat Defense 会在其内存达到配置的限制时报告运行状况警告。（例如，如果您的 防火墙管理中心 管理 Firepower 2110 和 4125，则当并发用户会话数接近其最大值 64,000 时，2110 会报告运行状况警告。）

Microsoft Active Directory 的用户限制

表 *113: Firewall Threat Defense*的并发用户登录的最大数量限制

Firewall Threat Defense 型号	每个领域的并发用户登录最大数量
Firewall Threat Defense Virtual 5、10、20、30、50 （任何受支持的虚拟机监控程序）	64,000
Secure Firewall 220	10,000（见备注）
Firepower 1010、1120、1140、1150 Cisco Secure Firewall 1210、1220、1230、1240、1250 Firepower 2110、2120、2130 Cisco Secure Firewall 3105、3110、3120	64,000

Firewall Threat Defense 型号	每个领域的并发用户登录最大数量
Firepower 2140 Cisco Secure Firewall 3130、3140 Firepower 4112、 4115、 4125	150,000
Firepower 4145 Firepower 9300	300,000
Cisco Secure Firewall 4215	300,000
Cisco Secure Firewall 4225、4245、4250	315,000
Cisco Secure Firewall 6160,6170	315,000



注释 Cisco Secure Firewall 220 最多可累计下载 10,000 个用户 IP、SXP 映射、SGT 映射和动态对象。在总共下载 10,000 个对象后，Cisco Secure Firewall 220 会停止下载任何对象，直到删除之前的一些对象为止。（例如，如果用户注销，则内存可用于其他对象。）

用户限制按 Microsoft Active Directory 领域应用。也就是说，如果尝试下载的用户数量超过了单个领域的最大用户数量，下载就会停止，同时显示运行状况警告。但是，如果您尝试下载的用户数量超过了分布在不同领域的最大用户数量，则下载会成功（除非任何一个领域的用户数量超过 150,000 个，在这种情况下，该领域的下载会失败）。

表 *114:* 按 防火墙管理中心 型号划分的最大下载用户数

防火墙管理中心 型号	最大下载用户数
FMC 1000	50,000
FMC 1600	50,000
FMC 1700	50,000
FMC 1800	50,000
FMC 2500	150,000
FMC 2600	150,000
FMC 2700	150,000
FMC 2800	150,000
FMC 4500	600,000
FMC 4600	600,000
FMC 4700	600,000

防火墙管理中心 型号	最大下载用户数
FMC 4800	600,000
Firewall Management Center Virtual （任何受支持的虚拟机监控程序）	50,000
Firewall Management Center Virtual 300（任何受支持的虚拟机监控程序）	150,000

达到限制后，当系统检测到之前未检测到的新用户时，会根据其身份源确定用户数据的优先级：

- 如果新用户来自非授权源，则系统不会将该非授权用户添加到数据库。要允许添加新用户，您必须手动删除用户或清除数据库。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新授权用户添加到数据库。

  如果只有授权用户，则系统会删除非活动时间最长的授权用户，并将新用户添加到数据库。

故障排除信息可在用户控制故障排除，第 2231 页中看到。

提示 请注意，如果使用的是基于流量的检测，则您可按协议限制客户日志记录，以最大程度低减少用户名干扰并保留数据库空间。例如，您可以防止系统添加在 AIM、POP3 和 IMAP 流量中发现的用户，因为您了解此流量来自您不想监控的特定承包商或访客。

多实例设备中的最大用户映射数

本主题介绍运行 Snort 3 的多实例设备中可用的最大用户映射数。用户映射将已登录用户的 IP 地址与 SXP 或用户及组，或动态对象映射相关联。Secure Firewall Management Center 在策略中使用映射，也在日志中显示相关信息。

下表显示了 Snort 3 根据可用内存支持的最大用户映射数。当预留内存的使用率超过 80% 时，Secure Firewall Management Center 会发出警报。

设备可用 **RAM**	最大用户映射数
< 24 GB	64,000
24 GB 到 80 GB 之间	200000
80 GB 到 256 GB 之间	300,000
超过 256 GB	400,000

身份映射的数量取决于实例可用的 Snort 内存；内存会根据 CPU 核心数分配给实例。有关每个实例的可用数量和 CPU 核心数（或线程数）的信息，请参阅实例的准则和限制，第 220 页。

身份领域限制

无论 Firewall Threat Defense 型号如何，我们都将您的领域数量限制为最多 25 个；云交付的防火墙管理中心 也适用相同限制。

可下载到系统的用户数量受限于以下文档中提供的信息：

Microsoft Active Directory 的用户限制，第 1988 页

Microsoft Azure Active Directory 领域的用户限制

Microsoft Azure Active Directory 用户限制

关于用户限制

防火墙管理中心型号确定可监控的个人用户数量。

请注意以下事项：

- 下载用户的最大数目取决于您的 防火墙管理中心 型号。
- 并发用户会话（即登录）的最大数量取决于您的托管设备型号。一个用户可以拥有来自不同的唯一 IP 地址的多个会话。

注释 系统将所有用户会话下载到所有 Firewall Threat Defense 设备。如果您的设备具有不同的用户并发用户会话限制，则具有最小限制的 Firewall Threat Defense 会在其内存达到配置的限制时报告运行状况警告。（例如，如果您的 防火墙管理中心 管理 Firepower 2110 和 4125，则当并发用户会话数接近其最大值 64,000 时，2110 会报告运行状况警告。）

请参阅下表。

表 *115:* 按 防火墙管理中心 型号 [1] 划分的最大下载用户数

防火墙管理中心 型号	Dynamic Attributes Connector 连接器数量	最大下载用户数
FMC1600、FMC1700	10	50,000
FMC1800	10	50,000
FMC2600、FMC2700	20	150,000

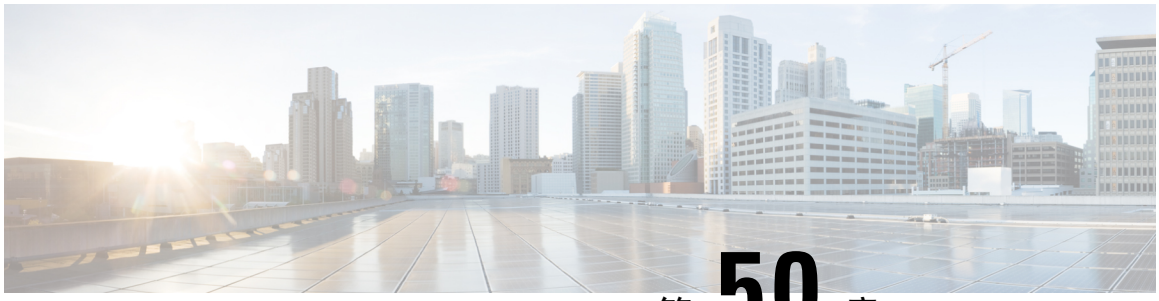
防火墙管理中心 型号	**Dynamic Attributes Connector** 连接器数量	最大下载用户数
FMC2800	20	150,000
FMC4600、FMC4700	30	600,000
FMC4800	30	600,000
Firewall Management Center Virtual （任何受支持的虚拟机监控程序）	10	50,000
Firewall Management Center Virtual 300（任何受支持的虚拟机监控程序）	20	150,000

[1]-防火墙管理中心 型号可能会终止销售。有关详细信息，请参阅生命周期终止和销售终止通知。

表 *116: Firewall Threat Defense*的并发用户登录的最大数量限制

Firewall Threat Defense 型号	并发用户登录的最大数量
Firewall Threat Defense Virtual 5、10、20、30、50（任何受支持的虚拟机监控程序）	50,000
Secure Firewall 220	10,000（见备注）
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130 Cisco Secure Firewall 3110、3120、3130、3140	50,000
Firepower 2140 Cisco Secure Firewall 3130、3140	150,000
Firepower 4140、 4145、 4150 Firepower 9300 Cisco Secure Firewall 4215	225,000
Cisco Secure Firewall 4225、4245	300,000
Cisco Secure Firewall 6160,6170	300,000

Secure Firewall 220 设备可下载累计总计 10,000 个用户 IP、SXP/SGT 映射、终端配置文件和动态对象。在总共下载 10,000 个对象后，Cisco Secure Firewall 220 会停止下载任何对象，直到删除之前的一些对象为止。（例如，如果用户注销，则内存可用于其他对象。）



第 50 章

领域

以下主题介绍领域和身份策略：

- 领域的许可证要求， 第 1993 页
- 领域的要求和先决条件， 第 1993 页
- 创建Microsoft Azure AD (SAML)领域， 第 1994 页
- 创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页
- 创建领域序列， 第 2039 页
- 将防火墙管理中心配置为跨域信任：设置， 第 2040 页
- 管理领域， 第 2048 页
- 比较领域， 第 2049 页
- 领域和用户下载故障排除， 第 2049 页
- 领域的历史记录， 第 2057 页

领域的许可证要求

威胁防御 许可证

任意

领域的要求和先决条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建Microsoft Azure AD (SAML)领域

您可以使用 Microsoft Azure Active Directory (AD)（现在称为 *Entra ID*）领域进行被动身份验证或主动身份验证。

如果启用了变更管理，则必须批准此程序中使用的所有证书。打开新故障单或编辑现有故障单。有关详细信息，请参阅创建变更管理工单 ， 第 162 页和。支持变更管理的策略和对象 ， 第 157 页

被动身份验证

被动身份验证发生在用户利用 Cisco ISE 进行身份验证时。

您有以下选项，具体取决于您选择的用户和组存储库：

- 要将 Cisco ISE 用作用户的存储库并使用 Entra ID 执行被动身份验证。有关详细信息，请参阅：
  - 关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE ， 第 1996 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ， 第 1996 页
- 要从 Entra ID 下载组。

  有关设置 Entra ID 的详细信息，请参阅 为被动身份验证配置 Microsoft Entra ID ， 第 1997 页。

主动身份验证

主动身份验证发生在用户通过预先配置的托管设备进行身份验证时。强制网络门户又称为主动身份验证。主动身份验证通常使用与被动身份验证相同的用户存储库（ISE/ISE-PIC TS 代理和 被动身份代理例外，它们仅是被动身份验证）。

要将 Microsoft Entra ID 用作强制网络门户，需要用户使用 Entra ID 进行身份验证。我们将领域称为安全断言标记语言 (SAML) 领域，因为 SAML 用于在以下各项之间建立信任关系：

- 服务提供商 （向其发送身份验证请求的 Cisco Secure Firewall Threat Defense 个设备）。
- 身份提供程序 (Microsoft Entra ID)。

SAML 是由 OASIS 标准机构开发的开放标准；有关详细信息，请参阅 SAML 概述。

有关详细信息，请参阅如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户） ， 第 2005 页。

如何为被动身份验证创建 Microsoft Azure AD (SAML)

本主题讨论创建Microsoft Azure AD (SAML)（现在称为 *Entra ID*）领域以用于 Secure Firewall Management Center 的被动身份验证的高级任务。

过程

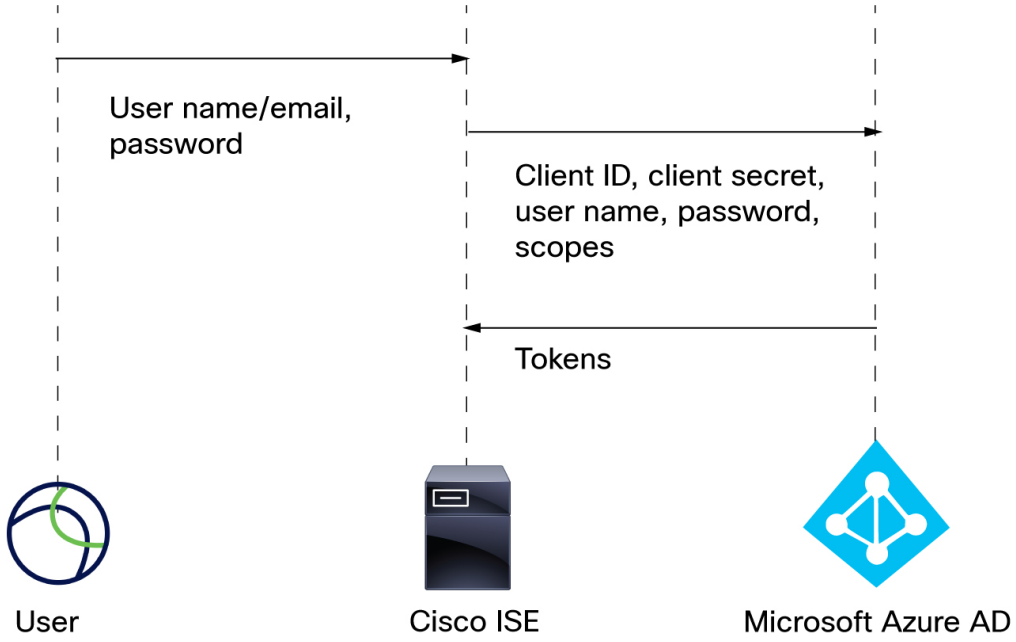
	命令或操作	目的
步骤 1	启用Dynamic Attributes Connector。	Dynamic Attributes Connector 要使用 Microsoft Azure AD (SAML) 领域。您可以先执行此操作，也可以在创建领域时启用它。有关详细信息，请参阅启用 dynamic attributes connector，第 2116 页。
步骤 2	配置 Microsoft Entra ID。	需要执行多项配置任务，包括设置事件中心、向应用授予访问 Microsoft Graph API 的权限以及启用审核日志。 请参阅为被动身份验证配置 Microsoft Entra ID，第 1997 页。
步骤 3	配置 Cisco ISE。	配置 ISE 的方式取决于用户对您的系统进行身份验证的方式。有关详细信息，请参阅如何为 Microsoft Azure AD (SAML) 配置Cisco ISE，第 1997 页。
步骤 4	创建 Cisco ISE 身份源。	身份源使 ISE 能够与 Secure Firewall Management Center通信。
步骤 5	获取配置 Microsoft Azure AD (SAML) 领域所需的信息。	此信息包括客户端和租户 ID、客户端密钥以及 Microsoft Entra ID 中存储的其他信息。
步骤 6	配置并验证您的领域。	在开始在访问控制策略中使用该领域的配置之前，请对其进行测试。 如创建Microsoft Azure AD (SAML)领域，第 1994 页中所述，创建 Microsoft Azure AD (SAML) 领域。
步骤 7	使用 Microsoft Azure AD (SAML) 领域创建访问控制策略和规则。	与其他类型的领域不同，您不需要创建身份策略或将身份策略与访问控制策略相关联。 请参阅创建基本访问控制策略，第 1708 页和创建和编辑访问控制规则，第 1764 页。

下一步做什么

请参阅关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE ，第 1996 页。

关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE

下图总结了具有 Cisco ISE 和资源拥有的密码凭证 (ROPC) 的 Azure AD（现在称为 *Entra ID*）领域：



使用 ROPC，

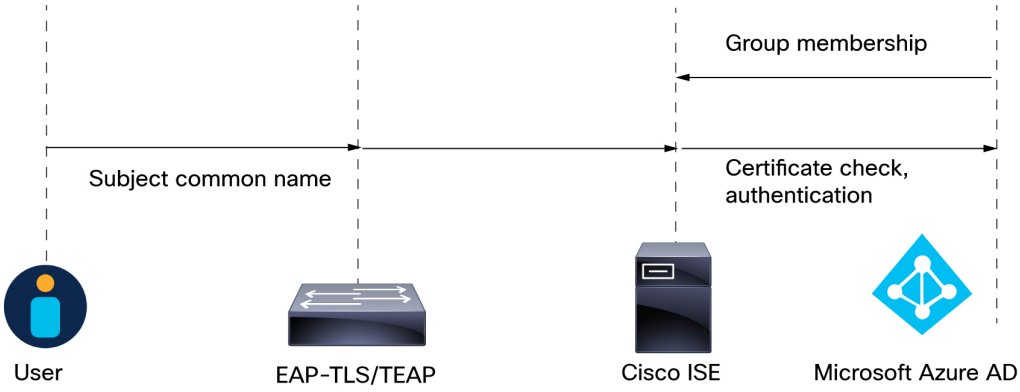
1. 用户使用 VPN 客户端（例如 Cisco Secure Client）使用用户名（或邮件地址）和密码登录。
2. 客户端 ID、客户端密钥、用户名、密码和范围将发送到 Entra ID。
3. 令牌从 Entra ID 发送到 Cisco ISE，然后将用户会话发送到 Secure Firewall Management Center。

有关配置 Cisco ISE 的详细信息，请参阅 使用 Azure Active Directory 配置 ISE 3.0 REST ID。

其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE

RFC7170定义的隧道可扩展身份验证协议 (TEAP) 可与 ISE 配合使用， Secure Firewall Management Center 如下所示：



以下内容基于 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS：

1. 用户的证书通过 EAP-TLS 或使用 EAP-TLS 作为内部方法的 TEAP 发送到 ISE。
2. ISE 评估用户的证书（有效期、受信任的证书颁发机构、证书吊销列表等）。
3. ISE 获取证书使用者名称 (CN) 并查询 Azure Graph API 以获取用户的组和其他属性。这被 Azure 称为用户主体名称 (UPN)。
4. ISE 授权策略根据从 Azure 返回的用户属性进行评估。

如何为 Microsoft Azure AD (SAML) 配置Cisco ISE

在 Microsoft Azure AD (SAML)（现在称为 *Entra ID*）领域，ISE 负责向 Secure Firewall Management Center 发送用户会话（登录、注销）。本主题讨论如何设置 ISE 以便与 Azure AD 领域配合使用。

资源拥有的密码凭证身份验证

要在资源所有者密码凭证 (ROPC) 的帮助下，通过具象状态传输 (REST) 身份 (ID) 服务将 ISE 与 Microsoft Azure AD (SAML) 配合使用，请参阅使用 Azure Active Directory 配置 ISE 3.0 REST ID。

TEAP/EAP-TLS

要将 ISE 与基于 Azure AD 组成员身份和其他用户属性的授权策略配合使用，并将 EAP-TLS 或 TEAP 作为身份验证协议，请参阅 使用 Microsoft Azure Active Directory 配置思科 ISE 3.2 EAP-TLS。

后续操作

获取 Microsoft Azure AD (SAML) 领域所需的信息， 第 2000 页

为被动身份验证配置 Microsoft Entra ID

本主题提供有关如何将 Microsoft Entra ID（之前称为 *Microsoft Azure Active Directory (AD)*）设置为可与 Secure Firewall Management Center 配合使用的领域的基本信息。我们希望您已经熟悉 Entra ID；否则，请在开始之前查阅文档或支持资源。

为您的应用授予 Microsoft Graph 权限

如 Microsoft 站点上的授权和 Microsoft Graph 安全 API 中所述，向 Entra ID 应用授予 Microsoft Graph 的以下权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限让 Secure Firewall Management Center 能够首次从 Entra ID 下载用户和组。

对于在 Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。Secure Firewall Management Center 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

重要事项 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

对于在 Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

为 Entra ID 配置 Cisco ISE

要将用户会话信息发送到 Secure Firewall Management Center，请按照使用 Azure Active Directory 配置 ISE 3.0 REST ID 中的说明为 Entra ID 配置 Cisco ISE。

后续操作

请参阅如何为 Microsoft Azure AD (SAML) 配置Cisco ISE，第 1997 页。

配置 Entra ID 基本设置

为您的应用授予 Microsoft Graph 权限

如 Microsoft 站点上的授权和 Microsoft Graph 安全 API 中所述，向您的 Entra ID 应用（原名为 *Azure AD*）授予 Microsoft Graph 的以下权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限让 防火墙管理中心 能够首次从 Entra ID 下载用户和组。

对于在 防火墙管理中心 中设置 Entra ID 领域，此步骤所需的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。防火墙管理中心 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

重要事项 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

对于在 Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

获取 Microsoft Azure AD (SAML) 领域所需的信息

此任务说明如何获取在 Secure Firewall Management Center 中设置 Microsoft Azure AD (SAML)（现在称为 *Entra ID*）领域。在设置 Microsoft Azure AD 时，您可能已经获取了这些信息，如为被动身份验证配置 Microsoft Entra ID，第 1997 页中所述。

过程

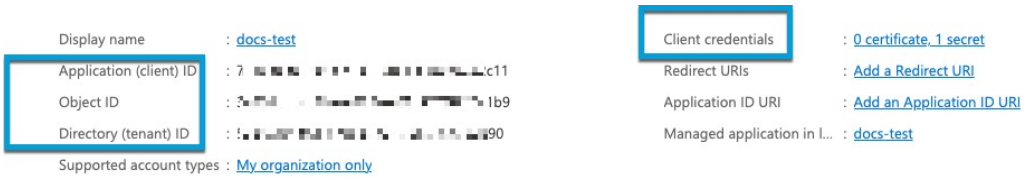
步骤 1 以至少具有产品设计师角色的用户身份登录 https://portal.azure.com/。

步骤 2 在页面顶部，点击 **Microsoft Entra ID**。

步骤 3 在左侧列中，点击**应用注册 (App Registrations)**。

步骤 4 如有必要，过滤显示的应用列表以便显示要使用的应用。

步骤 5 点击应用的名称。



步骤 6 点击此页面上以下值旁边的 **复制** ()，然后将这些值粘贴到文本文件中。

- **应用（客户端）ID**
- **目录（租户）ID**

步骤 7 点击**客户端凭证 (Client Credentials)**。

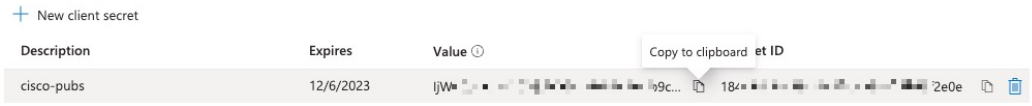
步骤 8 除非您已经知道客户端密钥值 （而不是客户端密钥 *ID*），否则必须按如下方式创建新的客户端密钥：

a) 点击**新建客户端密钥 (New Client Secret)**。

b) 在提供的字段中输入要求的信息。

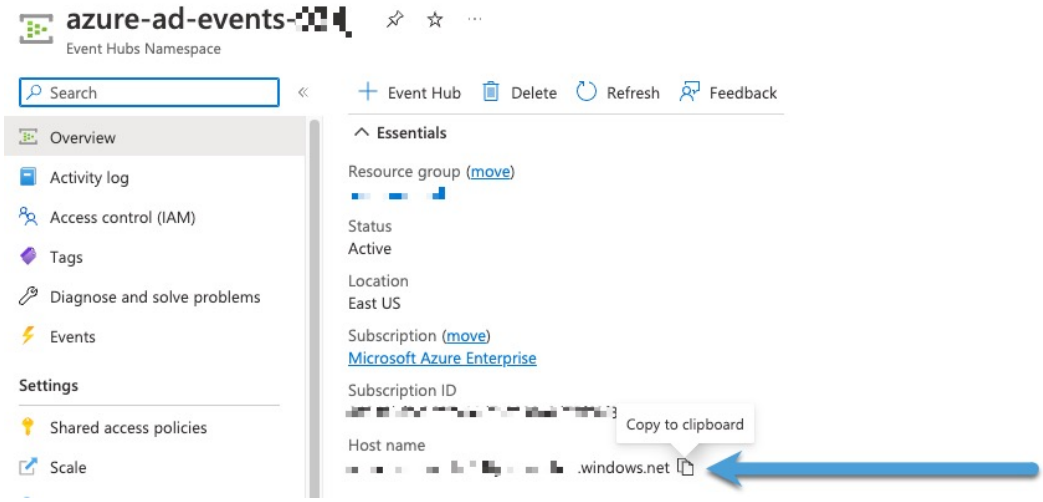
c) 点击**添加 (Add)**。

d) 点击 Value 旁边的 **复制** ()，如下图所示。



步骤 9 在 https://portal.azure.com/ 中，点击**事件中心 (Event Hubs)** > （**事件中心的名称**）。

步骤 10 在右侧窗格中，点击 **主机名 (Host name)** 值旁边的 **复制** (⧉) 并将值粘贴到剪贴板。这是事件中心主机名。

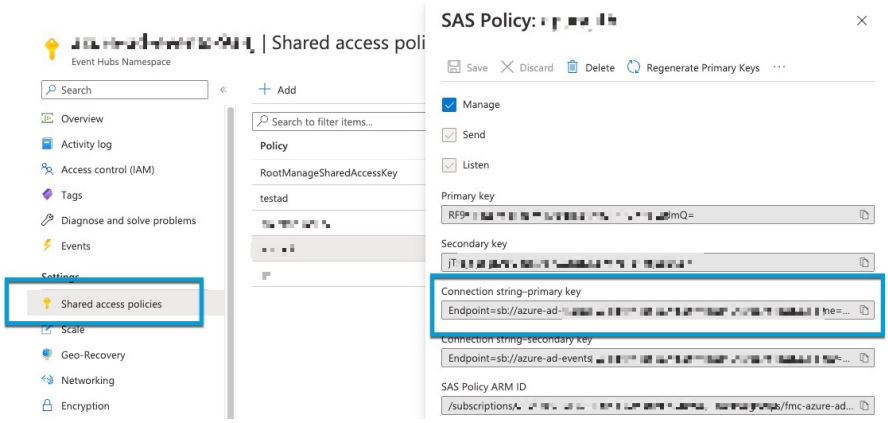


步骤 11 记下事件中心的名称或将其复制到文本文件（与页面顶部的**事件中心命名空间 (Event Hubs Namespace)** 相同）。

步骤 12 在左侧窗格中的设置下，点击**共享访问策略 (Shared access policies)**。

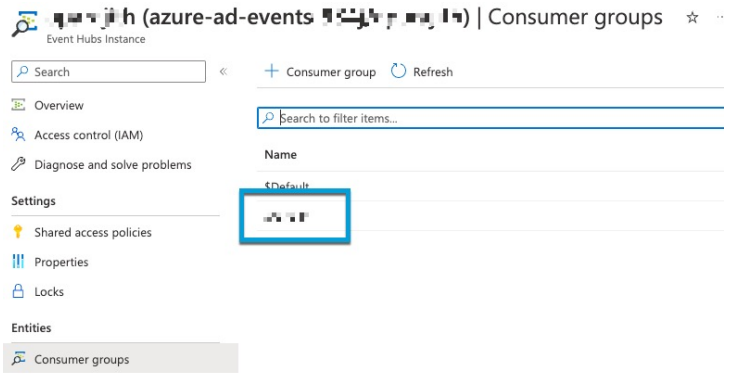
步骤 13 点击策略名称。

步骤 14 点击**连接字符串 - 主键 (Connection string-primary key)** 旁边的 **复制** (⧉)。



步骤 15 点击 **概述 (Overview)** > **实体 (Entities)** > **事件中心 (Event Hubs)** > （事件中心的名称） > **实体 (Entities)** > **使用者组 (Consumer Groups)**。

记下以下值或将其复制到剪贴板。这是您的使用者组名称。



步骤 16 在左侧窗格中点击**概览 (Overview)**。

步骤 17 点击**命名空间 (Namespace)** 旁边的 **复制** ()。



这是事件中心主题名称。

为被动身份验证创建Microsoft Azure AD (SAML)领域

以下主题讨论如何运行为被动身份验证创建 Microsoft Azure AD (SAML)（现在称作 *Entra ID*）领域所需的多步向导。

您可以将 Microsoft Azure Active Directory (AD) 领域与 Cisco ISE 配合使用来对用户进行身份验证并获取用户会话以进行用户控制。我们从 Entra ID 获取组，从 Cisco ISE 获取登录用户会话数据。

您有以下选择：

- 资源拥有的密码凭证 (ROPC)：使用户能够使用用户名和密码通过 Cisco Secure Client 等客户端登录。ISE 将用户会话发送到 Secure Firewall Management Center。有关详细信息，请参阅关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE ，第 1996 页。

  其他资源：learn.microsoft.com 上的 Microsoft 身份平台和 OAuth 2.0 资源所有者密码凭证 。

- 可扩展身份验证协议 (EAP) 链与基于隧道的可扩展身份验证协议 (TEAP) 和传输层安全 (TLS)，缩写为 EAP/TEAP-TLS：TEAP 是一种基于隧道的 EAP 方法，可建立安全隧道并执行其他 EAP 方法在该安全隧道的保护下。ISE 用于验证用户凭证并将用户会话发送到 Secure Firewall Management Center。有关详细信息，请参阅关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ，第 1996 页。

要配置领域，请按以下顺序完成所有任务：

1. 配置 Entra ID 基本设置，第 1999 页。

2. 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息，第 2000 页 中所述。
3. Microsoft Azure AD (SAML)领域：SAML 详细信息，第 2003 页。

Microsoft Azure AD (SAML)领域：SAML 详细信息

此任务讨论创建 Microsoft Azure AD (SAML) 领域的多步骤向导中的第一步。您必须完成向导中的所有步骤才能设置领域。根据您创建的领域是用于主动身份验证还是被动身份验证，这些步骤会有所不同。

开始之前

在创建领域之前，请完成以下所有任务：

- （仅使用 Cisco ISE 进行被动身份验证。）如果您使用 Cisco ISE 作为用户和组的存储库，请设置 ISE：
  - 关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE，第 1996 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE，第 1996 页
- 要将 Entra ID 用作用户和组的存储库，请参阅为被动身份验证配置 Microsoft Entra ID，第 1997 页。
- 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息，第 2000 页中所述。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 点击 **添加领域** > **SAML - Azure AD**。

步骤 4 输入以下信息。

项目	说明
名称	用于标识领域的唯一名称。
说明	（可选。）领域的描述。
身份提供程序	始终显示 **Azure AD**。

项目	说明
配置类型	点击以下选项之一： • **使用 ISE 进行被动身份验证，以**进行被动身份验证。 • **使用 Azure AD 的被动身份验证或强制网络门户**，以便将 Entra ID 用作被动身份验证或主动身份验证的用户存储（即，强制网络门户）。

步骤 5 点击**下一步 (Next)**。

下一步做什么

以下项之一：

- 被动身份验证：Microsoft Azure AD (SAML) 领域：Azure AD 详细信息，第 2004 页。
- 主动身份验证：Microsoft Azure AD (SAML)领域：SAML 服务提供商 (SP) 元数据，第 2016 页

Microsoft Azure AD (SAML) 领域：Azure AD 详细信息

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

过程

步骤 1 从向导中的上一步继续操作。

步骤 2 输入以下信息。

项目	说明
名称	输入可标识领域的唯一名称。
客户端密钥 **租户 ID** **事件中心主机名** **事件中心名称** **事件中心连接字符串**	输入您找到的信息，如中所述： • 被动身份验证：如何为被动身份验证创建 Microsoft Azure AD (SAML)，第 1995 页 • 主动身份验证：获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 2011 页
（可选。）**用户组**	滑动到 **滑块已启用** () 以指定要包含在策略中或从策略中排除的组。
（可选。）**排除的用户组**	如果在此字段中输入一个或多个组名称，则为 它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。 每行输入一个组名，后跟一个换行符。组名区分大小写。

项目	说明
（可选。）**包含的用户组**	如果在此字段中输入一个或多个组名称，则为 只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。 每行输入一个组名，后跟一个换行符。组名区分大小写。 建议您使用“包含的用户组”字段，仅下载您打算使用Cisco Secure Firewall监控的组。

步骤 3 点击**测试 (Test)**。
在继续下一步之前，请确保测试连接成功。

步骤 4 点击**下一步 (Next)**。

Microsoft Azure AD (SAML) 领域：用户会话超时

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

此选项设置系统终止非活动会话之前的秒数。

过程

步骤 1 从向导中的上一步继续操作。

步骤 2 输入以下信息。

项目	说明
ISE 用户	默认为 1440 秒（24 小时）。
强制网络门户用户	默认为 1440 秒（24 小时）。

超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则防火墙管理中心会将该用户视为未知（**失败的强制网络门户用户**除外）。

步骤 3 点击**保存**。

如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）

本主题讨论创建用于 Secure Firewall Management Center 的 Microsoft Azure Active Directory (AD) 领域（现在被称作*Entra ID*）的高级任务。

开始之前

如果启用了“更改管理”(hange Management)，则必须为以下每个对象打开或编辑、分配和批准票单，然后才能创建领域：

- 基本 URL
- 服务提供商证书注册（PKCS12 格式）
- 身份供应商证书注册（手动格式）
- 领域本身（创建并分配通知单，直到领域创建完成，然后批准它）

有关详细信息，请参阅为配置更改开单，第 163 页和支持变更管理的策略和对象，第 157 页。

过程

	命令或操作	目的
步骤 1	使用 DNS 服务器创建完全限定的主机名 (FQDN) 并将 Firewall Threat Defense 的内部证书上传至 Secure Firewall Management Center。如果您之前从未使用过例如 此类 资源，可以咨询此类资源。在 Secure Firewall Management Center 托管的一台设备上指定路由接口的 IP 地址。	请参阅 DNS 服务器参考。
步骤 2	启用Dynamic Attributes Connector。	要使用 Microsoft Azure AD 领域， Dynamic Attributes Connector 为必填项。您可以先执行此操作，也可以在创建领域时启用它。有关详细信息，请参阅启用 dynamic attributes connector，第 2116 页。
步骤 3	使用关联的内部证书创建网络对象。	请参阅创建网络对象，第 2660 页。
步骤 4	获取签名证书并将其上传到将向其发送 Entra ID 身份验证请求的 Cisco Secure Firewall Threat Defense。	该证书应由受信任的证书颁发机构 (CA) 签署并以**.p12**以下格式（也称为PKCS#12；另请参阅 ssl.com 上的这篇文章）交付给您。 有关背景信息，请参阅 Cisco Secure Firewall Management Center 设备配置指南 或 stackoverflow.com中有关公钥基础设施的部分。 上传签名证书，请参阅使用 PKCS12 文件安装证书，第 2751 页。
步骤 5	配置 Microsoft Entra ID 基本设置。	需要执行多项配置任务，包括设置事件中心、向应用授予访问 Microsoft Graph API 的权限以及启用审核日志。

	命令或操作	目的
		请参阅配置 Entra ID 基本设置，第 1999 页。
步骤 6	在 Azure AD 中创建单点登录 (SSO) 应用。	SSO 应用使请求访问受保护网络资源的用户能够使用 Entra ID 进行身份验证。SSO 应用具有可用于简化领域创建的联合 XML，以及 Cisco Secure Firewall Threat Defense 使用 Entra ID 进行安全身份验证所需的身份提供程序证书。 请参阅在 Entra ID 中创建单点登录 (SSO) 应用，第 2009 页。
步骤 7	获取配置 Microsoft Azure AD (SAML) 领域所需的信息。	此信息包括客户端和租户 ID、客户端密钥以及 Microsoft Entra ID 中存储的其他信息。 请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息，第 2000 页。
步骤 8	使用 Azure 身份验证服务的**解密 - 重新签名**规则配置 a 解密策略，以便用户可以使用 HTTPS 协议访问网页。	只有在将 HTTPS 流量发送到领域之前，Microsoft Azure AD (SAML) 领域才能对用户进行身份验证。Microsoft Azure AD (SAML) 领域本身被系统视为 **Azure 身份验证服务** 应用。 创建具有“解密-重新签名”操作的解密规则，第 2010 页。
步骤 9	使用主动身份验证规则创建身份策略。	在使用 Microsoft Azure AD (SAML) 领域执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。 有关详细信息，请参阅创建身份策略，第 2213 页。
步骤 10	使用 Microsoft Azure AD 领域创建访问控制策略和规则。	与其他类型的领域不同，您不需要创建身份策略或将身份策略与访问控制策略相关联。 请参阅创建基本访问控制策略，第 1708 页和创建和编辑访问控制规则，第 1764 页。
步骤 11	将身份和 解密策略 与第 3 步的访问控制策略相关联。	这是最后一步，此后系统即可使用 Microsoft Azure AD (SAML) 领域进行用户身份验证。 有关详细信息，请参阅将其他策略与访问控制相关联，第 1719 页。

下一步做什么

请参阅配置 Entra ID 基本设置，第 1999 页。

配置 Entra ID 基本设置

为您的应用授予 Microsoft Graph 权限

如 Microsoft 站点上的授权和 Microsoft Graph 安全 API 中所述，向您的 Entra ID 应用（原名为 *Azure AD*）授予 Microsoft Graph 的以下权限：

- Reader role
- User.Read.All permission
- Group.Read.All permission

此权限让 防火墙管理中心 能够首次从 Entra ID 下载用户和组。

对于在 防火墙管理中心 中设置 Entra ID 领域，此步骤所需的信息：

- 您注册的应用的名称
- **应用（客户端）ID**
- **客户端密钥**
- **目录（租户）ID**

设置事件中心

按照 Microsoft 站点上的快速入门：使用 Azure 门户创建事件中心中的说明来设置事件中心。防火墙管理中心 会使用事件中心审核日志为用户和组下载定期更新。

详细信息： Azure 事件中心的功能和术语

重要事项 您必须选择**标准**或更好的定价层。如果选择 **基础**，则无法使用该领域。

对于在 Secure Firewall Management Center 中设置 Entra ID 领域，此步骤所需的信息：

- 命名空间**名称**
- **连接字符串 - 主键**
- 事件中心**名称**
- 使用者组**名称**

启用审核日志

启用审核日志，如 Microsoft 站点上的教程：将 Azure Active Directory 日志传输到 Azure 事件中心中所述。

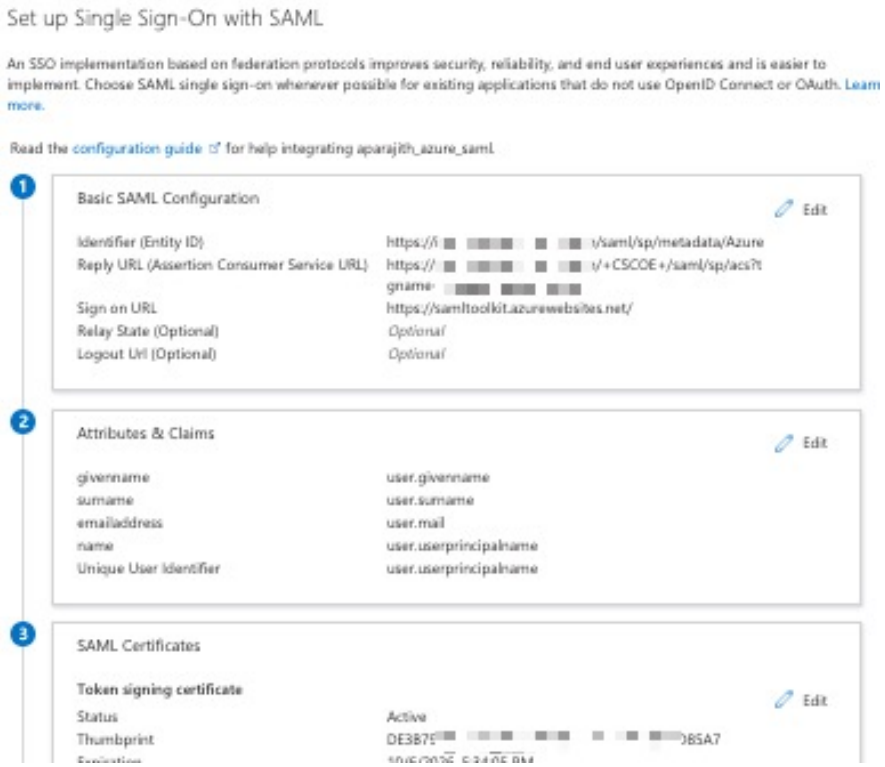
在 Entra ID 中创建单点登录 (SSO) 应用

本主题讨论当网络用户尝试访问受保护的网络时，如何在 Microsoft Entra ID 中创建应用来处理来自 Entra ID 的单点登录 (SSO)。

创建应用

在 Microsoft Entra ID 门户中，点击主页上的**企业应用**，然后按照 learn.microsoft.com 上配置 Microsoft Entra SSO 中的说明进行操作。

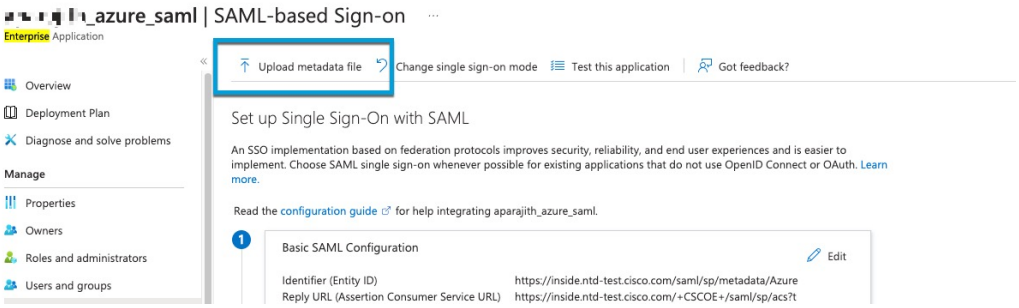
下图显示了 SSO 应用配置的一部分。配置 Microsoft Azure AD (SAML) 领域时，必须在此页面上提供一些信息。有关详细信息，请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 2011 页。



（可选。）上传服务提供程序元数据

如果您已配置 Microsoft Azure AD (SAML) 领域，请点击页面顶部的上传元数据文件，以快速提供 SSO 应用的配置值。

下图显示了一个示例。



将用户和组添加到 SSO 应用

按照learn.microsoft.com 上 的将用户账号添加到企业应用 中所述，将用户和组添加到您的应用

后续操作

请参阅获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 2011 页。

创建具有“解密-重新签名”操作的解密规则

程序的此部分介绍如何创建 a 解密策略，以在流量到达 SAML 领域之前解密和重签流量。领域仅可对解密的流量进行身份验证。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 如果尚未进行此操作，则请创建内部证书授权对象，以 TLS/SSL 流量进行解密，如PKI，第 2661 页中所述。

步骤 3 请点击 **策略** > **安全策略** > **解密**。

步骤 4 点击**新建策略 (New Policy)**。

步骤 5 为策略输入**名称**，然后选择**默认操作**。默认操作将在基于规则的解密策略默认操作，第 1899 页中讨论。

步骤 6 点击**保存**。

步骤 7 点击**添加规则 (Add Rule)**。

步骤 8 为规则输入**名称 (Name)**。

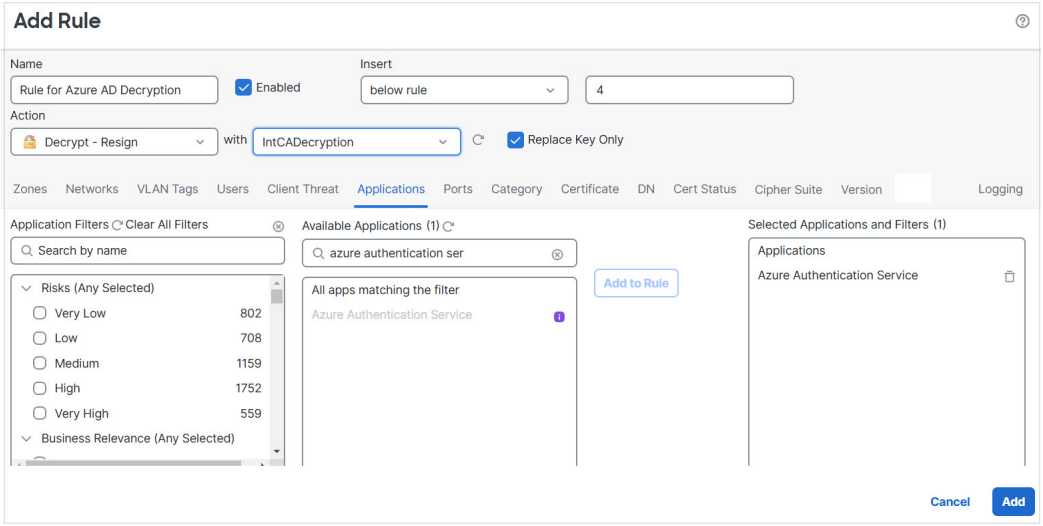
步骤 9 从**操作**列表中，选择**解密 - 放弃**。

步骤 10 从**通过 (with)** 列表中，选择您的服务提供商证书对象。

步骤 11 点击**应用 (Applications)** 选项卡页面。

步骤 12 在可用应用部分，搜索 **Azure Authentication Service** 。

步骤 13 点击 **Azure 身份验证 (Azure Authentication)**，然后点击**添加到规则 (Add to Rule)**。
下图显示了一个示例。



步骤 14 （可选。）设置其他选项，如解密规则基于规则的解密规则 条件，第 1920 页中所述。

步骤 15 点击**添加 (Add)**。

步骤 16 在该页面顶部，点击**保存**。

下一步做什么

获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证）

此任务说明如何获取在防火墙管理中心 中设置 Microsoft Azure AD (SAML) 领域所需的信息 （现在被称作 *Entra ID*）。

过程

步骤 1 以至少具有产品设计师角色的用户身份登录 https://portal.azure.com/。

步骤 2 在页面顶部，点击 **Microsoft Entra ID**。

步骤 3 在左侧列中，点击**应用注册 (App Registrations)**。

步骤 4 如有必要，过滤显示的应用列表以便显示要使用的应用。

步骤 5 点击应用的名称。



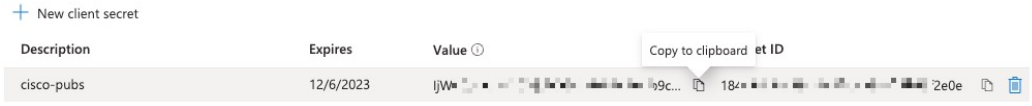
步骤 6 点击此页面上以下值旁边的 **复制** ( )，然后将这些值粘贴到文本文件中。

- 应用（客户端）ID
- 目录（租户）ID

步骤 7 点击**客户端凭证 (Client Credentials)**。

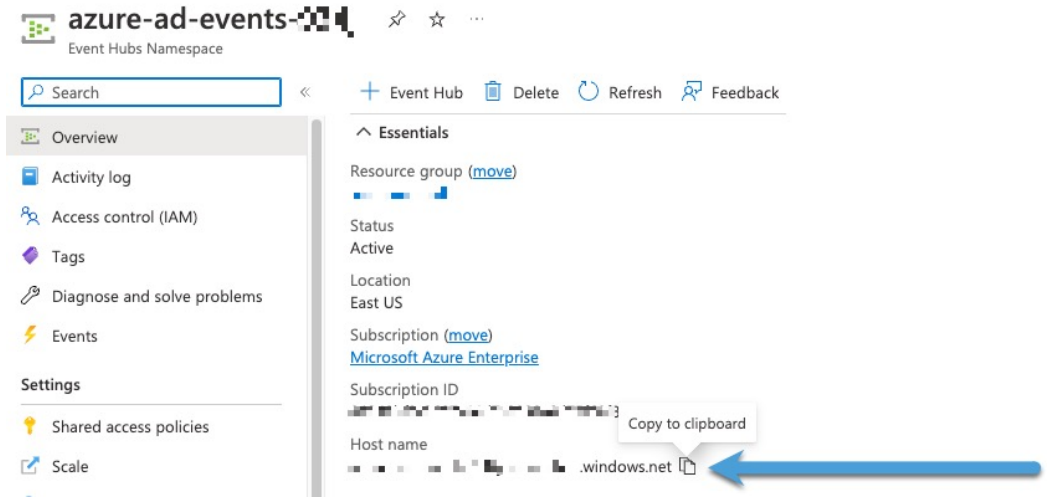
步骤 8 除非您已经知道客户端密钥值 （而不是客户端密钥 *ID*），否则必须按如下方式创建新的客户端密钥：

a) 点击**新建客户端密钥 (New Client Secret)**。
b) 在提供的字段中输入要求的信息。
c) 点击**添加 (Add)**。
d) 点击 Value 旁边的 **复制** ()，如下图所示。



步骤 9 在 https://portal.azure.com/ 中，点击**事件中心 (Event Hubs)** > （**事件中心的名称**）。

步骤 10 在右侧窗格中，点击 **主机名 (Host name)** 值旁边的 **复制** () 并将值粘贴到剪贴板。这是事件中心主机名。

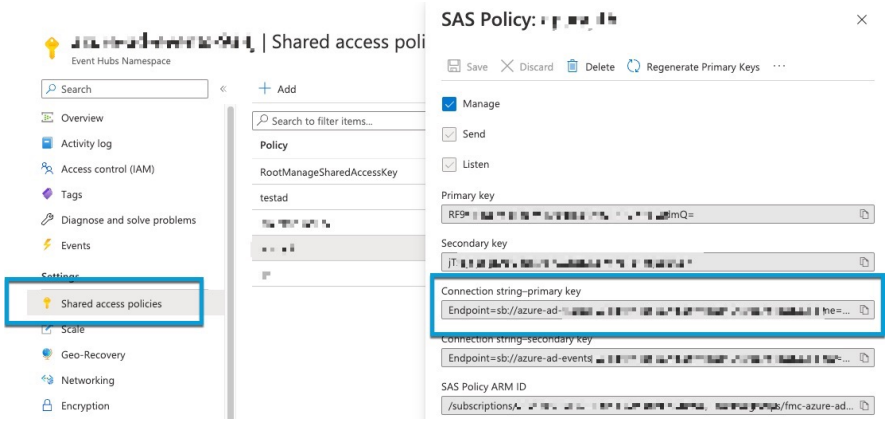


步骤 11 记下事件中心的名称或将其复制到文本文件（与页面顶部的**事件中心命名空间 (Event Hubs Namespace)** 相同）。

步骤 12 在左侧窗格中的设置下，点击**共享访问策略 (Shared access policies)**。

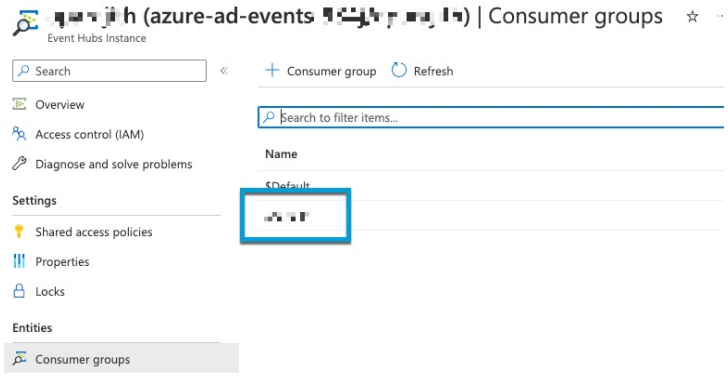
步骤 13 点击策略名称。

步骤 14 点击**连接字符串 - 主键 (Connection string-primary key)** 旁边的 **复制** ()。



步骤 15 点击 **概述 (Overview)** > **实体 (Entities)** > **事件中心 (Event Hubs)** > （事件中心的名称） > **实体 (Entities)** > **使用者组 (Consumer Groups)**。

记下以下值或将其复制到剪贴板。这是您的使用者组名称。



步骤 16 在左侧窗格中点击**概览 (Overview)**。

步骤 17 点击**命名空间 (Namespace)** 旁边的 **复制** ()。



这是事件中心主题名称。

步骤 18 返回主页并在必要时登录：https://portal.azure.com/#home。

步骤 19 点击 **Microsoft Entra ID**。

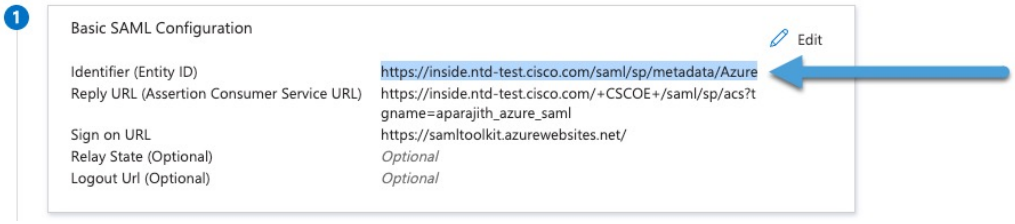
步骤 20 在左侧窗格中，点击**企业应用 (Enterprise Applications)**。

步骤 21 如有必要，请过滤应用列表以查找您的应用。

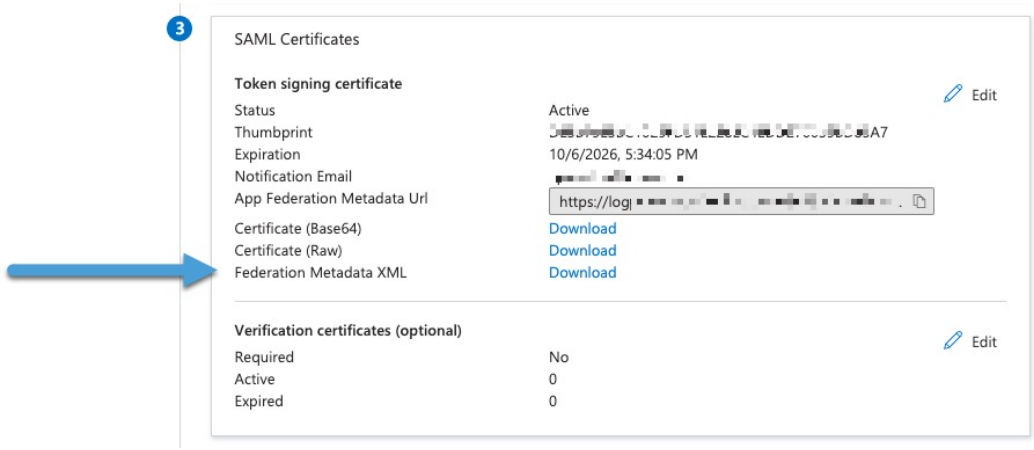
步骤 22 点击企业应用的名称。

步骤 23 点击“设置单点登录 (Set up single sign on)”下的 **启动 (Get Started)** 。

步骤 24 在 SSO 应用页面上，将标识符（实体 ID）的值复制到剪贴板。
下图显示了一个示例。

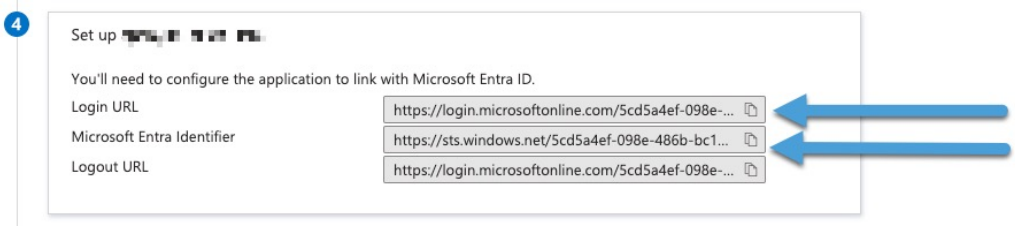


步骤 25 在 SSO 应用页面上，点击联合元数据 XML 旁边的**下载 (Download)** 链接，如下图所示。
下图显示了一个示例。



步骤 26 如果您已经设置了 SSO 应用，可以在此处停止。联合元数据 XML 包含在 Secure Firewall Management Center中配置身份提供程序所需的所有信息。

步骤 27 （如果已下载联合 XML，则可选。）点击以下两个值旁边的 **复制** (⧉) 并将其保存到文本文件。
下图显示了一个示例。



下一步做什么

请参阅创建具有“解密-重新签名”操作的解密规则，第 2010 页。

创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户）

以下主题讨论如何运行为主动身份验证创建 Microsoft Entra ID 领域所需的多步骤向导。

在主动身份验证（也称为强制网络门户）中，Microsoft Azure AD 是用户存储。当用户尝试访问访问控制规则中定义的受保护资源时，用户必须先通过 Microsoft Entra ID 进行身份验证。

要配置领域，请按以下顺序完成所有任务：

1. 配置 Entra ID 基本设置， 第 1999 页。
2. 在 Entra ID 中创建单点登录 (SSO) 应用， 第 2009 页。
3. 获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证）， 第 2011 页

Microsoft Azure AD (SAML)领域：SAML 详细信息

此任务讨论创建 Microsoft Azure AD (SAML) 领域的多步骤向导中的第一步。您必须完成向导中的所有步骤才能设置领域。根据您创建的领域是用于主动身份验证还是被动身份验证，这些步骤会有所不同。

开始之前

在创建领域之前，请完成以下所有任务：

- （仅使用 Cisco ISE 进行被动身份验证。）如果您使用 Cisco ISE 作为用户和组的存储库，请设置 ISE：
  - 关于具有资源拥有的密码凭证的 Entra ID 和Cisco ISE ， 第 1996 页
  - 关于使用 TEAP/EAP-TLS 的 Entra ID 和 Cisco ISE ， 第 1996 页
- 要将 Entra ID 用作用户和组的存储库，请参阅为被动身份验证配置 Microsoft Entra ID， 第 1997 页。
- 获取您的领域所需的信息，如 获取 Microsoft Azure AD (SAML) 领域所需的信息， 第 2000 页中所述。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 点击 **添加领域** > **SAML - Azure AD**。

步骤 4 输入以下信息。

项目	说明
名称	用于标识领域的唯一名称。
说明	（可选。）领域的描述。
身份提供程序	始终显示 **Azure AD**。

项目	说明
配置类型	点击以下选项之一： • **使用 ISE 进行被动身份验证，以**进行被动身份验证。 • **使用 Azure AD 的被动身份验证或强制网络门户**，以便将 Entra ID 用作被动身份验证或主动身份验证的用户存储（即，强制网络门户）。

步骤 5 点击**下一步 (Next)**。

下一步做什么

以下项之一：

- 被动身份验证：Microsoft Azure AD (SAML) 领域：Azure AD 详细信息，第 2004 页。
- 主动身份验证：Microsoft Azure AD (SAML)领域：SAML 服务提供商 (SP) 元数据，第 2016 页

Microsoft Azure AD (SAML)领域：SAML 服务提供商 (SP) 元数据

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

开始之前

完成 Microsoft Azure AD (SAML)领域：SAML 详细信息，第 2003 页中讨论的任务

过程

步骤 1 继续 Microsoft Azure AD (SAML)领域：SAML 详细信息，第 2003 页。

步骤 2 输入以下信息。

项目	说明
基本 URL	从列表中，点击之前创建的网络对象。网络用户在尝试访问受保护的网络资源时会被定向到此 URL。 您也可以点击 **添加** (+) 立即创建对象。
实体 ID	SSO 应用的实体 ID。
断言使用者服务 (ACS) URL	根据之前的值自动生成。

项目	说明
服务提供程序证书	从列表中，点击要用于解密对 Cisco Secure Firewall Threat Defense 的请求的证书。 您也可以点击 添加 (+) 立即创建对象。
下载服务提供程序元数据	（可选。）下载与服务提供商（即托管设备）关联的元数据，以简化 Microsoft Entra ID SSO 应用的配置。

步骤 3 点击下一步 **(Next)**。

下一步做什么

Microsoft Azure AD (SAML)领域：SAML 身份提供程序 (IdP) 元数据，第 2017 页。

Microsoft Azure AD (SAML)领域：SAML 身份提供程序 (IdP) 元数据

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

开始之前

完成 Microsoft Azure AD (SAML)领域：SAML 服务提供商 (SP) 元数据，第 2016 页中讨论的任务。

过程

步骤 1 继续 Microsoft Azure AD (SAML)领域：SAML 服务提供商 (SP) 元数据，第 2016 页。

步骤 2 如果您之前下载了 Entra ID SSO 应用的联合 XML，请点击**上传 XML** 并立即上传。然后您可以跳过此步骤。

步骤 3 输入以下信息。

项目	说明
实体 ID	输入身份提供程序的实体 ID。
单点登录 (SSO) URL	输入应用的 SSO URL。
IdP 证书	从列表中，点击要用于 Microsoft Entra ID 身份验证的证书。 您也可以点击 添加 (+) 立即创建对象。

步骤 4 点击下一步 **(Next)**。

下一步做什么

Microsoft Azure AD (SAML)领域：SAML 详细信息，第 2003 页。

Microsoft Azure AD (SAML) 领域：Azure AD 详细信息

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

过程

步骤 1 从向导中的上一步继续操作。

步骤 2 输入以下信息。

项目	说明
名称	输入可标识领域的唯一名称。
客户端密钥 租户 ID 事件中心主机名 事件中心名称 事件中心连接字符串	输入您找到的信息，如中所述： • 被动身份验证：如何为被动身份验证创建 Microsoft Azure AD (SAML)，第 1995 页 • 主动身份验证：获取 Microsoft Azure AD (SAML) 领域所需的信息（仅限主动身份验证），第 2011 页
（可选。）用户组	滑动到 滑块已启用 ( ) 以指定要包含在策略中或从策略中排除的组。
（可选。）排除的用户组	如果在此字段中输入一个或多个组名称，则为 它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。 每行输入一个组名，后跟一个换行符。组名区分大小写。
（可选。）包含的用户组	如果在此字段中输入一个或多个组名称，则为 只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。 每行输入一个组名，后跟一个换行符。组名区分大小写。 建议您使用“包含的用户组”字段，仅下载您打算使用 Cisco Secure Firewall 监控的组。

步骤 3 点击测试 **(Test)**。
在继续下一步之前，请确保测试连接成功。

步骤 4 点击下一步 **(Next)**。

Microsoft Azure AD (SAML) 领域：用户会话超时

此任务讨论了多页向导中的一页，使您能够创建 Microsoft Azure AD (SAML) 领域。

此选项设置系统终止非活动会话之前的秒数。

过程

步骤 1 从向导中的上一步继续操作。

步骤 2 输入以下信息。

项目	说明
ISE 用户	默认为 1440 秒（24 小时）。
强制网络门户用户	默认为 1440 秒（24 小时）。

超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则防火墙管理中心会将该用户视为未知（**失败的强制网络门户用户**除外）。

步骤 3 点击**保存**。

创建 LDAP 领域或 Active Directory 领域和领域目录

如果要设置没有领域的 ISE/ISE-PIC，请注意，存在会影响 Secure Firewall Management Center用户查看方式的用户会话超时。有关详细信息，请参阅领域字段，第 2029 页。

通过以下程序，您可以创建 领域 （ 防火墙管理中心 与 Active Directory 目录领域之间的连接）和 目录 （ 防火墙管理中心 与 LDAP 服务器或 Active Directory 域控制器之间的连接）。

（推荐。）要从 防火墙管理中心 安全连接到 Active Directory 服务器，请先执行以下任务：

- 导出 Active Directory 服务器的根证书，第 2036 页
- 查找 Active Directory 服务器名称，第 2035 页

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

有关领域目录配置字段的详细信息，请参阅领域字段，第2029页和领域目录和同步字段，第2032页。

将防火墙管理中心配置为跨域信任：设置，第2040页中显示了使用跨域信任设置领域的分步示例。

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

如果要设置没有领域的 ISE/ISE-PIC，请注意，存在会影响 Secure Firewall Management Center用户查看方式的用户会话超时。有关详细信息，请参阅领域字段，第 2029 页。

开始之前

如果您对强制网络门户使用 Kerberos 身份验证，请在开始之前参阅以下部分：Kerberos 身份验证的必备条件，第 2029 页。

如果启用了“更改管理”(hange Management)，则必须为以下每个对象打开或编辑、分配和批准票单，然后才能创建领域：

- 如果要安全连接 Microsoft AD 或 LDAP，服务器的受信任证书颁发机构
- 领域本身

有关详细信息，请参阅为配置更改开单，第 163 页和支持变更管理的策略和对象，第 157 页。

重要事项 要减少 Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 要创建新领域，请从**添加领域 (Add Realm)** 下拉列表中选择。

步骤 4 要执行其他任务（如启用、禁用或删除领域），请参阅管理领域，第 2048 页。

步骤 5 按照领域字段，第 2029 页中的描述输入领域信息。

步骤 6 在目录服务器配置部分中，输入目录信息，如 领域目录和同步字段，第 2032 页中所述。

步骤 7 （可选。）要为此领域配置其他域，请点击**添加其他目录 (Add another directory)**。

步骤 8 点击**配置组和用户 (Configure Groups and Users)**。
输入以下信息：

信息	说明
AD 主域 (AD Primary Domain)	用于需要对用户进行身份验证的 Active Directory 服务器的域。有关其他信息，请参阅领域字段，第 2029 页。 您必须使用域的原始域名而不是该域的任何备用用户主体名称 (UPN) 后缀创建领域。否则，用户和组将无法下载，并且身份策略不会实施。例如，如果原始域为 `domain.example.com`，备用 UPN 名称为 `domain2.mydomain.com`，则必须将领域配置为使用 `domain.example.com`。有关配置备用 UPN 后缀的详细信息，请参阅 learn.microsoft.com 上的配置备用登录 ID 等资源。
基本 DN	防火墙管理中心应在其上开始搜索用户数据的服务器上的目录树。
组 DN (Group DN)	防火墙管理中心 应在其上开始搜索组数据的服务器上的目录树。
加载组	点击以从 Active Directory 服务器加载组。如果未显示组，请在 **AD 主域 (AD Primary Domain)**、**基本 DN (Base DN)** 和**组 DN (Group DN)** 字段中输入或编辑信息，然后点击**加载组 (Load Groups)**。 有关这些字段的信息，请参阅领域字段，第 2029 页。
可用组部分	通过将组移动到 **包含的组和用户** 或 **排除的组和用户** 列表中，限制要在策略中使用的组。 例如，将一个组移动到 **包含的组和用户** 列表中，仅允许在策略中使用该组。 **排除的组和用户** 中的组及其包含的用户将被排除在用户感知和控制之外。所有其他组和用户 均为 可用。 有关详细信息，请参阅领域目录和同步字段，第 2032 页。

步骤 9 点击**领域配置**选项卡。

步骤 10 输入 **组属性**，然后（如果您对强制网络门户使用 Kerberos 身份验证）输入 **AD 加入用户名** 和 **AD 加入密码**。有关详细信息，请参阅领域目录和同步字段，第 2032 页。

步骤 11 如果使用 Kerberos 身份验证，请点击 **测试**。如果测试失败，请等待片刻，然后重试。

步骤 12 输入用户会话超时值，以分钟为单位，为 **ISE/ISE-PIC 用户**、**终端服务器代理用户**、**强制网络门户用户**、 **出现故障的强制网络门户用户**、 和 **访客强制网络门户用户**。

步骤 13 完成配置领域后，点击 **保存**。

下一步做什么

- 将防火墙管理中心配置为跨域信任：设置，第 2040 页
- 同步用户和组，第 2037 页
- 编辑、删除、启用或禁用领域；请参阅管理领域，第 2048 页。

- 比较领域，第 2049 页。
- 或者，监控任务状态；请参阅*Cisco Secure Firewall Management Center* 管理指南中的查看任务消息。

关于领域和领域序列

领域是 Secure Firewall Management Center 和您监控的服务器上的用户账号之间的连接。它们可指定该服务器的连接设置和身份验证过滤器设置。领域可以：

- 指定要监控其活动的用户和用户组。
- 查询用户存储库上有关授权用户以及某些非授权用户的用户元数据：通过基于流量的检测而检测到的 POP3 和 IMAP 用户以及通过基于流量的检测、TS 代理/或 ISE/ISE-PIC 而检测到的用户。

（仅限 *Microsoft AD* 领域。）领域序列是要在身份策略中使用的两个或更多 Active Directory 领域的排序列表。将领域序列与身份规则关联时，系统会按照领域序列中指定的从第一个到最后的顺序来搜索 Active Directory 域。

您可以将多个域控制器添加为一个领域内的目录，但它们必须共享相同的基本领域信息。领域内的目录必须为专门的 LDAP 或专门的 Active Directory (AD) 服务器。启用领域后，保存的更改将在 Secure Firewall Management Center下一次查询服务器时生效。

要执行用户感知，必须为任何一种支持的服务器类型配置一个领域。系统使用这些连接查询服务器上与 POP3 和 IMAP 用户关联的数据，并收集有关通过基于流量的检测发现的 LDAP 用户的数据。

系统使用 POP3 和 IMAP 登录中的邮件地址与 Active Directory、Microsoft Azure Active Directory 或 OpenLDAP 上的 LDAP 用户相关联。例如，如果托管设备检测到某个用户使用与某个 LDAP 用户相同的邮件地址登录 POP3，则系统会将 LDAP 用户的元数据与该用户关联。

要执行用户控制，可以配置以下任何项目：

- Active Directory、Microsoft Azure Active Directory、 服务器或 ISE/ISE-PIC 的领域或领域序列



注释 如果您计划配置 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置 Microsoft AD 领域或领域序列。

领域序列不适用于 Microsoft Azure AD 领域。

- TS 代理的 Microsoft AD 服务器的领域或领域序列。
- 对于强制网络门户，则为 LDAP 领域。

  LDAP 不支持领域序列。

您最多可以嵌套 Microsoft AD 组， Secure Firewall Management Center 将下载这些组及其包含的用户。您可以选择限制下载的组和用户，如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述。

关于用户同步

您可以配置领域或领域序列以便在 防火墙管理中心 和 LDAP 或 Microsoft AD 服务器之间建立连接，以检索检测到的某些用户的用户和用户组元数据：

- 由强制网络门户进行身份验证或由 ISE/ISE-PIC 报告的 LDAP 和 Microsoft AD 用户。这些元数据可用于用户感知和用户控制。
- 基于流量的检测功能检测到的 POP3 和 IMAP 用户登录（如果这些用户的电子邮件地址与 LDAP 或 AD 用户相同）。这些元数据可用于用户感知。

防火墙管理中心获取关于每个用户的以下信息和元数据：

- LDAP 用户名
- 名字和姓氏
- 电子邮件地址
- 部门
- 电话号码



重要事项 要减少 Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

关于用户活动数据

用户活动数据存储在用户活动数据库，而用户身份数据存储在用户数据库。可在访问控制中存储和使用的最大用户数取决于防火墙管理中心型号。选择要包含的用户和组时，请确保用户总数小于型号限制。如果访问控制参数范围太宽泛，则 防火墙管理中心会获取尽可能多的用户的信息，并报告其无法在消息中心的“任务”选项卡页面中检索的用户数。

要选择性地限制托管设备监控用户感知数据的子网，您可以使用*Cisco Secure Firewall Threat Defense 命令参考*中所述的 **configure identity-subnet-filter** 命令。



注释 即使您从存储库移除系统检测到的用户，防火墙管理中心也不会从其用户数据库中移除这些用户；您必须手动删除。但是，在 防火墙管理中心下次更新其授权用户列表时，LDAP 更改会反映在访问控制规则中。

领域和受信任的域

在 防火墙管理中心中配置 Microsoft Active Directory (AD) 领域 时，该领域与 Microsoft Active Directory 或 LDAP 域 关联。

一组相互信任的 Microsoft Active Directory (AD) 域通常被称为林。此信任关系可使域以不同方式访问彼此的资源。例如，在域 A 中定义的用户账号可以标记为域 B 中所定义组的成员。

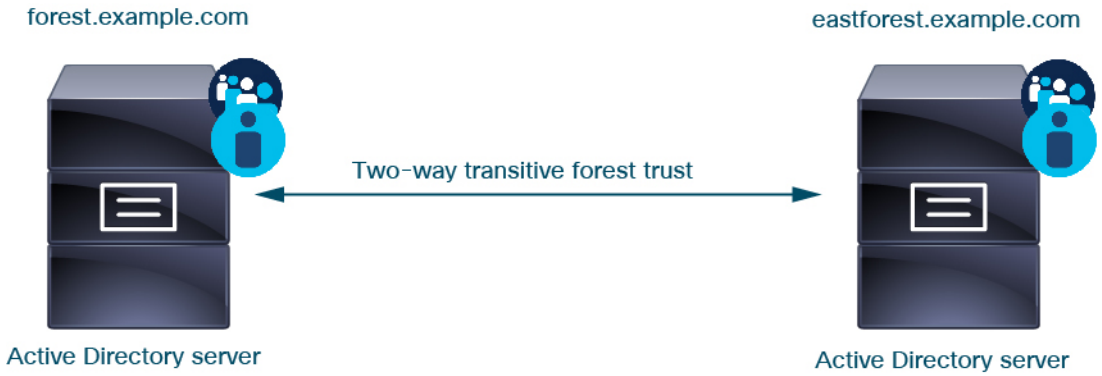
注释 受信任的域仅适用于 Microsoft Active Directory 域。它们不适用于 Microsoft Azure Active Directory 或 LDAP 域。

系统和受信任的域

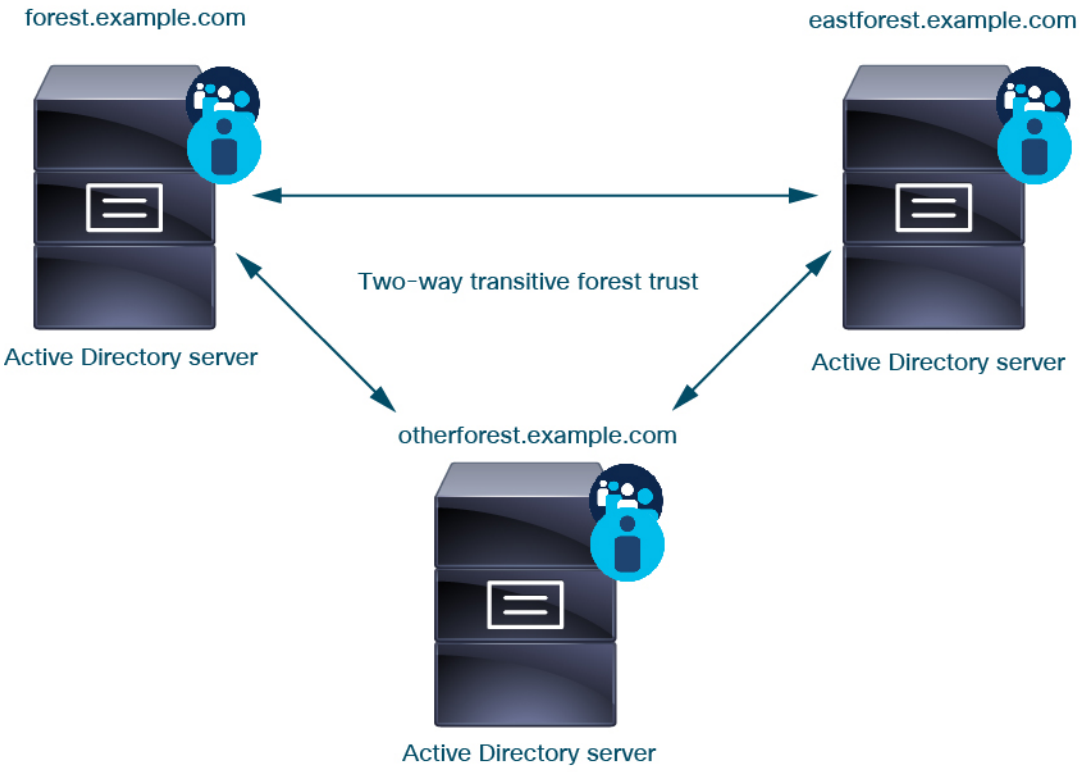
系统支持在信任关系中配置的 AD 林。有几种类型的信任关系；本指南讨论双向传递森林信任关系。以下简单示例显示两个林： **forest.example.com** 和 **eastforest.example.com**。每个林中的用户和组可以通过另一个林中的 AD 进行身份验证，前提是您以这种方式配置了这些林。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

您无需为没有您希望在访问控制策略中使用的用户的任何域配置领域。

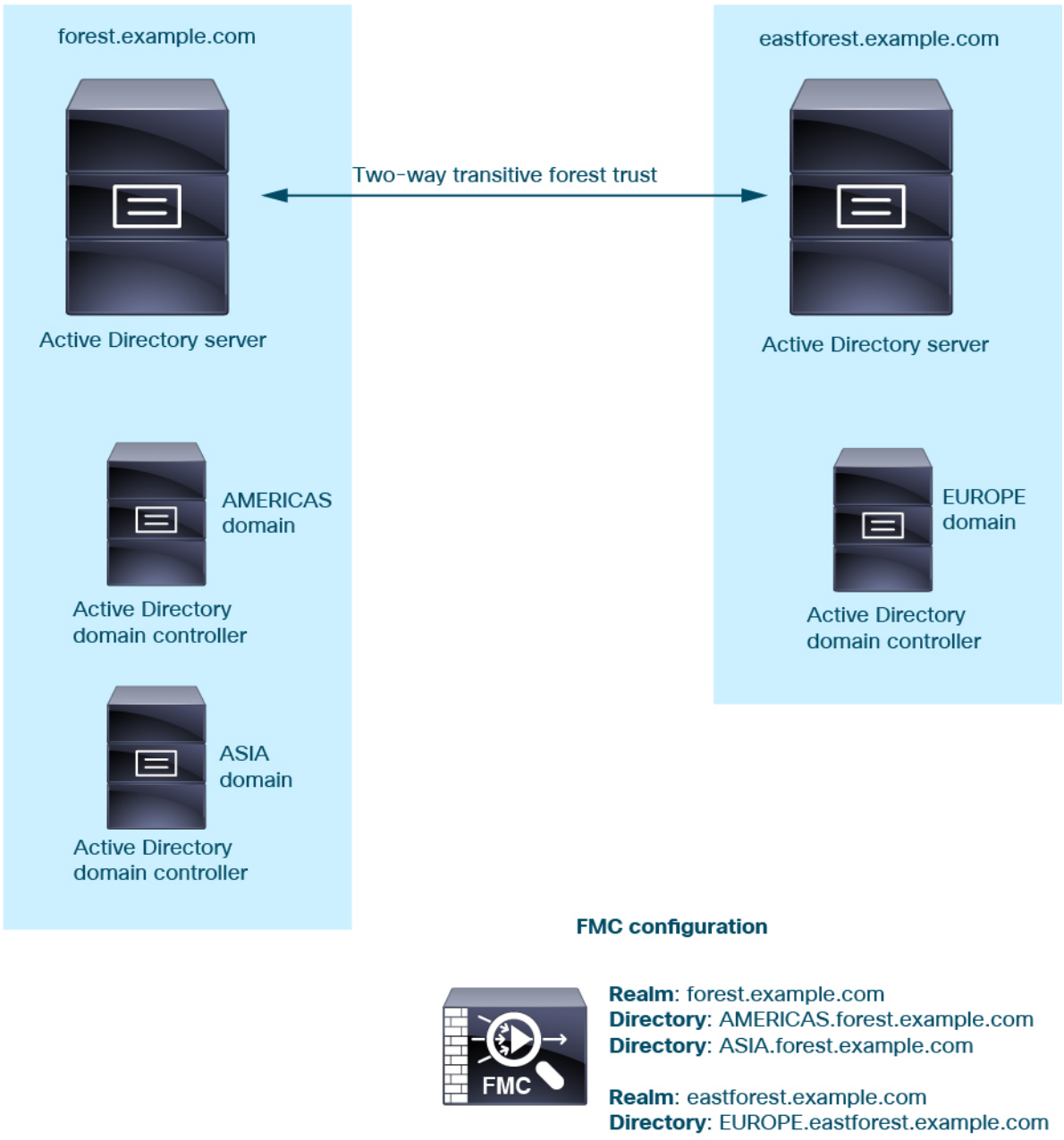


继续本示例，假设您有三个 AD 林（其中一个可以是子域或独立林），都设置为双向传递林关系，所有用户和组在所有三个林中以及系统。（如上例所示，必须将所有三个 AD 域设置为领域，并将所有域控制器配置为这些领域中的目录。）



最后，您可以将防火墙管理中心设置为能够在具有双向传递林信任的双林系统中对用户和组实施身份策略。假设每个林至少有一个域控制器，每个域控制器对不同的用户和组进行身份验证。要使 防火墙管理中心能够在这些用户和组上实施身份策略，必须将每个包含相关用户的域设置为 防火墙管理中心 领域，并将每个域控制器设置为相应领域中的 防火墙管理中心 目录。

未能正确配置防火墙管理中心会阻止某些用户和组在策略中使用。在这种情况下，当您尝试同步用户和组时，您将看到警告。



使用前面的示例，设置 防火墙管理中心 如下：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **AMERICAS.forest.example.com**领域中的目录
  - **ASIA.forest.example.com**领域中的目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域
  - **EUROPE.eastforest.example.com**领域中的目录

注释 防火墙管理中心 使用 AD 字段 **msDS-PrincipalName** 来解析引用，以查找每个域控制器中的用户名和组名。 **msDS-PrincipalName** 返回 NetBIOS 名称。

领域支持的服务器

可以配置领域以连接到以下类型的服务器（如果这些服务可从防火墙管理中心进行TCP/IP访问）：

服务器类型	支持 ISE/ISE-PIC 数据检索？	支持 TS 代理数据检索？	支持强制网络门户数据检索？
Windows 服务器 2012、2016 和 2019 上的 Microsoft Active Directory	支持	支持	支持
Microsoft Azure AD	支持	否	否
Linux 上 的 OpenLDAP	否	否	支持

不支持 将 Active Directory 全局目录服务器作为领域目录。有关全局目录服务器的详细信息，请参阅 learn.microsoft.com 上的 全局目录 。

注释 如果 TS 代理安装在与另一个被动身份验证身份源（ISE/ISE-PIC）共享的 Microsoft Active Directory Windows 服务i去上，则 防火墙管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 防火墙管理中心。

请注意以下与服务器组配置有关的事项：

- 要对用户组或组内用户执行用户控制，则必须在 LDAP 或 Active Directory 服务器上配置用户组。
- 组名称不能以 `s-` 开头，因为它由 LDAP 在内部使用。

  组名称和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 或反斜线 (\)；否则，这些组或组织单位中的用户不会被下载，也不会可用于身份策略。
- 要配置包含或排除作为服务器上某个子组成员的用户的 Active Directory 领域，请注意，Microsoft 建议在 Windows 服务器 2012 上，Active Directory 每组包含不超过 5000 个用户。有关详细信息，请参阅 MSDN 上的“Active Directory 的最大限制-可扩展性”。

  如果需要，可以修改 Active Directory 服务器配置以增加此默认限制并容纳更多用户。

- 要在您的远程桌面服务环境中唯一识别由服务器报告的用户，则必须配置 Cisco 终端服务 (TS) 代理。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可唯一识别这些用户。（Microsoft将 终端服务 名称更改为 远程桌面服务。）

  有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

支持的服务器对象类和属性名称

领域中的服务器必须使用下表中列出的属性名称，以使 Secure Firewall Management Center能够检索服务器中的用户元数据。如果服务器中的属性名称不正确，Secure Firewall Management Center将无法使用该属性中的信息来填充其数据库。

表 *117:* 属性名称与 *Secure Firewall Management Center*字段的映射

元数据	防火墙管理中心属性	LDAP ObjectClass	Active Directory 属性	OpenLDAP 属性
LDAP 用户名	用户名	• 用户 • inetOrgPerson	samaccountname	cn uid
名字	名字		givenname	givenname
姓氏	姓氏		sn	sn
电子邮件地址	电子邮件		mail Userprincipalname（如果 mail 没有值）	mail
department	部门		department distinguishedname（如果 department 没有值）	ou
电话号码	电话		telephonenumber	telephonenumber

注释 组的 LDAP ObjectClass 为 `group`、`groupOfNames`（`group-of-names` 适用于 Active Directory）或 `groupOfUniqueNames`。

有关 ObjectClasses 和属性的详细信息，请参阅以下参考资料：

- Microsoft Active Directory：
  - ObjectClasses：MSDN 上的所有类
  - 属性：MSDN 上的所有属性
- OpenLDAP：RFC 4512

Kerberos 身份验证的必备条件

如果使用 Kerberos 对强制网络门户用户进行身份验证，请记住以下几点。

主机名字符限制

如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 响应字符数限制

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

领域字段

以下字段用于配置领域。

领域配置字段

这些设置适用于领域中的所有 Active Directory 服务器或域控制器（也称为目录）。

名称

领域的唯一名称。

- 要在身份策略中使用领域，系统需支持字母数字和特殊字符。
- 要在 RA-VPN 配置中使用领域，系统需支持字母数字、连字符 (-)、下划线 (_) 和加号 (+) 字符。

说明

（可选。）输入领域的描述。

类型 (Type)

领域类型， **AD** 表示 Microsoft Active 目录， **LDAP** 表示其他支持的 LDAP 存储库，或 **本地**。有关支持的 LDAP 存储库的列表，请参阅领域支持的服务器，第 2027 页。您可以使用 LDAP 存储库对强制网络门户用户进行身份验证；所有其他都需要 Active Directory。

注释 仅强制网络门户支持 LDAP 领域。

领域类型 **LOCAL** 用于配置本地用户设置。LOCAL 领域用于远程访问用户身份验证。

为 LOCAL 领域添加以下本地用户信息：

- **用户名**-用户的名称。
- **密码**-本地用户密码。

- **确认密码**-确认本地用户密码。



注释 **点击添加其他本地用户** 以将更多用户添加到 LOCAL 领域。

您可以在创建领域并为本地用户更新密码后添加更多用户。您还可以创建多个 LOCAL 领域，但不能将其禁用。

AD 主域 (AD Primary Domain)

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。



注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

AD 加入用户名和 AD 加入密码 (AD Join Username and AD Join Password)
（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

用于专为 Kerberos 强制网络门户主动身份验证设计的 Microsoft Active Directory 领域，表示具有可在 Active Directory 域中创建域计算机帐户的适当权限的任何 Active Directory 用户的标识用户名和密码。

记住以下几点：

- DNS 必须能够将域名解析为 Active Directory 域控制器的 IP 地址。
- 指定的用户必须能够将计算机加入到 Active Directory 域。
- 用户名必须是完全限定的（例如，**`administrator@mydomain.com`**，而不是 **`administrator`**）。

如果选择 **`Kerberos`**（或 **`HTTP 协商`**，如果希望 Kerberos 作为选项）作为身份规则中的**身份验证协议**，则必须为您所选的 **领域** 配置 **AD 加入用户名** 和 **AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。



注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

目录用户名和目录密码 (Directory Username and Directory Password)

为具有检索用户信息的相应权限的用户提供的标识用户名和密码。

请注意以下事项：

- 对于 OpenLDAP，用户的访问权限由 OpenLDAP 规范第 8 部分中讨论的 `<level>` 参数确定。用户的 `<level>` 应为 `auth` 或更高。
- 用户名必须是完全限定的（例如，**`administrator@mydomain.com`**，而不是 **`administrator`**）。



注释 SHA-1 散列算法无法在 Active Directory 服务器上存储密码，因此不应使用。有关详细信息，请参阅参考，例如 Microsoft TechNet 上的将证书颁发机构散列算法从 SHA1 迁移到 SHA2 或 Open Web 应用安全项目网站上的 密码存储备忘单 。

我们建议使用 SHA-256 与 Active Directory 通信。

基本 DN

（可选。）Secure Firewall Management Center应在其上开始搜索用户数据的服务器上的目录树。如果未指定 **基本 DN**，则系统会检索可连接到服务器的顶级 DN。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **`ou=security,dc=example,dc=com`**。

组 DN (Group DN)

（可选。）Secure Firewall Management Center应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 2028 页中显示。如果未指定 **组 DN**，则系统会检索可连接到服务器的顶级DN。



注释 以下是系统在您的目录服务器中的用户、组和 DN 中 支持 的字符列表。使用除以下字符以外的任何字符可能会导致系统无法下载用户和组。

实体	支持的字符
用户名	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
组名称	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
基础 DN 和组 DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

用户名中的任何位置均不支持空格，包括末尾。

编辑现有领域时，以下字段可用。

用户会话超时

（在编辑领域时，在 **领域配置** 选项卡页面上可用。）

输入用户会话超时前持续的分钟数。在用户登录事件后，默认值为 1440（24 小时）。超时后，用户的会话结束。如果用户继续访问网络，而不再次登录，则 Secure Firewall Management Center 会将该用户视为未知（**失败的强制网络门户用户**除外）。

此外，如果在没有领域的情况下设置 ISE/ISE-PIC，并且超时，则需要解决方法。有关详细信息，请联系 思科技术支持中心。

您可以为以下内容设置超时值：

- **用户代理和 ISE/ISE-PIC 用户**：由用户代理或 ISE/ISE-PIC（被动身份验证类型）跟踪的用户的超时。

  您指定的超时值 不 适用于 pxGrid SXP 会话主题订用（例如，目标 SGT 映射）。相反，只要没有来自 ISE 的给定映射的删除或更新消息，会话主题映射就会保留。

  有关 ISE / ISE-PIC 的详细信息，请参阅 The ISE/ISE-PIC 身份源，第 2079 页。

- **终端服务代理用户**：由 TS 代理（一种被动身份验证类型）跟踪的用户的超时。有关详细信息，请参阅终端服务 (TS) 代理身份源，第 2207 页。

- **强制网络门户用户**：使用强制网络门户（一种主动身份验证类型）成功登录的用户的超时。有关详细信息，请参阅强制网络门户身份源，第 2059 页。

- **失败的强制网络门户用户**：未使用强制网络门户成功登录的用户的超时。您可以配置 Secure Firewall Management Center 将用户视为身份验证失败的用户之前的 **最大登录尝试次数** 。可以选择使用访问控制策略为身份验证失败的用户授予对网络的访问权限，如果是这样，此超时值将应用于这些用户。

  有关失败的强制网络门户登录的详细信息，请参阅强制网络门户字段，第 2073 页。

- **访客强制网络门户用户**：以访客用户身份登录到强制网络门户的用户的超时。有关详细信息，请参阅强制网络门户身份源，第 2059 页。

领域目录和同步字段

领域目录字段

这些设置适用于领域中的各个服务器（例如 Active Directory 域控制器）。

主机名/IP 地址

Active Directory 域控制器计算机的完全限定主机名。要查找完全限定名称，请参阅 查找 Active Directory 服务器名称，第 2035 页。

如果您使用 Kerberos 对强制网络门户进行身份验证，还请确保您了解以下内容：

如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

端口 (Port)

服务器的端口。

加密

（强烈建议。）要使用的加密方法：

- **STARTTLS** - 加密的 LDAP 连接
- **LDAPS** - 加密的 LDAP 连接
- **无 (None)** - 未加密的 LDAP 连接（不安全的流量）

要与 Active Directory 服务器安全通信，请参阅安全地连接到 Active Directory 或 LDAP，第 2035 页。

CA 证书

用于对服务器进行身份验证的 TLS/SSL 证书。必须配置 **STARTTLS** 或 **LDAPS** 作为 **加密** 类型才能使用 TLS/SSL 证书。

如果使用证书进行身份验证，则证书中的服务器名称必须与服务器**主机名/IP 地址 (Hostname / IP Address)** 匹配。例如，如果将 10.10.10.250 作为 IP 地址，而不是证书中的 **computer1.example.com**，连接会失败。

用于连接目录服务器的接口

仅 RA VPN 身份验证需要，以便 Cisco Secure Firewall Threat Defense 可以安全地连接到 Active Directory 服务器。但是，此接口不用于下载用户和组。

只能选择路由接口组。有关详细信息，请参阅接口，第 2655 页。

点击以下选项之一：

- **通过路由查找进行解析**：使用路由连接到 Active Directory 服务器。
- **选择接口**：选择要连接到 Active Directory 服务器的特定托管接口。

用户同步字段

AD 主域 (AD Primary Domain)

仅用于 Microsoft Active Directory 领域。用于需要对用户进行身份验证的 Active Directory 服务器的域。



注释 您必须为每个 Microsoft Active Directory (AD) 领域都指定一个唯一的 **AD 主域**。虽然系统允许对不同 Microsoft AD 领域指定相同的 **AD 主域**，但系统将无法正常运行。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。由于系统无法正确识别用户和组，因此会阻止您对多个领域指定相同的 **AD 主域**。发生这种情况，是因为系统会向每个领域的每个用户和每个组都分配一个唯一 ID，因此系统无法明确识别任何特定用户或组。

输入查询以查找用户和组

基本 DN：

（可选。）防火墙管理中心应在其上开始搜索用户数据的服务器上的目录树。

通常，基本可分辨名称 (DN) 具有指示公司域名和运营单位的基础结构。例如，Example 公司的 Security 部门的基础 DN 可能为 **ou=security,dc=example,dc=com**。

组 DN (Group DN)：

（可选。）防火墙管理中心应在其上搜索具有组属性的用户的服务器上的目录树。支持的组属性的列表在支持的服务器对象类和属性名称，第 2028 页中显示。

注释 组名和组织单位名称都不能包含特殊字符，如星号 (*)、等号 (=) 和后斜线 (\)，因为这些组中的用户不会被下载，也不能用于身份策略。

加载组

让您能够下载要用于用户感知和用户控制的用户和组。

可用组 (Available Groups)、添加以包含 (Add to Include)、添加以排除 (Add to Exclude)

限制可在策略中使用的组。

- 除非将组移至 **包含的组和用户** 或 **排除的组或用户** 字段，否则 **可用组** 字段中显示的组可用于策略。
- 如果您将组移动到**包含的组和用户 (Included Groups and Users)** 字段中，只有那些所包含的组和用户被下载，用户数据可用于用户感知和用户控制。
- 如果您将组移动到**排除的组和用户 (Excluded Groups and Users)** 字段中，它们所包含的所有组和用户，除了这些被下载并可用于用户认知和用户控制。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。
- 若要包括来自未包括的组的用户，请在 **用户入侵** 下面的字段中输入用户名，然后点击 **添加**。

注释 使用公式 **R = I - (E+e) + i**计算下载到 防火墙管理中心 的用户，其中：

- R 是已下载用户的列表
- I 是包含的组
- E 是排除的组
- e 是排除的用户
- i 是包含的用户

立即同步
点击以将组和用户与 AD 同步。

开始自动 同步 ， 在
输入从 AD下载用户和组的时间和时间间隔。

安全地连接到 Active Directory 或 LDAP

要在 Active Directory 服务器和 Secure Firewall Management Center（我们强烈建议）之间创建安全连接，您必须执行以下所有任务：

- 导出服务器的根证书。
- 将根证书导入 Secure Firewall Management Center 作为受信任 CA 证书 (**对象 (Objects)** > **PKI** > **受信任 CA (Trusted CAs)**）。
- 查找服务器的完全限定名称。
- 创建领域目录。

有关详细信息，请参阅以下任务之一。

相关主题

导出 Active Directory 服务器的根证书 ， 第 2036 页
查找 Active Directory 服务器名称 ， 第 2035 页
创建 LDAP 领域或 Active Directory 领域和领域目录 ， 第 2019 页

查找 Active Directory 服务器名称

要在 防火墙管理中心中配置领域目录，您必须知道完全限定服务器名称，您可以在后续程序中找到该名称。

这些任务仅适用于 Microsoft Active Directory。如果您使用 LDAP，请咨询相应的参考人员以了解该程序。

开始之前

您必须以具有足够权限查看计算机名称的用户身份登录 Active Directory 服务器。

过程

步骤 1 登录 Active Directory 服务器
步骤 2 点击**开始 (Start)**。
步骤 3 右键点击 **此 PC (This PC)**。
步骤 4 点击**属性 (Properties)**。
步骤 5 点击**高级系统设置 (Advanced System Settings)**。
步骤 6 点击**计算机名称 (Computer Name)** 选项卡。

步骤 7 注意 **完整计算机名称**的值。
在 防火墙管理中心 中配置领域目录时，必须输入此确切名称。

下一步做什么

创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。

相关主题

导出 Active Directory 服务器的根证书， 第 2036 页

导出 Active Directory 服务器的根证书

接下来的任务讨论如何导出 Active Directory 服务器的根证书，这是安全连接到 防火墙管理中心 以获取用户身份信息所必需的。

这些任务仅适用于 Microsoft Active Directory。如果您使用 LDAP，请咨询相应的参考人员以了解该程序。

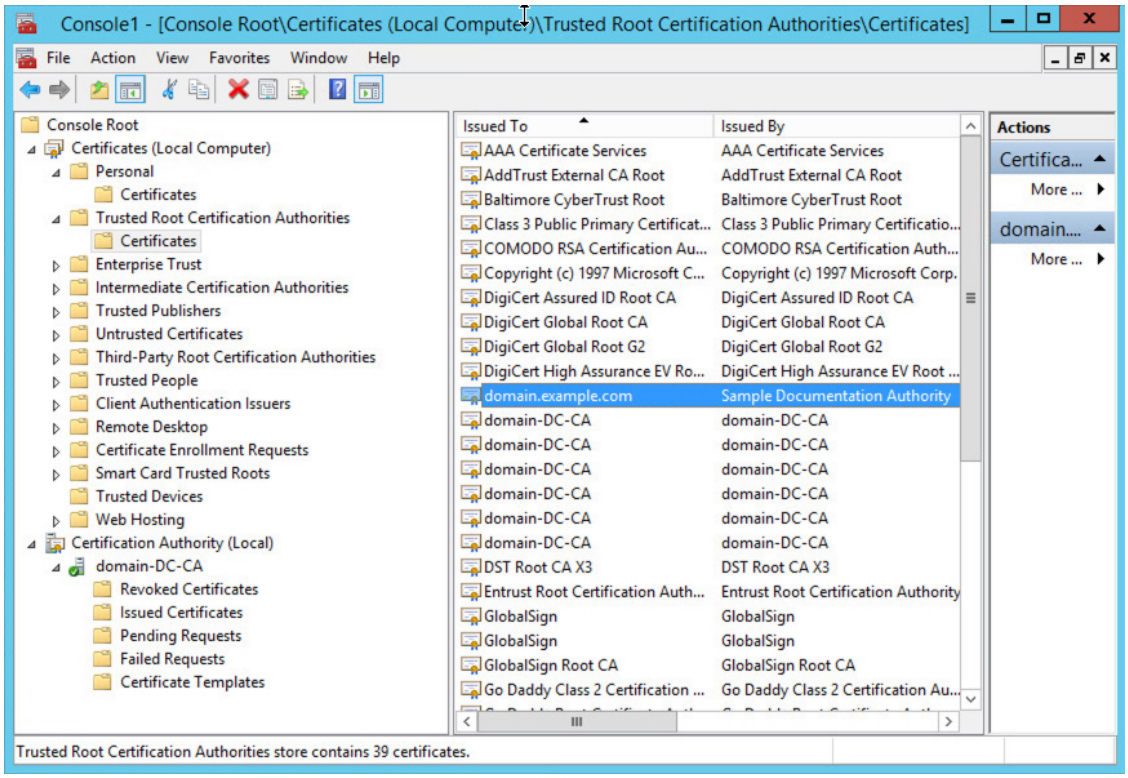
开始之前

您必须知道 Active Directory 服务器的根证书的名称。根证书的名称可能与域的名称相同，或者证书的名称可能不同。后面的程序显示了查找名称的一种方法；可能还有其他方式。

过程

步骤 1 以下是查找 Active Directory 服务器根证书名称的一种方法；有关详细信息，请参阅 Microsoft 文档：

a) 以具有运行 Microsoft 管理控制台权限的用户身份登录 Active Directory 服务器。
b) 点击 **开始** 并输入 **mmc**。
c) 点击 **文件** > **添加/删除 Snap-in**
d) 从左侧窗格的可用管理单元列表中，点击 **证书**（**本地**）。
e) 点击**添加 (Add)**。
f) 在证书管理单元对话框中，点击 **计算机帐户** 然后点击 **下一步**。
g) 在“选择计算机”对话框中，点击 **本地计算机** 然后点击 **完成**。
h) 仅限 *Windows Server 2012*。重复上述步骤以添加证书颁发机构管理单元。
i) 点击 **控制台根** > **受信任证书颁发机构** > **证书**。
服务器的受信任证书显示在右侧窗格中。下图只是 Windows Server 2012 的示例；您的产品可能看起来有所不同。



步骤 2 使用 **certutil** 命令导出证书。

这只是导出证书的一种方式。这是导出证书的便捷方式，尤其是在您可以运行Web浏览器并从 Active Directory 服务器连接到 防火墙管理中心 的情况下。

a) 点击 **开始** 并输入 **cmd**。
b) 输入命令 **certutil -ca.cert** 证书-名称。
服务器的证书显示在屏幕上。
c) 将整个证书复制到剪贴板，以 **-----BEGIN CERTIFICATE-----** 开头和以 **-----END CERTIFICATE-----** 结尾（包括这些字符串）。

下一步做什么

将 Active Directory 服务器的证书作为受信任 CA 证书导入 防火墙管理中心，如 添加受信任 CA 对象，第 2666 页中所述。

相关主题

查找 Active Directory 服务器名称，第 2035 页

同步用户和组

同步 用户和组意味着 防火墙管理中心 查询您为组和这些组中的用户配置的领域和目录。所有用户都可以在身份策略中使用 防火墙管理中心 查找。

如果发现问题，您很可能需要添加包含 防火墙管理中心 无法加载的用户和组的领域。有关详细信息，请参阅领域和受信任的域， 第 2023 页。

开始之前

为每个 Active Directory 域创建一个 Secure Firewall Management Center 领域，并为每个林中的每个 Active 导向器域控制器创建一个 防火墙管理中心 目录。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。

注释 Microsoft Azure AD 领域不需要同步用户和组。

必须仅为具有要在用户控制中使用的用户的域创建领域。

您最多可以嵌套 Microsoft AD 组， Secure Firewall Management Center 将下载这些组及其包含的用户。您可以选择限制下载的组和用户，如 创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页中所述。

您必须使用域的原始域名而不是该域的任何备用用户主体名称 (UPN) 后缀创建领域。否则，用户和组将无法下载，并且身份策略不会实施。例如，如果原始域为 `domain.example.com`，备用 UPN 名称为 `domain2.mydomain.com`，则必须将领域配置为使用 `domain.example.com`。有关配置备用 UPN 后缀的详细信息，请参阅 learn.microsoft.com 上的 配置备用登录 ID 等资源。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 点击每个领域旁边的 **下载** （）。

步骤 4 要查看结果，请点击**同步结果 (Sync Results)** 选项卡。
“领域”列指示 Active Directory 林中的用户和组同步是否存在问题。查找每个领域旁边的以下指示器。

领域中的指示器列	含义
（无）	所有用户和组同步无错误。无需任何操作。
黄色三角形（）	同步用户和组时出现问题。确保为每个 Active Directory 域添加了一个领域，并为每个 Active Directory 域控制器添加了一个目录。 有关详细信息，请参阅排除跨域信任故障， 第 2054 页。

创建领域序列

通过以下程序，您可以创建领域序列，这是系统在应用身份策略时搜索的领域的有序列表。将领域序列添加到身份规则的方式与添加领域的方式完全相同；区别在于系统在应用身份策略时按领域序列中指定的顺序搜索所有领域。

开始之前

您必须创建并启用至少两个领域，每个领域对应于与 Active Directory 服务器的连接。您无法为 LDAP 领域创建领域序列。

按创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述创建领域。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域序列**。

步骤 3 点击 **领域序列** 选项卡。

步骤 4 点击**添加序列 (Add Sequence)**。

步骤 5 在 **名称** 字段中，输入用于标识领域序列的名称。

步骤 6 （可选。）在 **说明**字段中，输入领域序列的说明。

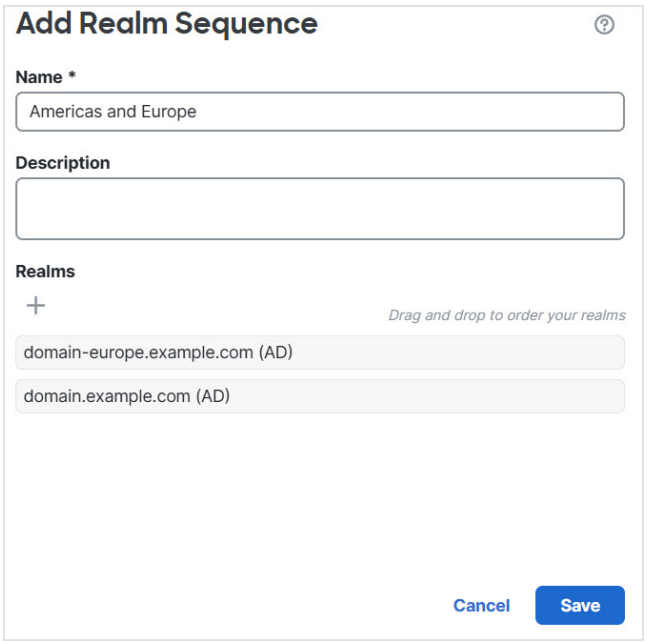
步骤 7 在领域下，点击 **添加** (+)。

步骤 8 点击每个领域的名称以添加到序列。

要缩小搜索范围，请在 **过滤器** 字段中输入全部或部分领域名称。

步骤 9 点击**确定**。

步骤 10 在添加领域序列对话框中，按照您希望系统搜索这些领域的顺序拖放领域。
下图显示由两个领域组成的领域序列的示例。 **domain-europe.example.com** 领域将用于搜索 **domain.example.com** 领域前的用户。



步骤 11 点击**保存**。

下一步做什么

请参阅创建身份策略，第 2213 页。

将防火墙管理中心配置为跨域信任：设置

这是对几个主题的介绍，这些主题将引导您配置 防火墙管理中心 使用跨域信任的两个领域。

此分步示例涉及两个林： **forest.example.com** 和 **eastforest.example.com**。配置目录林，以便每个目录林中的某些用户和组可以由另一个目录林中的 Microsoft AD 进行身份验证。

注释 本主题仅适用于 Microsoft AD 领域。它不适用于 Microsoft Azure AD 领域。

以下是本示例中使用的示例设置。



使用前面的示例，您可以按如下所示设置 防火墙管理中心：

- **forest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录
- **eastforest.example.com** 中包含要使用访问控制策略控制的用户的任何域的领域和目录

示例中的每个领域都有一个域控制器，在 防火墙管理中心 中配置为目录。本示例中的目录配置如下：

- **forest.example.com**
  - 用户的基本可分辨名称 (DN)： **ou=UsersWest,dc=forest,dc=example,dc=com**
  - 组的基本 DN： **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - 用户的基本 DN： **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - 组的基本 DN： **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

相关主题

为Secure Firewall Management Center配置跨域信任 步骤 1：配置领域和目录，第 2041 页

为Secure Firewall Management Center配置跨域信任 步骤 1：配置领域和目录

这是分步程序中的第一个任务，解释如何配置防火墙管理中心来识别在跨域信任关系中配置的Active Directory 服务器，这是企业组织越来越常见的配置。有关此样本配置的概述，请参阅将防火墙管理中心配置为跨域信任：设置，第 2040 页。

如果您为每个域设置一个领域和每个域控制器一个目录的系统，则系统可以发现最多 100,000 个外部安全主体（用户和组）。如果这些外部安全主体与另一个领域中下载的用户匹配，则可以在访问控制策略中使用它们。

开始之前

您必须在跨域信任关系中配置 Microsoft Active Directory 服务器；有关详细信息，请参阅领域和受信任的域，第 2023 页。

如果使用 LDAP 或 Microsoft Azure AD 对用户进行身份验证，则无法使用此程序。

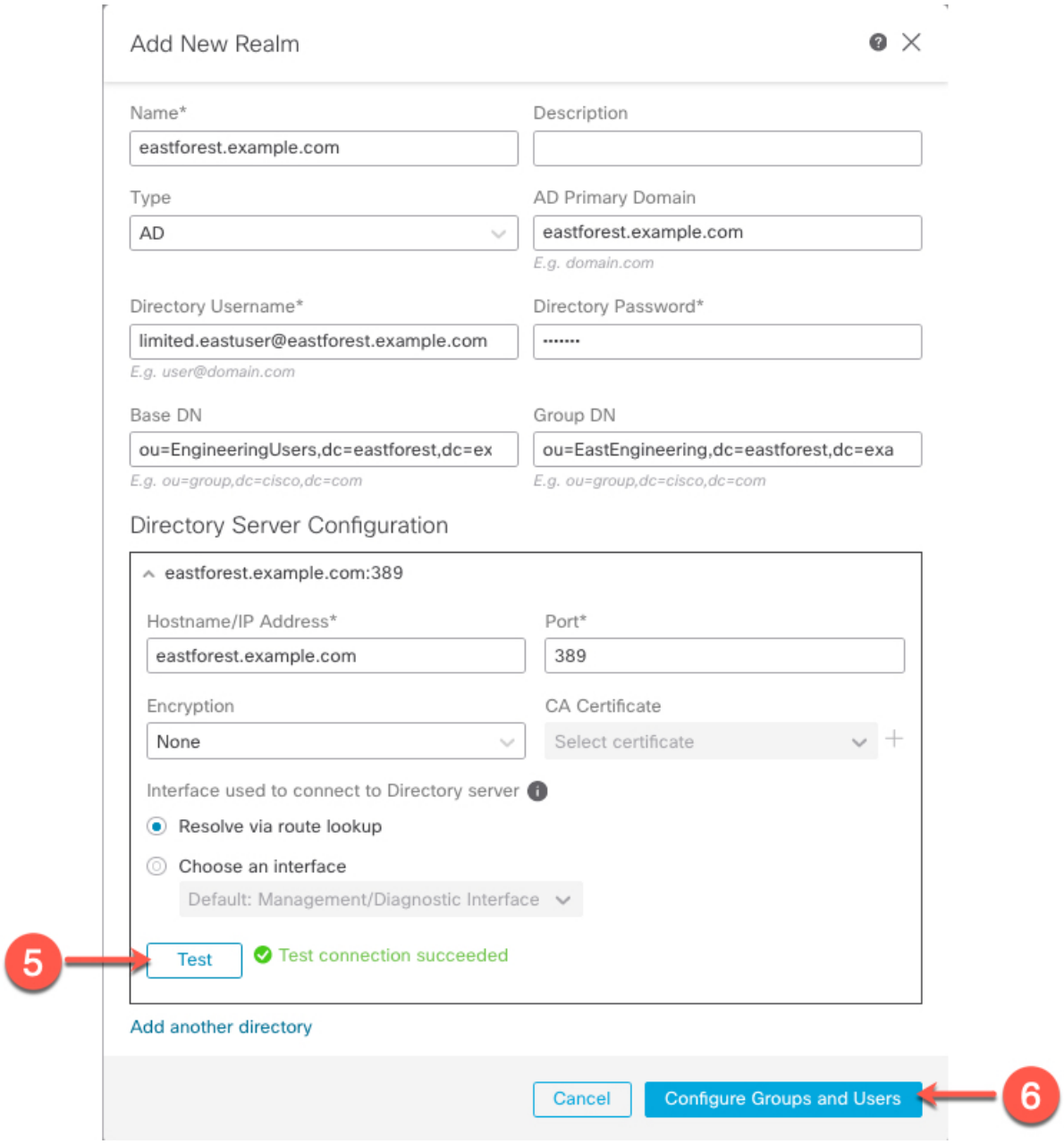
过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 点击 **添加领域** > **Active Directory/LDAP**。

步骤 4 要配置 **forest.example.com**，请输入以下信息。



注释

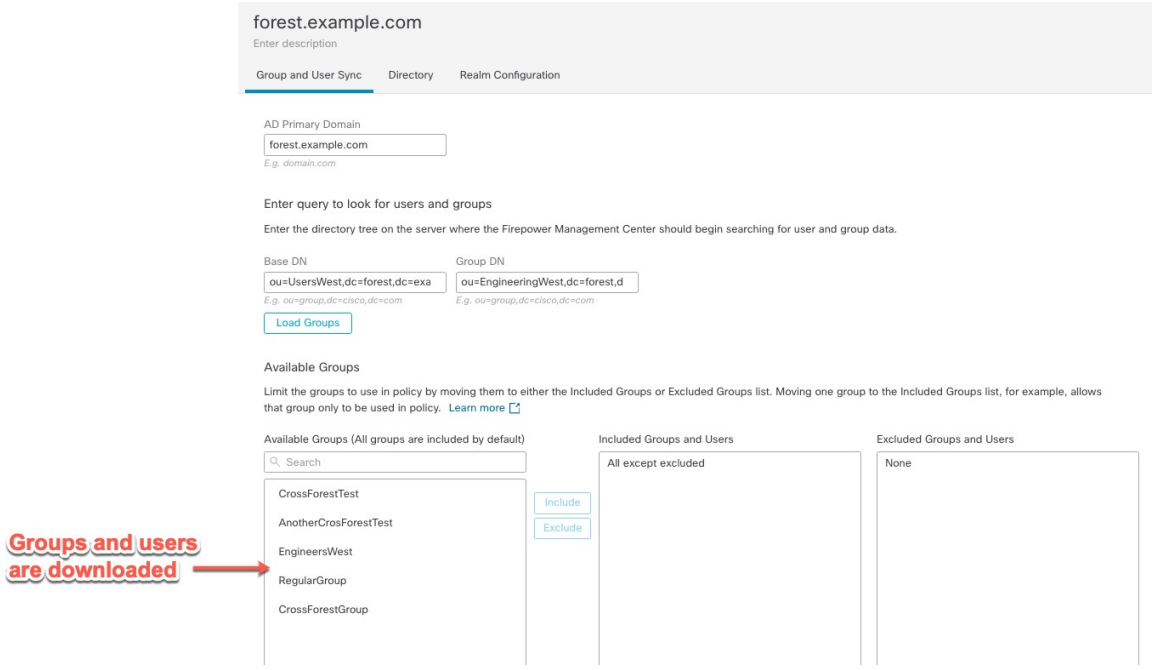
目录用户名 可以是 Active Directory 域中的任何用户；无需特殊权限。

用于连接到目录服务器的接口 可以是可以连接到 Active Directory 服务器的任何接口。

步骤 5 点击**测试 (Test)** 并确保测试成功后再继续。

步骤 6 点击**配置组和用户 (Configure Groups and Users)**。

步骤 7 如果配置成功，则会显示下一页，如下所示。



注释

如果未下载组和用户，请验证 **基本 DN** 和 **组 DN** 字段中的值，然后点击 **加载组**。

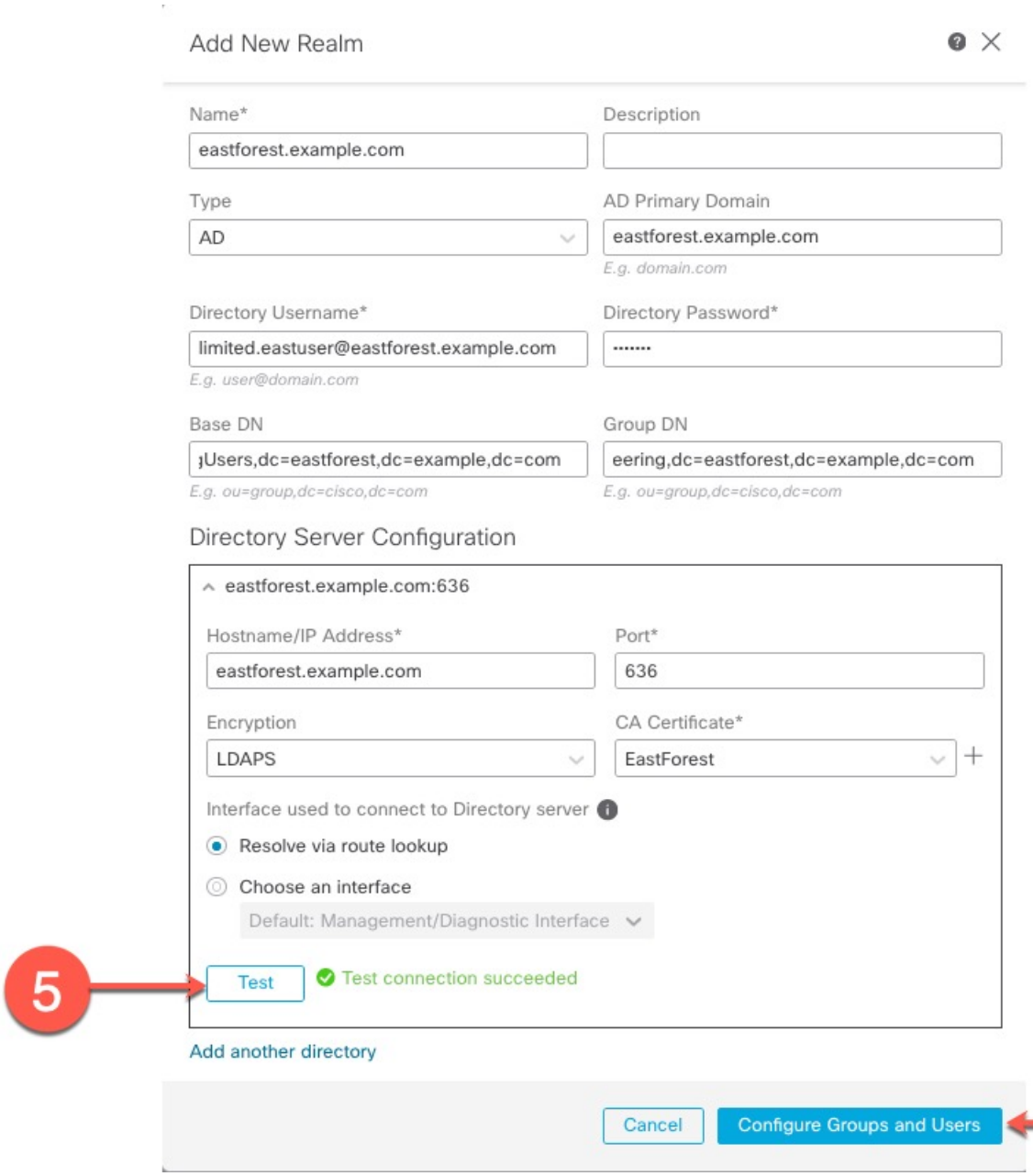
此页面上还有其他可选配置；有关它们的详细信息，请参阅 领域字段，第 2029 页 和 领域目录和同步字段，第 2032 页。

步骤 8 如果在此页面或选项卡页面上进行了更改，请点击 **保存**。

步骤 9 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 10 点击**添加领域 (Add Realm)**。

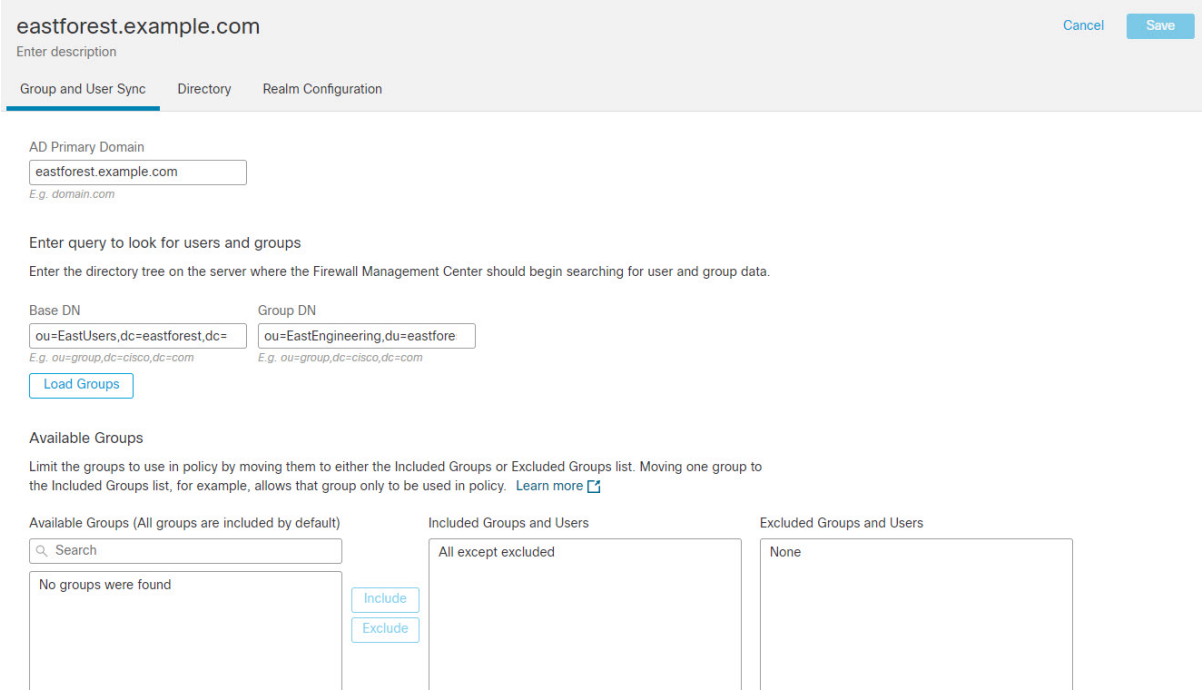
步骤 11 要配置 **eastforest.example.com**，请输入以下信息。



步骤 12 点击测试 **(Test)** 并确保测试成功后再继续。

步骤 13 点击配置组和用户 **(Configure Groups and Users)**。

步骤 14 如果配置成功，则会显示下一页，如下所示。



相关主题

为Secure Firewall Management Center配置跨域信任 步骤 2：同步用户和组，第 2046 页

为Secure Firewall Management Center配置跨域信任 步骤 2：同步用户和组

配置两个或多个具有跨域信任关系的 Active Directory 服务器后，必须下载用户和组。该过程会暴露 Active Directory 配置的可能问题（例如，为一个 Active Directory 域而不是为另一个 Active Directory 域下载的组或用户）。

开始之前

确保您已执行 为Secure Firewall Management Center配置跨域信任 步骤 1：配置领域和目录，第 2041 页中讨论的任务。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 在跨域信任中任何领域行的末尾，点击 **立即下载** （），然后点击**是 (Yes)**。

步骤 4 点击 **复选标记**（） （通知） > **任务**。

如果组和用户下载失败，请重试。如果后续尝试失败，请查看您的领域和目录设置，如领域字段，第 2029 页 和 领域目录和同步字段，第 2032 页中所述。

步骤 5 请点击 **集成** > **身份** > **领域** > **同步结果**。

相关主题

为跨域信任配置Secure Firewall Management Center 步骤 3：解决问题，第 2047 页

为跨域信任配置Secure Firewall Management Center 步骤 3：解决问题

在防火墙管理中心中设置跨域信任的最后一步是确保下载的用户和组没有错误。用户和组无法正确下载的一个典型原因是它们所属的领域尚未下载到 防火墙管理中心。

本主题讨论如何诊断由于某个域未配置为在域控制器层次结构中查找该组而无法下载一个林中引用的组。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

在领域列中，如果领域名称旁边显示 **黄色三角形**（），则您必须解决问题。否则，您的结果配置正确，您可以退出。

步骤 3 从显示问题的领域重新下载用户和组。

a) 点击 **领域 (Realms)** 选项卡。

b) 点击 （立即下载），然后点击**是 (Yes)**。

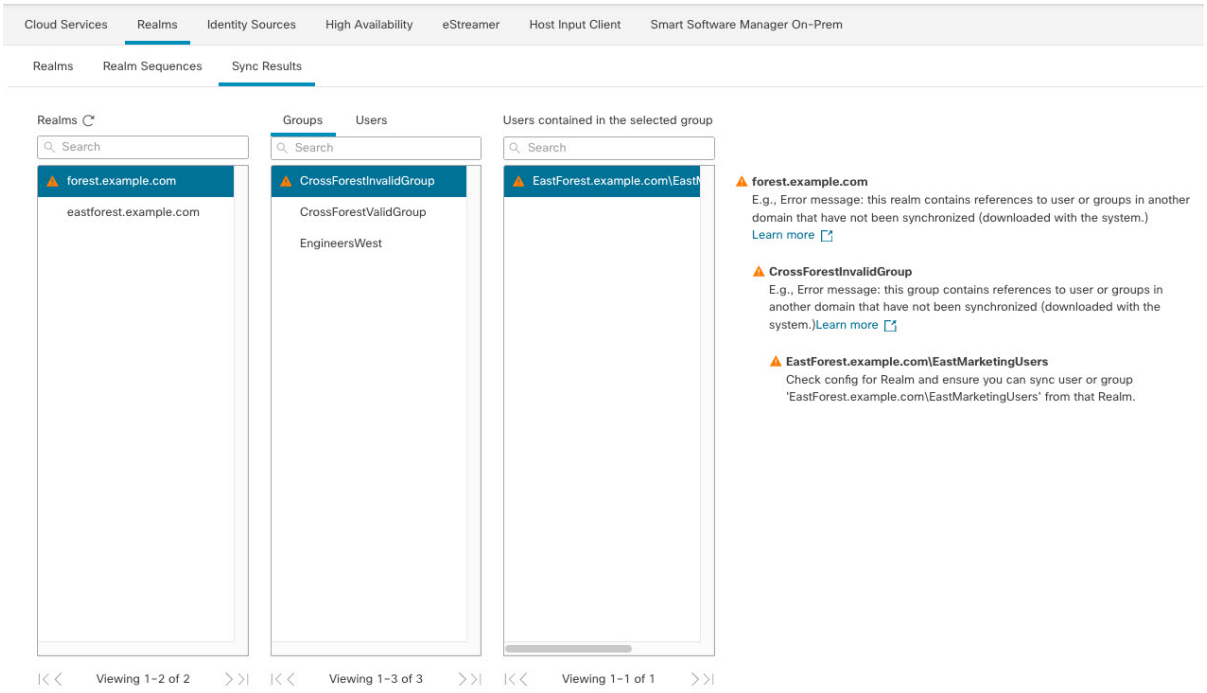
步骤 4 点击 **同步结果 (Sync Results)** 选项卡页面。

如果“领域”(Realms) 列中显示 **黄色三角形**（），请点击存在问题的领域旁边的 **黄色三角形**（）。

步骤 5 在中间列中，点击**组 (Groups)** 或**用户 (Users)** 以查找更多信息。

步骤 6 在组或用户选项卡页面中，点击 **黄色三角形**（）以显示更多信息。

右列应显示足够的信息，以便您可以确定问题的来源。



在上述示例中， **forest.example.com** 包括一个跨域组 **CrossForestInvalidGroup** ，其中包含未由 防火墙管理中心下载的另一个组 **EastMarketingUsers** 。如果在再次同步 **eastforest.example.com** 领域后，错误未解决，则可能意味着 Active Directory 域控制器不包括 **EastMarketingUsers**。

要解决此问题，您可以：

- 从 **CrossForestInvalidGroup**中删除 **EastMarketingUsers** ， 再次同步 **forest.example.com** 领域，然后重新检查。
- 从 **eastforest.example.com** 领域的 **组 DN** 中删除 **ou=EastEngineering** 值，这会导致 防火墙管理中心 从 Active Directory 层次结构的最高级别检索组，进行 **eastforest.example.com**同步并重新检查。

管理领域

本部分讨论如何使用“领域”页上的控件来为领域执行各种维护任务：

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。。如果显示**视图**( )，则表明配置属于祖先域，或者您没有修改配置的权限。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 要删除领域，请点击 **删除** ()。

步骤 4 要编辑领域，请点击领域旁边的 **编辑** () 并进行更改，如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述。

步骤 5 要启用领域，请将**状态**向右滑动；要禁用某个领域，请将其向左滑动。

步骤 6 要下载用户和用户组，请点击 **下载** （）。

步骤 7 要复制领域，请点击 **复制** ()。

步骤 8 要比较领域，请参阅比较领域，第 2049 页。

比较领域

您必须是 管理员、 访问管理员、 网络管理员或 安全审批人 才能执行此任务。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **领域** > **领域**。

步骤 3 点击**比较领域 (Compare Realms)**。

步骤 4 从**比较对象**下拉列表中选择**比较领域**。

步骤 5 从**领域 A** 和**领域 B** 下拉列表中选择要比较的领域。

步骤 6 点击**确定**。

步骤 7 如果要逐一浏览更改，请点击标题栏上方的**上一个**或**下一个**。

步骤 8 （可选。）点击**比较报告**生成领域比较报告。

步骤 9 （可选。）点击**新增比较**生成新的领域比较视图。

领域和用户下载故障排除

如果发现意外的服务器连接行为，请考虑调整领域配置、设备设置或服务器设置。有关其他相关故障排除信息，请参阅：

- 排除 Cisco ISE/ISE-PIC 或思科 TrustSec 问题，第 2101 页
- TS 代理身份源故障排除，第 2208 页
- 强制网络门户身份源故障排除，第 2075 页
- 远程访问 VPN 身份源的故障排除准则，第 2205 页

- 用户控制故障排除，第 2231 页

症状：报告但不下载领域和组

Secure Firewall Management Center的运行状况监控器会通知您用户或领域不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 Secure Firewall Management Center 。

  造成用户不匹配通常是因为该用户属于不予下载至 Secure Firewall Management Center。请回顾 *Cisco Secure Firewall Management Center* 设备配置指南中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 防火墙管理中心未知的某个领域。

例如，如果您定义了一个与 防火墙管理中心 中名为 **domain.example.com** 的域相对应的领域，但系统报告从名为 **another-domain.example.com**的域进行了登录，这种情况就属于 领域不匹配。 防火墙管理中心 将此域中的用户识别为“未知”。

您将不匹配阈值设置为某个百分比，高于此百分比时会触发运行状况警告。示例：

- 如果您使用默认为 50% 的不匹配阈值，则在八个传入会话中有两个不匹配领域（不匹配百分比为 25%）的情况下不会触发任何警告。
- 如果您将不匹配阈值设置为 30%，在五个传入会话中有三个不匹配领域（不匹配百分比为 60%）的情况下则会触发警告。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

有关详细信息，请参阅检测领域或用户不匹配，第 2053 页。

症状：无法下载用户

可能的原因如下：

- 如果您配置的领域**类型**不正确，则将由于系统期望的属性与存储库提供的属性之间不匹配而无法下载用户和组。例如，如果您为 Microsoft Active Directory 领域将**类型**配置为 **LDAP**，则系统期望 `uid` 属性，而在 Active Directory 上它将被设置为`无`。（Active Directory 存储库将 `sAMAccountName` 用于用户 ID。）

  解决方案：适当设置领域**类型**字段：对于 Microsoft Active Directory，设置为 **AD**；对于其他受支持的 LDAP 存储库，设置为 **LDAP**。

- 组或组织单位名称中包含特殊字符的 Active Directory 组中的用户，可能不可用于身份策略规则。例如，如果组或组织单位名称包含字符星号 (*)、等号 (=) 或反斜线 (\)，则这些组中的用户无法下载，并且无法用于身份策略。

  解决方案：从组或组织单位名称中删除特殊字符。



重要事项 要减少 Secure Firewall Management Center 和主用目录域控制器间的延迟，我们强烈建议您配置一个在地理位置上尽可能靠近 Secure Firewall Management Center的领域目录（即域控制器）。

例如，如果您的 Secure Firewall Management Center 位于北美，请配置一个也位于北美的领域目录。否则，可能会导致用户和组下载超时等问题。

症状：并非一个领域的所有用户都被下载

可能的原因如下：

- 如果尝试下载的用户数超过任何一个领域的最大数量，则下载将在达到最大用户数时停止，同时显示运行状况警报。用户下载限制按 Secure Firewall Management Center 型号来设置。有关详细信息，请参阅Microsoft Active Directory 的用户限制，第 1988 页。
- 每个用户都必须是组的成员。不属于任何组的用户不会被下载。

症状：访问控制策略不匹配组成员

此解决方案适用于与其他 AD 域建立信任关系的 AD 域。在以下讨论中，外部域指用户登录的域之外的域。

如果用户属于受信任的外部域中定义的某个组， Secure Firewall Management Center 则不会跟踪外部域中的成员。例如，请考虑以下情景：

- 域控制器 1 和 2 相互信任
- A 组在域控制器 2 上定义
- 控制器 1 中的用户 `mparvinder` 是 A 组的成员

即使用户 `mparvinder` 在 A 组中，指定 A 组成员身份的 Secure Firewall Management Center 访问控制策略规则也不与之匹配。

解决方案：在包含属于 B 组的所有域 1 帐户的域控制器 1 中创建类似的组。更改访问控制策略规则以匹配 A 组或 B 组的任何成员。

症状：访问控制策略与子域成员资格不匹配

如果用户属于母域的子域，Firepower 不跟踪域之间的母/子关系。例如，请考虑以下情景：

- 域 `child.parent.com` 是域 `parent.com` 的子域
- 用户 `mparvinder` 在 `child.parent.com` 中定义

即使用户 `mparvinder` 在子域中，与 `parent.com` 匹配的 Firepower 访问控制策略规则也与 `child.parent.com` 域中的 `mparvinder` 不匹配。

解决方案：将访问控制策略规则更改为匹配 `parent.com` 或 `child.parent.com` 中的成员。

症状：领域或领域目录测试失败

目录页面上的**测试**按钮将向您输入的主机名或 IP 地址发送 LDAP 查询。如果该查询失败，请检查以下事项：

- 您输入的**主机名**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- 您输入的 **IP 地址**无效。

领域配置页面上的 **测试 AD 加入** 按钮将验证以下事项：

- DNS 将 **AD 主域**解析到 LDAP 服务器或 Active Directory 域控制器的 IP 地址。
- **AD 加入用户名**和 **AD 加入密码**正确无误。

  AD 加入用户名必须是完全限定的（例如， **`administrator@mydomain.com`** ，而不是 **`administrator`**）。
- 用户有足够的权限在域中创建计算机，并将 Secure Firewall Management Center 作为域计算机加入到该域。

症状：在非正常时间发生用户超时

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 服务器上的时间与 Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

如果您发现系统在非预期时间间隔时执行用户超时，请确认 ISE/ISE-PIC 或 TS 代理服务器上的时间与 Secure Firewall Management Center上的时间是否同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

症状：先前未发现的 ISE/ISE-PIC 用户代理用户的用户数据未显示在 Web 界面上

在系统检测到其数据尚未包含在数据库中的 ISE/ISE-PIC 或 TS 代理用户的活动后，系统会从服务器检索其有关信息。在某些情况下，系统需要额外时间来从 Microsoft Windows 服务器成功检索此信息。在数据检索成功之前，ISE/ISE-PIC 或 TS 代理用户发现的活动不显示在 Web 界面中。

请注意，这还可防止系统使用访问控制规则处理用户的流量。

症状：事件中的用户数据为意外

如果您发现用户或用户活动事件包含意外 IP 地址，请检查您的领域。系统不支持为多个领域配置相同的 **AD 主域**值。

症状：源于终端服务器登录的用户未被系统唯一识别

如果部署包括终端服务器，并为连接到该终端服务器的一个或多个服务器配置领域，则必须部署思科终端服务 (TS) 代理以准确报告终端服务器环境中的用户登录。在安装并配置后，TS 代理将唯一端口分配给个人用户，因此系统可在 Web 界面中唯一识别这些用户。

有关 TS 代理的详细信息，请参阅《思科终端服务 *(TS)* 代理指南》。

检测领域或用户不匹配

本部分讨论如何检测领域或用户不匹配，其定义为：

- 用户不匹配：系统不下载某个用户而是报告给 Secure Firewall Management Center 。

  造成用户不匹配通常是因为该用户属于不予下载至 Secure Firewall Management Center。请回顾 *Cisco Secure Firewall Management Center* 设备配置指南中介绍的信息。

- 领域不匹配：某个用户登录到某个域，而该域对应 防火墙管理中心未知的某个领域。

有关其他详细信息，请参阅领域和用户下载故障排除，第 2049 页。

系统不会对不匹配身份规则的未知用户应用任何策略。（虽然可以对未知用户设置身份规则，但我们建议您正确识别用户和领域，将规则数量保持在最低限度。）

过程

步骤 1 启用领域或用户不匹配检测：

a) 如果尚未登录，请登录 Firewall Management Center。
b) 请点击 **故障排除** > **+ 显示更多** > **运行状况** > **策略** 。
c) 创建新运行状况策略或编辑现有运行状况策略。
d) 在“编辑策略”页面上，设置**策略运行时间间隔**。
这是所有运行状况监控任务的运行频率。
e) 在左侧窗格中，点击**领域 (Realm)**。
f) 输入以下信息：

- **启用**：点击**打开**
- **警告用户匹配阈值百分比**：在运行状况监控器中触发警告的领域不匹配或用户不匹配的百分比。有关详细信息，请参阅领域和用户下载故障排除，第 2049 页。

g) 在页面底部，点击**保存策略并退出**。
h) 如*Cisco Secure Firewall Management Center* 管理指南中的应用运行状况策略所述，对托管设备应用运行状况策略。

步骤 2 通过以下任意方式查看用户和领域不匹配：

- 如果超出警告阈值，点击 防火墙管理中心顶部导航中的 **经过** > **运行状况** 。这将打开运行状况监控器。
- 请点击 > **运行状况** > **监控器故障排除** 。

步骤 3 在“运行状况监控器”页面上的“显示”列中，展开**领域：域**或**领域：用户**来查看有关不匹配的详细信息。

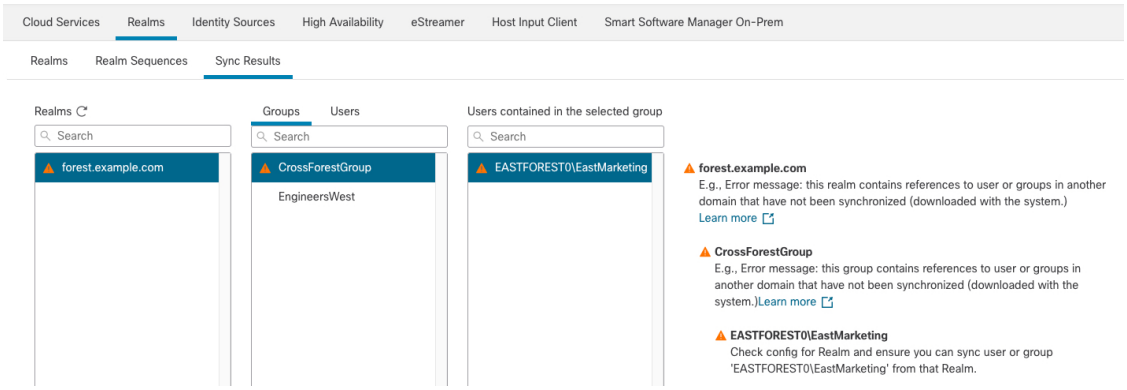
排除跨域信任故障

对跨域信任 Secure Firewall Management Center 配置进行故障排除的典型问题包括：

- 不为具有共享组的所有林添加领域或目录。
- 配置领域以排除下载用户，并且这些用户在不同领域的组中被引用。
- 某些临时问题。

了解问题

如果 Firewall Management Center 能够将用户和组与您的 Active Directory 目录林同步存在问题，系统将显示“同步结果”选项卡页面，如下所示。



下表介绍如何解释信息。

列	含义
领域	显示系统中配置的所有领域。点击 **刷新** （）以更新领域列表。 **黄色三角形**（）显示来指示领域中的问题。 如果所有用户和组成功同步，则领域旁边不显示任何内容。
组	点击**组 (Groups)** 以显示领域中的所有组。与领域一样，**黄色三角形**（）显示表示问题。 点击 **黄色三角形**（）查看有关此问题的更多详细信息。
用户	点击**用户 (Users)** 以显示按组排序的所有用户。
所选组中包含的用户	显示您在“组”列中选择的组中的所有用户。点击 **黄色三角形**（）可在表的右侧显示更多信息。
包含所选用户的组	显示所选用户所属的所有组。点击 **黄色三角形**（）可在表的右侧显示更多信息。

列	含义
错误详细信息（显示在表的右侧）。	系统会显示无法同步的 NetBIOS 林名称和组名称。系统无法同步这些用户和组的典型原因如下： • **问题：**包含组和用户的林没有在 Firewall Management Center中配置相应的领域。 **解决方案：**如 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述，为包含该组的林添加一个领域。 • **问题：**已将组下从载到 Firewall Management Center中排除。 **解决方案：**点击**领域 (Realms)** 选项卡页面，点击 **编辑** ()，然后从**排除的组和用户 (Excluded Groups and Users)** 列表中移动指示的组或用户。

再次尝试下载用户和组

如果问题是临时的，请下载所有领域的用户和组。

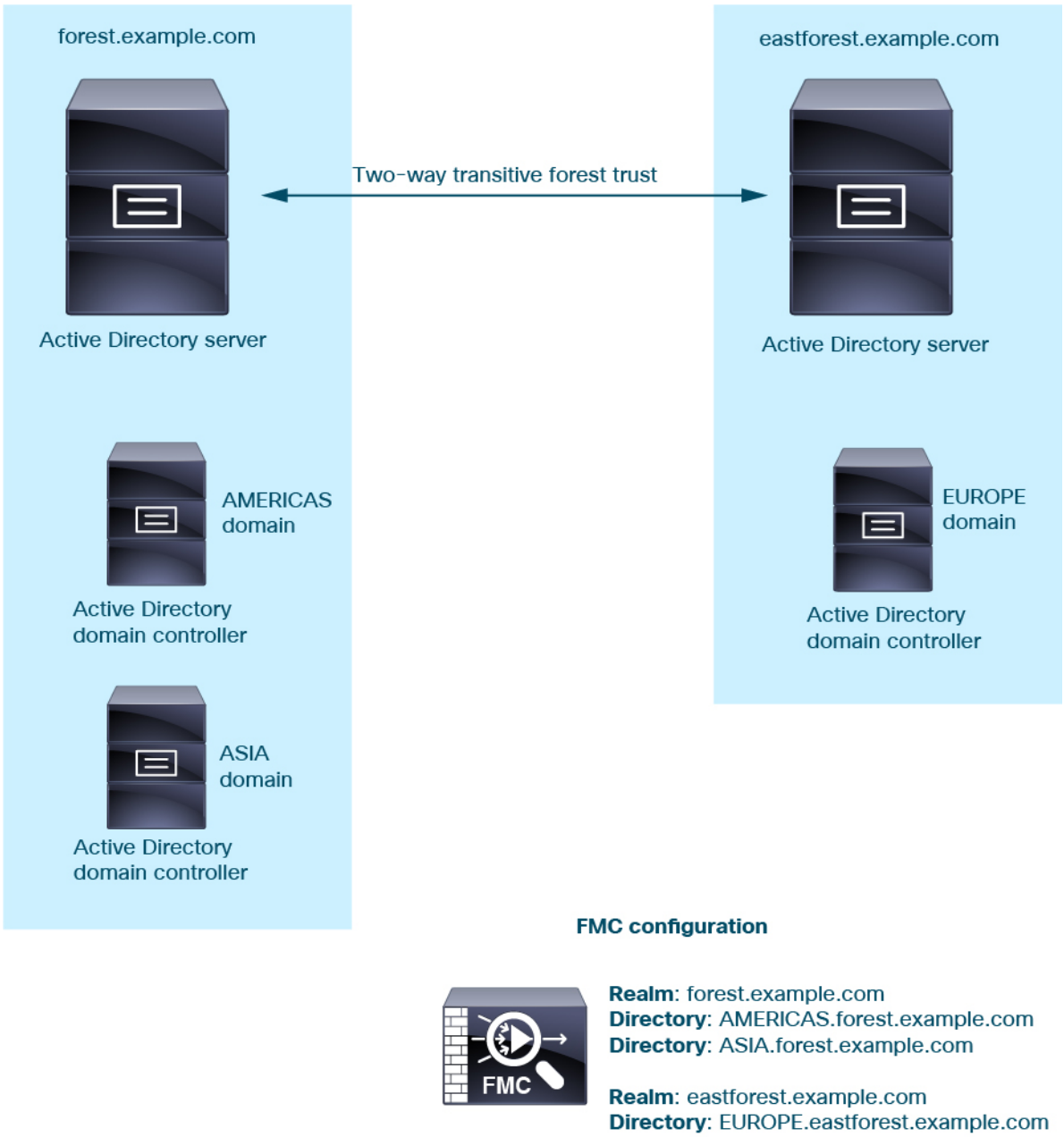
1. 如果尚未登录，请登录 Firewall Management Center。
2. 请点击 **集成** > **身份** > **领域** > **领域**。
3. 请点击 **下载** （）。
4. 点击 **同步结果 (Sync Results)** 选项卡页面。
5. 如果“领域”列中的条目未显示指示器，则问题已解决。

为所有林添加领域

确保已配置：

- 具有要在身份策略中使用的用户的每个林的Firewall Management Center 领域。
- 该林中每个域控制器的 Firewall Management Center 目录，其中包含要在身份策略中使用的用户。

下图显示了一个示例。

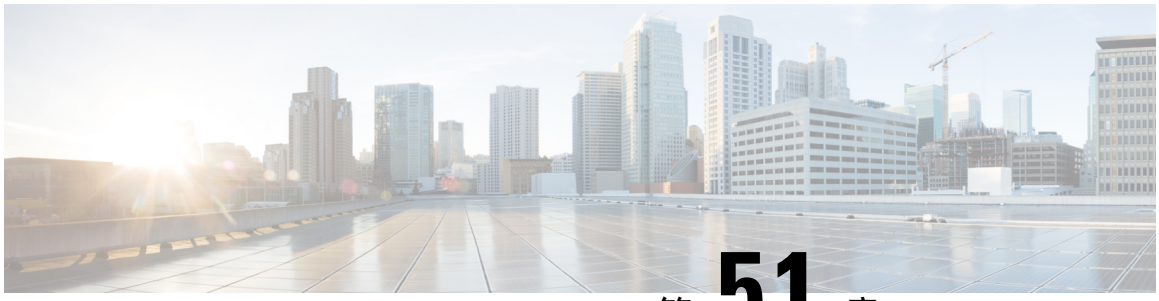

forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

领域的历史记录

表 *118:*

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Microsoft Azure Active Directory (SAML) 领域。	7.6.0	7.4.0	您现在可以使用 Microsoft Azure Active Directory (AD) 领域进行主动和被动身份验证： • 使用 Azure AD 进行主动身份验证：使用 Azure AD 作为强制网络门户。 • 使用思科 ISE（版本 7.4.0 中引入）的被动身份验证：防火墙管理中心从 Azure AD 获取组，从 ISE 获取登录用户会话数据。 我们使用 SAML（安全断言标记语言）在服务提供程序（处理身份验证请求的设备）和身份提供程序 (Azure AD) 之间建立信任关系。 **升级影响**。如果您在升级之前配置了 Microsoft Azure AD 领域，它将显示为 SAML - 为被动身份验证配置的 Azure AD 领域。所有以前的用户会话数据都将保留。 新增/修改的屏幕： **集成 (Integration)** > **其他集成 (Other Integrations)** > **领域 (Realms)** > **添加领域 (Add Realm)** > **SAML - Azure AD** 新增/修改的 CLI 命令：无
Microsoft Azure Active Directory (AD) 领域。	7.4.0	7.4.0	您可以将 Microsoft Azure Active Directory (AD) 领域与 ISE 配合使用来对用户进行身份验证并获取用户会话以进行用户控制。 新增/修改的屏幕：**系统** > **集成** > **领域** > **添加领域** > **Azure AD**
代理序列。	7.2.0	7.2.0	与领域序列类似，代理序列是在 Security Cloud Control 无法与 LDAP 或 Active Directory 服务器通信的情况下可以与 Security Cloud Control 通信的一个或多个托管设备。 新增/修改的屏幕：**集成** > **其他集成** > **领域** > **代理序列**
Active Directory 域的跨域信任。	7.2.0	7.0.0	一组相互信任的 Microsoft Active Directory (AD) 域通常被称为林。此信任关系可使域以不同方式访问彼此的资源。例如，在域A中定义的用户账号可以标记为域 B 中所定义组的成员。 防火墙管理中心 可以从 Active Directory 目录林获取用户以进行身份规则。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
领域序列。	7.2.0	6.7.0	领域序列是要应用身份规则的两个或多个领域的排序列表。将领域序列与身份策略关联时，Firepower 系统会按照领域序列中指定的从第一个到最后的顺序来搜索 Active Directory 域。 新增/修改的屏幕：**集成** > **其他集成** > **领域** > **领域序列系统** > **集成** > **领域** > **领域序列**
用于用户控制的领域。	7.2.0	任意	领域是 防火墙管理中心（Active Directory 或 LDAP 用户存储库）之间的连接。



第 51 章

身份源：强制网络门户

- 强制网络门户身份源， 第 2059 页
- 强制门户的许可证要求， 第 2060 页
- 强制网络门户的要求和先决条件， 第 2060 页
- 强制网络门户准则和限制， 第 2060 页
- 如何为用户控制配置强制网络门户， 第 2063 页
- 强制网络门户身份源故障排除， 第 2075 页
- 强制网络门户历史记录， 第 2077 页

强制网络门户身份源

强制网络门户是系统支持的授权身份源之一。强制网络门户是一种主动身份验证方法，其中用户可以使用托管设备验证网络登录。（RA-VPN 是另一种类型的主动身份验证。）主动身份验证与被动身份验证的不同之处在于，托管设备会向用户显示登录页面，而被动身份验证会查询身份验证领域（例如 Microsoft AD）来对用户进行身份验证。

通常使用强制网络门户要求身份验证访问互联网，或者访问受限制的内部资源；可以选择配置对资源的访客访问。在系统对强制网络门户用户进行身份验证后，会根据访问控制规则处理其用户流量。强制网络门户仅会对 HTTP 和 HTTPS 流量执行身份验证。

注释 要将 Microsoft Azure AD (SAML) 领域用于强制网络门户，请参阅创建一个 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户），第 2014 页。

注释 必须先对 HTTPS 流量进行加密，然后强制网络门户才能执行身份验证。

强制网络门户还记录失败的身份验证尝试。如果尝试失败，则不会将新用户添加到数据库的用户列表中。强制网络门户报告的身份验证活动失败的用户活动类型是**身份验证失败的用户 (Failed Auth User)**。

从强制网络门户获取的身份验证数据可用于用户感知和用户控制。

相关主题

如何为用户控制配置强制网络门户，第 2063 页

关于主机名重定向

（仅限 Snort 3。）主动身份验证身份规则会使用其配置的接口重定向到强制网络门户端口。由于重定向通常是指向 IP 地址，因此用户会收到不受信任的证书错误，并且由于此行为类似于中间人攻击，因此用户可能不愿意接受不受信任的证书。

为避免此问题，您可以将强制网络门户配置为使用托管设备的完全限定域名 (FQDN)。使用正确配置的证书时，用户不会收到不受信任的证书错误，并且身份验证将更加无缝，且看起来更加安全。

相关主题

重定向到主机名的网络规则条件，第 2216 页

强制门户的许可证要求

威胁防御 许可证

任意

强制网络门户的要求和先决条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

强制网络门户准则和限制

在身份策略中配置和部署强制网络门户时，来自指定领域的用户会使用 Firewall Threat Defense 来进行身份验证，以访问您的网络。

注释 如果远程接入VPN用户已通过作为安全网关的托管设备进行主动身份验证，则不会执行强制网络门户主动身份验证，即便身份策略中配置了该验证方式。

强制网络门户和策略

在身份策略中配置强制网络门户并在身份规则中调用主动身份验证。身份策略与访问控制策略相关联，访问控制策略定义对网络中资源的访问。例如，您可以排除 US-West/Finance 组中的用户访问 Engineering 服务器，也可以禁止用户访问网络上的非安全应用。

您可以在身份策略的**主动身份验证**选项卡页面上配置一些强制网络门户身份策略设置，并在与访问控制策略关联的身份规则中配置其余部分。

主动身份验证规则具有**主动身份验证**规则操作或**被动身份验证**规则操作，并且**如果无法建立被动或 VPN 识别，则使用主动身份验证**已选中。不管上述哪种情况，系统都会透明地启用或禁用 TLS/SSL 解密，从而重启 Snort 进程。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 a 解密策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”(Unknown)。为避免用户被识别为未知，请将领域 或领域序列 配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

有关同步用户和组的详细信息，请参阅同步用户和组，第 2037 页。

需要路由接口

只有配置了路由接口的设备，才能执行强制网络门户主动身份验证。如果要为强制网络门户配置身份规则，并且您的强制网络门户设备包含内联接口和路由接口，则必须在访问控制策略中配置接口规则条件，以便仅针对设备上的路由接口。

如果访问控制策略相关的身份策略包含一个或多个强制网络门户身份规则，并且您在管理一个或多个配置了路由接口的设备的 Secure Firewall Management Center 上部署策略，则策略部署成功且路由接口执行主动身份验证。

所需的证书和证书颁发机构

在使用强制网络门户进行用户控制和感知之前，您必须满足以下所有条件：

- 要使用 Microsoft AD 进行身份验证，请导出服务器的根证书并将其作为受信任的 CA 证书导入到 Secure Firewall Management Center 中。

- 用于向部署了身份策略的托管设备进行身份验证的内部证书对象。
- 所需解密规则的内部证书颁发机构。

您可以在创建解密策略时创建内部证书和内部证书颁发机构。

强制网络门户要求和限制

请注意以下要求和限制：

- 强制网络门户不支持 HTTP/3 QUIC 连接。
- 系统每秒最多支持 20 次强制网络门户登录。
- 对于计入最大登录尝试次数的失败登录尝试，失败登录尝试之间存在最长五分钟的时间限制。该五分钟限制不可配置。

  （最大登录尝试次数显示在连接事件中：**事件和日志** > **+ 显示更多** > **连接** > **事件**。）

  如果失败登录之间的间隔时间超过五分钟，则用户将被重定向到强制网络门户进行身份验证，而不会被指定为登录失败的用户或访客用户，也不会报告给 Secure Firewall Management Center。
- 强制网络门户不会协商 TLS v1.0 连接。

  仅支持 TLS v1.1、v1.2 和 TLS 1.3 连接。
- 要从强制网络门户安全地注销用户并防止用户再次登录，管理员可以关闭其会话：**事件和日志**> **用户** > **活动会话**。如果用户关闭浏览器，则浏览器不会自动重新进行身份验证。
- 如果为父域创建了领域，并且托管设备检测到有用户登录到该父域的子域，则托管设备不会检测用户的后续注销。
- 您的访问控制规则必须允许流量流向计划用于强制网络门户的设备的 IP 地址和端口。
- 要对 HTTPS 流量执行强制网络门户主动身份验证，必须使用 a 解密策略解密来自要对其进行身份验证的用户的流量。您无法解密托管设备上强制网络门户用户的 Web 浏览器和强制网络门户后台守护程序之间的连接中的流量；此连接用于对强制网络门户用户进行身份验证。
- 要限制允许流经托管设备的非 HTTP 或 HTTPS 流量的量，您应在身份策略的**端口**选项卡页面中输入典型的 HTTP 和 HTTPS 端口。

  托管设备在确定传入请求未使用 HTTP 或 HTTPS 协议时，会将先前未发现的用户从**待定**更改为**未知**。托管设备将用户从 **待定** 状态更改为其他状态之后，访问控制、服务质量和 解密策略 便可以应用到该流量。如果您的其他策略不允许非 HTTP 或 HTTPS 流量，则在强制网络门户身份策略上配置端口可以防止允许不需要的流量流经托管设备。

Kerberos 前提条件

如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。

DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。

如何为用户控制配置强制网络门户

开始之前

要使用强制网络门户进行主动身份验证，必须设置一个 LDAP 领域；或者一个Microsoft AD 领域 或领域序列；Microsoft Azure AD (SAML) 领域；访问控制策略；一个身份策略；a 解密策略；并将身份和解密策略与相同的访问控制策略关联。最后，必须将这些策略部署到托管设备。此主题介绍这些任务的高度概要。



注释 要将 Microsoft Azure AD (SAML) 领域用作强制网络门户，请参阅如何创建 用于主动身份验证的 Microsoft Azure AD (SAML) 领域（强制网络门户），第 2005 页。

首先，请执行以下任务：

- 确认您的 Secure Firewall Management Center 使用已配置的路由接口管理一台或多台设备。
- 要将加密身份验证用于强制网络门户，要么为进行身份验证的托管设备创建一个 PKI 对象，要么使证书数据和密钥可在用于访问 Secure Firewall Management Center的机器上使用。要创建 PKI 对象，请参阅PKI，第 2661 页。

过程

步骤 1 按照以下主题中所述，创建一个 LDAP 领域并将其启用；或者创建一个 Microsoft AD 领域以及可选的领域序列并将其启用：

- 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页
- 同步用户和组，第 2037 页

要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅同步用户和组，第 2037 页。

步骤 2 获取所需的证书和证书颁发机构
您必须具备以下所有条件：

- 要使用 Microsoft AD 进行身份验证，请导出服务器的根证书并将其作为受信任的 CA 证书导入到 Secure Firewall Management Center 中。
- 用于向部署了身份策略的托管设备进行身份验证的内部证书对象。
- 所需解密规则的内部证书颁发机构。

您可以在创建解密策略时创建内部证书和内部证书颁发机构。

步骤 3 使用关联的证书颁发机构创建网络对象。

请参阅 创建网络对象，第 2064 页。

步骤 4 使用主动身份验证规则创建身份策略。

在使用强制网络门户执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。

有关详细信息，请参阅创建身份策略和主动身份验证规则，第 2066 页。

步骤 5 为强制网络门户配置允许强制网络门户端口（默认情况下为 TCP 885）上的流量的访问控制规则。

您可以为要使用的强制网络门户选择任何可用的 TCP 端口。无论选择哪个端口，都必须创建一条允许该端口上的流量的规则。

有关详细信息，请参阅创建 TCP 端口访问控制规则，第 2068 页。

步骤 6 再添加一条访问控制规则，以允许所选领域或领域序列中的用户使用强制网络门户访问资源。

有关详细信息，请参阅创建用户访问控制规则，第 2069 页。

步骤 7 为 **未知** 用户配置 a 解密策略 和 **解密 - 重签** 规则，以使强制网络门户用户能够使用 HTTPS 协议访问网页。

仅当HTTPS流量在流量发送到强制网络门户之前被解密的情况下，强制网络门户才能进行用户身份验证。系统本身将强制网络门户视为**未知**用户。

创建带有出站规则的解密策略，第 2070 页

步骤 8 将身份和 解密策略 与第 3 步的访问控制策略相关联。

这是最后一步，此后系统即可使用强制网络门户进行用户身份验证。

有关详细信息，请参阅将身份策略和解密策略与访问控制策略相关联，第 2072 页。

下一步做什么

请参阅创建网络对象，第 2064 页。

相关主题

排除强制网络门户中的应用，第 2074 页
PKI，第 2661 页
强制网络门户身份源故障排除，第 2075 页
Snort 重新启动场景，第 172 页

创建网络对象

此任务讨论如何开始将强制网络门户配置为身份源。

开始之前

（仅限 Snort 3。）使用 DNS 服务器创建完全限定的主机名 (FQDN) 并将 Firewall Threat Defense 的内部证书上传至 Firewall Management Center。如果您之前从未使用过例如 此类 资源，可以咨询此类资源。在 Firewall Management Center 托管的一台设备上指定路由接口的 IP 地址。

有关网络对象的详细信息，请参阅 重定向到主机名的网络规则条件，第 2216 页。

过程

步骤 1 如果尚未这样子，请登录 Firewall Management Center。

步骤 2 请点击 **对象**。

步骤 3 展开 **PKI**。

步骤 4 点击 **内部证书**。

步骤 5 点击 **Add Internal Cert**。

步骤 6 在**名称 (Name)** 字段中，输入名称以标识内部证书（例如，**`MyCaptivePortal`**）。

步骤 7 在 **证书数据** 字段中，粘贴证书或使用 **浏览** 按钮查找证书。

证书公用名必须与您想要强制网络门户用户进行身份验证的 FDQN 完全匹配。

步骤 8 在 **密钥** 字段中，粘贴证书的私钥或使用 **浏览** 按钮查找证书。

步骤 9 如果证书已加密，请选中 **已加密** 复选框并在相邻字段中输入密码。

步骤 10 点击**保存**。

步骤 11 点击**网络 (Network)**。

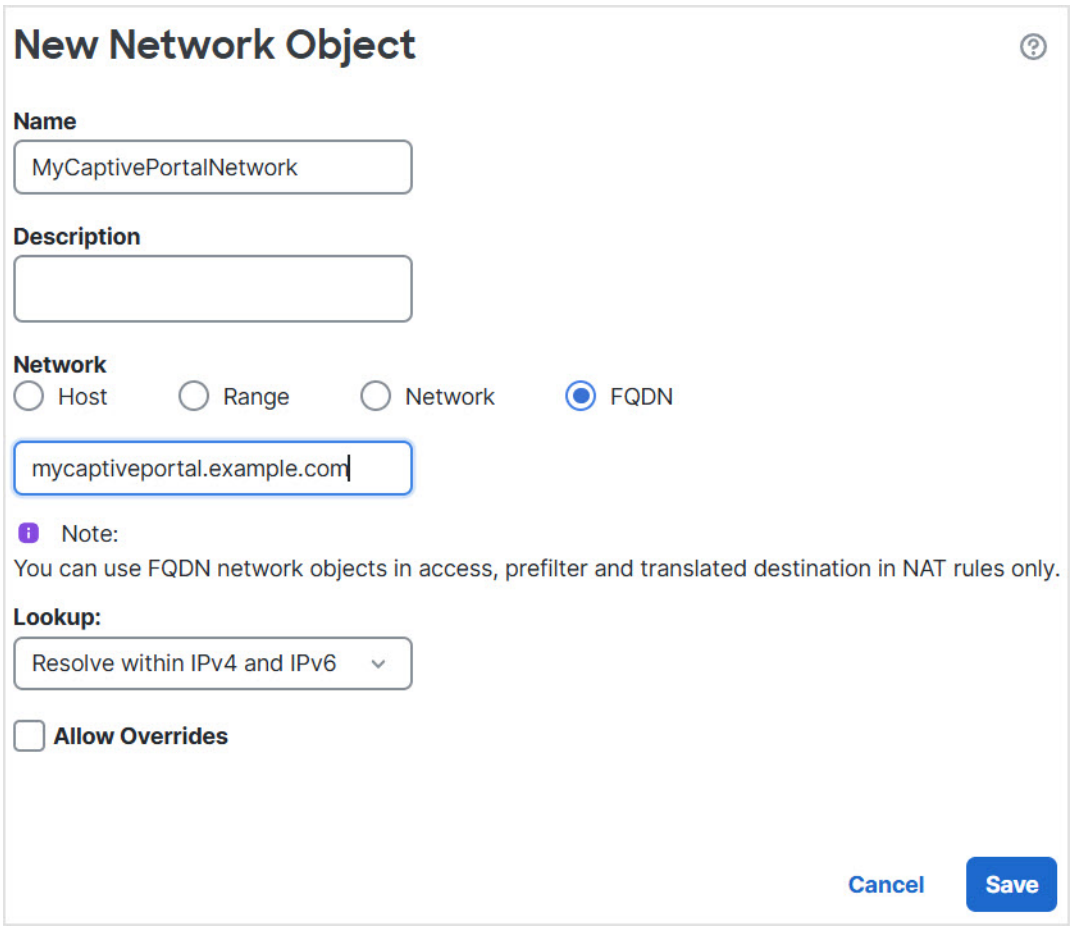
步骤 12 点击 **添加网络 (Add Network)** > **添加对象 (Add Object)**。

步骤 13 在 **名称** 字段中，输入名称以标识对象（例如， **`MyCaptivePortalNetwork`**）。

步骤 14 点击 **FDQN**，然后在字段中输入强制网络门户的FDQN的名称。

步骤 15 点击 **查找**选项。

下图显示了一个示例。



步骤 16 点击**保存**。

下一步做什么

创建身份策略和主动身份验证规则， 第 2066 页

创建身份策略和主动身份验证规则

开始之前

此由多个部分组成的程序展示如何使用默认 TCP 端口 885 以及将 Secure Firewall Management Center 服务器证书用于强制网络门户和 TLS/SSL 解密来设置强制网络门户。本示例中的每个部分介绍启用强制网络门户来执行主动身份验证所需的一项任务。

如果您遵循此程序中的所有步骤，则可以将强制网络门户配置为供您的域中的用户使用。您可以选择执行在程序的各个部分中介绍的其他任务。

有关完整程序的概述，请参阅如何为用户控制配置强制网络门户， 第 2063 页。

过程

步骤 1 如果尚未登录，请登录 Firewall Management Center。

步骤 2 选择 **策略** > **安全策略** > **身份**，并创建或编辑身份策略。

步骤 3 （可选。）点击**添加类别**，为强制网络门户身份规则添加类别，然后为该类别输入一个**名称**。

步骤 4 点击**主动身份验证**选项卡。

步骤 5 从列表中选择适当的根**服务器证书**，或者点击 **添加** (+) 以添加证书。

有关详细信息，请参阅 安全地连接到 Active Directory 或 LDAP，第 2035 页。

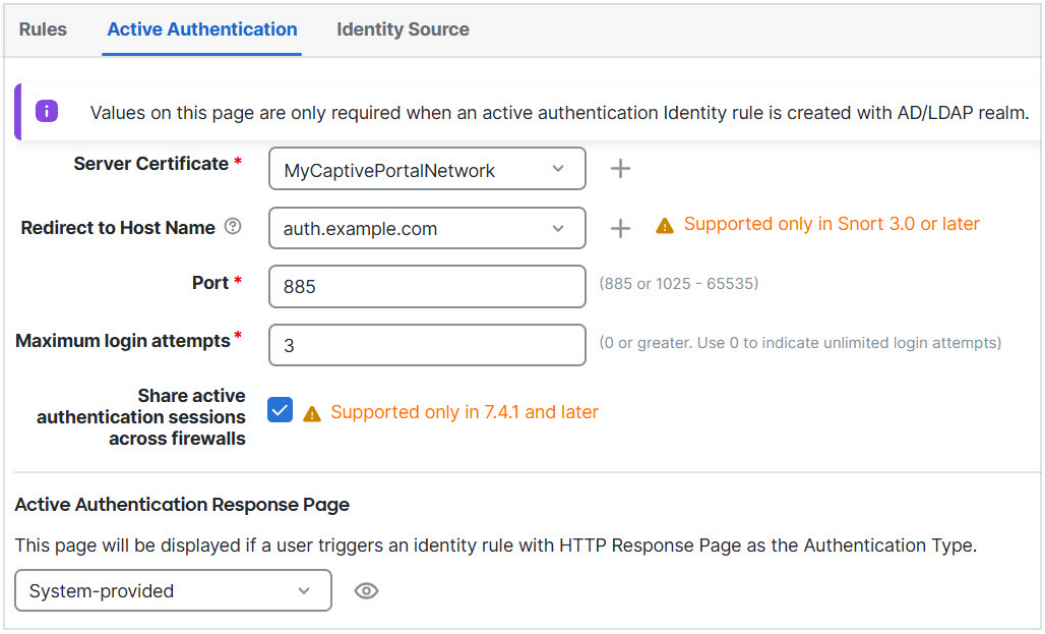
注释
强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

步骤 6 从 **重定向到主机名 (Redirect to Host Name)** 字段中，点击之前创建的网络对象或者点击 **添加** (+)。

步骤 7 在**端口**字段中输入 **885**，然后指定**最大登录尝试次数**。

步骤 8 取消选中 **跨防火墙共享主动身份验证 (Share active authentication across firewalls)**，以便让 Firewall Management Center 强制要求用户在每次使用与上次不同的托管设备访问您的网络时重新进行身份验证。
有关此选项的详细信息，请参阅强制网络门户字段，第 2073 页。

步骤 9 （可选。）选择**主动身份验证响应页面**，如强制网络门户字段，第 2073 页中所述。



步骤 10 （如果仅从早期版本升级到版本 7.4.1，并且使用领域序列对用户进行身份验证。）点击 **编辑** (✎) 并查看 更新自定义身份验证表单，第 2068 页。

步骤 11 点击**保存**。

步骤 12 点击**规则 (Rules)**。

步骤 13 点击 **添加规则** 以添加新的强制网络门户身份策略规则，或者点击 **编辑** (✎) 以编辑现有规则。

步骤 14 为规则输入**名称 (Name)**。

步骤 15 从**操作**列表中，选择**主动身份验证**。

步骤 16 点击 **领域和设置**。

步骤 17 从**领域 (Realms)** 列表中，选择要用于用户身份验证的领域或领域序列。

步骤 18 （可选。）选中**如果身份验证无法识别用户，则识别为访客**。有关详细信息，请参阅强制网络门户字段，第 2073 页。

步骤 19 从列表中选择**身份验证协议 (Authentication Protocol)**。

如果选择 **NTLM**、 **Kerberos**或 **HTTP 协商 (HTTP Negotiate)** 身份验证协议，则无法使用领域序列来对用户进行身份验证。改为选择 **HTTP 基本 (HTTP Basic)** 或 **HTTP 响应页面 (HTTP Response Page)** 。

步骤 20 （可选。）要豁免强制网络门户中的特定应用流量，请参阅排除强制网络门户中的应用，第2074页。

步骤 21 向规则（端口、网络等）添加条件，如身份规则条件，第 2215 页中所述。

步骤 22 点击**添加 (Add)**。

步骤 23 在该页面顶部，点击**保存**。

下一步做什么

继续执行创建 TCP 端口访问控制规则，第 2068 页。

更新自定义身份验证表单

从早期版本升级到版本 7.4.1（或更高版本）后，必须将以下行添加到自定义身份验证表单，用户才能在使用强制网络门户进行身份验证时查看域列表。（如果使用 HTTP 响应页面身份验证类型，则始终需要执行此任务；如果用户使用其他身份验证类型对领域进行身份验证，则此任务为可选任务。）

在身份规则的**主动身份验证 (Active Authentication)** 选项卡页面上，点击 **编辑** (✎) 并在表单中要求用户登录的部分输入以下内容：

```
<select name="realm" id="realm"></select>
```

创建 TCP 端口访问控制规则

该程序的这一部分显示如何创建访问控制规则，以允许强制网络门户使用 TCP 端口 885（它是强制网络门户的默认端口）与客户端通信。如果您希望，也可以选择另一个端口，但该端口必须与您在创建身份策略和主动身份验证规则，第 2066 页中选择的端口匹配。

开始之前

有关整个强制网络门户配置的概述，请参阅如何为用户控制配置强制网络门户，第 2063 页。

过程

步骤 1 如果尚未登录，请登录 Firewall Management Center。

步骤 2 如果尚未进行此操作，则请创建强制网络门户证书，如 PKI，第 2661 页中所述。

步骤 3 点击 **策略** > **安全策略** > **访问控制** 并创建或编辑访问控制策略。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 为规则输入**名称 (Name)**。

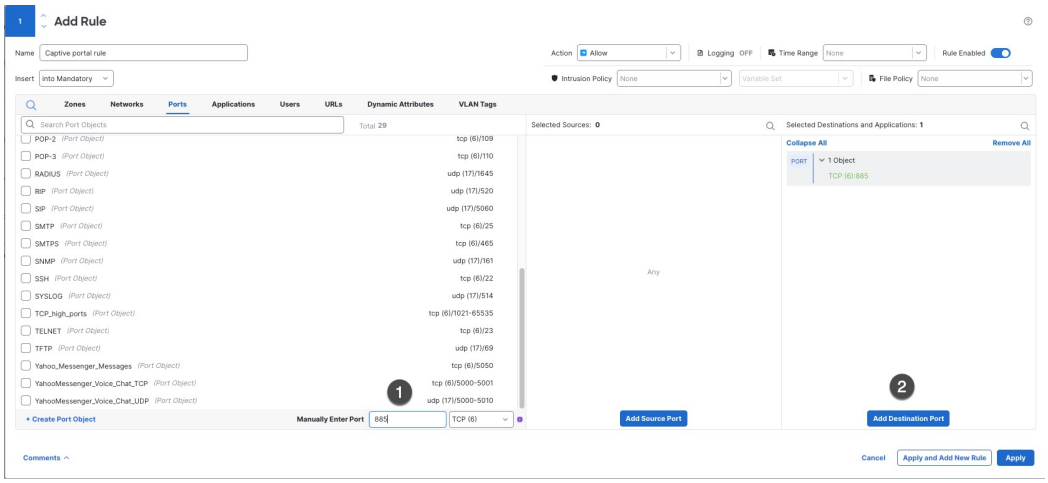
步骤 6 从**操作**列表中选择**允许**。

步骤 7 点击**端口 (Ports)**。

步骤 8 从**所选目标端口**字段下的**协议**列表中，选择 **TCP**。

步骤 9 在**端口**字段中，输入 **885**。

步骤 10 点击**端口 (Port)** 字段旁边的**添加 (Add)**。
下图显示了一个示例。



步骤 11 点击页面底部的**添加 (Add)**。

下一步做什么

继续执行创建用户访问控制规则，第 2069 页。

创建用户访问控制规则

该过程的此部分讨论如何添加访问控制规则，以使领域中的用户能够使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如何为用户控制配置强制网络门户 ， 第 2063 页。

过程

步骤 1 在规则编辑器中，点击**添加规则 (Add Rule)**。

步骤 2 为规则输入**名称 (Name)**。

步骤 3 从**操作**列表中选择**允许**。

步骤 4 点击**用户 (Users)**。

步骤 5 在**可用领域**列表中，点击要允许的领域。

步骤 6 如果没有显示领域，则请点击 **刷新** ( )。

步骤 7 在**可用用户**列表中，选择要添加到规则的用户，然后点击**添加到规则**。

步骤 8 （可选。）向访问控制策略添加条件，如身份规则条件 ， 第 2215 页中所述。

步骤 9 点击**添加 (Add)**。

步骤 10 在访问控制规则页面上，点击**保存**。

步骤 11 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

下一步做什么

创建带有出站规则的解密策略 ， 第 2070 页

创建带有出站规则的解密策略

程序的此部分介绍如何创建 a 解密策略 ， 以在流量到达强制网络门户之前解密和重签流量。强制网络门户仅可对解密的流量进行身份验证。

开始之前

您的出站服务器必须具有内部证书颁发机构 (CA)；换言之，是指为强制网络门户用户解密流量以进行身份验证的托管设备。该证书必须不同于用于验证托管设备的强制网络门户的内部证书。

过程

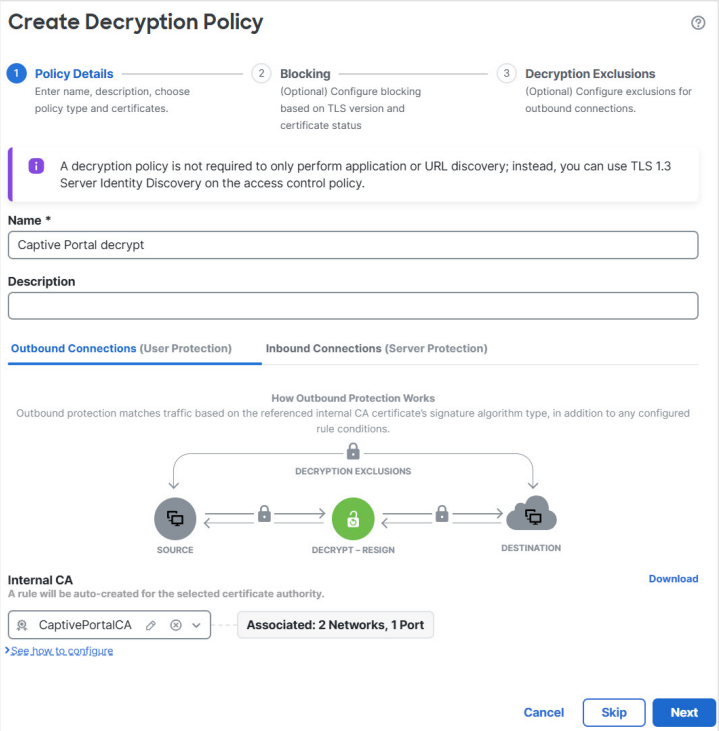
步骤 1 如果尚未登录，请登录防火墙管理中心。

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击**新建策略 (New Policy)**。

步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。



步骤 6 为规则上传或选择证书。

系统会根据 CA 和网络/端口的组合创建一条规则。

步骤 7 （可选。）选择网络和端口。

了解更多信息：

- 解密规则基于规则的解密规则 条件， 第 1920 页
- 网络规则条件， 第 1420 页
- 端口规则条件， 第 1421 页

步骤 8 点击**保存**。

步骤 9 点击您创建的解密策略旁边的 **编辑** ()。

步骤 10 点击强制网络门户的解密规则旁边的 **编辑** ()。

步骤 11 点击**用户 (Users)**。

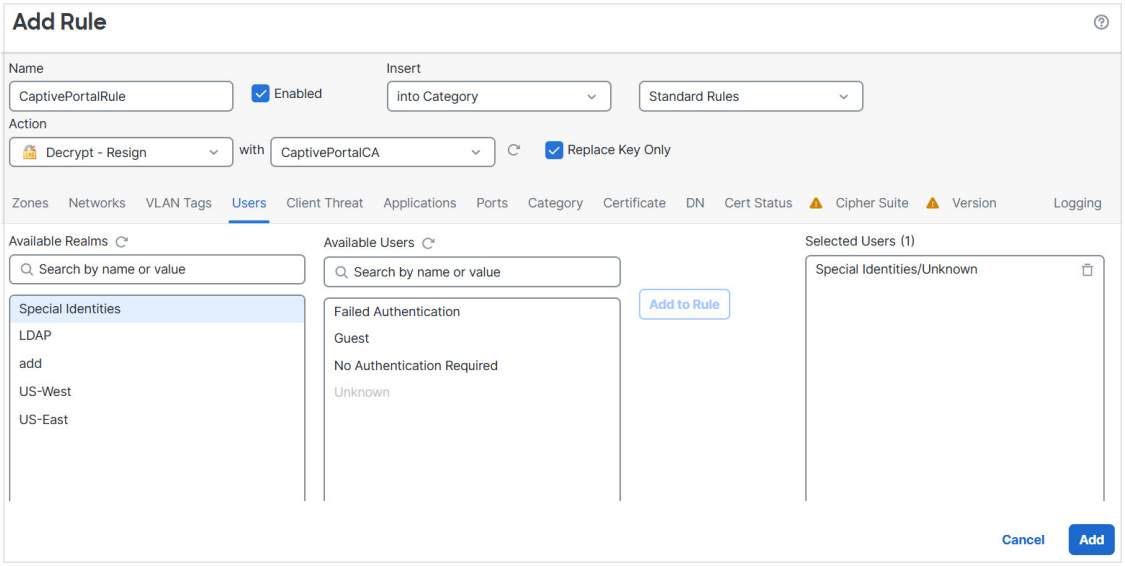
步骤 12 在 **可用领域** 列表上方，点击 **刷新** ()。

步骤 13 在**可用领域**列表中，点击**特殊身份**。

步骤 14 在**可用用户**列表中，点击**未知**。

步骤 15 点击**添加至规则**。

下图显示了一个示例。



步骤 16 （可选。）设置其他选项，如解密规则基于规则的解密规则 条件， 第 1920 页中所述。

步骤 17 点击添加 **(Add)**。

下一步做什么

将身份策略和解密策略与访问控制策略相关联， 第 2072 页

将身份策略和解密策略与访问控制策略相关联

该程序的这一部分讨论如何将身份策略和 TLS/SSL **解密 - 重新签名**规则与您先前创建的访问控制规则关联起来。在此之后，用户可以使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅如何为用户控制配置强制网络门户， 第 2063 页。

过程

步骤 1 点击 **策略 > 安全策略 > 访问控制**，然后按照创建 TCP 端口访问控制规则， 第 2068 页中所述编辑您创建的访问控制策略。 如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在该页面顶部，点击**身份 (Identity)** 字样。

步骤 4 从该列表中，选择身份策略的名称，然后在该页面顶部，点击**保存**。

步骤 5 重复前面的步骤，以使强制网络门户 解密策略与访问控制策略相关联。

步骤 6 如果尚未进行此操作，则请将托管设备作为该策略的目标，如将设备分配给访问控制策略，第 1717 页中所述。

下一步做什么

- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动，如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程所述。

强制网络门户字段

使用以下字段，在身份策略的**主动身份验证**选项卡页面上配置强制网络门户设置。另请参阅身份规则字段，第 2222 页和排除强制网络门户中的应用，第 2074 页。

服务器证书 (Server Certificate)

强制网络门户后台守护程序显示的内部证书。

注释 强制网络门户 不 支持使用数字签名算法（DSA）或椭圆曲线数字签名算法（ECDSA）证书。

端口

要用于强制网络门户连接的端口号。您必须使用 TCP 端口设置访问控制规则以用于强制网络门户，然后将身份策略与该访问控制策略相关联。有关详细信息，请参阅创建 TCP 端口访问控制规则，第 2068 页。

最大登录尝试次数 (Maximum login attempts)

系统拒绝用户登录请求前允许的最大失败登录尝试的次数。

跨防火墙共享主动身份验证会话

确定当用户的身份验证会话被发送到与之前连接的设备不同的托管设备时是否需要进行身份验证。如果您的组织要求用户在每次更改位置或站点时进行身份验证，则应禁用此选项。

- （默认，继续之前的行为。）选中此复选框可允许用户使用与主动身份验证身份规则相关联的任何托管设备进行身份验证。
- 清除复选框可要求用户使用不同的托管设备进行身份验证，即使他们已经使用部署了主动身份验证规则的另一个托管设备进行了身份验证。如果您的组织要求按位置或站点进行身份验证，并且按站点部署托管设备，请使用此选项。

托管设备要么是集群设备，要么是高可用性对，就好像它们是同一台设备；特别是

- 同一集群或高可用性对中的托管设备：保存用户会话以保持集群对的一致性。在故障转移时，辅助设备具有当前用户会话数据。
- 不同集群或高可用性对中的托管设备：不会共享用户会话数据，因此不存储在这些设备上。

主动身份验证响应页面 (Active Authentication Response Page)

要向强制网络门户用户显示的系统提供或自定义 HTTP 响应页面。在身份策略主动身份验证设置中选择**主动身份验证响应页面**后，还必须使用 **HTTP 响应页面**配置一个或更多个身份规则作为**身份验证协议**。

系统提供的 HTTP 响应页面包括**用户名 (Username)** 和**密码 (Password)** 字段，如果选择使用域序列进行身份验证，则还包括一个领域列表以及用于允许用户以访客身份访问网络的**以访客身份登录 (Login as guest)** 按钮。要显示单点登录方法，请配置自定义 HTTP 响应页面。

用户在使用响应页面登录时看到的内容的示例如使用主动身份验证规则创建示例身份策略，第 2226 页中所示。

选择以下选项：

- 要使用通用响应，请选择**系统提供**。可以点击 **视图** () 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择**自定义**。将显示一个具有系统提供的代码的窗口，您可以替换或修改该代码。完成时，保存更改。可以通过点击 **编辑** () 来编辑自定义页面。

相关主题

内部证书对象，第 2668 页

排除强制网络门户中的应用

您可以选择应用（通过其 HTTP 用户-代理 字符串标识）并免于对它们执行强制网络门户主动身份验证。这允许所选应用的流量在未经身份验证的情况下通过身份策略。



注释 此列表中仅显示带有**用户代理排除标记**的应用。

过程

步骤 1 如果尚未登录，请登录 Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 编辑包含强制网络门户规则的身份策略。

步骤 4 在 **领域和设置** 选项卡页面上， 展开**HTTP 用户代理排除**。

- 在第一列中，选中要过滤应用的每个项目旁边的复选框，然后选择一个或多个应用，然后点击**添加到规则 (Add to Rule)**。

  复选框与 ANDed 在一起。

- 要减少显示的过滤器，请在**按名称搜索**字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击 **清除** ()。
- 要刷新过滤器列表并清除所有所选过滤器，请点击 **重新加载** ()。

注释
该列表每次显示 100 个应用。

步骤 5 从**可用应用**列表中选择要添加到过滤器的应用：

- 要减少显示的应用，请在**按名称搜索**字段中输入搜索字符串。要清除搜索，请点击 **清除** ()。
- 使用位于列表底部的页码可浏览各个可用应用的列表。
- 要刷新应用列表并清除所有所选应用，请点击 **重新加载** ()。

步骤 6 添加所选应用以免除外部身份验证。可以点击并拖动，也可以点击**添加到规则 (Add to Rule)**。由此则得到您所选的应用过滤器组合。

下一步做什么

- 继续配置身份规则，如创建身份规则，第 2221 页中所述。

强制网络门户身份源故障排除

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 2049 页和用户控制故障排除，第 2231 页。

如果您遇到强制网络门户证问题，请检查以下事项：

- 强制网络门户托管设备上的时间必须与 防火墙管理中心上的时间同步。
- 如果您已配置DNS解析并创建了身份规则来执行**Kerberos**（或**HTTP 协商**，如果希望Kerberos作为选项）强制网络门户，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。

  有关详细信息，请参阅关于主机名重定向，第 2060 页。
- 如果使用 Kerberos 身份验证，则托管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置托管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章： Active Directory 中计算机、域、站点和 OU 的命名约定。
- DNS 必须向主机名返回 64KB 或更少的响应；否则，AD 连接测试失败。此限制在两个方向上都适用，将在 RFC 6891 第 6.2.5 节中讨论。
- 如果强制网络门户配置正确，但重定向到 IP 地址或完全限定域名 (FQDN) 失败，请禁用终端安全软件。此类软件可能会干扰重定向。
- 如果您选择**Kerberos**（或**HTTP 协商**，如果您要将Kerberos作为一个选项）作为身份规则的**身份验证类型**，则您选择的**领域**必须配置**AD 加入用户名**和**AD 加入密码**，以便执行Kerberos强制网络门户主动身份验证。

- 如果选择 **HTTP 基本身份验证** 作为身份规则中的 **身份验证类型**，则您的网络上的用户可能不会注意到其会话超时。大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。
- 如果您的防火墙管理中心和托管设备之间的连接失败，则无法在停机期间识别设备报告的所有强制网络门户登录，除非以前查看过这些用户并已将他们下载到 防火墙管理中心。无法识别的用户在 防火墙管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。
- 如果要用于强制网络门户的设备包含内联接口和路由接口，则必须在强制网络门户身份规则中配置区域条件，以便仅针对强制网络门户设备上的路由接口。
- 托管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。
- 要从强制网络门户安全地注销用户并防止用户再次登录，管理员可以关闭其会话：**事件和日志**> **用户** > **活动会话**。如果用户关闭浏览器，则浏览器不会自动重新进行身份验证。
- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。
- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”(Unknown)。为避免用户被识别为未知，请将领域 或领域序列 配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

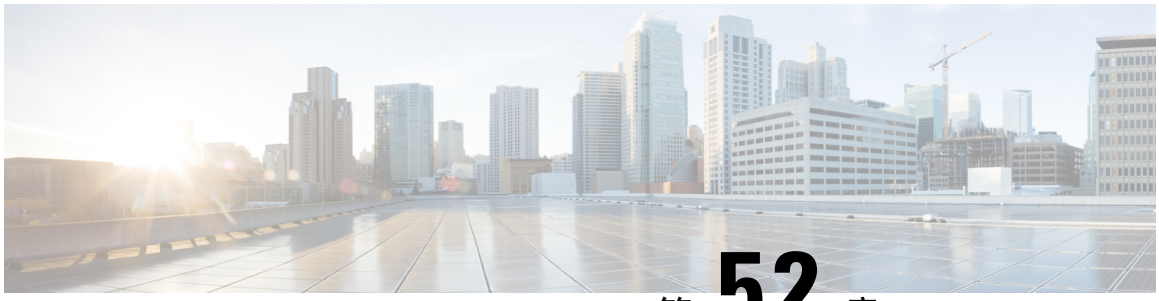
  要确保系统下载领域 或领域序列中的所有用户，请确保组位于领域配置的可用组列表中。

  有关详细信息，请参阅同步用户和组，第 2037 页。

强制网络门户历史记录

功能	防火墙管理中心最低版本防火墙管理中心	**Firewall Threat Defense**最低版本	详细信息
使用领域或领域序列进行身份验证。	7.4.1	7.4.1	您可以为 LDAP 领域、Microsoft Active Directory 领域或领域序列配置主动身份验证。此外，您还可以配置被动身份验证规则，使用领域或领域序列退回到主动身份验证。您可以选择在访问控制规则中共享相同身份策略的托管设备之间共享会话。 此外，您可以选择要求用户在使用不同于之前访问的托管设备访问系统时再次进行身份验证。 Microsoft Azure Active Directory 不能与强制网络门户一起使用。 新增/修改的菜单项： • **策略 (Policies)** > **身份 (Identity)** > （编辑策略） > **主动身份验证 (Active Authentication)** > **跨防火墙共享主动身份验证会话 (Share active authentication sessions across firewalls)** • **身份策略 (Identity policy)** > （编辑） > **添加规则 (Add Rule)** > **被动身份验证 (Passive Authentication)** > **领域和设置 (Realms & Settings)** > **如果无法建立被动或 VPN 身份，则使用主动身份验证 使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)** • **身份策略 (Identity policy)** > （编辑） > **添加规则 (Add Rule)** > **主动身份验证 (Active Authentication)** > **领域和设置 (Realms & Settings)** > **如果无法建立被动或 VPN 身份，则使用主动身份验证 使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)**
跨防火墙共享主动身份验证会话。	7.4.1	7.4.1	确定当用户的身份验证会话被发送到与之前连接的设备不同的托管设备时是否需要进行身份验证。如果您的组织要求用户在每次更改位置或站点时进行身份验证，则应禁用此选项。 • （默认。）启用可允许用户使用与主动身份验证身份规则相关联的任何托管设备进行身份验证。 • 禁用可要求用户使用不同的托管设备进行身份验证，即使他们已经使用部署了主动身份验证规则的另一个托管设备进行了身份验证。 新增/修改的屏幕： **策略 (Policies)** > **身份 (Identity)** > （编辑策略） > **主动身份验证 (Active Authentication)** > **跨防火墙共享主动身份验证会话 (Share active authentication sessions across firewalls)**

功能	防火墙管理中心最低版本防火墙管理中心	**Firewall Threat Defense**最低版本	详细信息
主机名重定向。	7.1.0	7.1.0 与 Snort 3	你可以使用一个网络对象，其中包含强制网络门户可用于主动认证请求的接口的完全限定主机名（FQDN）。
访客登录。	6.1.0	6.1.0	用户可以使用强制网络门户以访客身份登录。
强制网络门户。	6.0.0	6.0.0	引入的功能。可以使用强制网络门户要求用户在浏览器窗口出现提示时输入其凭证。映射还允许策略基于用户或用户组。



第 52 章

身份源：ISE/ISE-PIC

以下主题介绍如何通过 ISE/ISE-PIC 执行用户感知和用户控制：

- The ISE/ISE-PIC 身份源， 第 2079 页
- ISE/ISE-PIC 的许可证要求， 第 2081 页
- ISE/ISE-PIC 的要求和先决条件， 第 2081 页
- ISE/ISE-PIC 准则和限制， 第 2081 页
- 如何为用户控制配置 ISE/ISE-PIC， 第 2084 页
- 配置 ISE/ISE-PIC， 第 2086 页
- 配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页
- 排除 Cisco ISE/ISE-PIC 或思科 TrustSec 问题， 第 2101 页
- ISE/ISE-PIC 的历史记录， 第 2103 页

The ISE/ISE-PIC 身份源

您可以将您的思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与系统相集成以使用 ISE/ISE-PIC 进行被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。此外，您还可以对 Active Directory 用户执行用户控制。ISE/ISE-PIC 不报告 ISE 访客服务用户的失败登录尝试或活动。

除了用户感知和控制，如果使用 ISE Cisco ISE 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。这允许您可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址或网络。有关详细信息，请参阅配置动态属性条件。 另请参阅ISE/ISE-PIC 准则和限制， 第 2081 页。

注释 系统不会解析 IEEE 802.1x 计算机身份验证，但会解析 802.1x 用户身份验证。如果将 802.1x 与 ISE 配合使用，则必须包括用户身份验证。802.1x 计算机身份验证不会向可在策略中使用的 防火墙管理中心 提供用户身份。

有关 Cisco ISE/ISE-PIC 的详细信息，请参阅Cisco Identity Services Engine Passive Identity Connector 管理员指南或Cisco Identity Services Engine 管理员指南。



注释 我们强烈建议您使用最新版本的ISE/ ISE-PIC 获取最新功能集和最多数量的问题修复程序。

源和目标安全组标记 (SGT) 匹配

如果您使用 Cisco ISE 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。这允许您可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址或网络。有关详细信息，请参阅配置动态属性条件。

您还可以在 DNS 规则中使用源 SGT 匹配，如 根据安全组标记或动态属性控制流量中所述。

匹配 SGT 标签具有以下优势：

- 防火墙管理中心 可以从 ISE 订阅安全组标记交换协议 (SXP) 映射。

  ISE 使用 SXP 将 IP 到 SGT 映射数据库传播到托管设备。当您将 防火墙管理中心 配置为使用 ISE 服务器时，必须打开该选项才能从 ISE 侦听 SXP 主题。这会导致 防火墙管理中心 直接从 ISE 了解安全组标记和映射。然后，防火墙管理中心 将 SGT 和映射发布到托管设备。

  SXP 主题接收基于 ISE 与其他 SXP 兼容设备（例如交换机）之间通过 SXP 协议获取的静态和动态映射的安全组标记。

  您可以在 ISE 创建安全组标记，并将主机或网络 IP 地址分配至各标记。您还可以将 SGT 分配给用户账号，并将 SGT 分配给用户流量。如果网络中的交换机和路由器配置为执行此操作，则在数据包进入 ISE（Cisco TrustSec 云) 控制的网络时，这些标记会分配给数据包。

  ISE-PIC 不 支持 SXP。

- 防火墙管理中心 和托管设备可以了解SGT映射，而无需部署其他策略。（换句话说，您可以在不部署访问控制策略的情况下查看 SGT 映射的连接事件。）

- 支持 Cisco TrustSec，使您能够对网络进行分段，以保护关键业务资产。

- 受管设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

  1. 数据包中定义的源 SGT 标记（如有）。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

  2. 分配给用户会话的 SGT，从 ISE 会话目录下载。 SGT 可以与源或目标相匹配。

  3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

示例：

- 在 ISE 中，创建名为 Guest Users 的 SGT 标记并将其与 192.0.2.0/24 网络关联。

  例如，您可以将访客用户用作访问控制规则中的源 SGT 条件，并限制访问您网络的任何人对某些 URL、网站类别或网络的访问。

- 在 ISE 中，创建名为 Restricted Networks 的 SGT 标记并将其与 198.51.100.0/8 网络关联。

  例如，您可以使用“受限网络”作为目标 SGT 规则条件，并阻止来自访客用户和具有未经授权访问网络的用户的其他网络的访问。

相关主题

ISE/ISE-PIC 准则和限制 ，第 2081 页

ISE/ISE-PIC 的许可证要求

威胁防御 许可证

任意

ISE/ISE-PIC 的要求和先决条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

ISE/ISE-PIC 准则和限制

请在配置 ISE/ISE-PIC 时使用本节所讨论的准则。

ISE/ISE-PIC 版本和配置兼容性

您的 ISE/ISE-PIC 版本和配置会影响其与 Secure Firewall Management Center的集成和交互，如下所示：

- 我们强烈建议您使用最新版本的 ISE/ ISE-PIC 来获取最新的功能集。

- 同步 ISE/ISE-PIC 服务器和 Secure Firewall Management Center 上的时间。否则，系统可能会以意外间隔执行用户超时。
- 要使用 ISE 或 ISE-PIC 数据实施用户控制，请配置并启用担任 pxGrid 角色的 ISE 服务器的领域，如创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述。
- 每个连接到 ISE 服务器的 Secure Firewall Management Center主机名必须是唯一的；否则，将丢弃与其中一个 Secure Firewall Management Center的连接。
- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。

  对于运行版本 6.7 或更高版本的任何设备，您可以选择使用 **configure identity-subnet-filter** 命令限制托管设备监控的子网。有关详细信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*。

  或者，您可以配置网络对象并将该对象应用为身份策略中的身份映射过滤器。请参阅创建身份策略，第 2213 页。

有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅 Cisco Firepower 兼容性指南。

IPv6 支持

- 兼容版本的 ISE/ISE-PIC 版本 2.x 包括对支持 IPv6 的终端的支持。
- 版本 3.0（补丁 2）及更高版本的 ISE/ISE-PIC 启用 ISE/ISE-PIC 与 防火墙管理中心 之间的 IPv6 通信。

在 ISE 中批准客户端

在 ISE 服务器与 防火墙管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

您还可以按照《思科身份服务引擎管理员指南》中关于管理用户和外部身份源的章节中所述，在 ISE 中启用**自动批准新帐户**。

删除无法访问的会话

如果 ISE/ISE-PIC 中的用户会话被报告为无法访问，则 > 会删除该会 话，因此 具有相同 IP 的其他用户无法匹配不可访问的用户的身份规则。

您可以在 ISE/ISE-PIC 中控制此行为，方法是转至**提供程序 (Providers)** > **终端探测器 (Endpoint Probes)** 并点击以下选项之一：

- **启用 (Enabled)**，ISE/ISE-PIC 将监控终端连接，从而导致 Secure Firewall Management Center 删除无法访问的用户的会话。
- **禁用 (Disabled)**，可导致 ISE/ISE-PIC 忽略终端连接。

安全组标记 (SGT)

安全组标记 (SGT) 指定受信任网络中的流量源的权限。思科 ISE 和思科 TrustSec 使用称为安全组访问 (SGA) 的功能将 SGT 属性实时应用于进入网络的数据包。这些 SGT 对应于 ISE 或 TrustSec 中的用户分配的安全组。如果将 ISE 配置为身份源，则 Firepower 系统可以使用这些 SGT 过滤流量。

安全组标签可用作访问控制和 DNS 规则中的源和目标匹配标准。

注释 要仅使用 ISE SGT 属性标记实施用户控制，则无需为 ISE 服务器配置领域。ISE SGT 属性条件可在具有或不具有关联身份策略的策略中进行配置。

注释 在某些规则中，自定义 SGT 条件可匹配带有非 ISE 分配的 SGT 属性标记的流量。这不属于用户控制，并且仅在不使用 ISE/ISE-PIC 作为身份源时才起作用；请参阅自定义 SGT 条件。

如果同时使用内联 SGT 和 SXP，您必须注意以下事项：

- 如果交换机转发内联 SGT，则Cisco Secure Firewall Threat Defense会根据该标记采取操作。
- 如果交换机未转发任何标记，则Cisco Secure Firewall Threat Defense应使用 SXP 映射做出决定。

  但是，如果未指定标记，交换机默认会添加 SGT 0。如果同时使用这两种配置，则必须确保下一跳网络设备 不 会为预期由 Cisco Secure Firewall Threat Defense 上的 SXP 添加 SGT 标记的流量附加 SGT 标记（如 0）。

  这是无法更改的预期行为。

除源 SGT 标记外，要匹配目标 SGT 标记，请执行以下操作：

所需的 ISE 版本： 2.6 补丁 6 或更高版本，2.7 补丁 2 或更高版本

路由器支持：任何支持通过以太网 SGT 内联标记的Cisco路由器。有关详细信息，请参阅《Cisco 基于组的策略平台和功能列表》

限制：

- 服务质量（QoS）策略仅使用源 SGT 匹配；它 不 使用目标 SGT 匹配
- RA-VPN 不直接通过 RADIUS 接收 SGT 映射

ISE 和高可用性

当主 ISE / ISE-PIC 服务器发生故障时，会发生以下情况：

由于与 pxGrid v2 集成， Secure Firewall Management Center 已配置 ISE 主机之间的轮询，直到一台主机接受连接。

如果连接丢失， Secure Firewall Management Center 会恢复对连接主机的轮询尝试。

终端位置（或位置 IP）

终端位置属性为 ISE 识别的使用了 ISE 验证用户的网络设备的 IP 地址。

您必须配置和部署身份策略，才能根据**终端位置（位置 IP）**控制流量。

ISE 属性

配置 ISE 连接会使用 ISE 属性数据填充 Secure Firewall Management Center数据库。对于用户感知和用户控制，可以使用以下 ISE 属性。 SE-PIC 不支持这样做。

终端配置文件（或设备类型）

终端配置文件属性为 ISE 识别的用户终端设备类型。

您必须配置和部署身份策略，才能根据**终端配置文件**（**设备类型**）控制流量。

如何为用户控制配置 ISE/ISE-PIC

您可以在以下任何配置中使用 ISE/ISE-PIC：

- 具有领域、身份策略和关联的访问控制策略。

  在策略中使用领域来控制用户对网络资源的访问。您仍可以在策略中使用 ISE/ISE-PIC 安全组标记 (SGT) 元数据。

- 仅使用一个访问控制策略。不需要领域或身份策略。

  使用此方法可单独使用 SGT 元数据来控制网络访问。

相关主题

如何在不使用领域的情况下配置 ISE/ISE-PIC，第 2084 页
如何为无领域的用户控制配置 ISE/ISE-PIC，第 2085 页

如何在不使用领域的情况下配置 ISE/ISE-PIC

本主题简要介绍了配置 ISE 以允许或阻止使用 SGT 标记访问网络时所必须完成的任务。

过程

	命令或操作	目的
步骤 1	SGT 匹配：在 ISE 上启用 SXP。	这使 Secure Firewall Management Center 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置思科身份服务引擎(Cisco ISE)身份源的方法，第 2092 页。
步骤 3	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标 SGT 元数据用作访问控制规则中的匹配条件。请参阅关于访问控制规则，第 1743 页。

	命令或操作	目的
步骤 4	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改，第 180 页。

下一步做什么

从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center中使用，第 2089 页

如何为无领域的用户控制配置 ISE/ISE-PIC

开始之前

本主题简要介绍为配置 ISE/ISE-PIC 进行用户控制并允许或阻止用户或组访问网络而必须完成的任务。用户和组可以存储在 领域支持的服务器，第 2027 页 中列出的任何服务器上。

过程

	命令或操作	目的
步骤 1	仅目标 SGT：在 ISE 上启用 SXP。	这使 Secure Firewall Management Center 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	创建领域。	您必须仅创建一个领域来控制所选择的用户和组对网络的访问。 请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。
步骤 3	下载用户和组并启用领域。	下载用户和组让您能够在访问控制规则中使用它们。请参阅同步用户和组，第2037 页。
步骤 4	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页。
步骤 5	创建身份策略。	身份策略是一个或多个身份规则的容器。请参阅创建身份策略，第 2213 页。
步骤 6	创建身份规则。	身份规则指定了如何使用领域来控制用户和组对网络的访问。请参阅创建身份规则，第 2221 页。
步骤 7	将身份策略与访问控制策略相关联。	这会让访问控制策略能够使用领域中的用户和组。

	命令或操作	目的
步骤 8	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标 SGT 元数据用作访问控制规则中的匹配条件。请参阅关于访问控制规则，第 1743 页。
步骤 9	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改，第 180 页。

下一步做什么

从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center中使用，第 2089 页

配置 ISE/ISE-PIC

以下主题讨论如何配置 ISE/ISE-PIC 服务器，以便与 防火墙管理中心 中的身份策略配合使用。

这些主题讨论如何：

- （仅限思科 ISE 高级配置。）从 ISE/ISE-PIC 服务器导出证书，以使用 防火墙管理中心 进行身份验证。
- 发布 SXP 主题，以便使用 ISE 服务器上的安全组标记 (SGT) 更新 防火墙管理中心。

相关主题

在 ISE 中配置安全组和 SXP 发布，第 2086 页
从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center中使用，第 2089 页

在 ISE 中配置安全组和 SXP 发布

您必须在思科身份服务引擎 (ISE) 中执行许多配置，才能创建 TrustSec 策略和安全组标记 (SGT)。有关实施 TrustSec 的更完整信息，请参阅 ISE 文档。

以下操作步骤将挑选出必须在 ISE 中配置的核心设置的要点，以便 Firewall Threat Defense 设备能够下载和应用静态 SGT-IP 地址映射，然后在访问控制规则中用于源 SGT 和目标 SGT 匹配。有关详细信息，请参阅 ISE 文档。

如果同时使用内联 SGT 和 SXP，您必须注意以下事项：

- 如果交换机转发内联 SGT，则Cisco Secure Firewall Threat Defense会根据该标记采取操作。
- 如果交换机未转发任何标记，则Cisco Secure Firewall Threat Defense应使用 SXP 映射做出决定。

  但是，如果未指定标记，交换机默认会添加 SGT 0。如果同时使用这两种配置，则必须确保下一跳网络设备 不 会为预期由 Cisco Secure Firewall Threat Defense 上的 SXP 添加 SGT 标记的流量附加 SGT 标记（如 0）。

这是无法更改的预期行为。

此过程中的图示基于 ISE 2.4。在后续版本中，这些功能的确切路径可能会发生变化，但概念和要求是相同的。虽然建议使用 ISE 2.4 或更高版本（最好是 2.6 或更高版本），但配置应从 ISE 2.2 补丁 1 开始。

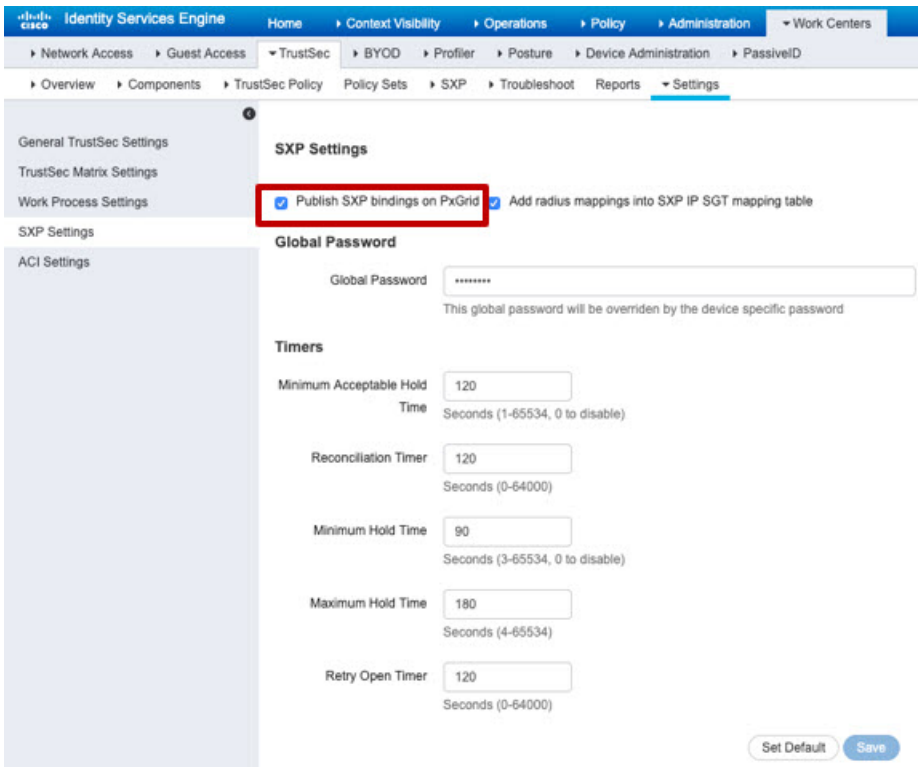
开始之前

您必须拥有 ISE Plus 许可证，才能发布从 SGT 到 IP 地址的静态映射和获取从用户会话到 SGT 的映射，以便 Firewall Threat Defense 设备可以接收这些映射。

过程

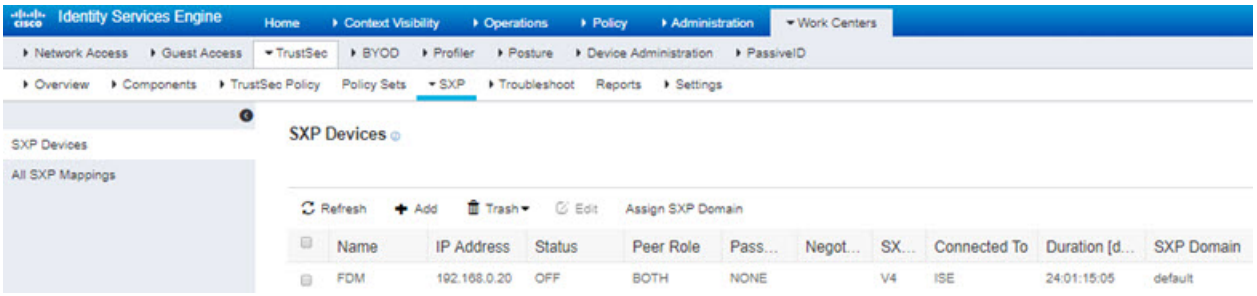
步骤 1 选择工作中心 > **TrustSec** > **设置** > **SXP 设置**，然后选择**在 PxGrid 上发布 SXP 绑定**选项。

选择该选项后，ISE 使用 SXP 发送 SGT 映射。您必须选择此选项， Firewall Threat Defense 设备才能“收听”从列表至 SXP 主题等一切内容。必须选择此选项， Firewall Threat Defense 设备才能获取静态 SGT-IP 地址映射信息。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则没有必要。

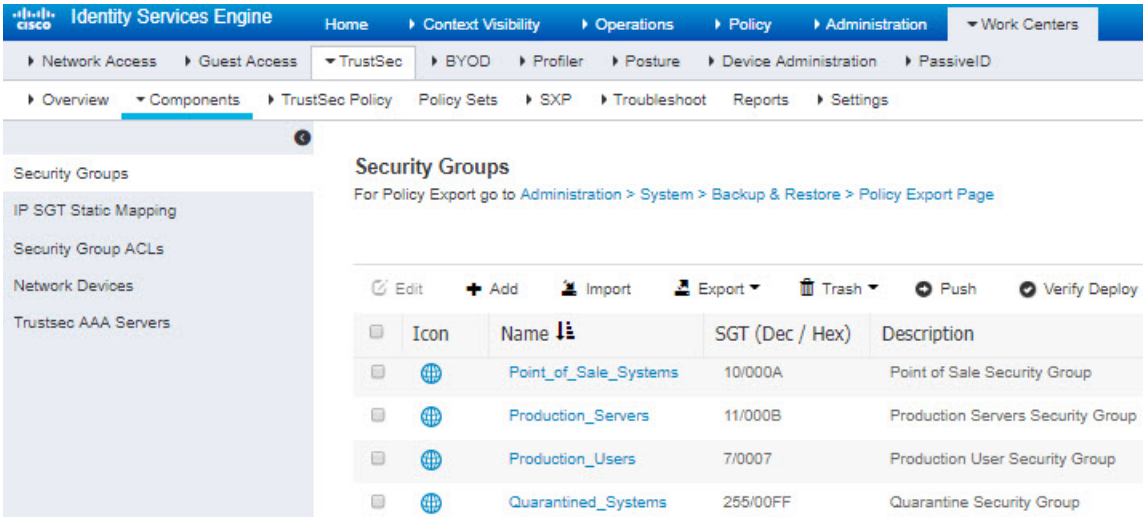


步骤 2 选择工作中心 > **TrustSec** > **SXP** > **SXP 设备**，然后添加设备。

这并不一定是真正的设备，您甚至可以使用 Firewall Threat Defense 设备的管理 IP 地址。该表只需要至少一台设备来促使 ISE 发布静态 SGT-IP 地址映射。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。

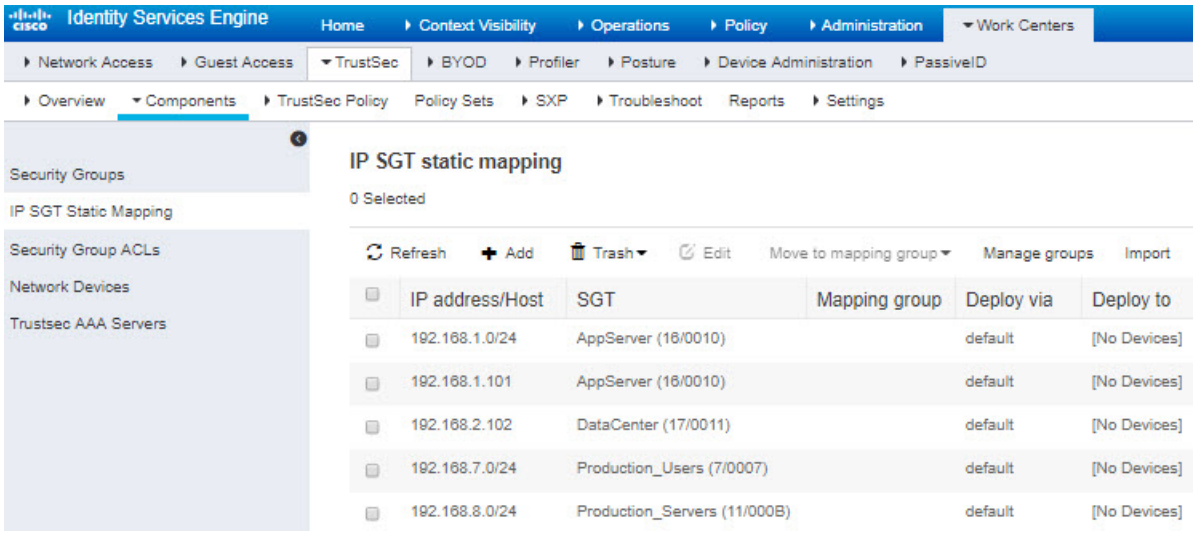


步骤 3 选择**工作中心** > **TrustSec** > **组件** > **安全组**并验证是否定义了安全组标记。按需新建。



步骤 4 选择**工作中心** > **TrustSec** > **组件** > **IP SGT 静态映射**，并将主机和网络 IP 地址映射至安全组标记。

如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。



从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center中使用

以下各节介绍如何：

- 从 ISE / ISE-PIC 服务器导出系统证书。

  这些证书是安全连接到 ISE / ISE-PIC 服务器所必需的。您可能需要导出一个或多达三个证书，具体取决于 ISE 系统的设置方式：

  - pxGrid 服务器的一个证书
  - 监控（MNT）服务器一个证书
  - 一个证书，包括私钥，用于 pxGrid 客户端（即 防火墙管理中心）

    与前两个证书不同，这是一个自签名证书。

- 将这些证书导入 防火墙管理中心：
  - pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**) 的内部证书
  - pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **PKI** > **受信任 CA (Trusted CAs)**)
  - MNT 证书：受信任 CA

相关主题

导出系统证书

导入 ISE/ISE-PIC 证书，第 2091 页

导出系统证书

您可以导出系统证书或某个证书及其关联的专用密钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。

步骤 3 选择是仅导出证书，还是导出证书及其关联的私钥。

提示
由于可能会暴露专用密钥值，我们不建议导出与证书关联的专用密钥。如果您必须导出专用密钥（例如，导出要导入其他思科 ISE 节点以用于节点间通信的通配符系统证书时），请指定专用密钥加密密码。在将此证书导入另一思科 ISE 节点时，必须指定此密码以解密专用密钥。

步骤 4 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

步骤 5 点击**导出 (Export)** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以 PEM 的格式进行存储。如果同时导出证书和专用密钥，则证书会导出为 .zip 文件，其中包含 PEM 格式的证书和已加密的专用密钥文件。

生成自签名证书

通过生成自签证书添加新的本地证书。思科建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署思科 ISE，尽可能使用 CA 签名证书，确保生产网络中更统一地接受。

注释 如果您使用自签名证书并且必须更改思科 ISE 节点的主机名，请登录思科 ISE 节点的管理门户，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，思科 ISE 会继续使用采用旧主机名的自签证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 选择在思科 ISE GUI 中，点击**菜单**图标 (☰) 并选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

要从辅助节点生成自签证书，请选择**管理 (Administration)** > **系统 (System)** > **服务器证书 (Server Certificate)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单**图标 (☰)，然后选择 **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 3 点击**生成自签证书 (Generate Self Signed Certificate)** 并在显示的窗口中输入详细信息。

步骤 4 根据想要对其使用此证书的服务，选中 **Usage** 区域的复选框。

步骤 5 点击**提交**生成证书。

要从 CLI 重新启动辅助节点，则按给定顺序输入以下命令：

a) **application stop ise**
b) **application start ise**

导入 ISE/ISE-PIC 证书

此步骤为可选。您还可以通过向 ISE 服务器提供登录凭证来自动导入证书，如 配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页中所述。

按以下方式导入证书：

- pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**) 的内部证书
- pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **PKI** > **受信任 CA (Trusted CAs)**)
- MNT 证书：受信任 CA

开始之前

（可选。）从 ISE/ISE-PIC 服务器导出证书，如导出系统证书，第 2090 页中所述。证书和密钥必须存在于您登录 Secure Firewall Management Center 的计算机上。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **对象 (Objects)** > **PKI** > **内部证书 (Internal Certs)**。

步骤 3 点击 **Add Internal Cert**。

步骤 4 按照屏幕上的提示导入证书和私钥。

步骤 5 点击**受信任 CA (Trusted CAs)**。

步骤 6 点击**添加可信 CA**。

步骤 7 按照屏幕上的提示导入 pxGrid 服务器证书。

步骤 8 如有必要，请重复上述步骤，以便导入 MNT 服务器的受信任 CA。

下一步做什么

配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页

配置思科身份服务引擎 (Cisco ISE)身份源的方法

您可以通过以下方式配置 Cisco ISE 身份源：

- 快速配置（新）：仅限 *Cisco ISE*；*ISE-PIC* 目前不支持快速配置。输入外部 RESTful 服务 (ERS) 操作员组中用户的用户名和密码。 Secure Firewall Management Center 登录 Cisco ISE 主身份验证节点 (PAN)，下载证书，并配置身份源。您可以选择保存 ISE 配置以供以后使用。

  有关组的详细信息，请参阅Cisco Identity Services Engine 管理员指南中有关 Cisco ISE 管理员组的部分。

  有关详细信息，请参阅快速配置， 第 2094 页。

- 高级配置（旧）：与以前的 Secure Firewall Management Center 版本相同，适用于 Cisco ISE 和 ISE-PIC。您必须从 ISE/ISE-PIC 服务器获取证书和其他信息，如配置 ISE/ISE-PIC， 第 2086 页中所述。

  有关高级配置的详细信息，请参阅Cisco ISE 高级配置， 第 2098 页。

相关主题

关于Cisco ISE快速配置， 第 2092 页
Cisco ISE 高级配置， 第 2098 页

关于Cisco ISE快速配置

首先完成这些任务：Cisco ISE快速配置的前提条件， 第 2093 页。

您必须拥有以下信息：

- 策略管理节点 (PAN) 的完全限定域名或 IP 地址。
- 外部 RESTful 服务 (ERS) 操作员组中用户的用户名和密码。

请注意以下有关 SGT 到 IP 的映射和 SXP：

- 要获得 Cisco ISE 中定义的所有映射，包括通过 SXP 发布的 SGT 到 IP 地址的映射，请使用以下程序。或者，您可以选择以下选项：

- 要想只使用数据包中的SGT信息，而不使用从Cisco ISE下载的映射，请跳过创建和编辑访问控制规则，第1764页中讨论的步骤。请注意，在这种情况下，您只能使用SGT标记作为源条件；这些标记永远不会匹配目标条件。
- 要仅在数据包和用户-IP-地址/SGT映射中使用SGT，请不要订阅Cisco ISE身份源中的SXP主题，也不要将ISE配置为发布SXP映射。您可以将此信息用于源匹配条件和目标匹配条件。

相关主题

Cisco ISE快速配置的前提条件，第2093页
快速配置，第2094页
关于Cisco ISE快速配置，第2092页
Cisco ISE高级配置，第2098页

Cisco ISE快速配置的前提条件

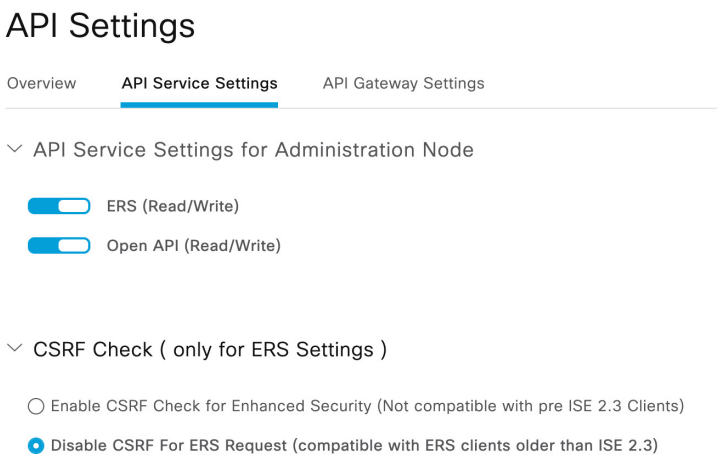
要成功进行ISE快速配置，您必须以ISE管理员身份执行以下两项操作：

- 启用外部RESTful服务(ERS)（读/写）、Open API（读/写），并禁用跨站点请求伪造(CSRF)检查

  转至 > **管理** > **xi同** > **设置** > **API设置** > **API服务设置**

  有关详细信息，请参阅Cisco Identity Services Engine管理员指南中的启用API服务。

  下图显示了一个示例。

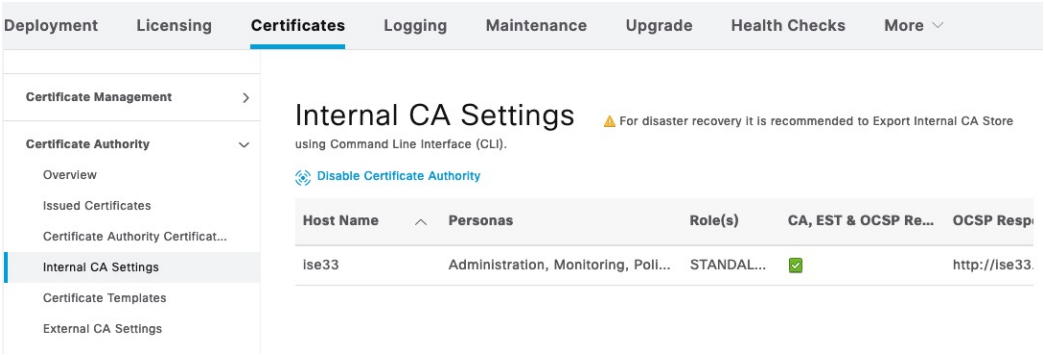


- 将**ERS（读/写）(ERS [Read/Write])**滑动到**已启用 (Enabled)**。
- 启用证书颁发机构

  转至 > **管理** > **系统** > **证书** > **证书颁发机构** > **内部CA设置**

  有关详细信息，请参阅Cisco Identity Services Engine管理员指南中的内部CA设置。

  下图显示了一个示例。



相关主题

关于Cisco ISE快速配置， 第 2092 页
Cisco ISE 高级配置， 第 2098 页

快速配置

此任务讨论如何通过输入用户名和密码来配置思科 ISE（而非 ISE-PIC）。然后， Secure Firewall Management Center 登录 ISE 并下载必要的证书以对两个应用进行身份验证。

Firewall Threat Defense 功能历史记录：

7.6—引入了此功能。

开始之前

请首先参阅以下主题：

- 关于Cisco ISE快速配置， 第 2092 页
- Cisco ISE快速配置的前提条件， 第 2093 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **身份源**。

步骤 3 为**服务类型**点击**身份服务引擎**以启用 ISE 连接。

注释
要禁用连接，请点击**无**。

步骤 4 点击 **快速配置（新）**。

步骤 5 在**主 PAN FQDN/IP 地址 (Primary PAN FQDN/IP Address)** 字段中，输入策略管理节点 (PAN) 的完全限定域名或 IP 地址。 请勿输入方案（例如 **https://**）。

步骤 6 在**用户名 (Username)** 字段中，至少输入 ERS 操作员组中的用户的用户名。

有关组的详细信息，请参阅Cisco Identity Services Engine 管理员指南中有关思科 ISE 管理员组的部分。

步骤 7 在**密码 (Password)** 字段中，输入用户的密码。

步骤 8 （可选。）使用 CIDR 块符号输入 **ISE 网络过滤器**。

步骤 9 在“订阅”部分中，选中以下项：

- **会话目录主题**，用于从 ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**，用于接收来自 ISE 服务器的 SGT 到 IP 映射的更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。

步骤 10 要测试连接，请点击**测试 (Test)**。

思科身份服务引擎 (Cisco ISE)快速配置结果，第 2095 页中讨论了连接和集成结果。

步骤 11 （可选。）成功执行 trest 后，点击页面顶部的 **保存此配置 (Save this Config)** 以在 Secure Firewall Management Center上保存配置。

下一步做什么

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 使用思科 ISE 中的安全组标记 (SGT) 作为访问控制策略中的动态属性。

  有关详细信息，请参阅配置动态属性条件。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动，如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程所述。

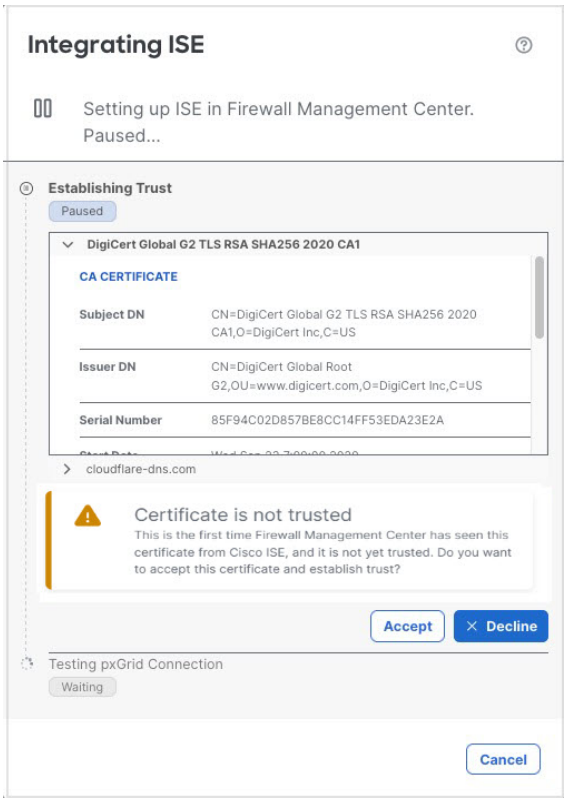
相关主题

关于Cisco ISE快速配置，第 2092 页
Cisco ISE 高级配置，第 2098 页

思科身份服务引擎 (Cisco ISE)快速配置结果

不受信任证书的初始信息页面

当您在 **快速配置（新建）(Quick Configuration [New])** 选项卡页面中输入所需信息时，系统会首先检查证书是否由受信任的颁发机构签名。否则，系统将显示类似于以下的页面。



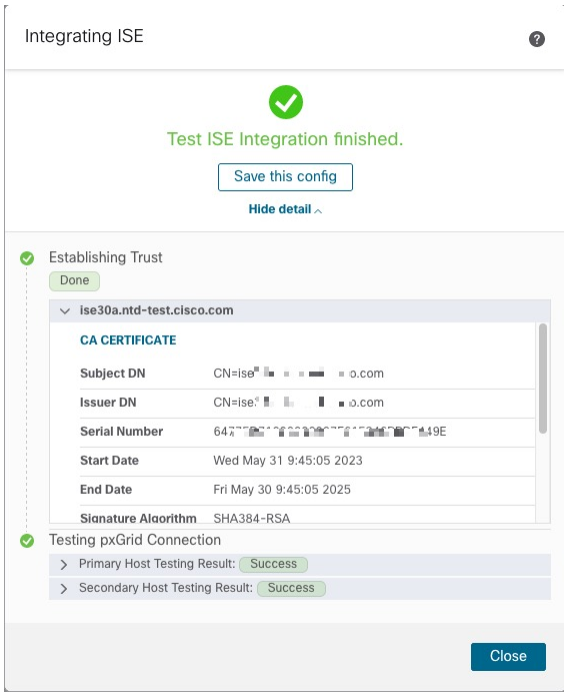
您有以下选择：

- 点击 > 的 **接受 (Accept)** 以信任证书并继续使用 ISE 进行身份验证。
- 点击**拒绝 (Decline)** 以退出，而不使用 ISE 进行身份验证。

  然后，您可以在**快速配置（新建）(Quick Configuration [New])** 选项卡页面上验证 ISE 配置并重试。

ISE 集成成功

如果 Secure Firewall Management Center 能够使用您提供的信息成功进行身份验证，系统将显示类似于以下内容的页面。

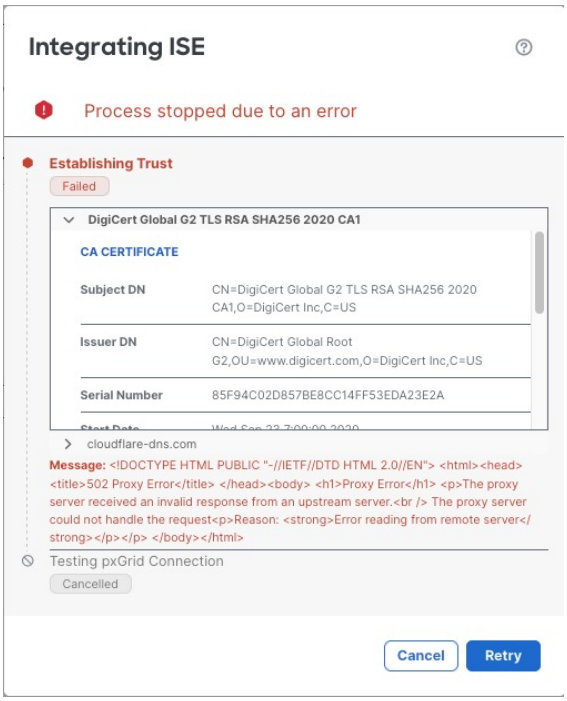


点击**保存此配置 (Save this Config)** 进行保存，以便将来能够使用身份源。

或者，展开测试 pxGrid 连接下的列表之一，以显示从这些源下载的证书。

不成功的 ISE 集成

如果 Secure Firewall Management Center 出于任何原因未能通过 ISE 进行身份验证，系统将显示类似于以下内容的页面。



错误消息以红色文本显示。

您有以下选择：

- 如果错误是暂时的（例如，暂时性网络问题），请点击**重试 (Retry)**。
- 要使用其他 ISE 凭证重试，请点击**取消 (Cancel)**。

相关主题

关于Cisco ISE快速配置， 第 2092 页
Cisco ISE 高级配置， 第 2098 页

Cisco ISE 高级配置

以下程序讨论如何配置 ISE/ ISE-PIC 身份源。您必须在全局域中才能执行此任务。

开始之前

- 要从 Microsoft Active Directory 服务器或受支持的 LDAP 服务器获取用户会话，请配置并启用 Cisco ISE 服务器的领域（假设为 pxGrid 角色），如创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页中所述。
- 要获得 Cisco ISE 中定义的所有映射，包括通过 SXP 发布的 SGT 到 IP 地址的映射，请使用以下程序。或者，您可以选择以下选项：
  - 要想只使用数据包中的 SGT 信息，而不使用从 Cisco ISE 下载的映射，请跳过创建和编辑访问控制规则， 第 1764 页中讨论的步骤。请注意，在这种情况下，您只能使用 SGT 标记作为源条件；这些标记永远不会匹配目标条件。

- 要仅在数据包和用户-IP-地址/SGT 映射中使用 SGT，请不要订阅 Cisco ISE 身份源中的 SXP 主题，也不要将 ISE 配置为发布 SXP 映射。您可以将此信息用于源匹配条件和目标匹配条件。

- （仅高级配置。）从 ISE/ ISE-PIC 服务器导出证书，也可以选择将其导入到 Secure Firewall Management Center 中，如 从 ISE/ISE-PIC 服务器导出证书以在Secure Firewall Management Center 中使用，第 2089 页中所述。
- 要发布 SXP 主题，以便在 ISE 服务器上使用安全组标记 (SGT) 更新 Secure Firewall Management Center，请参阅配置 ISE/ISE-PIC，第 2086 页。

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **身份源**。

步骤 3 为**服务类型**点击**身份服务引擎**以启用 ISE 连接。

注释
要禁用连接，请点击**无**。

步骤 4 输入**主要主机名/IP 地址**以及**辅助主机名/IP 地址**（后者为可选）。

步骤 5 从 **pxGrid 服务器 CA** 和 **MNT 服务器 CA** 列表中点击相应的证书颁发机构，然后从 **pxGrid 客户端证书** 列表中点击相应的证书。也可以点击 **添加** (+) 来添加证书。

注释
pxGrid 客户端证书 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

步骤 6 （可选。）使用 CIDR 块符号输入 **ISE 网络过滤器**。

步骤 7 在“订阅”部分中，选中以下项：

- **会话目录主题**，用于从 ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**，用于接收来自 ISE 服务器的 SGT 到 IP 映射的更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。

步骤 8 要测试连接，请点击**测试 (Test)**。

如果测试失败，请点击**其他日志 (Additional Logs)** 以了解有关连接失败的详细信息。

注释
如果使用 ISE 设置负载均衡，则响应测试的节点应为当前的活动节点。有关详细信息，请参阅Cisco pxGrid Node。

下一步做什么

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 使用思科 ISE 中的安全组标记 (SGT) 作为访问控制策略中的动态属性。

  有关详细信息，请参阅配置动态属性条件。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动，如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程所述。

相关主题

关于Cisco ISE快速配置，第 2092 页
Cisco ISE 高级配置，第 2098 页

ISE/ISE-PIC 配置字段

以下字段用于配置与 ISE/ISE-PIC 的连接。

主要和辅助主机名/IP 地址 (Primary and Secondary Host Name/IP Address)

主要和辅助（可选）pxGrid ISE 服务器的主机名或 IP 地址。

您指定的主机名所使用的端口必须可由 ISE 和 Secure Firewall Management Center访问。

pxGrid 服务器 CA (pxGrid Server CA)

可信 pxGrid 框架的证书颁发机构。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。

MNT 服务器 CA (MNT Server CA)

当执行批量下载时 ISE 证书的可信证书颁发机构。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

pxGrid 客户端证书

Secure Firewall Management Center 必须向 /ISE-PIC 提供的内部证书和密钥，以连接到 /ISE-PIC 或进行批量下载。

注释 **pxGrid 客户端证书** 必须包含 clientAuth 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

ISE 网络过滤器 (ISE Network Filter)

一个可选过滤器，可以将其设置为限制 ISE 报告给 Secure Firewall Management Center的数据。如果提供网络过滤器，则 ISE 会报告来自该过滤器中的网络的数据。可通过以下方式指定过滤器：

- 将此字段留空以指定**任意 (any)** 值。

- 使用 CIDR 符号输入单一 IPv4 地址块。
- 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

注释 无论您的 ISE 是何版本，此版本的系统均不支持使用 IPv6 地址进行过滤。

订用：

会话目录主题：选中此复选框可从 ISE 服务器订阅用户会话信息。包括 SGT 和终端元数据。

SXP 主题：选中此复选框可从 ISE 服务器订阅 SXP 映射。

相关主题

受信任证书颁发机构对象，第 2666 页
内部证书对象，第 2668 页
关于Cisco ISE快速配置，第 2092 页
Cisco ISE 高级配置，第 2098 页

排除 Cisco ISE/ISE-PIC 或思科 TrustSec 问题

排除 Cisco TrustSec 问题

设备接口可以配置为从 ISE/ ISE-PIC 或从网络上的 Cisco 设备（称为 Cisco TrustSec）传播安全组标记 (SGT)。在设备管理页面（**设备 (Devices)** > **设备管理 (Device Management)**）上，默认情况下，选中接口的**传播安全组标记 (Propagate Security Group Tag)** 复选框。 如果您希望接口传播 TrustSec 数据，请选中此复选框。

排除 ISE/ ISE-PIC 问题

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 2049 页和用户控制故障排除，第 2231 页。

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与系统成功集成。
- 当主服务器出现故障时，您必须手动将辅助服务器升级为主服务器；不会进行自动故障转移。
- 在 ISE 服务器与 防火墙管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

  您还可以按照 Cisco Identity Services Engine 管理员指南中"管理用户和外部身份源"的章节中所述，在 ISE 中启用 **自动批准新帐户** 。
- **pxGrid 客户端证书** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。
- ISE 服务器上的时间必须与 Secure Firewall Management Center 上的时间同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。

- 如果部署包括主要和辅助 pxGrid 节点，
  - 则两个节点的证书必须由同一个证书颁发机构签名。
  - ISE 服务器和 Secure Firewall Management Center必须可以访问主机名使用的端口。
- 如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

要从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网，请使用 **configure identity-subnet-filter** {**add** | **remove**} 命令。您通常应对内存较低的托管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中检索到它们的相关信息之前，它们不会显示在 Web 界面中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- Secure Firewall Management Center不会收到 ISE 访客服务用户的用户数据。
- 如果 ISE 与 TS 代理监控的用户相同，则 Secure Firewall Management Center 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 Secure Firewall Management Center。
- 您的ISE版本和配置会影响您在系统中使用ISE的方式。有关详细信息，请参阅The ISE/ISE-PIC 身份源，第 2079 页。
- 如果您配置了 Secure Firewall Management Center 高可用性并且主管理中心出现故障，请参阅ISE/ISE-PIC 准则和限制，第 2081 页中有关 ISE 和高可用性的部分。
- ISE-PIC 不提供 ISE 属性数据。
- ISE-PIC 无法执行 ISE ANC 补救。
- 活动FTP会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动FTP中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

如果您遇到支持的功能问题，请参阅The ISE/ISE-PIC 身份源，第 2079 页了解版本兼容性的详细信息。

ISE/ISE-PIC 用户超时

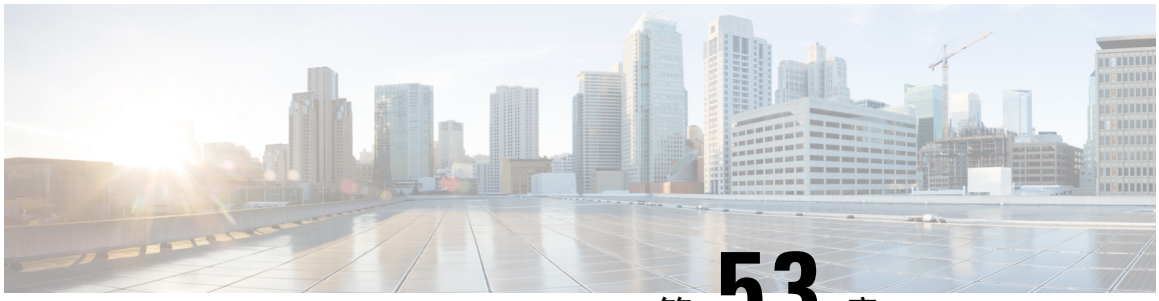
如果要设置没有领域的 ISE/ISE-PIC，请注意，存在会影响 Secure Firewall Management Center用户查看方式的用户会话超时。有关详细信息，请参阅领域字段，第 2029 页。

ISE/ISE-PIC 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
快速配置	7.6	7.6.0	您可以选择仅使用外部 RESTful 服务 (ERS) 操作员组中用户的用户名和密码配置 ISE。（此功能仅适用于 *ISE*，不适用于 *ISE-PIC*。） **升级影响**。您在升级之前创建的任何 ISE 或 ISE-PIC 身份源在 **高级配置（旧）** 选项卡页面上仍然可用。快速配置仅影响升级后创建的新 ISE 身份源。 新增/修改的菜单项：**集成 (Integration)** > **其他集成 (Other Integrations)** > **身份源 (Identity Sources)** > **身份服务引擎 (Identity Services Engine)**。有两个选项卡页面：**快速配置（新）(Quick Configuration [New])** 和 **高级配置（旧）(Advanced Configuration [Old])**。 新增/修改的 CLI 命令：无
与身份情报（动态防火墙）集成	10.0.0	• 7.3 及更高版本（如果使用 Microsoft AD 领域） • 7.4 及更高版本（如果您使用 Microsoft Entra ID 领域）	您可以将pxGrid 云身份源 与 身份情报 集成，以向 SGT、终端配置文件和安全状况添加用户和设备信任数据。 **升级影响**。无。 新增/修改的菜单项：**集成 (Integration)** > **其他集成 (Other Integrations)** > **身份源 (Identity Sources)** > **身份服务引擎 (Identity Services Engine)**。可以选择使用此身份源创建动态防火墙。 新增/修改的 CLI 命令：无

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
pxGrid 2.0 是支持的 ISE/ISE-PIC 版本的默认值	6.7.0	6.7.0	请注意以下提示： • 支持的 ISE/ISE-PIC 版本：2.6 补丁 6 或更高版本，2.7 补丁 2 或更高版本 • 自适应网络控制 (ANC) 策略会取代终端保护服务 (EPS) 补救。如果在 防火墙管理中心 中配置了 EPS 策略，则您必须将其迁移才能使用 ANC。
（可选）从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网。您通常应对内存较低的托管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。	6.7.0	6.7.0	新命令：**configure identity-subnet-filter** {**add** | **remove**}
目标安全组标记匹配 (SGT)	6.5.0	6.5.0	引入的功能。让您能够在访问控制规则中将 ISE SGT 标记用于源匹配条件和目标匹配条件。 SGT 标记是 ISE 获取的标签到主机/网络映射。 新增/修改的菜单项： • 用于配置目标 SGT 匹配的新选项： **系统 (System)** > **集成 (Integration)** > **身份源 (Identity Sources)** > **ISE/ISE-PIC** • **会话目录主题 (Session Directory Topic)**：订阅 ISE 用户会话信息。 • **SXP 主题 (SXP Topic)**：订用 ISE 服务器上的 SGT 标记更新。 • **分析 (Analysis)** > **连接 (Connections)** > **事件 (Events)**中的新增列和重命名列 • 已重命名：安全组标记重命名为源 SGT • 新：目标 SGT
与 ISE-PIC 集成	6.2.1	6.2.1	现在可以使用来自 ISE PIC 的数据。
SGT 标记用于用户控制。	6.2.1	6.2.0	无需再创建领域或身份策略来基于 ISE 安全组标记 (SGT) 数据执行用户控制。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
与 ISE 集成。	6.0	6.0	引入的功能。通过订用思科的 Platform Exchange Grid (pxGrid)，Firepower 管理中心可以下载更多用户数据、设备类型数据、设备位置数据和安全组标记（SGT - ISE 用来提供网络访问控制的方法）。



第 53 章

身份源：被动身份代理

以下主题讨论如何配置和使用被动身份代理。

- 被动身份代理身份源， 第 2107 页
- 部署 被动身份代理， 第 2109 页
- 如何创建 被动身份代理 身份源， 第 2114 页
- 配置 被动身份代理， 第 2116 页
- 监控 被动身份代理， 第 2133 页
- 管理被动身份代理， 第 2134 页
- 被动身份代理 故障排除， 第 2136 页
- 被动身份代理 的安全要求， 第 2137 页
- 被动身份代理的互联网接入要求， 第 2138 页
- 被动身份代理 的历史记录， 第 2139 页

被动身份代理身份源

被动身份代理 身份源将会话数据从 Microsoft Active Directory (AD) 发送到 Secure Firewall Management Center。您只需要 关于领域和领域序列， 第 2022 页中讨论的受支持的 Microsoft AD 设置即可。

被动身份代理 版本 1.0 仅发送 IPv4 用户会话，但版本 1.1 发送 IPv4 和 IPv6 用户会话。

注释 您无需配置Cisco Identity Services Engine (ISE) 即可使用此身份源。

被动身份代理 角色

被动身份代理 支持以下角色：

- 独立：不属于冗余对的 被动身份代理 。独立代理可以从多个 Active Directory 服务器和域控制器下载用户和组，前提是所有这些服务器和域控制器上都安装了该软件。
- 主：（冗余对中的主代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

处理与 Secure Firewall Management Center 的所有通信，除非它停止通信，在这种情况下，通信将由辅助代理处理。

- 辅助：（冗余对中的辅助或备份代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  监控主代理的运行状况，并在主代理停止与 Secure Firewall Management Center通信时进行接管。

被动身份代理 系统要求

被动身份代理 需要满足以下条件：

- 如果将 被动身份代理 安装在 Windows Active Directory 服务器上，则该服务器必须运行以下版本之一：
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022
- 如果将 被动身份代理 安装在连接到域的 Windows 客户端上，则客户端必须运行 Windows 11 或更高版本。
- 所有系统的系统时钟必须同步。强烈建议在所有这些服务器上使用相同的 NTP 服务器。这意味着：
  - Secure Firewall Management Center。

    有关详细信息，请参阅时间同步，第 1030 页。
  - 所有 Windows Active Directory 服务器和域控制器。
  - 安装了 被动身份代理 的计算机。
- Secure Firewall Management Center 必须运行 7.6 或更高版本。
- 由 Secure Firewall Management Center 托管的任何 Cisco Secure Firewall Threat Defense 必须运行 7.1 或更高版本。
- 您必须在 Cisco Secure Firewall Threat Defense 设备上启用 Snort 3。

被动身份代理 限制

被动身份代理 以下限制：

- 最多同时有 10 个代理
- 一个 被动身份代理 身份源最多可以监控 50 个 AD 目录
- 最多 300,000 个并发用户会话
- 不支持 IPv6 地址 (被动身份代理 1.0)

- 不支持 IPv6 地址 (被动身份代理 1.1)

部署 被动身份代理

有关部署选项的信息，请参阅 部署 被动身份代理，第 2109 页。



注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件，第 2133 页

部署 被动身份代理

您可以在属于您想要用于用户感知和控制的 Microsoft Active Directory (AD) 域的任何计算机上安装 被动身份代理 软件。换句话说，您可以将其安装在以下任何位置：

- Microsoft Active Directory 服务器
- 域控制器
- 连接到网络的客户端既不是目录服务器，也不是域控制器

任何特定 被动身份代理 都可以监控一个或多个 Active Directory 域。

被动身份代理 必须使用 TLS/SSL 协议与 Secure Firewall Management Center] 通信的计算机。有关详细信息，请参阅被动身份代理的互联网接入要求，第 2138 页。

代理类型

您可以在 Microsoft AD 目录服务器、域控制器或连接到域的任何客户端上配置以下类型的代理：

- 独立代理：一个代理，可以监控同一域中的一个或多个 Active Directory 域控制器。
- 可以监控同一域中的一个或多个 AD 域控制器的主代理和辅助代理：为了提供冗余，您可以在不同的计算机上安装主代理和辅助代理。主代理负责与 Secure Firewall Management Center 进行通信，但如果通信失败，则由辅助代理接管。

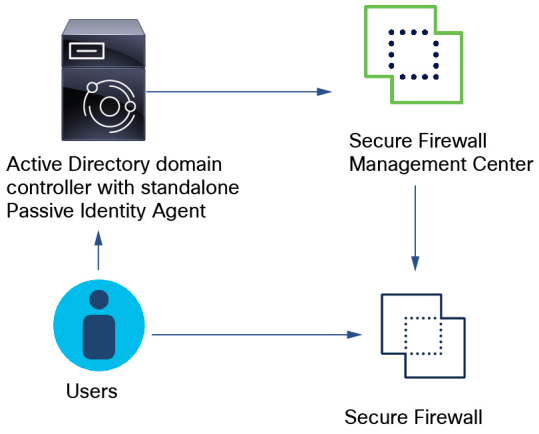
有关详细信息，请参阅以下主题之一：

相关主题

简单 被动身份代理 部署，第 2110 页
单 被动身份代理 监控多个域控制器，第 2110 页
多个 被动身份代理 监控多个域控制器，第 2111 页
被动身份代理 主/辅助代理部署，第 2113 页

简单 被动身份代理 部署

下图显示了最简单的 被动身份代理 部署。

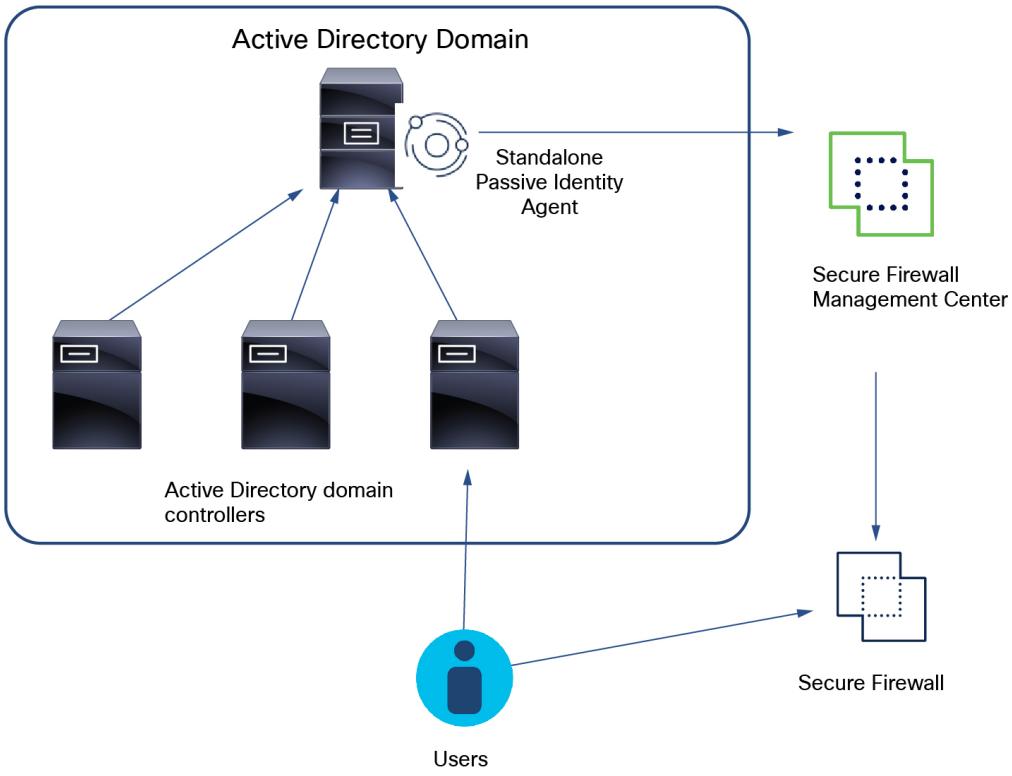


在前面的示例中，一个独立的 被动身份代理 安装在 AD 域控制器上。用户登录和注销 AD 域，代理会将用户名和 IP 地址信息发送到 Secure Firewall Management Center。当用户访问网络时，部署到 Cisco Secure Firewall Threat Defense 的访问控制和身份策略会确定是否允许访问以及如何访问。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

单 被动身份代理 监控多个域控制器

下图显示了监控多个 AD 域控制器的独立 被动身份代理。



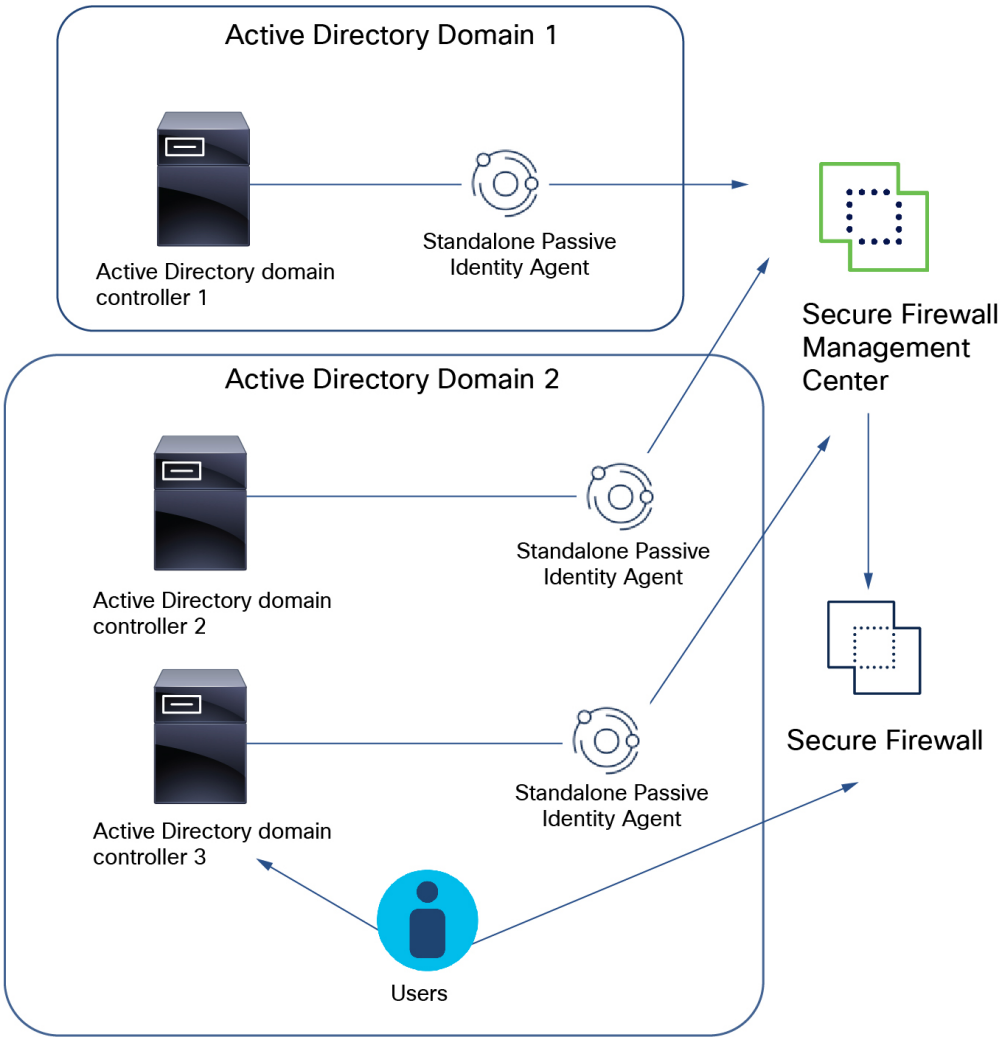
在上图中，独立 被动身份代理 安装在连接到 AD 域的客户端上（或域控制器本身）。登录到任何域控制器的用户和代理会将用户和 IP 地址信息发送到 Secure Firewall Management Center。当用户访问网络时，部署到 Cisco Secure Firewall Threat Defense 的访问控制和身份策略会确定是否允许访问以及如何访问。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

多个 被动身份代理 监控多个域控制器

下图显示了监控多个 AD 域控制器的独立集群：

- 在 AD 域 1 中，安装在与 AD 域控制器 1 连接的计算机上的独立 被动身份代理 会将用户和 IP 地址映射数据发送到 Secure Firewall Management Center。
- 在 AD 域 2 中，AD 域控制器 1 和 2 上安装的独立代理会将用户和 IP 地址映射数据发送到 Secure Firewall Management Center。



您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

上图显示了三个 被动身份代理，而每个均配置为独立端口。为此：

1. 创建两个 Microsoft AD 领域：每个 AD 域一个。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。

2. 对于 AD 域 2，创建两个目录，每个域控制器一个。

3. 在可以登录该域的客户端上安装 被动身份代理 软件。

   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件，第 2129 页。

4. 创建 被动身份代理 身份源。

   请参阅创建主身份源或辅助被动身份代理身份源，第 2120 页。

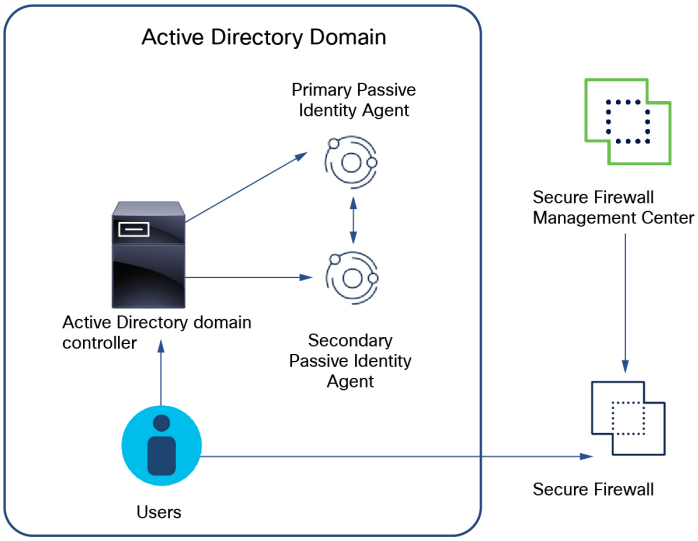
被动身份代理 主/辅助代理部署

要提供冗余并避免单点故障，您可以按照本主题中所示的任何方式配置主和辅助 被动身份代理。

您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。

带主代理和辅助代理的单个 AD 域控制器

下图显示如何在一个 AD 域控制器上设置主和辅助 被动身份代理。如果主代理发生故障，则辅助代理将接管其任务。



要进行此项设置，请执行以下操作：

1. 创建一个 Microsoft AD 领域，其中包含一个用于域控制器的目录。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。

2. 在连接到域控制器的任意两台网络计算机上安装 被动身份代理 软件。

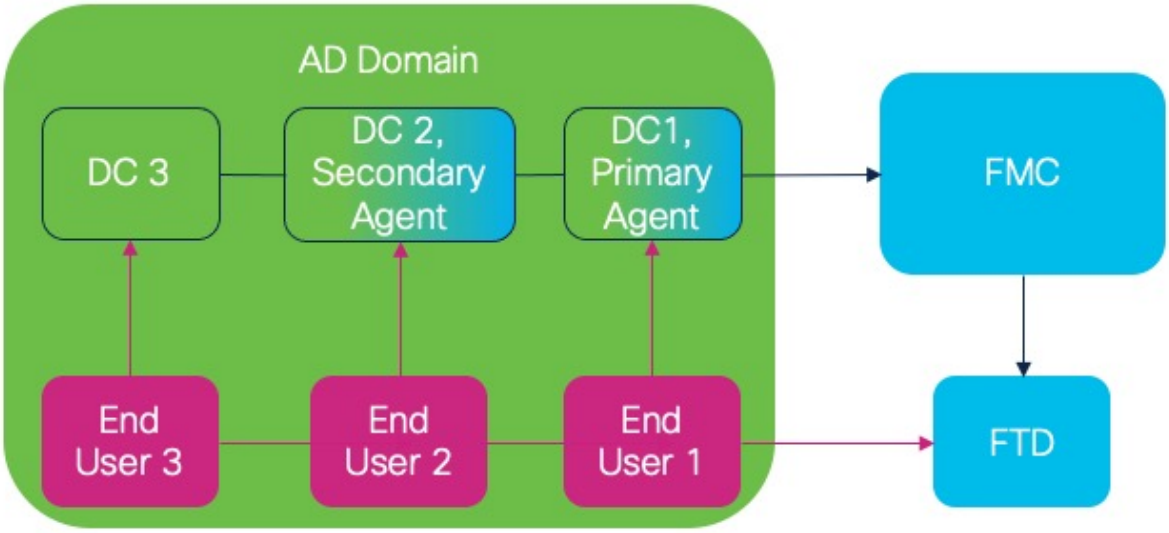
   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件，第 2129 页。

3. 创建身份源。

   请参阅创建主身份源或辅助被动身份代理身份源，第 2120 页。

多个 **AD** 域控制器、主和辅助代理



上图显示了如何配置主和辅助代理以监控三个 AD 域控制器。如果主代理发生故障，则辅助代理将接管其任务。

要进行此项设置，请执行以下操作：

1. 创建一个 Microsoft AD 领域，其中包含一个用于域控制器的目录。

   请参阅创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。

2. 在连接到域控制器的任何计算机上安装 被动身份代理 软件。

   单独配置每个 被动身份代理，以便与您在其上配置 被动身份代理 源的 Secure Firewall Management Center 进行通信。

   请参阅安装 被动身份代理 软件， 第 2129 页。

3. 创建身份源。

   请参阅创建主身份源或辅助被动身份代理身份源， 第 2120 页。

如何创建 被动身份代理 身份源

以下提供了在 Secure Firewall Management Center 中配置 被动身份代理 身份源以及将代理软件部署到您的 Microsoft Active Directory (AD) 服务器所需的高级任务。

过程

	命令或操作	目的
步骤 1	启用Dynamic Attributes Connector。	dynamic attributes connector 是使用 被动身份代理 的一项要求。 请参阅启用 dynamic attributes connector， 第 2116 页。
步骤 2	为您的 Microsoft AD 域和域控制器创建一个领域。	领域是 Secure Firewall Management Center 和您监控的服务器上的用户账号之间的连接。它们可指定该服务器的连接设置和身份验证过滤器设置。 有关详细信息，请参阅创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。
步骤 3	创建 被动身份代理 身份源。	身份源允许 Secure Firewall Management Center 和 被动身份代理 相互通信。根据需要创建独立、主或辅助代理。 有关详细信息，请参阅： • 关于被动身份代理角色， 第 2122 页 • 创建被动身份代理身份源， 第 2117 页
步骤 4	在 Secure Firewall Management Center上创建 被动身份代理 用户。	我们为代理和管理器提供了一个足以相互沟通的角色。我们建议将该角色用于 被动身份代理 用户而不是其他角色。
步骤 5	安装 被动身份代理 软件。	代理的安装方式取决于您的部署。 您可以将 被动身份代理 安装在 AD 域控制器、目录服务器或连接到要监控的域的任何客户端上。 有关详细信息，请参阅： • 部署 被动身份代理， 第 2109 页 • 安装 被动身份代理 软件， 第 2129 页

下一步做什么

创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。

配置 被动身份代理

以下主题讨论如何配置 被动身份代理。

相关主题

创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页
创建被动身份代理身份源， 第 2117 页
安装 被动身份代理 软件， 第 2129 页
为被动身份代理创建Secure Firewall Management Center用户， 第 2123 页

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器， 第 2340 页。

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

创建 Microsoft Active Directory 领域

被动身份代理 要求您创建 Microsoft Active Directory (AD) 领域和 Secure Firewall Management Center 中的目录，如创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页中所述。

创建被动身份代理身份源

此任务讨论如何创建一个会将用户会话活动发送到 Secure Firewall Management Center 的 被动身份代理。

开始之前

完成以下操作：

- 查看关于被动身份代理角色，第 2122 页中讨论的 被动身份代理 角色。
- 如创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述，创建 Microsoft AD 领域。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **身份** > **身份源**。

步骤 3 点击**被动身份代理**。

步骤 4 如果尚未启用 dynamic attributes connector，系统会提示您启用。

有关启用 dynamic attributes connector 的详细信息，请参阅启用 dynamic attributes connector，第 2116 页。

步骤 5 点击**创建代理**。

步骤 6 在“配置代理”对话框中，输入以下信息：

项目	说明
名称	输入可标识 被动身份代理 的唯一名称。
说明	输入可选的说明。
角色	点击以下选项之一： • **主 (Primary)**：负责与 Secure Firewall Management Center 通信的代理。 如果您选择**独立**则不可用。 • **辅助 (Secondary)**：如果主代理与 Secure Firewall Management Center 失去联系，则其会成为主代理。 如果您选择**独立**则不可用。 • **独立**：如果只有一个 被动身份代理。 有关角色的详细信息，请参阅关于被动身份代理角色，第2122页。

步骤 7 继续：

- 创建独立被动身份代理身份源， 第 2118 页
- 创建主身份源或辅助被动身份代理身份源， 第 2120 页

创建独立被动身份代理身份源

此任务讨论如何配置独立 被动身份代理。

开始之前

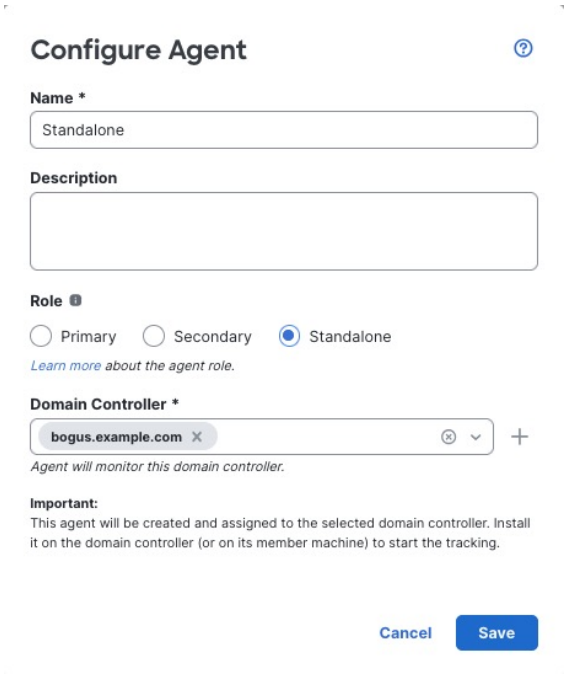
完成 创建被动身份代理身份源， 第 2117 页中讨论的任务。

过程

步骤 1 在“配置代理”对话框中，输入以下信息：

项目	说明
角色	点击**独立**。
域控制器	从列表中选择每个域控制器旁边的复选框，该域控制器有一个您希望用于身份管理和用户控制的 被动身份代理。 （可选。）点击 **添加** (+) 添加新的。

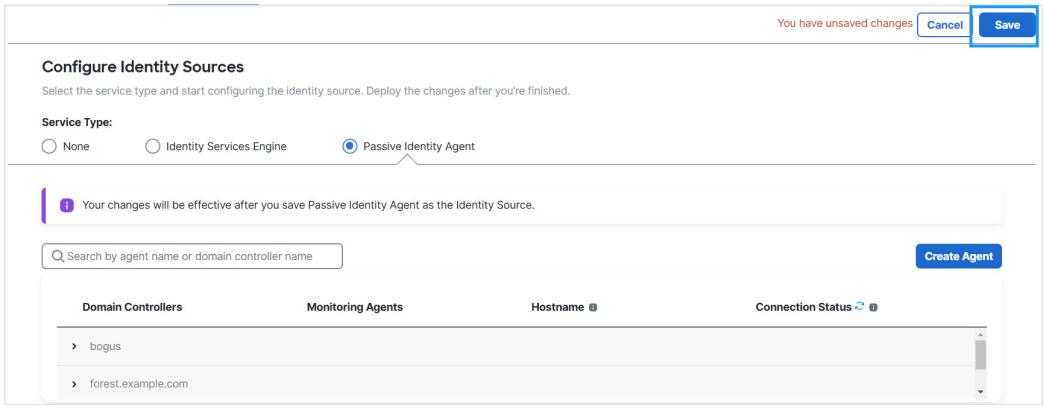
下图显示了独立 被动身份代理 身份源的示例。



步骤 2 在“配置代理”对话框中，点击**保存**。

步骤 3 在页面右上角，点击**保存**。

下图显示了一个示例。



注释
在您创建用户并安装软件之前，被动身份代理 不会处于活动状态。

下一步做什么

- 请参阅为被动身份代理创建Secure Firewall Management Center用户，第 2123 页
- 请参阅关于被动身份代理安装，第 2124 页

创建主身份源或辅助被动身份代理身份源

以下任务会从 创建被动身份代理身份源，第 2117 页继续。

开始之前

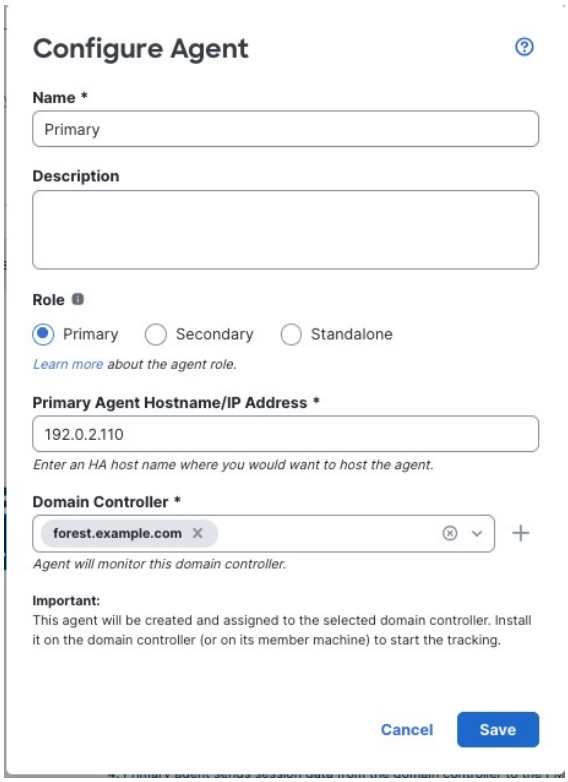
完成 创建被动身份代理身份源，第 2117 页中讨论的任务。

过程

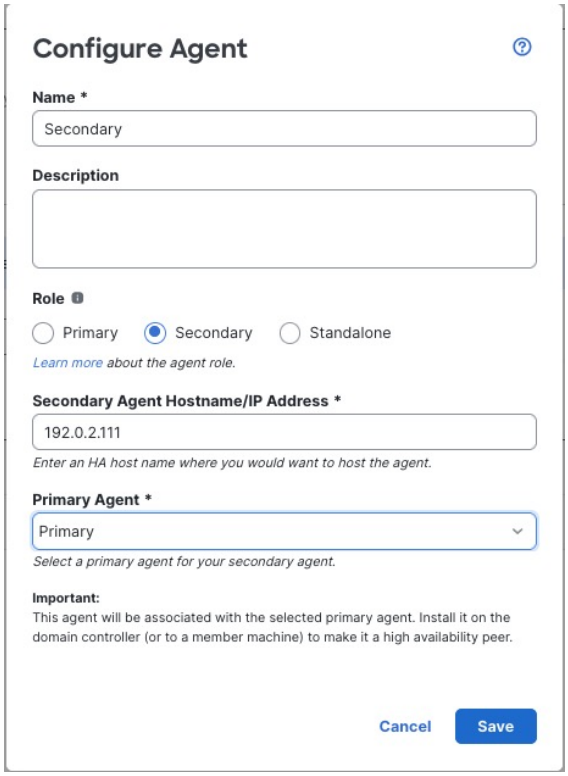
步骤 1 在“配置代理”对话框中，输入以下信息：

项目	说明
角色	点击以下选项之一： • **主 (Primary)**：负责与 Secure Firewall Management Center 通信的代理。 • **辅助 (Secondary)**：如果主代理与 Secure Firewall Management Center 失去联系，则其会成为主代理。 有关角色的详细信息，请参阅关于被动身份代理角色，第2122页。
主代理主机名/IP 地址	（仅限主代理。）输入安装了主被动身份代理的服务器的完全限定域名或 IP 地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
辅助代理主机名/IP 地址	（仅限辅助代理。）输入安装了辅助 被动身份代理 的服务器的完全限定主机名或 IP 地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
主代理	（仅限辅助代理。）在列表中点击主设备的名称 被动身份代理。
域控制器	（仅限主代理。）从列表中选择每个域控制器旁边的复选框，该域控制器有一个您希望用于身份管理和用户控制的 被动身份代理。

下图显示了主代理的示例：



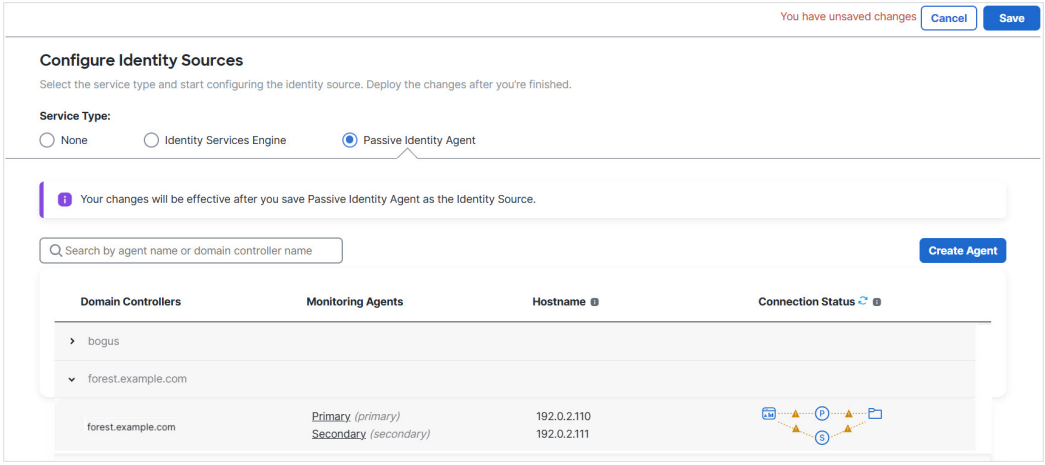
下图显示了辅助代理的示例：



步骤 2 在“配置代理”对话框中，点击**保存**。

步骤 3 在页面右上角，点击**保存**。

下图显示了一个示例。



注释
在您创建用户并安装软件之前，被动身份代理 不会处于活动状态。

下一步做什么

- 请参阅为被动身份代理创建Secure Firewall Management Center用户，第 2123 页
- 请参阅关于被动身份代理安装，第 2124 页

关于被动身份代理角色

被动身份代理 具有以下角色：

- 独立：不属于冗余对的 被动身份代理 。独立代理可以从多个 Active Directory 服务器和域控制器下载用户和组，前提是所有这些服务器和域控制器上都安装了该软件。
- 主：（冗余对中的主代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  处理与 Secure Firewall Management Center 的所有通信，除非它停止通信，在这种情况下，通信将由辅助代理处理。
- 辅助：（冗余对中的辅助或备份代理。）可以安装在 Microsoft AD 域控制器、目录服务器或任何网络客户端上。

  监控主代理的运行状况，并在主代理停止与 Secure Firewall Management Center通信时进行接管。

可以监控属于同一域的多个 AD 域控制器。

为被动身份代理创建Secure Firewall Management Center用户

此任务讨论如何创建具有足够权限的 Secure Firewall Management Center 用户以便与 被动身份代理通信。此用户具有执行其他任务的有限权限；预期用户只能启用与 被动身份代理 通信。

注释 请仅对 被动身份代理 用户使用 **Passive Identity User** 角色。特别是， 请勿对 被动身份代理 用户 使用 **Administrator** 角色，因为当 被动身份代理 与 Secure Firewall Management Center通信时，**Administrator** 将被定期注销。

开始之前

完成 创建被动身份代理身份源， 第 2117 页中讨论的任务。

注释 您不能对 被动身份代理 用户使用外部身份验证。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。

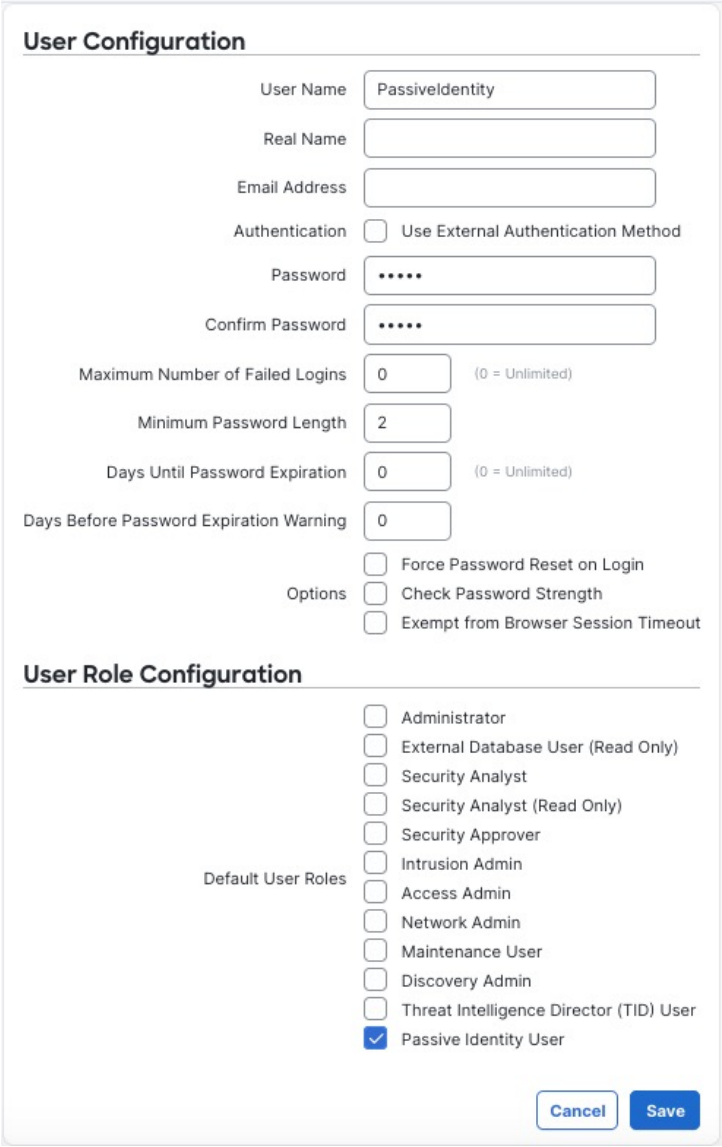
步骤 2 请点击 **管理** > **用户**、 > **用户账户**、 。

步骤 3 点击**创建用户**。

步骤 4 按照《*Cisco Secure Firewall Management Center* 管理指南》中的添加或编辑内部用户所述创建用户。

步骤 5 选择**被动身份用户**角色。

下图显示了一个示例。



注释
不要为 被动身份代理 用户选择 **Passive Identity User** 之外的角色，否则代理将无法正常工作。

步骤 6 点击**保存**。

下一步做什么

关于被动身份代理安装，第 2124 页。

关于被动身份代理安装

以下主题讨论安装 被动身份代理 所需的前提条件和任务。

注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件，第 2133 页

安装 被动身份代理 的先决条件

在安装 被动身份代理 软件之前，您必须完成以下所有任务。

被动身份代理 系统要求

被动身份代理 系统要求

被动身份代理 需要满足以下条件：

- 如果将 被动身份代理 安装在 Windows Active Directory 服务器上，则该服务器必须运行以下版本之一：
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022
- 如果将 被动身份代理 安装在连接到域的 Windows 客户端上，则客户端必须运行 Windows 11 或更高版本。
- 所有系统的系统时钟必须同步。强烈建议在所有这些服务器上使用相同的 NTP 服务器。这意味着：
  - Secure Firewall Management Center。

    有关详细信息，请参阅时间同步，第 1030 页。
  - 所有 Windows Active Directory 服务器和域控制器。
  - 安装了 被动身份代理 的计算机。
- Secure Firewall Management Center 必须运行 7.6 或更高版本。
- 由 Secure Firewall Management Center 托管的任何 Cisco Secure Firewall Threat Defense 必须运行 7.1 或更高版本。
- 您必须在 Cisco Secure Firewall Threat Defense 设备上启用 Snort 3。

启用 Windows 事件查看器以记录 Kerberos 身份验证尝试

以下任务显示如何配置 Windows 组策略对象 (GPO) 安全设置，以便让 记录成功和失败的 Kerberos 身份验证尝试。 被动身份代理 会从事件查看器中读取用户会话，因此要 被动身份代理 正常运行，需要此设置。

有关详细信息，请参阅 learn.microsoft.com 上的审核策略建议。

过程

步骤 1 以管理员身份登录 Active Directory 服务器。

步骤 2 以管理员身份打开 DOS 命令提示符。

步骤 3 输入 `gpmc.msc` 以启动组策略管理编辑器。

步骤 4 如有必要，创建新 GPO；如已存在，则进行编辑。

有关创建 GPO 的详细信息，请参阅 learn.microsoft.com 上的创建组策略对象等资源。

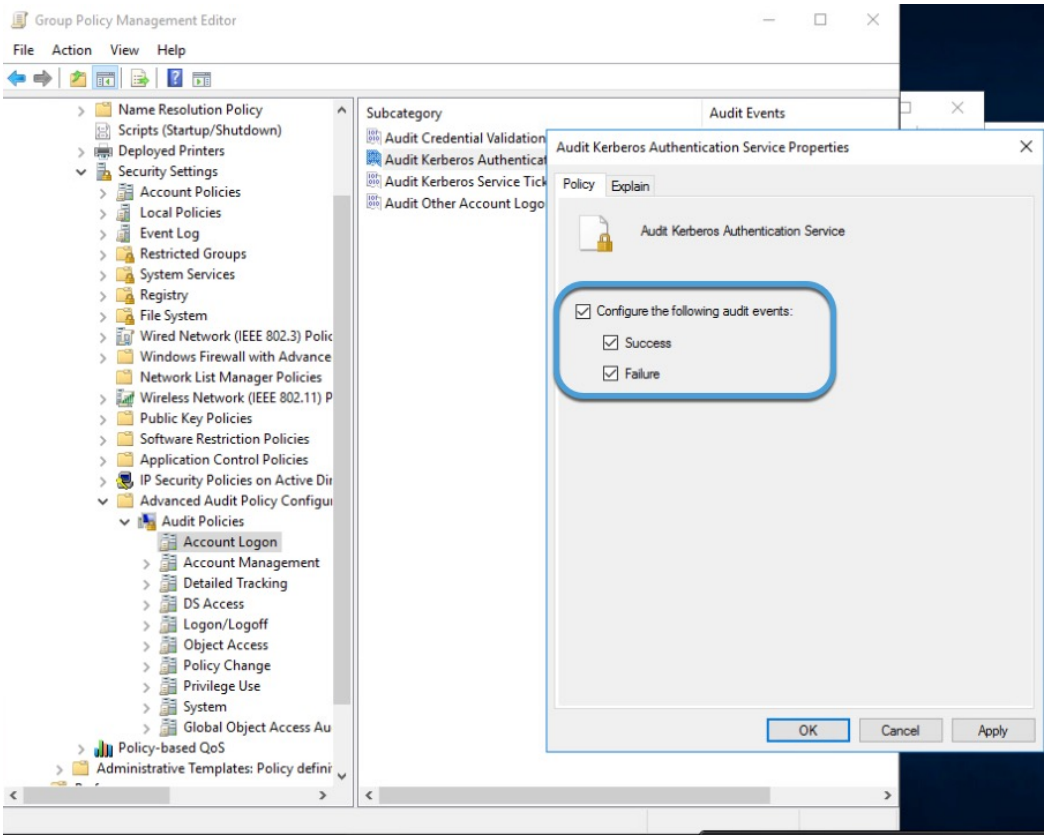
步骤 5 在 GPO 中，展开**计算机配置 (Computer Configuration)** > **策略 (Policies)** > **Windows 设置 (Windows Settings)** > **安全设置 (Security Settings)** > **高级策略配置 (Advanced Policy Configuration)** > **审核策略 (Audit Policies)**。

步骤 6 点击**帐户登录 (Account Logon)**。

步骤 7 在右侧窗格中，双击**审核 Kerberos 验证服务 (Audit Kerberos Authentication Service)**。

步骤 8 在显示的对话框中，选中让系统能够记录成功和失败的所有复选框。

下图显示了一个示例。



步骤 9 按照屏幕上的提示保存更改。

步骤 10 （可选。）要立即更新 GPO，请在 DOS 命令提示符窗口中输入 **gpupdate /force**。

下一步做什么

请参阅将 Active Directory 用户添加到组 ，第 2127 页。

将 Active Directory 用户添加到组

使用此程序为 Active Directory 和 被动身份代理 服务用户授予足够的 Active Directory 权限。

要正常工作， 被动身份代理 必须能够连接域并读取 Windows 事件日志。本主题讨论如何对以下项授予相应权限：

- 被动身份代理 服务用户的设备。
- Active Directory 用户（即 Secure Firewall Management Center上 Active Directory 领域的 “**目录用户名**”用户）。

Before you begin

您必须是 Microsoft 服务器管理员，熟悉如何将用户添加到组以及如何将 Windows 服务设置为以特定用户身份运行。

过程

步骤 1 以管理员身份登录运行 被动身份代理 的系统。

您可以登录以下任一设备：

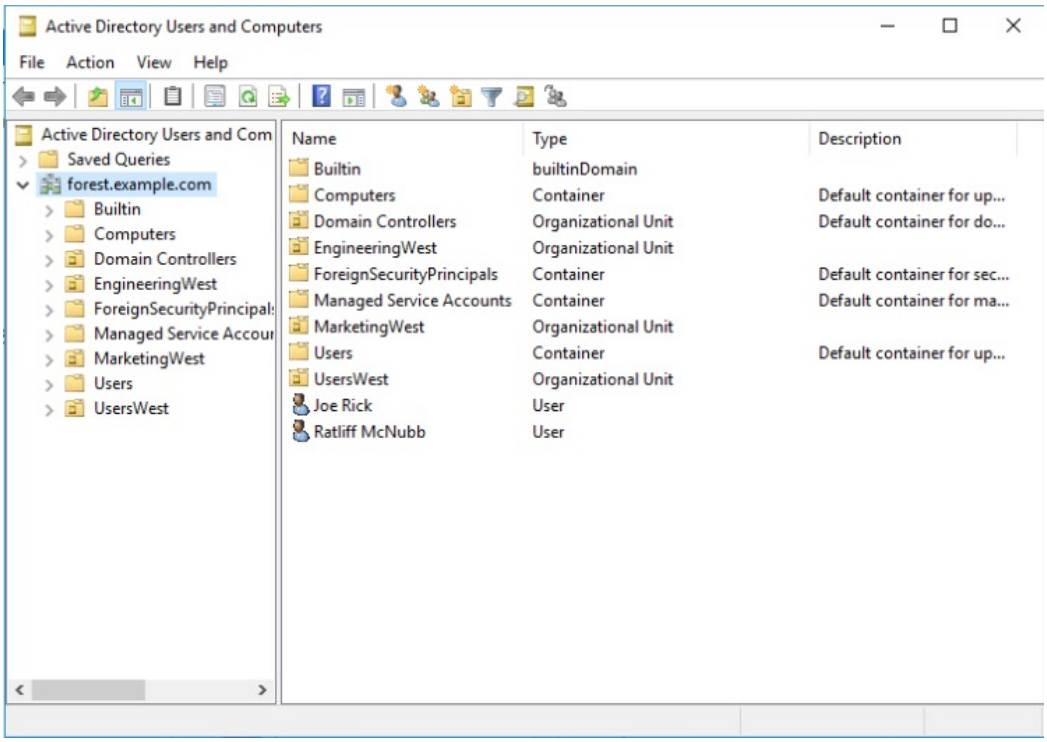
- 域控制器
- Active Directory 服务器。

步骤 2 启动服务器管理器工具。

步骤 3 点击**Active Directory** > **用户和计算机**。

步骤 4 在“Active Directory 用户和计算机”下，展开定义目录用户的林。

下图显示了一个示例。

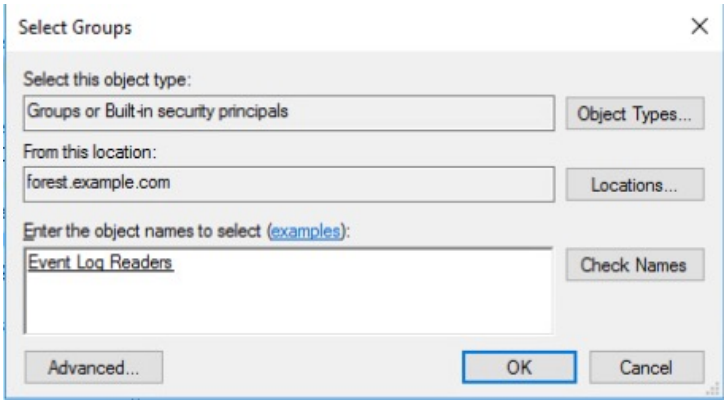


步骤 5 展开组织单位或组以显示目录用户。（点击 **新建用户 (New > User)** 可创建新用户。）

步骤 6 右键点击目录用户，然后点击 **添加到组 (Add to a group)**。

步骤 7 在选择组 (Select Groups) 对话框中，输入 **事件日志读取器 (Event Log Readers)**，然后点击 **检查名称 (Check Names)**。

下图显示了一个示例。



步骤 8 重复前述任务，将该用户添加到域用户组。

步骤 9 在“添加组”对话框中，点击 **确定**。

目录用户现在拥有适当的权限，并且 被动身份代理 服务会以该用户的身份运行。

下一步做什么

请参阅安装 被动身份代理 软件， 第 2129 页。

安装 被动身份代理 软件

此任务讨论如何安装 被动身份代理 软件。对于简单安装，您可以将其安装在 Microsoft Active Directory (AD) 域控制器上；有关其他选项，请参阅部署 被动身份代理， 第 2109 页。



注释 建议您使用最新版本的 被动身份代理。要查看可用版本，请转至 software.cisco.com。要升级 被动身份代理，请参阅升级被动身份代理软件， 第 2133 页

开始之前

完成以上全部任务…

- 启用 Windows 事件查看器以记录 Kerberos 身份验证尝试， 第 2125 页
- 将 Active Directory 用户添加到组， 第 2127 页
- 将登录添加到 被动身份代理 服务， 第 2131 页

过程

步骤 1 从 software.cisco.com 下载 被动身份代理。

步骤 2 以管理员组成员身份登录到要安装 被动身份代理 的计算机。

步骤 3 双击 **CiscoPassiveIdentityAgentInstaller-1.1.1.msi**。

步骤 4 点击**下一步 (Next)**。

步骤 5 选择要在其中安装 被动身份代理 的文件夹，然后点击**下一步 (Next)**。

默认安装文件夹为 **Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**。

步骤 6 点击**下一步 (Next)**。

步骤 7 点击 **Install**。

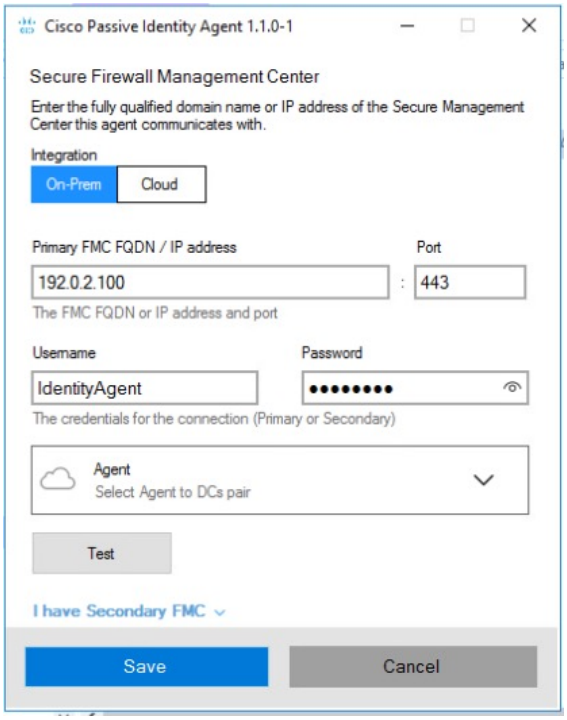
步骤 8 完成安装后，点击**完成 (Finish)**，然后可以选中此复选框以启动 被动身份代理。

步骤 9 当 被动身份代理 启动时，如果您将代理与本地 Secure Firewall Management Center（物理或虚拟）配合使用，则点击**本地 (On-Prem)** 选项卡；如果您将代理与 云交付的防火墙管理中心 配合使用，则点击**云 (Cloud)** 选项卡。

步骤 10 在“思科被动代理”对话框中，输入以下信息：

项目	说明
FMC FQDN / IP 地址	输入您在上面创建 被动身份代理 身份源的 Secure Firewall Management Center 的地址。 被动身份代理 版本 1.0 仅支持 IPv4 地址和完全限定域名。版本 1.1 支持 IPv4、IPv6 和完全限定域名。
端口	输入 Secure Firewall Management Center 侦听端口（默认情况下为 443）。
用户名	输入您在 为被动身份代理创建Secure Firewall Management Center 用户，第 2123 页 中创建的用户的用户名。
密码	输入用户的密码。
代理	点击列表找到您先前在 Secure Firewall Management Center 上创建的 被动身份代理 的域控制器。

下图显示了一个示例。

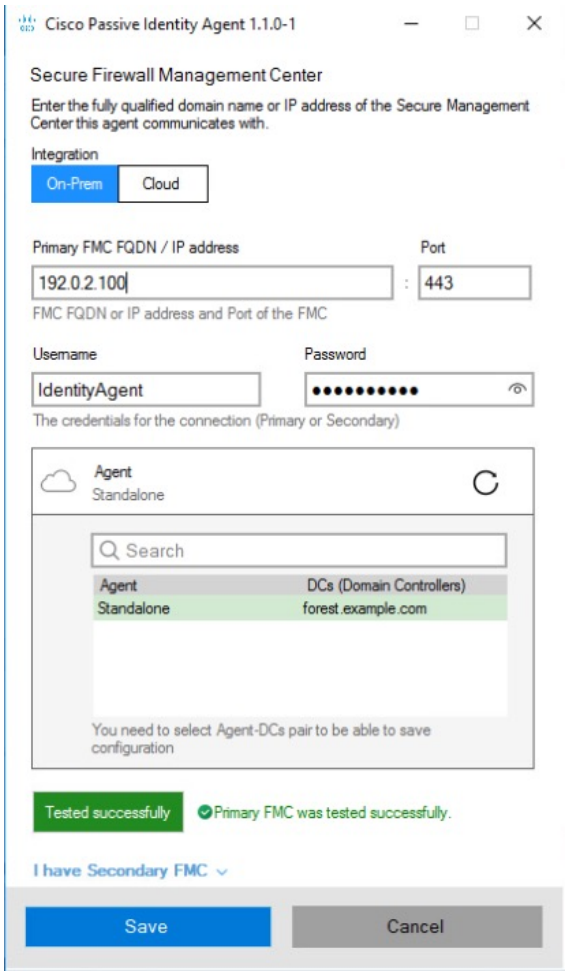


步骤 11 点击**代理**列表。

步骤 12 在列表中点击要监控的域控制器名称。

步骤 13 点击**测试**。

下图显示了一个示例。



步骤 14 如果您有高可用性对，请点击**我有辅助 FMC (I have Secondary FMC)**，然后输入辅助的 IP 地址或完全限定主机名及其侦听端口。

步骤 15 仅在测试成功时点击**保存**。

下一步做什么

请参阅将登录添加到 被动身份代理 服务，第 2131 页。

将登录添加到 被动身份代理 服务

使用此程序启用 被动身份代理 服务以 Active Directory 用户身份运行。（即 Secure Firewall Management Center上 Active Directory 领域的 “**目录用户名**” 用户）。

此任务是可选的，但建议执行此任务，以便 被动身份代理 服务使用将登录信息发送到 Secure Firewall Management Center所需的最小权限运行

Before you begin

完成 将 Active Directory 用户添加到组，第 2127 页中讨论的任务。

您必须是 Microsoft 服务器管理员，熟悉如何将用户添加到组以及如何将 Windows 服务设置为以特定用户身份运行。

过程

步骤 1 以管理员身份登录运行 被动身份代理 的系统。

您可以登录以下任一设备：

- 域控制器
- Active Directory 服务器。

步骤 2 在 Windows 搜索栏中，输入 **服务**。

步骤 3 在服务 (Services) 窗口中，右键点击 **Cisco 被动身份代理 (Cisco Passive Identity Agent)**。

步骤 4 点击**属性 (Properties)**。

步骤 5 在“属性”(Properties) 对话框中，点击 **登录 (Log On)** 选项卡。

步骤 6 点击 **此账户**。

步骤 7 点击 **浏览 (Browse)** 并按照屏幕上的提示选择目录用户。

步骤 8 在提供的字段中输入用户名和密码。

步骤 9 点击**应用 (Apply)**。

下一步做什么

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动，如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程所述。

卸载被动身份代理软件

此任务讨论如何从 Microsoft AD 服务器卸载 被动身份代理 软件。

过程

步骤 1 以管理员身份登录安装了 被动身份代理 的计算机。

步骤 2 搜索“添加或删除程序”。

步骤 3 点击**思科被动身份代理 (Cisco Passive Identity Agent)**。

步骤 4 点击**卸载 (Uninstall)**。

步骤 5 您需要确认卸载。

升级被动身份代理软件

要升级到较新版本的 被动身份代理，您必须卸载较早的版本并安装较新的版本。

请参阅以下信息：

- 卸载被动身份代理软件，第 2132 页
- 关于被动身份代理安装，第 2124 页

监控 被动身份代理

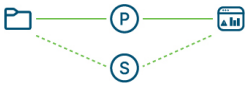
被动身份代理 指示如果其配置为主要-辅助代理，它是否可以与 Secure Firewall Management Center 和其他代理通信。您可以在 **集成** > **身份** > **身份源** 中查看状态。

部署

独立的 被动身份代理 表示如下。



主-辅助对表示如下。



下表解释了指示灯的含义。

对象	含义
	Secure Firewall Management Center
	独立 被动身份代理
	Active Directory 域控制器
	主代理
	辅助代理

状态指示灯和颜色

被动身份代理 使用线条（指明与 Secure Firewall Management Center 的通信是主用还是备用状态）和颜色（指示通信是否成功）指示状态。

下表显示了各行和颜色的含义：

对象	含义
实线	负责与 Secure Firewall Management Center 通信的代理。
虚线	仅限主/辅助配置。充当备份代理的代理。如果活动（实线）代理之间发生通信故障，此代理将与 Secure Firewall Management Center 之间的通信。
蓝色	代理通信正常。
琥珀色 	代理从未成功与 Secure Firewall Management Center 通信。新创建的代理线路显示为琥珀色，并在配置完成之前保持该状态。
红色 	通信失败。要解决此问题，请执行以下操作： • 检查以确保代理和 Secure Firewall Management Center 之间建立网络连接。 • 确保您已完成系统（Microsoft AD 服务器、域控制器和 Secure Firewall Management Center）的配置。 有关详细信息，请参阅如何创建 被动身份代理 身份源，第 2114 页。

管理被动身份代理

以下主题讨论如何编辑或删除您先前在 Secure Firewall Management Center 上配置的 被动身份代理。

相关主题

编辑 被动身份代理，第 2135 页
删除独立 被动身份代理，第 2135 页
删除主和辅助 被动身份代理，第 2135 页
卸载被动身份代理软件，第 2132 页

编辑 被动身份代理

此任务讨论如何编辑您之前在 Secure Firewall Management Center 中配置的 被动身份代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。
步骤 4 点击代理旁边的 **编辑** (✎) 进行编辑。
步骤 5 进行所需的更改。
步骤 6 点击**保存**。

删除独立 被动身份代理

此任务讨论如何删除独立 被动身份代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。
步骤 4 点击要删除的代理旁边的 **编辑** (✎)。
步骤 5 点击**删除 (Delete)**。
步骤 6 您需要确认操作。

删除主和辅助 被动身份代理

此任务讨论如何删除主和辅助 被动身份代理。您必须先删除辅助代理，然后才能删除主代理。

过程

步骤 1 以管理员身份登录 Secure Firewall Management Center。
步骤 2 请点击 **集成** > **身份** > **身份源**。
步骤 3 点击**被动身份代理**。

步骤 4 点击要删除的辅助代理旁边的 **编辑** (✎)。

步骤 5 点击**删除 (Delete)**。

步骤 6 您需要确认操作。

步骤 7 如果要删除主代理，请先删除所有辅助代理。

被动身份代理 故障排除

本主题讨论如何对 Windows AD 域控制器或目录服务器上的 被动身份代理 软件进行故障排除。

（可选。）设置日志级别

默认情况下，被动身份代理 会在 INFO 级别进行日志记录。（可选）要更改日志级别，请在文本编辑器中打开 **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**，保存文件，然后重新启动思科被动身份代理服务。

请勿重命名日志记录服务

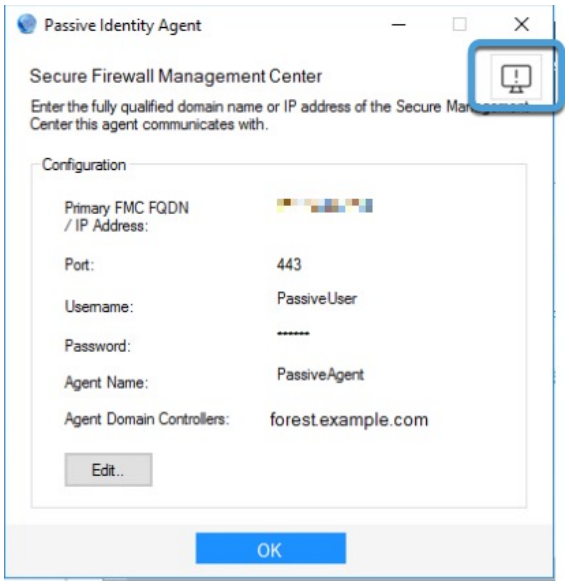
请勿重命名 **C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent\CiscoPassiveIdentityAgentService.exe.config**；否则，被动身份代理 将停止生成日志文件。请勿删除或更改 **.exe.config** 文件扩展名。

生成故障排除文件

要生成包含故障排除文件的 .zip 文件，请执行以下操作：

1. 登录 Microsoft Active Directory 域控制器。
2. 启动 被动身份代理 软件。
3. 点击窗口右上角的“故障排除”(Troubleshooting) 按钮。

   下图显示了一个示例。



屏幕上将显示一条确认消息。

您的故障排除日志将保存到系统的 Downloads 文件夹；文件名以 **TroubleshootLogs** 开头。

手动查看日志文件

被动身份代理 日志文件以纯文本格式存储在代理的安装目录中：**C:\Program Files\Program Files (x86)\Cisco\Cisco Passive Identity Agent**。

使用记事本或其他文本编辑器查看这些文件。日志文件大小在达到 10 MB 后轮换。

使用 Microsoft Active Directory 事件查看器

如果在 Secure Firewall Management Center 中看不到用户会话，您可以在 Microsoft Active Directory 服务器的事件查看器中查找以下 Kerberos 相关事件：

- 4770
- 4768

有关审核策略的一般信息，请参阅 learn.microsoft.com 上的审核策略建议。

有关 Windows 组策略对象设置的详细信息，请参阅 learn.microsoft.com 上的组策略对象。

被动身份代理 的安全要求

为了保护，应将 被动身份代理 安装在受保护的内部网络中。虽然被动身份代理被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到攻击。

如果 被动身份代理 和 Secure Firewall Management Center 位于同一个网络，您可以将 Secure Firewall Management Center 连接到与 被动身份代理 相同的受保护内部网络。

无论如何部署设备，内部系统通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

被动身份代理的互联网接入要求

默认情况下，被动身份代理 会被配置为使用端口 443/tcp (HTTPS) 上的 HTTPS 通过互联网与 Firepower 系统通信。如果您不希望 被动身份代理 直接访问互联网，则可以配置代理服务器。

以下信息告知您 被动身份代理 用于相互通信、与 Secure Firewall Management Center 以及与 Microsoft Active Directory 通信的端口。

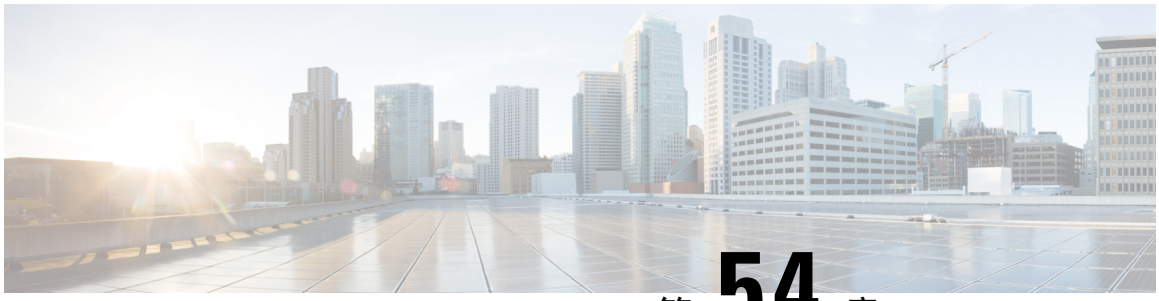
表 *119:* 被动身份代理 端口要求

端口	原因
443	与 Secure Firewall Management Center 通信。
135	使用 MSRPC 协议与 Microsoft Active Directory 通信。
9095	使用 UDP 协议相互通信。

被动身份代理 的历史记录

表 *120:* 被动身份代理 的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
被动身份代理	7.6	7.1	引入了此功能。 被动身份代理 版本 1.1 与 7.6.0 及更高版本兼容，并添加了以下内容： • 您可以使用 FQDN、IPv4 或 IPv6 从 被动身份代理 连接到 Secure Firewall Management Center 或 Security Cloud Control。 • 从 Microsoft Active Directory (AD) 向防火墙管理中心发送 IPv4 和 IPv6 用户会话。 • 您可以压缩故障排除日志。 • 在启动 被动身份代理 软件时，系统将显示前提条件列表。 被动身份代理 身份源将会话数据从 Microsoft Active Directory (AD) 发送到 防火墙管理中心。以下设备支持被动身份代理软件： • Microsoft AD 服务器（Windows Server 2008 或更高版本） • Microsoft AD 域控制器（Windows Server 2008 或更高版本） • 连接到要监控的域的任何客户端（Windows 8 或更高版本）



第 54 章

身份源：pxGrid Cloud 身份（ISE 3.3 及更低版本）

以下主题讨论如何配置和使用包含 Cisco ISE 3.3 及更早版本的 pxGrid 云身份源。

- 关于 pxGrid 云身份源， 第 2141 页
- 如何配置 pxGrid 云身份源， 第 2143 页
- 在 Cisco ISE 中启用 pxGrid Cloud 服务， 第 2146 页
- 使用 Catalyst 云门户 注册 Cisco ISE， 第 2146 页
- 向 Cisco ISE 注册 pxGrid 云 连接， 第 2149 页
- 创建一个 pxGrid 云身份源， 第 2150 页
- 创建动态属性过滤器， 第 2164 页
- 使用动态属性过滤器来创建访问控制规则或 DNS 规则， 第 2165 页
- pxGrid 云身份源 故障排除， 第 2167 页
- 停用并删除 pxGrid 云身份源， 第 2168 页

关于 pxGrid 云身份源

思科身份服务引擎 (Cisco ISE) pxGrid 云身份源 允许您在 Secure Firewall Management Center 访问控制规则中使用来自 的 服务器或集群 的订阅和用户数据。此外，身份源在 Secure Firewall Management Center的访问控制策略中使用来自 的不断变化的动态对象。

pxGrid 云身份源 还使用：

- Cisco Platform Exchange Grid (pxGrid)，可在安全监控和检测系统、网络策略平台、资产和配置管理、身份和访问管理等领域实现多供应商跨平台网络系统协作。 pxGrid 云是 Cisco ISE 的基于云的接口。

  有关 pxGrid 的更多信息可以在 devnet 上的“什么是 PxGrid？”等资源中找到。

- 思科全数字化网络架构 (Cisco DNA) 可提供自动化、安全性、预测性监控和策略驱动方法。它能够提供端到端网络可视性，利用网络洞察优化网络性能并提供最佳的用户和应用体验。

  要将 pxGrid 云身份源 和 Secure Firewall Management Center配合使用，您必须 创建一个思科帐户。

- devnet 上的什么是 pxGrid?
- devnet 上的思科平台交换架构云

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页

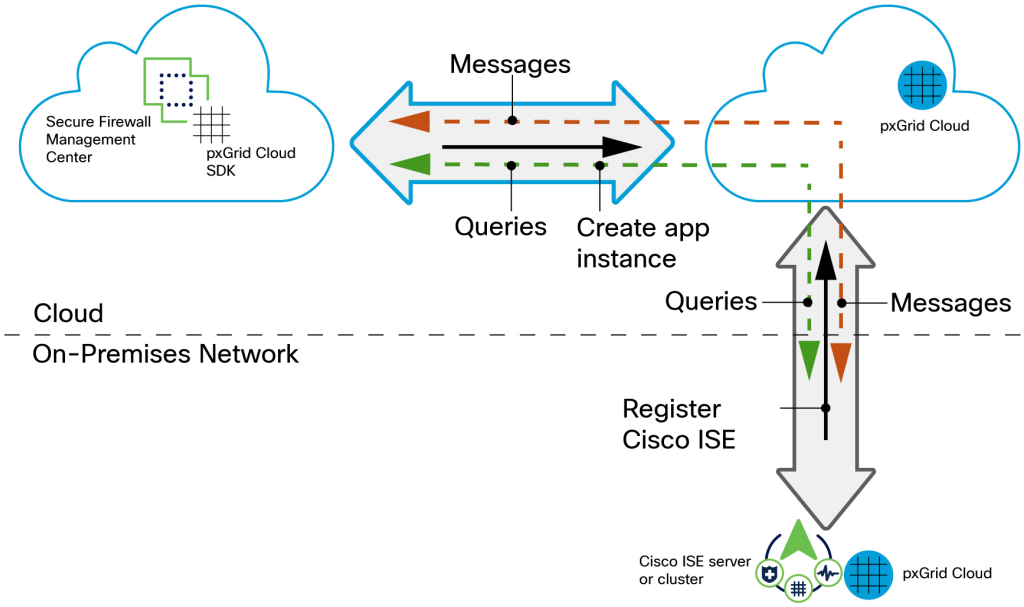
pxGrid 云身份源 的限制

在设置 pxGrid 云身份源 之前，请注意以下事项：

- pxGrid 云 支持以下区域：`us-west-2`、`eu-central-1` 和 `ap-southeast-1`。
- 有关 Cisco ISE 版本和查询大小的信息，请参阅 GitHub 上 pxGrid 云 SDK 中的查询限制。

pxGrid 云身份源 工作原理

下图显示了身份源的工作原理。



您的 Secure Firewall Management Center 使用 pxGrid 云 SDK 以编程方式从本地 Cisco ISE 服务器或集群 检索用户信息，以便可以在 Secure Firewall Management Center 上的身份策略中使用这些用户。

要授权和验证此数据交换，您必须：

1. 在 Cisco ISE 中，启用 pxGrid 云。
2. 在 pxGrid 云中将 Cisco ISE 注册为产品，这将对 Cisco ISE 和 pxGrid 云进行身份验证，并使它们能够相互通信。

身份验证过程要求您将一次性密码 (OTP) 从 pxGrid 云粘贴到 Cisco ISE 中。

3. 在 pxGrid 云中，创建一个“应用实例”，用于生成 OTP，以供您在 Secure Firewall Management Center 中用于对彼此进行身份验证。
4. 完成上述所有任务后，Secure Firewall Management Center（包括 pxGrid 云 SDK）可以使用 pxGrid 云查询 Cisco ISE 并检索包含用户信息、SGT、终端配置文件和其他详细信息的会话。
5. 可以过滤许多类型的动态对象，并将其作为要在访问控制规则中使用的动态对象发送到 Secure Firewall Management Center。其中包括：SGT、终端配置文件、终端安全评估状态和计算机身份验证。

   我们会从 Cisco ISE 检索用户信息，并从 Microsoft Active Directory 或 Azure Active Directory 检索组信息。

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页

如何配置 pxGrid 云身份源

这些主题总结了如何为 ISE 3.3 及更早版本或 ISE 3.4 及更高版本配置 pxGrid 云身份源。步骤不同，因此请确保完全按照步骤操作。

相关主题

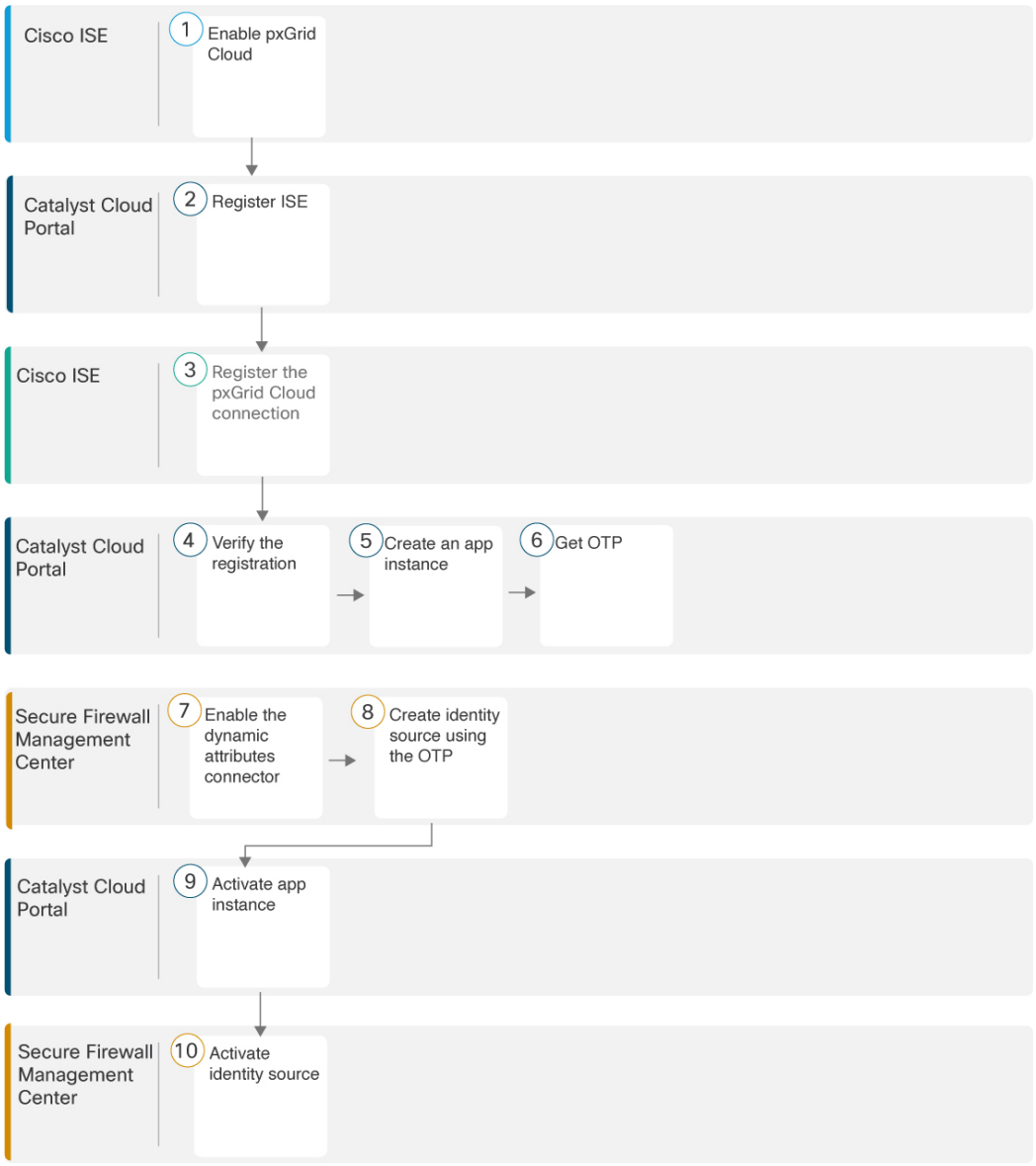
如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页
在 Cisco ISE 中启用 pxGrid 云 服务，第 2177 页
创建应用实例，第 2180 页
创建身份源，第 2152 页
激活应用实例，第 2153 页
激活 pxGrid 云身份源，第 2156 页

如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）

在开始之前，创建一个 Cisco 账户。

重要事项 本主题适用于 *Cisco ISE* 版本 *3.3* 或更早版本。如果您使用的是更高版本，另请参阅如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页。

下图显示了使用 Cisco ISE、Catalyst 云门户 和 Secure Firewall Management Center 来配置 pxGrid 云身份源 的步骤。



1 在 Cisco ISE 中启用 pxGrid Cloud 服务， 第 2146 页
2 使用 Catalyst 云门户 注册 Cisco ISE， 第 2146 页
3 使用 Catalyst 云门户 注册 Cisco ISE， 第 2146 页
4 创建应用实例， 第 2151 页
5 启用 dynamic attributes connector， 第 2116 页
6 创建应用实例， 第 2151 页
7 激活应用实例， 第 2153 页
8 激活 pxGrid 云身份源， 第 2156 页

表 *121:* 配置 *pxGrid* 云身份源

1	Cisco ISE	在 Cisco ISE 中启用 pxGrid Cloud。 pxGrid Cloud 使您能够订阅产品/服务，并注册应用（在此情况下为 Secure Firewall Management Center），以在云环境中进行安全数据交换。 有关详细信息，请参阅在 Cisco ISE 中启用 pxGrid Cloud 服务，第 2146 页。
2	Catalyst 云门户	在 Catalyst 云门户 中注册 Cisco ISE，并对 Cisco ISE 与 Catalyst 云门户 之间的通信进行身份验证。 有关详细信息，请参阅使用 Catalyst 云门户 注册 Cisco ISE，第 2146 页。
3, 4	Cisco ISE，Catalyst 云门户	向 Cisco ISE 注册 pxGrid Cloud 并验证注册。 有关详细信息，请参阅向 Cisco ISE 注册 pxGrid 云 连接，第 2149 页。
5, 6	Catalyst 云门户，Secure Firewall Management Center	在 Catalyst 云门户 中创建一个应用实例并获取一次性密码 (OTP)。 应用实例使 Secure Firewall Management Center 能够使用 pxGrid Cloud 服务向 Cisco ISE 进行身份验证。 下一步所需的 OTP 将在 60 分钟后到期。
7	Secure Firewall Management Center	如果尚未启用，请启用 dynamic attributes connector。 使用 pxGrid 云身份源 需借助 dynamic attributes connector。 有关详细信息，请参阅启用 dynamic attributes connector，第 2116 页。
8	Secure Firewall Management Center	使用您在上一步中获取的 OTP 创建 pxGrid 云身份源。 关联该应用后，可让 Secure Firewall Management Center 向 Cisco ISE 和 Catalyst 云门户进行身份验证，以便接收来自 Cisco ISE 的用户数据。 有关详细信息，请参阅创建身份源，第 2152 页。
9	Catalyst 云门户	激活应用实例。 有关详细信息，请参阅激活应用实例，第 2153 页。
10	Secure Firewall Management Center	激活 pxGrid 云身份源。 有关详细信息，请参阅激活 pxGrid 云身份源，第 2156 页

完成所有前述任务后，您可以：

- 测试 pxGrid 云身份源 以确保其正常运行。

  有关详细信息，请参阅测试 pxGrid 云身份源，第 2158 页。

- 创建动态属性过滤器，定义哪些动态对象发送到 Secure Firewall Management Center。

  有关详细信息，请参阅创建动态属性过滤器，第 2164 页。

- 配置 pxGrid 云身份源 后，您可以在访问控制规则中使用以下任何内容：
  - 动态对象
  - Microsoft AD 用户和组
  - Azure AD 用户和组

相关主题

在 Cisco ISE 中启用 pxGrid Cloud 服务，第 2146 页

在 Cisco ISE 中启用 pxGrid Cloud 服务

开始之前

- 确保在 Cisco ISE 部署中安装并激活 Advantage 许可证层。
- pxGrid Cloud 代理会创建与 Cisco pxGrid 云 的出站 HTTPS 连接。因此，如果客户网络使用代理访问互联网，则必须配置 Cisco ISE 代理设置。要在 Cisco ISE 中配置代理设置，点击**菜单**图标 (☰)，然后选择 **管理 > 系统 > 设置 > 代理**。
- 思科 ISE 受信任的证书储存必须包括验证 pxGrid 云 提供的服务器证书所需的根 CA 证书。确保已为此根 CA 证书启用 **信任思科服务的身份验证** 选项。要启用**信任对思科服务的身份验证**，请导航至**管理** > **系统** > **证书**。

过程

步骤 1 在思科 ISE GUI 中，点击**菜单** 图标 (☰)，然后选择 **管理 > 系统 > 部署**。

步骤 2 点击要在其上启用 pxGrid 云 服务的节点。

步骤 3 在**常规设置 (General Settings)** 选项卡中，启用 **pxGrid** 服务。

步骤 4 选中**启用 pxGrid 云 (Enable pxGrid Cloud)** 复选框。

为了实现高可用性，可在两个节点上启用 pxGrid 云服务。

注释

只有在该节点上启用了 **pxGrid** 服务后才能启用 **pxGrid 云 (pxGrid Cloud)** 选项。

使用 Catalyst 云门户 注册 Cisco ISE

此任务讨论如何在 Catalyst 云门户 中将 Cisco ISE 注册为应用，以及验证 Catalyst 云门户 与 Cisco ISE 之间的通信。

另请参阅《*pxGrid Cloud* 解决方案指南》中的注册 Cisco ISE。

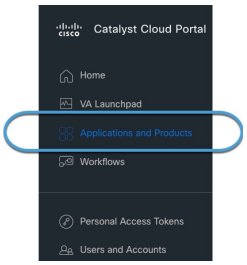
过程

步骤 1 登录到 Cisco Cloud Catalyst 门户。

步骤 2 如果出现提示，请选择要使用的账户。

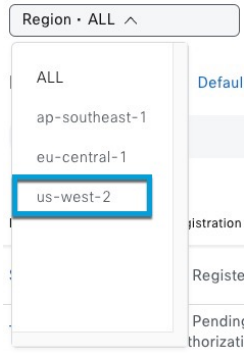
步骤 3 点击**注册 (Register)**。

步骤 4 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：

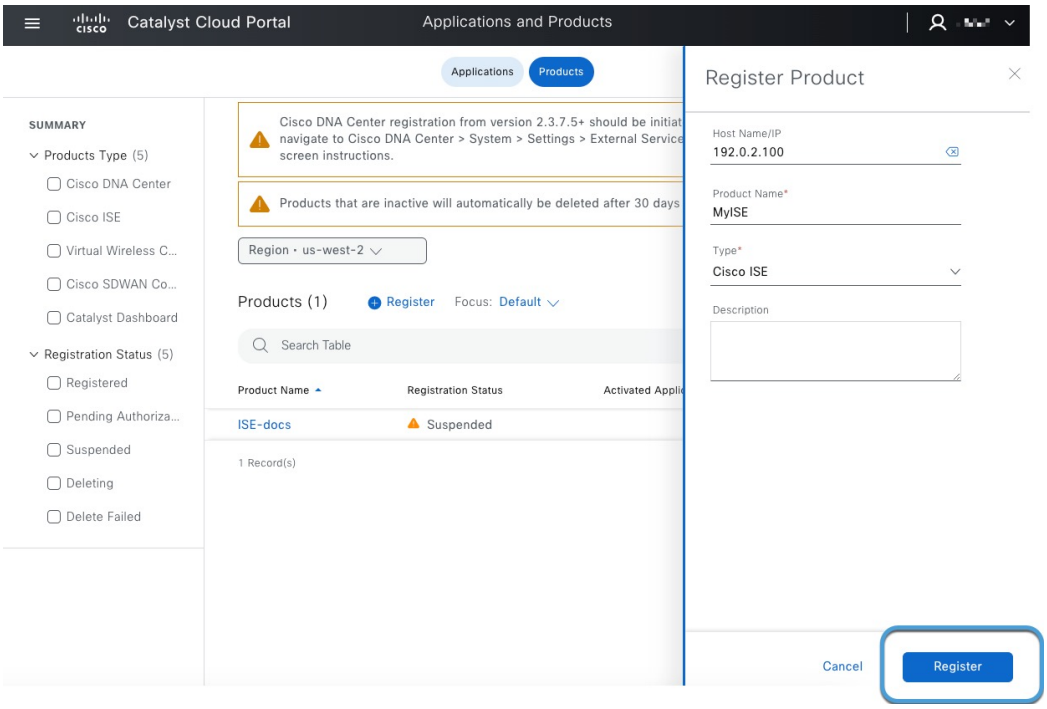


步骤 5 在页面顶部，点击**产品**。

步骤 6 从**区域**列表中，点击 **us-west-2**、**eu-central-1** 或 **ap-southeast-1**。



步骤 7 点击**注册 (Register)**。
下图显示了示例注册页面。



步骤 8 输入以下信息。

- **主机名/IP**：（可选）。输入 ISE 服务器的完全限定域名或 IP 地址。如果输入 IP 地址，请省略方案（例如 **https://**）和端口（如有）。
- **产品名称**：输入用于标识此服务器的唯一名称。
- **类型**：从列表中，点击 **Cisco ISE**。
- **说明**：输入可选说明。

步骤 9 点击**注册 (Register)**。

步骤 10 通过以下任一方式生成一次性密码 (OTP)：

- 如果您之前已注册 ISE 应用并在列表中看到您的应用，请点击**操作**列中的**生成 OTP**；您将在本过程的后续部分用到它。
- 如果您现在正在注册应用，将显示 OTP。点击 将其复制到剪贴板；您将在本过程的后续部分用到它。

下一步做什么

请参阅向 Cisco ISE 注册 pxGrid 云 连接，第 2149 页。

向 Cisco ISE 注册 pxGrid 云 连接

此任务讨论如何向 Cisco ISE 注册 pxGrid 云 连接，这将使 pxGrid 云 能够在 pxGrid 云身份源 中将用户数据发送到 Security Cloud Control。

开始之前

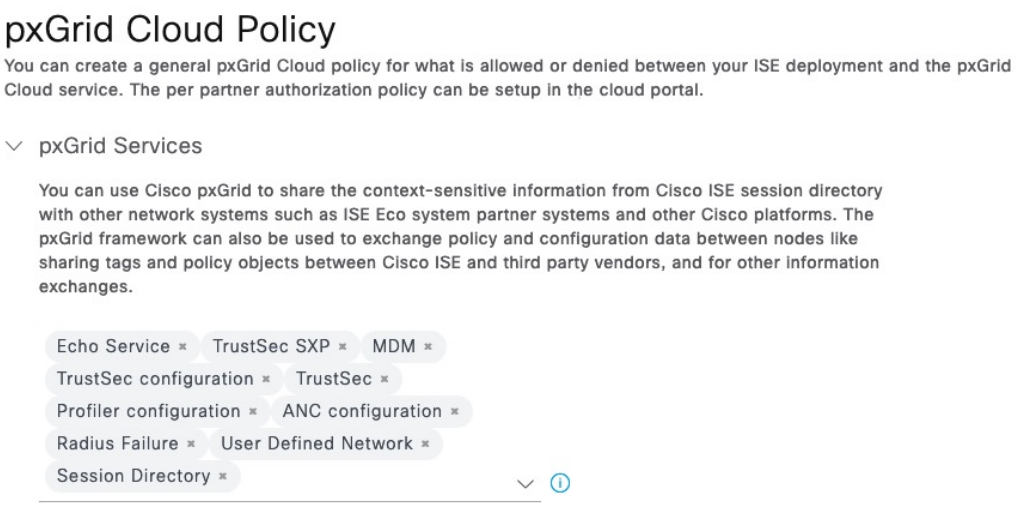
完成 使用 Catalyst 云门户 注册 Cisco ISE，第 2146 页中讨论的任务。

过程

步骤 1 以管理员身份登录 Cisco ISE。

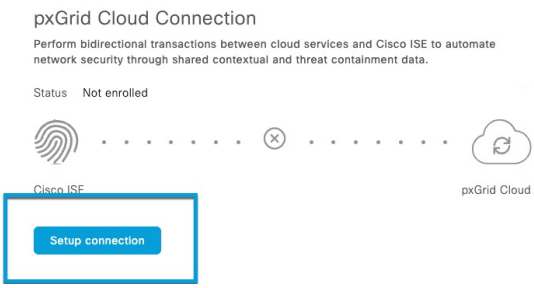
步骤 2 点击 ≡ > **管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接**。

步骤 3 确保所有服务均已启用并具有读/写权限。
下图显示了一个示例。



步骤 4 在左侧导航栏中，点击 **pxGrid Cloud 连接**。

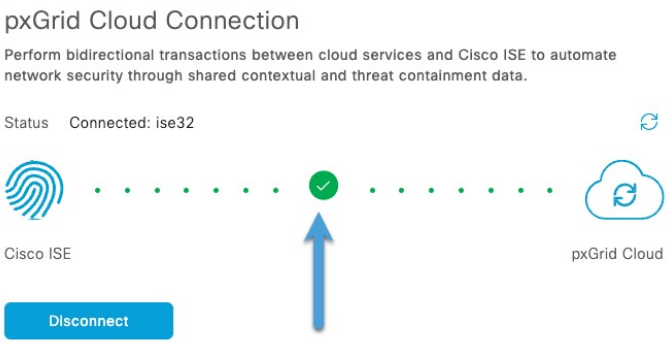
步骤 5 点击**设置连接**，如下图所示。



步骤 6 将 OTP 值粘贴到提供的字段中。

步骤 7 点击**连接 (Connect)**。

如下所示的绿色复选标记确认连接已成功。

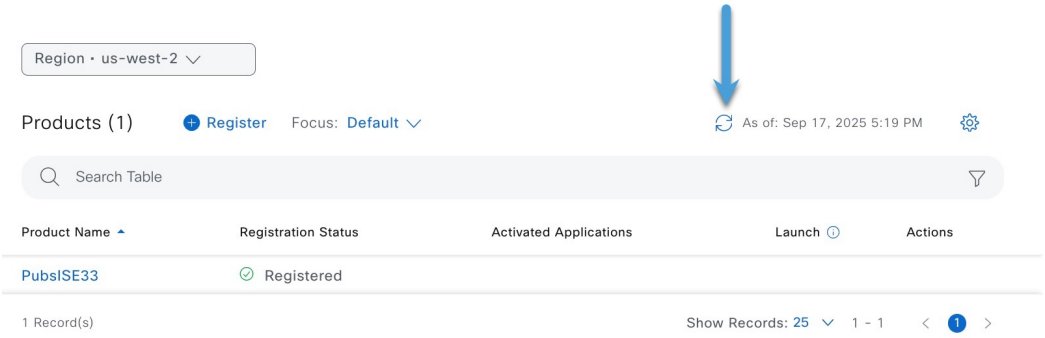


步骤 8 确认到目前为止设置已成功：

a) 登录Catalyst 云门户。

b) 点击 **产品** 选项卡。

c) 点击**刷新**，如下图所示。



d) 验证**已注册**显示为您的产品的状态。

下一步做什么

继续执行创建身份源，第 2152 页。

创建一个 pxGrid 云身份源

以下任务讨论如何使用 Cisco ISE、Catalyst 云门户 和 Security Cloud Control 来创建 pxGrid 云身份源。您必须按所示顺序完成所有任务；在某些情况下，由于所需一次性密码 (OTP) 的过期，存在时间限制。

相关主题

创建应用实例，第 2151 页
创建身份源，第 2152 页
激活应用实例，第 2153 页
激活 pxGrid 云身份源，第 2156 页
测试 pxGrid 云身份源，第 2158 页

创建应用实例

此任务是您必须执行的多项任务之一，目的是创建一个 pxGrid 云身份源，以便将用户会话数据发送到 Secure Firewall Management Center。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

开始之前

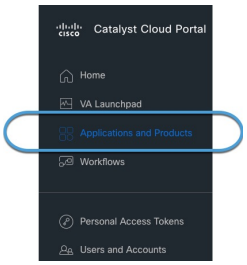
首先完成以下所有任务：

- 在 Cisco ISE 中启用 pxGrid Cloud 服务，第 2146 页
- 使用 Catalyst 云门户 注册 Cisco ISE，第 2146 页
- 向 Cisco ISE 注册 pxGrid 云 连接，第 2149 页

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：



步骤 3 在页面顶部，点击**应用**。

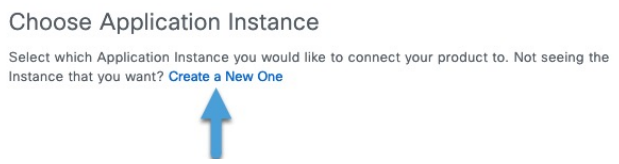
步骤 4 从**区域**列表中，点击 **us-west-2**、**eu-central-1** 或 **ap-southeast-1**。

步骤 5 点击 **Firepower 管理中心**旁边的**管理**（或**激活**）。

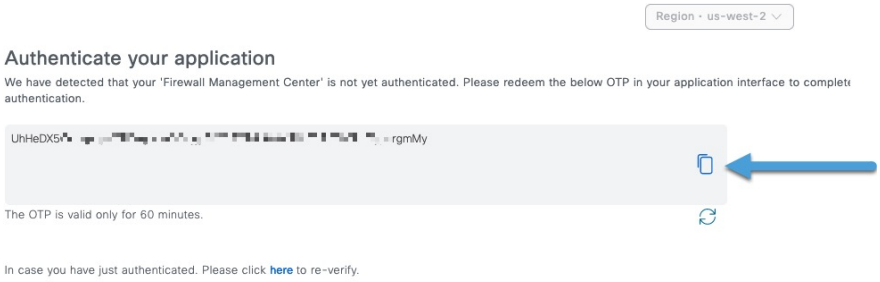
步骤 6 点击**添加 (Add)**。

步骤 7 点击**创建一个新的**。

下图显示了一个示例。



步骤 8 点击显示的 OTP 旁边的复制按钮，如下图所示：



步骤 9 将 OTP 复制到文本文件；它会在 60 分钟后过期。

步骤 10 继续执行创建身份源，第 2152 页。

创建身份源

此任务是创建 pxGrid 云身份源 以将用户会话数据发送到 Secure Firewall Management Center 的多项任务之一。

开始之前

完成 创建应用实例，第 2151 页中讨论的任务。

过程

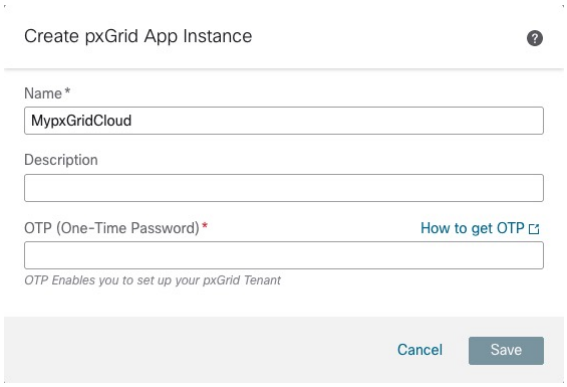
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击**创建 pxGrid 应用实例**。

下图显示了一个示例。



步骤 5 输入以下信息。

值	说明
名称	输入名称以唯一标识此连接器。
说明	可选说明。
OTP（一次性密码）	输入的 OTP。

步骤 6 点击**创建 (Create)**。

步骤 7 在该页面顶部，点击**保存**。

步骤 8 继续执行激活应用实例 ， 第 2153 页。

激活应用实例

本任务讨论如何创建 pxGrid 云身份源 向 Secure Firewall Management Center 发送用户会话数据。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

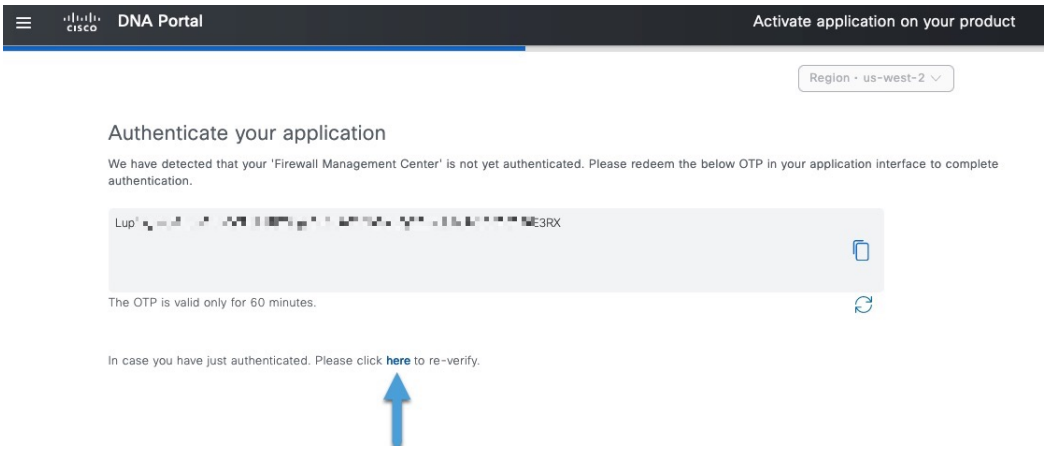
开始之前

完成 创建身份源 ， 第 2152 页中讨论的任务。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

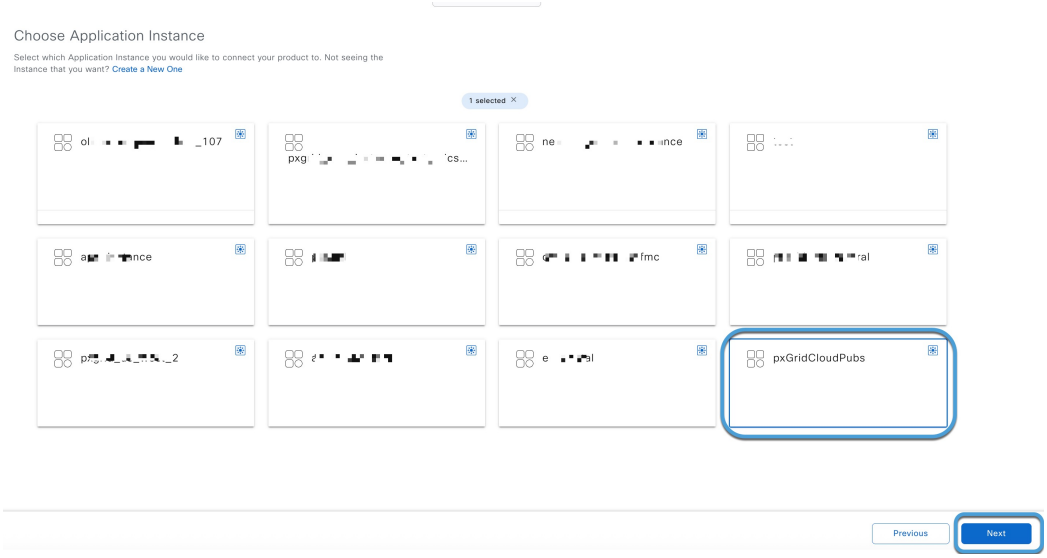
步骤 2 点击下图所示的单词**此处**，重新验证应用。



步骤 3 点击您刚刚在 Secure Firewall Management Center 中创建的应用实例的名称。

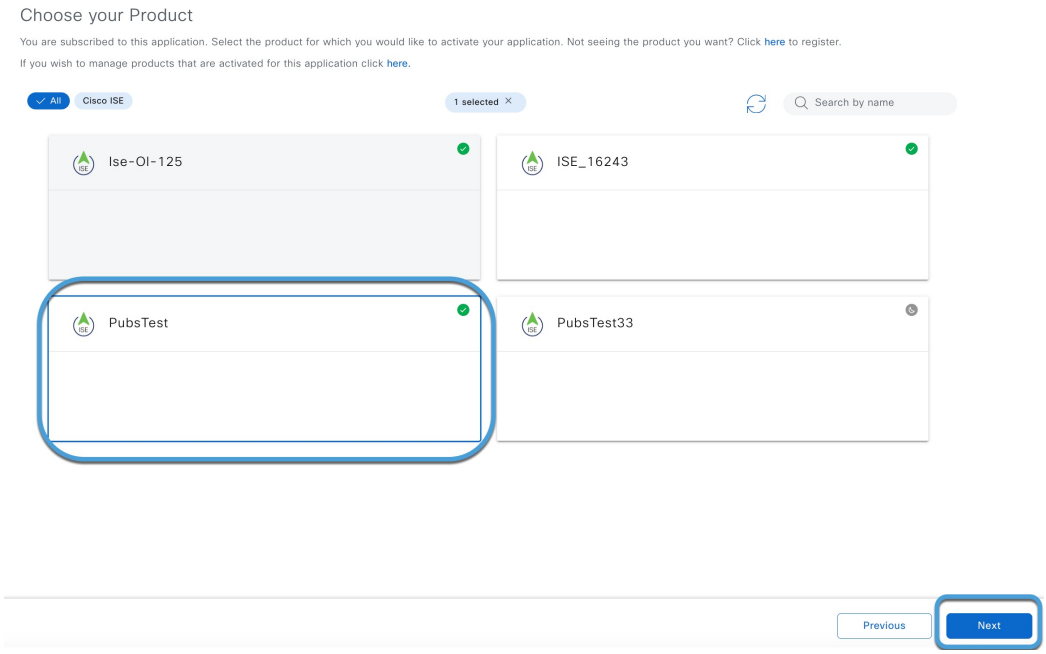
步骤 4 点击**下一步 (Next)**。

示例：

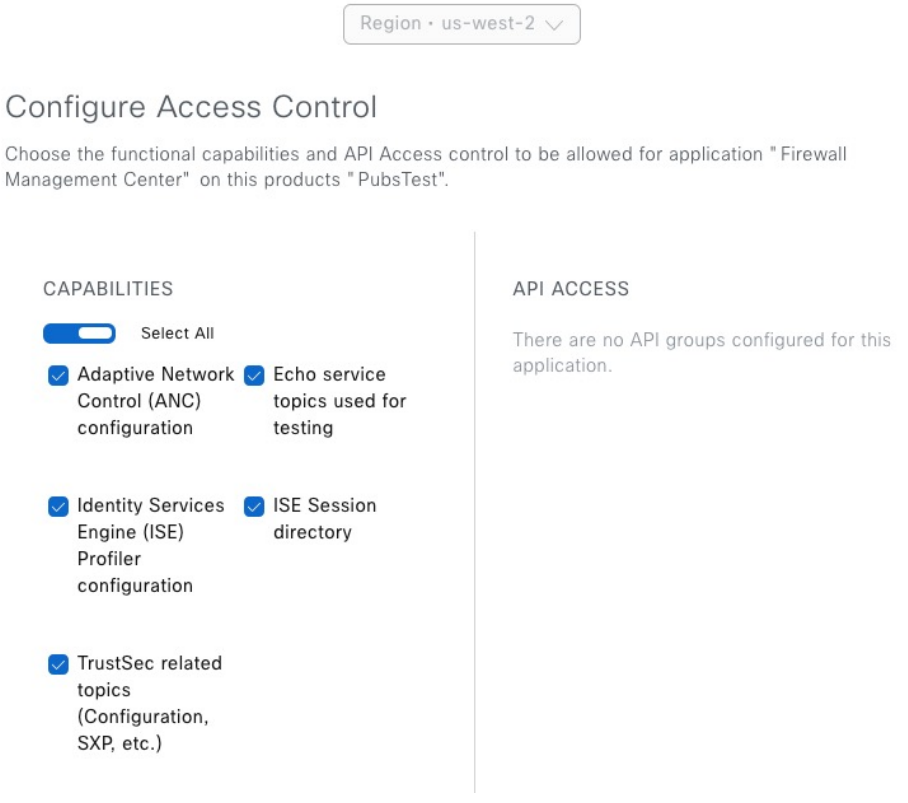


步骤 5 在“选择产品”页面上，点击 Cisco ISE 产品的名称，然后点击**下一步**。

示例：

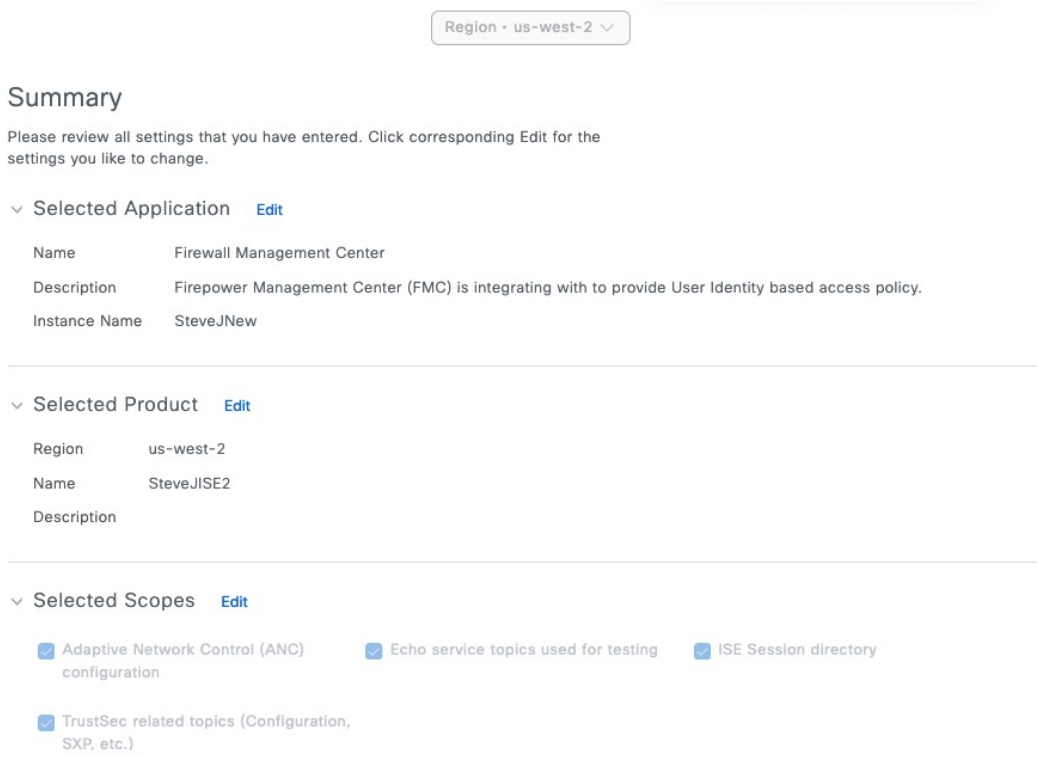


步骤 6 选中每个范围旁边的复选框。
下图显示了一个示例。



步骤 7 点击下一步 **(Next)**。

步骤 8 查看所显示信息的准确性。确保选中所有范围。
下图显示了一个示例。



步骤 9 点击**激活**。

激活应用实例可能需要几分钟时间。

步骤 10 继续执行激活 pxGrid 云身份源，第 2156 页。

激活 pxGrid 云身份源

此任务说明如何在 Secure Firewall Management Center 中激活 pxGrid 云身份源。

开始之前

完成激活应用实例，第 2153 页中讨论的任务。

注释 每次只能有一个 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录至 Secure Firewall Management Center

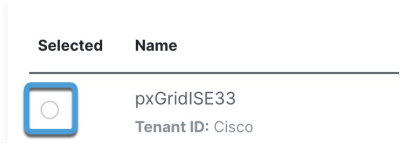
步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击页面顶部的**保存**。

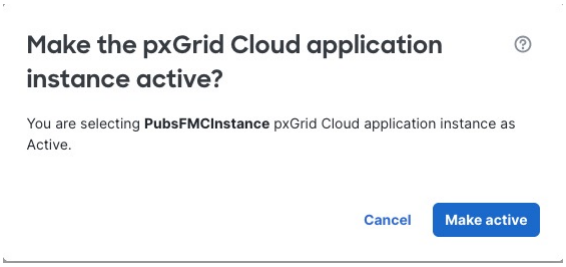
步骤 5 如果身份源名称旁边未显示绿色复选标记，请将其选中。

示例：



步骤 6 点击**设为主用**。

示例：



步骤 7 （可选。）如果需要，请选择以下选项：

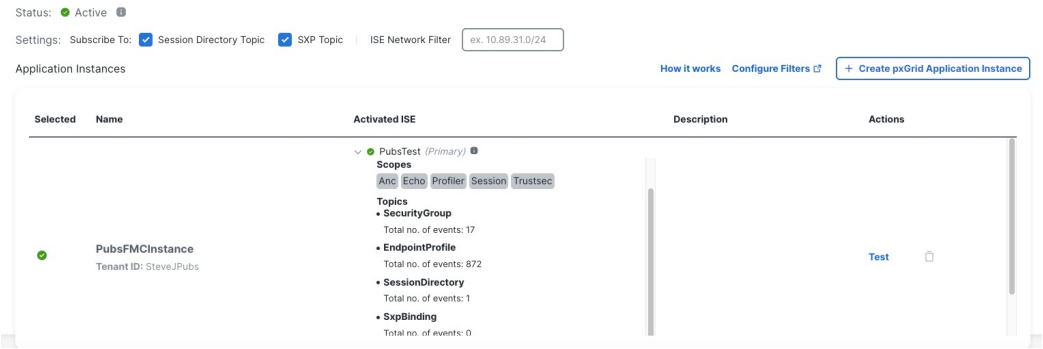
- **会话目录主题**：选中此复选框可从 Cisco ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**：选中此复选框，以便在 ISE 服务器提供 SGT 到 IP 映射的更新时接收更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。
- **ISE 网络过滤器**：您可以设置可选筛选条件来限制 Cisco ISE 报告的数据。如果提供网络过滤器，Cisco ISE 会报告来自该过滤器中的网络的数据。

  您有以下选择：

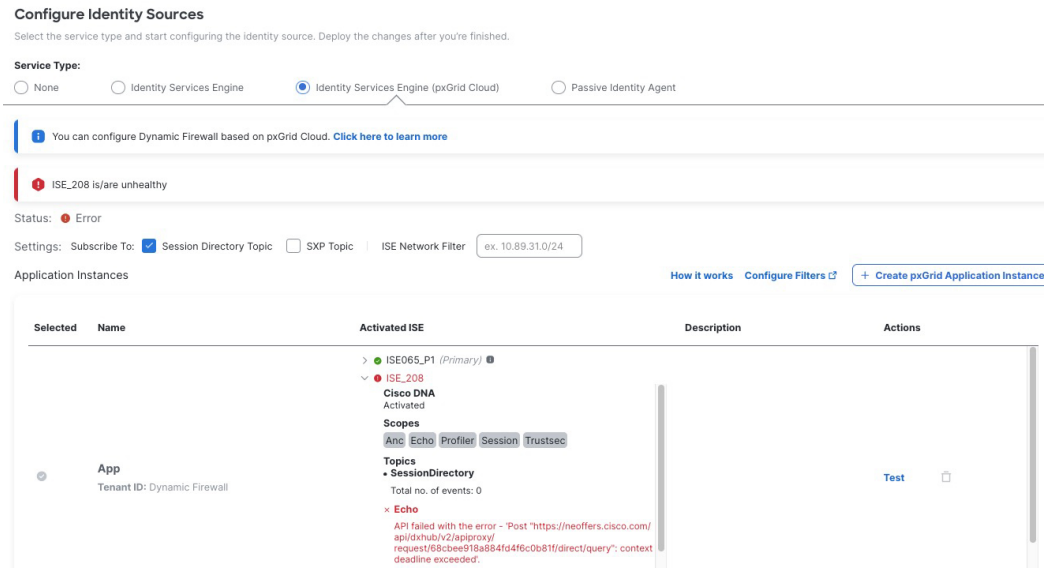
  - 将此字段留空以指定**任意 (any)** 值。
  - 使用 CIDR 符号输入单一 IPv4 地址块。
  - 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

步骤 8 在已激活的 ISE 下，展开身份源。

正常结果示例：



错误结果示例：



如有错误，请参阅测试 pxGrid 云身份源，第 2158 页。

步骤 9 验证状态是否为活动，以及是否已显示所有范围和主题。

步骤 10 等待几分钟以便下载数据。

下一步做什么

请参阅测试 pxGrid 云身份源，第 2158 页。

测试 pxGrid 云身份源

本主题讨论您可以使用 Secure Firewall Management Center 执行的诊断，以确定身份源是否正常工作。错误可能包括与 Cisco ISE 的通信，或与 Catalyst 云门户 的 Cisco ISE 配置问题。

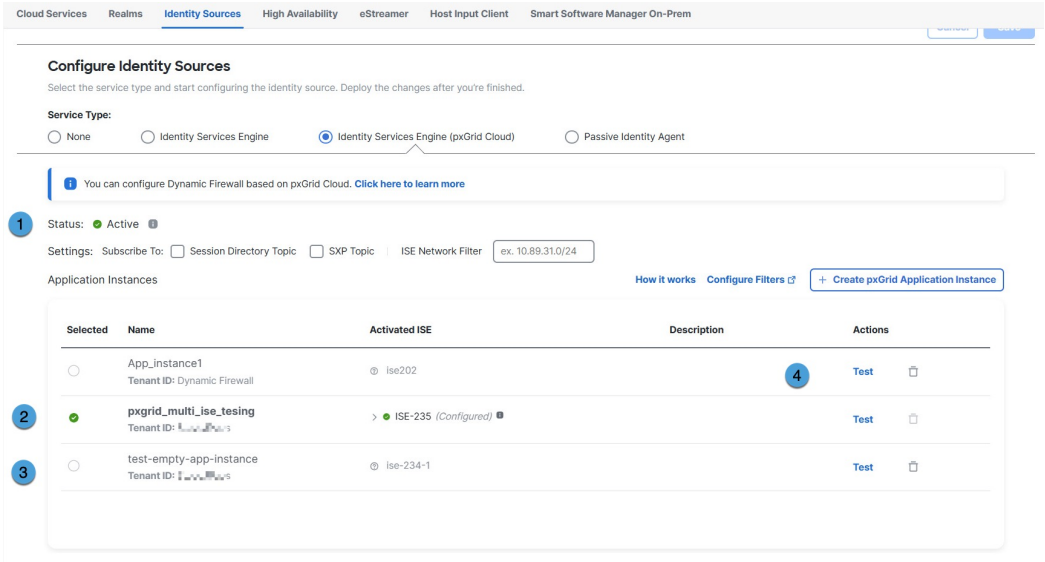
查看当前配置

如需了解入门信息：

1. 登录Secure Firewall Management Center。
2. 点击 **集成** > **身份** > **身份源**
3. 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

配置状态示例

下图所示为一个配置示例。

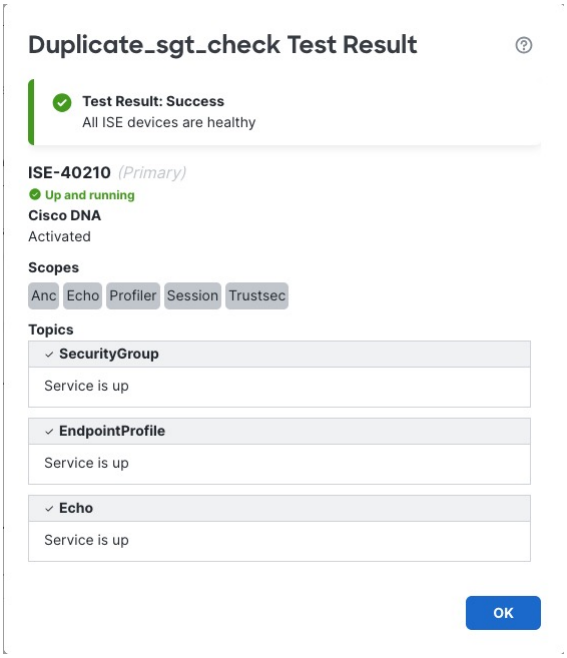


下表提供了有关图中编号区域的详细信息。

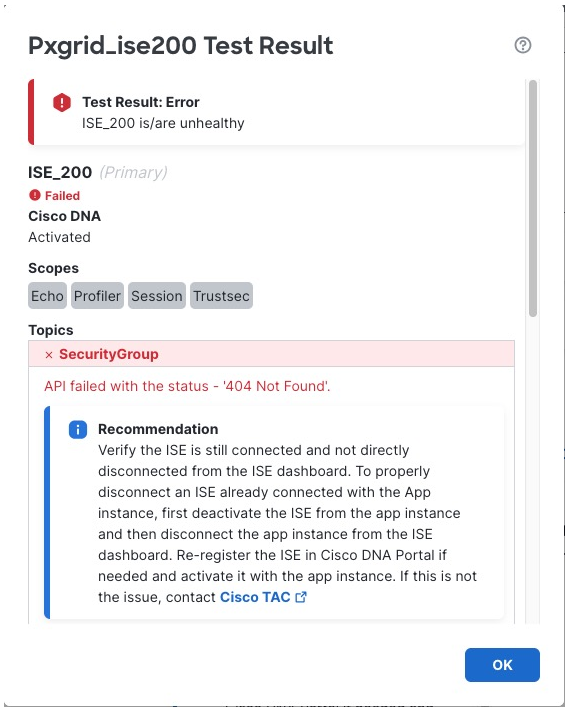
数字	含义
1	总体状态 系统会显示 Cisco ISE 应用实例的整体状态中的任何错误。在这种情况下，请滚动到该实例，然后展开错误消息或点击**测试**以了解更多信息。
2	主用 绿色复选标记表示应用处于活动状态。
3	非活动 灰显的应用实例处于非活动状态。您可以通过选中其名称旁边的复选框，然后点击**设为主用**来将其激活。

数字	含义
4	**测试**按钮 点击**测试**以执行显示更详细的应用实例状态的诊断测试。有关详细信息，请参阅下一节。

下图显示了一条示例成功消息。



下图为搜索结果的示例。



以下部分提供可能的错误的参考。

错误代码参考

提供以下信息可帮助您诊断和解决 Cisco ISE、pxGrid 云 和 Catalyst 云门户 的问题。如果这些建议不起作用，或者您遇到其他问题，请联系思科 TAC。

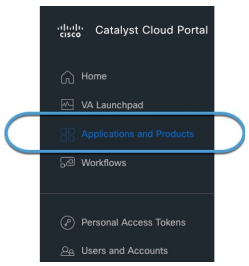
403 - Forbidden

请验证 Cisco ISE 产品在 Catalyst 云门户 中未处于**待处理**或**已中止**状态。如果设备已暂停，请按照在 Cisco ISE 中启用 pxGrid Cloud 服务并注册设备的步骤，验证 Cisco ISE 是否已注册。

此外，请验 pxGrid 云 证服务是否公开可用。

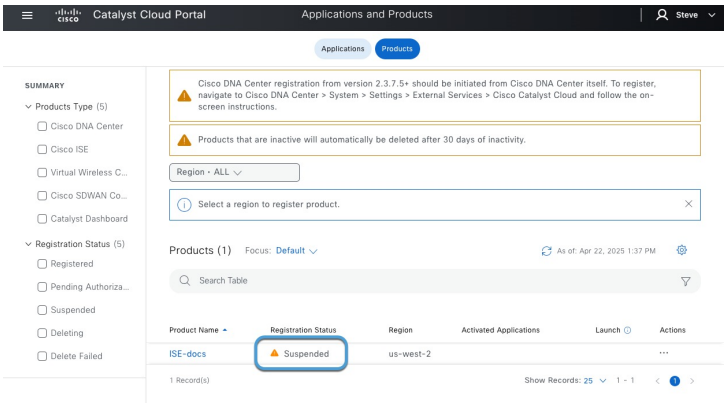
要验证您的产品是否处于活动状态，请执行以下操作：

1. 登录Catalyst 云门户。
2. 在 Catalyst 云门户 中，转到☰ > **应用程序和产品**，如下图所示：



3. 点击 **产品** 选项卡。

下图显示了已终止产品的示例。



4. 要更正此问题，请在操作列中点击 ***，然后点击**生成 OTP**。
5. 按照创建身份源，第 2152 页中所述使用 OTP。

404 – Not Found

验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

408 – Request Timeout

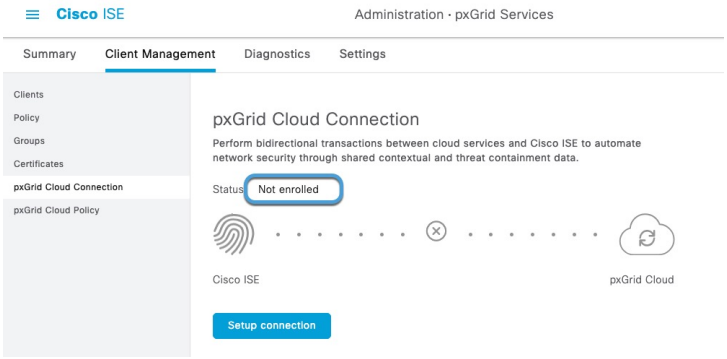
一般连接

检查 Cisco ISE是否存在任何常规连接问题，并在 ISE 面板中的 ☰ > **管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接** 下验证 pxGrid 云 连接状态是否为**已连接**。

下图显示了已连接的系统示例。



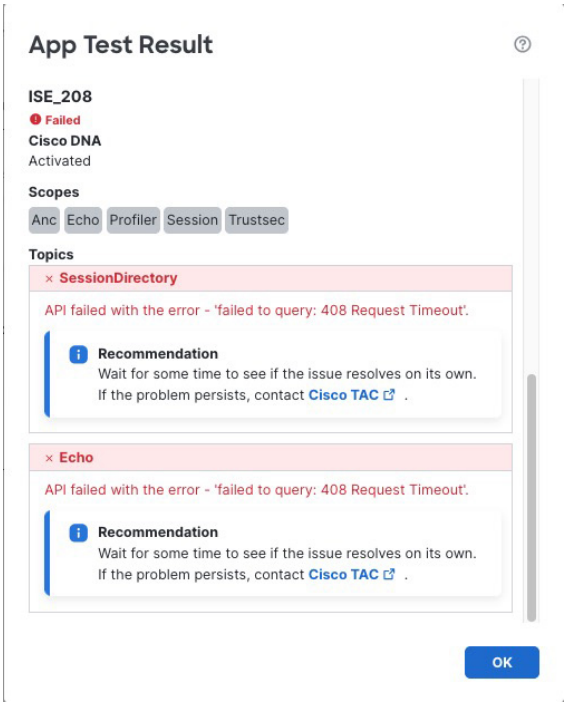
下图显示的是未注册（即未连接）的系统示例。



验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

集群成员无法访问

如果无法访问 Cisco ISE 集群的一个成员，系统将显示如下页面：



要查找无法访问的节点，请以管理员身份登录 Cisco ISE 主管理节点，然后点击 点击**菜单**图标 (☰)，然后选择 **管理** > **系统** > **部署**，查看 Cisco ISE 部署中的节点状态。

413 – 内容过大

我们建议您查看 GitHub 上的 pxGrid Cloud API 限制。如果需要，请考虑升级您的 Cisco ISE 版本，以充分利用 pxGrid 云 支持。

500 – Internal Server Error

检查 Cisco ISE 服务器是否正常运行以及 pxGrid 云服务是否处于活动状态（验证 MNT、SXP、pxGrid 节点等）。

有关更多信息，请参阅《思科身份识别服务引擎管理员指南》中 Cisco pxGrid 章节的“监控和调试”。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

开始之前

创建连接器，第 2340 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** (+)。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。

项目	说明
查询	请点击 添加  。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

您创建的动态属性查询应显示为动态对象。

使用动态属性过滤器来创建访问控制规则或 DNS 规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

要向 DNS 策略添加动态属性过滤器，请参阅创建基本 DNS 策略。

要将动态属性过滤器添加到 DNS 策略，请参阅创建基本 DNS 策略。

开始之前

按照创建动态属性过滤器，第 2164 页中所述，创建动态属性筛选器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录至 Secure Firewall Management Center

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

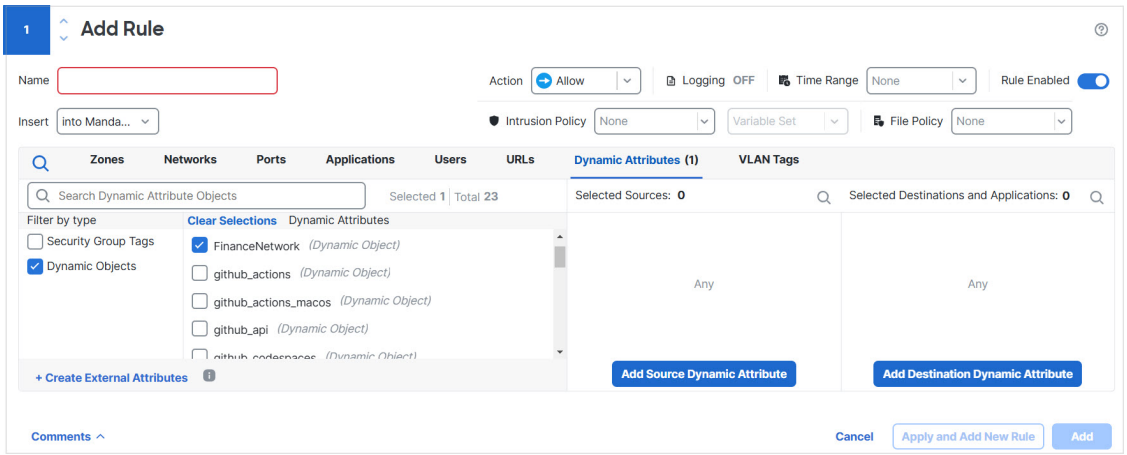
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



本示例显示一个名为 `APIC 动态属性`的动态对象，它对应于 dynamic attributes connector 中创建的动态属性筛选器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

请参阅动态属性规则条件，第 2383 页。

pxGrid 云身份源 故障排除

这些主题介绍如何对 pxGrid 云身份源 进行故障排除。

相关主题

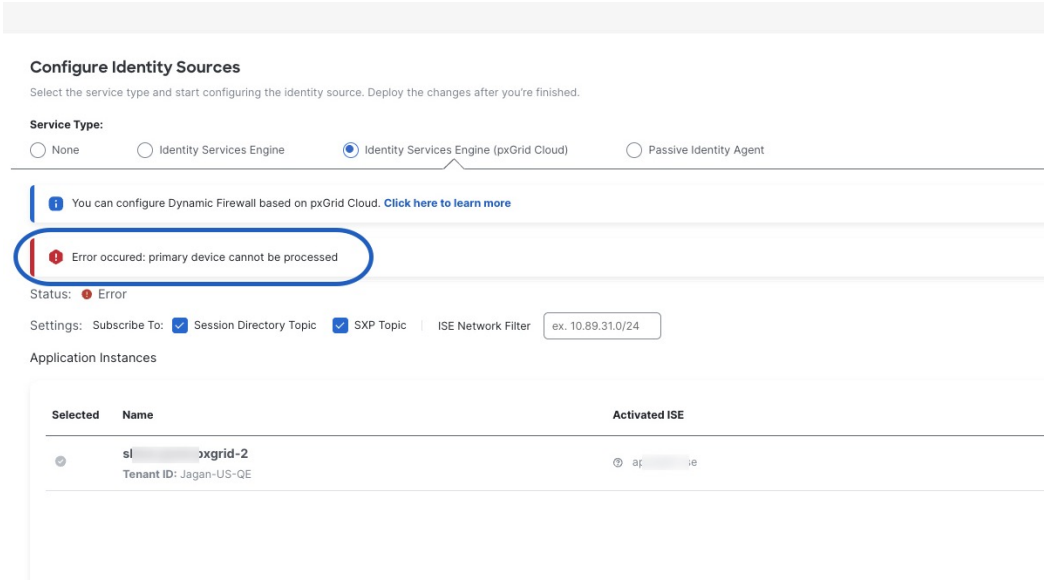
无法处理主设备，第 2167 页

无法处理主设备

每个 Cisco ISE 集群必须与且仅与一个应用实例相关联，且通常位于一个专用租户中。

如果将一个 Cisco ISE 与多个应用实例相关联，身份源将显示错误，例如错误：无法处理主设备或 `ISE 运行状况不正常。`

示例：



解决方案是，在将该租户用于任何其他租户或应用实例之前，先从该租户的其他应用实例中正确停用 ISE。

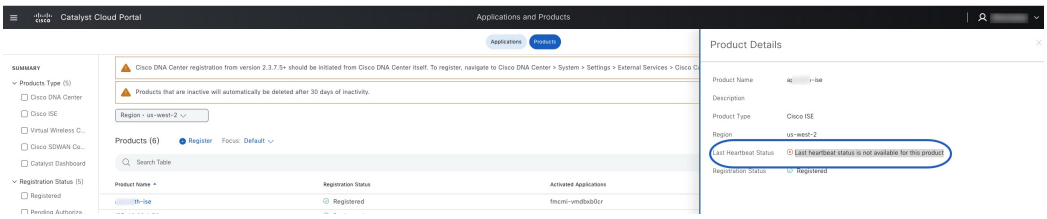
过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在页面顶部，点击**应用**。

步骤 3 找到一款已激活的 Cisco ISE 产品，并确认是该产品导致了相关问题。

示例：



步骤 4 等待产品被删除。

步骤 5 停用应用实例，如停用 pxGrid 云 应用实例，第 2168 页中所述。

停用并删除 pxGrid 云身份源

这些主题讨论了如何选择性地：

- 在 Catalyst 云门户 中停用 FMC 应用实例。

  您可以执行此可选任务来排除 Cisco ISE 集成问题。

- 从 Secure Firewall Management Center 中删除 pxGrid 云身份源。

  只有在确定不再使用身份源时，才应将其删除。

相关主题

停用 pxGrid 云 应用实例，第 2168 页
删除 pxGrid 云身份源，第 2171 页

停用 pxGrid 云 应用实例

（可选。）此任务介绍如何使用 Catalyst 云门户 停用 pxGrid 云 应用实例。只有当您的 Cisco ISE 或 pxGrid 云 停止工作或您需要更新时，才应执行此操作。

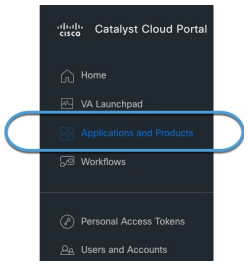
开始之前

如激活 pxGrid 云身份源，第 2156 页中所述，请确保当前的 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：

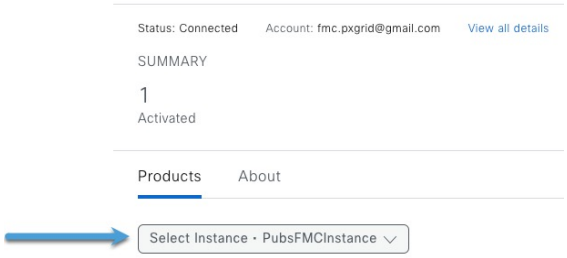


步骤 3 点击 **应用**。

步骤 4 点击防火墙管理中心的**管理**。

步骤 5 从**选择实例**列表中，点击您之前创建的防火墙应用的名称。

示例：



步骤 6 在“操作”列中，点击更多图标 （ ··· ） > **停用**。

步骤 7 等待直至移除产品。

如有必要，您可以点击 **刷新** ( ) 以查看更新后的状态。

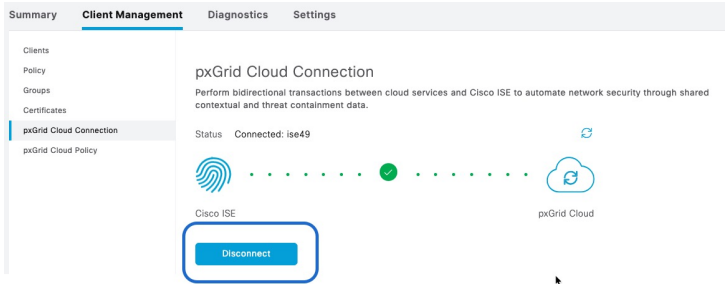
步骤 8 ISE 3.3 或更低版本：断开应用实例的连接：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接**。

c) 点击**断开连接**。

示例：



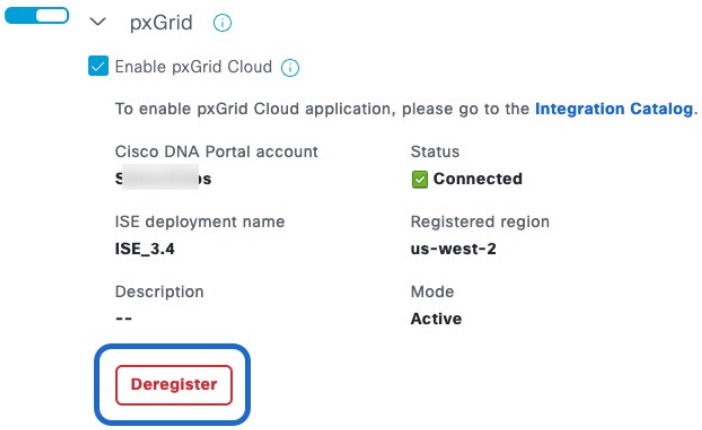
步骤 9 ISE 3.4 或更高版本：取消注册应用实例：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **系统** > **部署**。

c) 展开**部署**。
d) 点击 ISE 节点的名称。
e) 在**常规设置**选项卡页面中，滚动至找到 **pxGrid**。
f) 点击**取消注册**。

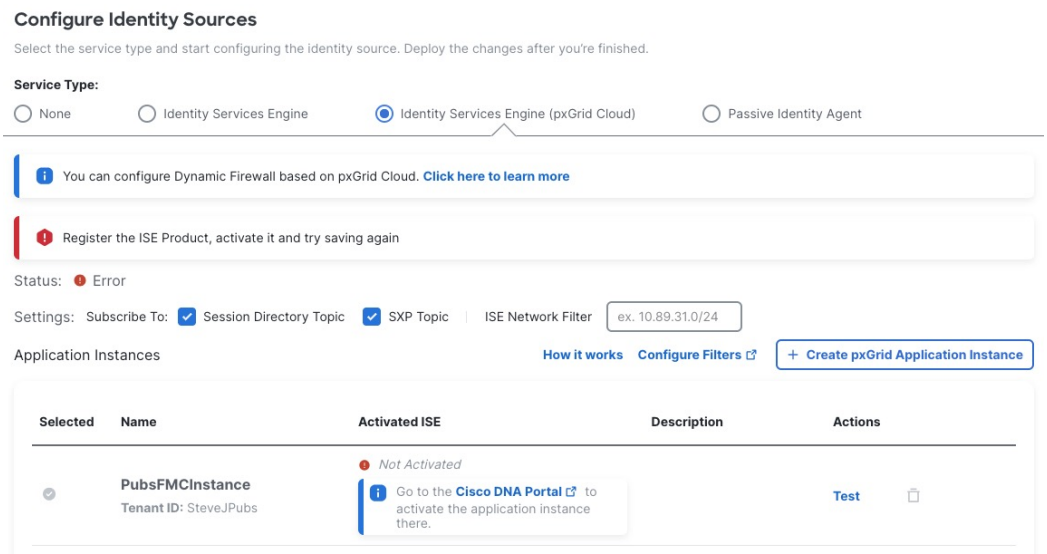
示例：



步骤 10 要验证已在 Secure Firewall Management Center 中停用应用实例：

a) 登录 Secure Firewall Management Center。
b) 点击 **集成** > **身份** > **身份源**
c) 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。
d) 验证已激活 ISE 列中是否显示**未激活**。

示例：



下一步做什么

- 要向 pxGrid 云 注册 Cisco ISE 并激活应用实例，请参阅：
  - ISE 3.3 及更早版本：使用 Catalyst 云门户 注册 Cisco ISE，第 2146 页。
  - ISE 3.4 及更高版本：创建应用实例，第 2180 页。
- 要彻底删除身份源，请参阅删除 pxGrid 云身份源，第 2171 页。

删除 pxGrid 云身份源

（可选。）此任务说明如何从 Secure Firewall Management Center 中删除不想再次使用的 pxGrid 云身份源。

开始之前

按照停用 pxGrid 云 应用实例，第 2168 页中所述，从 Catalyst 云门户 中停用 FMC 应用实例。

过程

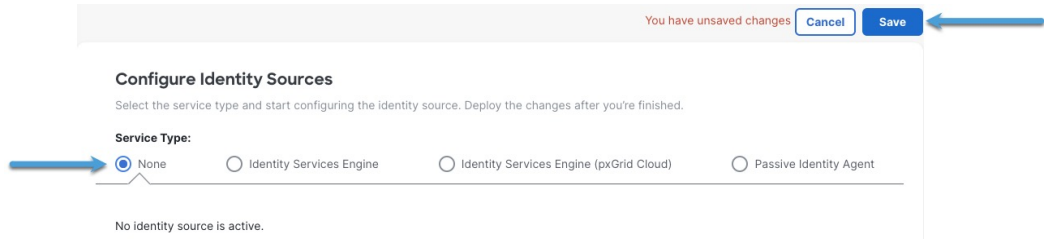
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 对于服务类型，请点击**无**。

示例：



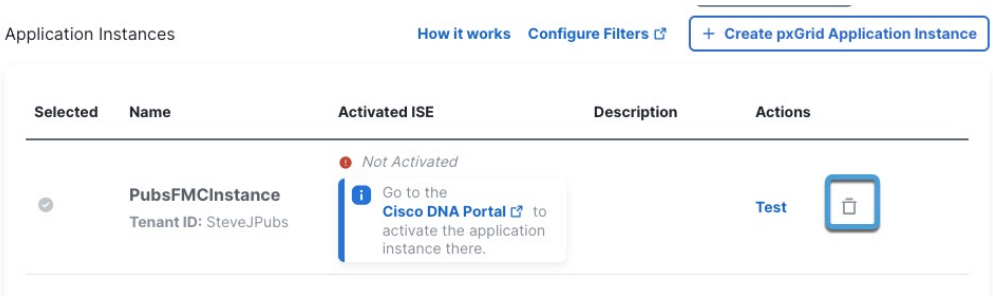
步骤 5 点击**保存**。

步骤 6 您需要确认您的选择。

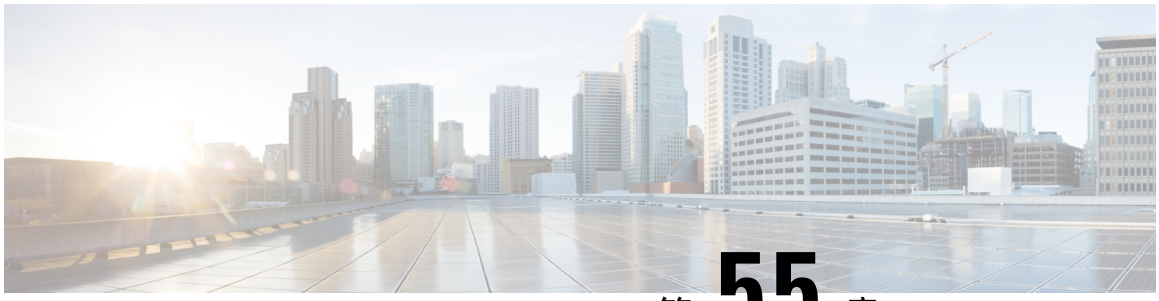
步骤 7 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 8 请点击 删除 ( )。

示例：


Application Instances
How it works
Configure Filters
+ Create pxGrid Application Instance
Selected
Name
Activated ISE
Description
Actions
Not Activated
PubsFMCInstance
Tenant ID: SteveJPubs
Go to the
Cisco DNA Portal
to activate the application instance there.
Test

步骤 9 您需要确认操作。



第 55 章

身份源：pxGrid Cloud 身份（ISE 3.4 及更高版本）

以下主题讨论如何配置和使用包含 Cisco ISE 3.4 及更早版本的 pxGrid 云身份源。

- 关于 pxGrid 云身份源， 第 2173 页
- 如何配置 pxGrid 云身份源， 第 2175 页
- 在 Cisco ISE 中启用 pxGrid 云 服务， 第 2177 页
- 创建应用实例， 第 2180 页
- 创建身份源， 第 2181 页
- 激活应用实例， 第 2182 页
- 激活 pxGrid 云身份源， 第 2185 页
- 测试 pxGrid 云身份源， 第 2187 页
- pxGrid 云身份源 故障排除， 第 2193 页
- 创建动态属性过滤器， 第 2194 页
- 使用动态属性过滤器来创建访问控制规则或 DNS 规则， 第 2196 页
- 停用并删除 pxGrid 云身份源， 第 2197 页

关于 pxGrid 云身份源

思科身份服务引擎 (Cisco ISE) pxGrid 云身份源 允许您在 Secure Firewall Management Center 访问控制规则中使用来自 的 服务器或集群 的订阅和用户数据。此外，身份源在 Secure Firewall Management Center的访问控制策略中使用来自 的不断变化的动态对象。

pxGrid 云身份源 还使用：

- Cisco Platform Exchange Grid (pxGrid)，可在安全监控和检测系统、网络策略平台、资产和配置管理、身份和访问管理等领域实现多供应商跨平台网络系统协作。 pxGrid 云是 Cisco ISE 的基于云的接口。

  有关 pxGrid 的更多信息可以在 devnet 上的“什么是 PxGrid？”等资源中找到。

- 思科全数字化网络架构 (Cisco DNA) 可提供自动化、安全性、预测性监控和策略驱动方法。它能够提供端到端网络可视性，利用网络洞察优化网络性能并提供最佳的用户和应用体验。

要将 pxGrid 云身份源 和 Secure Firewall Management Center配合使用，您必须 创建一个思科帐户。

- devnet 上的什么是 pxGrid?
- devnet 上的思科平台交换架构云

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页

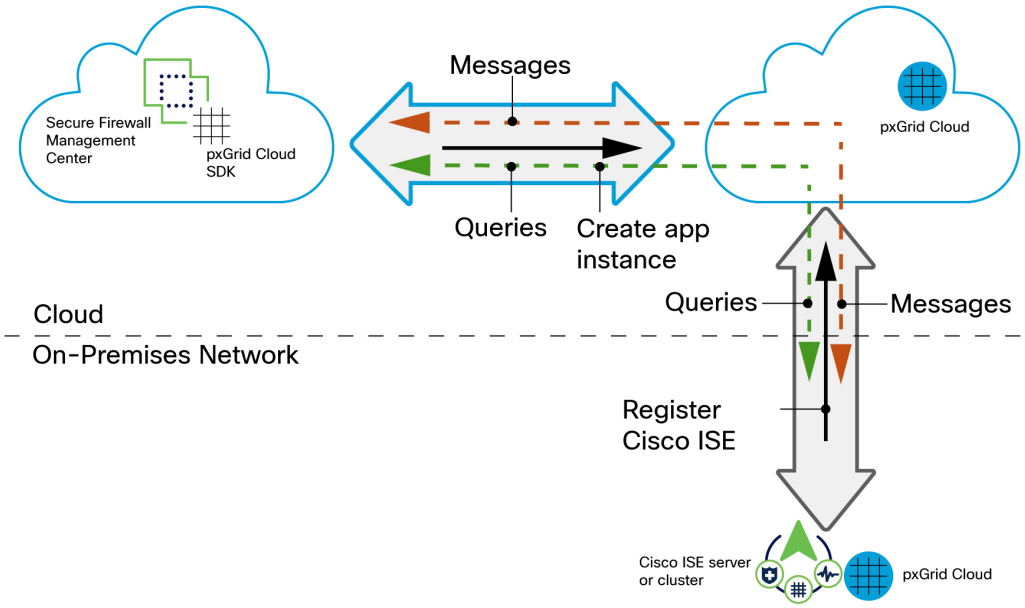
pxGrid 云身份源 的限制

在设置 pxGrid 云身份源 之前，请注意以下事项：

- pxGrid 云 支持以下区域：`us-west-2`、`eu-central-1` 和 `ap-southeast-1`。
- 有关 Cisco ISE 版本和查询大小的信息，请参阅 GitHub 上 pxGrid 云 SDK 中的查询限制。

pxGrid 云身份源 工作原理

下图显示了身份源的工作原理。



您的 Secure Firewall Management Center 使用 pxGrid 云 SDK 以编程方式从本地 Cisco ISE 服务器或集群 检索用户信息，以便可以在 Secure Firewall Management Center 上的身份策略中使用这些用户。

要授权和验证此数据交换，您必须：

1. 在 Cisco ISE 中，启用 pxGrid 云。

2. 在 pxGrid 云中将 Cisco ISE 注册为产品，这将对 Cisco ISE 和 pxGrid 云进行身份验证，并使它们能够相互通信。

   身份验证过程要求您将一次性密码 (OTP) 从 pxGrid 云粘贴到 Cisco ISE 中。

3. 在 pxGrid 云中，创建一个“应用实例”，用于生成 OTP，以供您在 Secure Firewall Management Center 中用于对彼此进行身份验证。

4. 完成上述所有任务后，Secure Firewall Management Center（包括 pxGrid 云 SDK）可以使用 pxGrid 云查询 Cisco ISE 并检索包含用户信息、SGT、终端配置文件和其他详细信息的会话。

5. 可以过滤许多类型的动态对象，并将其作为要在访问控制规则中使用的动态对象发送到 Secure Firewall Management Center。其中包括：SGT、终端配置文件、终端安全评估状态和计算机身份验证。

   我们会从 Cisco ISE 检索用户信息，并从 Microsoft Active Directory 或 Azure Active Directory 检索组信息。

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页

如何配置 pxGrid 云身份源

这些主题总结了如何为 ISE 3.3 及更早版本或 ISE 3.4 及更高版本配置 pxGrid 云身份源。步骤不同，因此请确保完全按照步骤操作。

相关主题

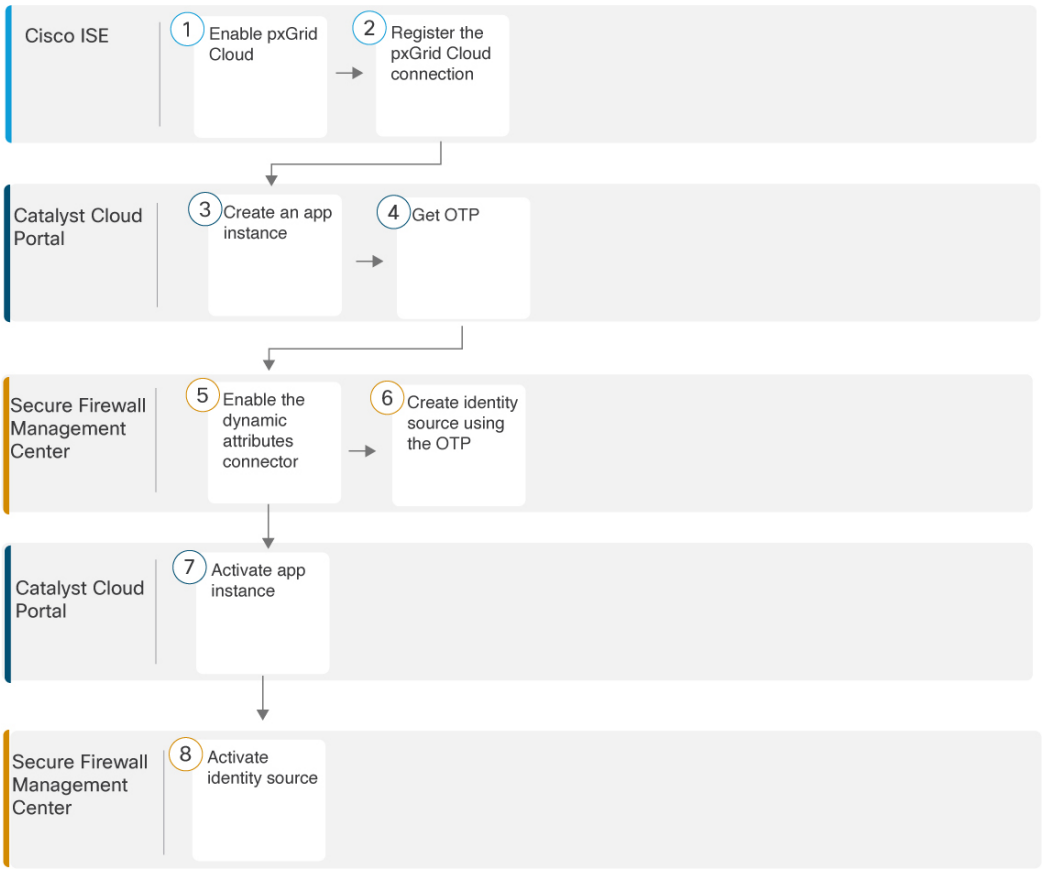
如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页
在 Cisco ISE 中启用 pxGrid 云 服务，第 2177 页
创建应用实例，第 2180 页
创建身份源，第 2152 页
激活应用实例，第 2153 页
激活 pxGrid 云身份源，第 2156 页

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）

在开始之前，创建一个 Cisco 账户。

重要事项 本主题适用于 *Cisco ISE* 版本 *3.4* 或更高版本。如果您使用的是早期版本，请改为参阅如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页。

下图显示了使用 Cisco ISE、Catalyst 云门户 和 Secure Firewall Management Center 来配置 pxGrid 云身份源 的步骤。



1 在 Cisco ISE 中启用 pxGrid 云 服务， 第 2177 页
2 向 Cisco ISE 注册 pxGrid 云 连接， 第 2149 页
3 创建应用实例， 第 2180 页
4 创建应用实例， 第 2180 页
5 启用 dynamic attributes connector， 第 2116 页
6 创建身份源， 第 2152 页
7 激活应用实例， 第 2153 页
8 激活 pxGrid 云身份源， 第 2156 页

表 *122:* 配置 *pxGrid* 云身份源

1, 2	Cisco ISE	在 Cisco ISE 中启用 pxGrid 云。 pxGrid Cloud 使您能够订阅产品/服务，并注册应用（在此情况下为 Secure Firewall Management Center），以在云环境中进行安全数据交换。 有关详细信息，请参阅在 Cisco ISE 中启用 pxGrid 云 服务， 第 2177 页。

3, 4	Catalyst 云门户	创建应用实例并获取创建 pxGrid 云身份源 所需的一次性密码 (OTP)。 有关详细信息，请参阅创建应用实例， 第 2180 页。
5	Secure Firewall Management Center	如果尚未启用，请启用 dynamic attributes connector。 使用 pxGrid 云身份源 需借助 dynamic attributes connector。 有关详细信息，请参阅启用 dynamic attributes connector， 第 2116 页。
6	Secure Firewall Management Center	创建 pxGrid 云身份源。 身份源使能够通过 Secure Firewall Management Center 向 Cisco ISE 和 Catalyst 云门户进行身份验证，从而可以从 Cisco ISE 接收用户数据。 有关详细信息，请参阅创建身份源， 第 2152 页。
7	Catalyst 云门户	激活应用实例。 有关详细信息，请参阅激活应用实例， 第 2153 页。
8	Secure Firewall Management Center	激活 pxGrid 云身份源。 有关详细信息，请参阅 激活 pxGrid 云身份源， 第 2156 页。

完成所有前述任务后，您可以：

- 测试 pxGrid 云身份源 以确保其正常运行。

  有关详细信息，请参阅测试 pxGrid 云身份源， 第 2158 页。
- 创建动态属性过滤器，定义哪些动态对象发送到 Secure Firewall Management Center。

  有关详细信息，请参阅创建动态属性过滤器， 第 2164 页。
- 配置 pxGrid 云身份源 后，您可以在访问控制规则中使用以下任何内容：
  - 动态对象
  - Microsoft AD 用户和组
  - Azure AD 用户和组

相关主题

在 Cisco ISE 中启用 pxGrid Cloud 服务， 第 2146 页

在 Cisco ISE 中启用 pxGrid 云 服务

此任务介绍如何在 Cisco ISE 中启用 pxGrid Cloud。

开始之前

- 在您的 Cisco ISE 部署中安装并激活 Advantage 许可证层级。
- pxGrid 云 代理会创建与 Cisco pxGrid 云 的出站 HTTPS 连接。因此，如果客户网络使用代理访问互联网，则必须配置 Cisco ISE 代理设置。要在思科 ISE 中配置代理设置，点击**菜单**图标 (☰)，然后选择 **管理 > 系统 > 设置 > 代理**。
- 思科 ISE 受信任的证书储存必须包括验证思科 pxGrid 云提供的服务器证书所需的根 CA 证书。验证已为此根CA证书启用**信任思科服务的身份验证**选项。要启用**信任对思科服务的身份验证**，请导航至**管理 > 系统 > 证书**。

过程

步骤 1 以管理员身份登录 Cisco ISE。

如果您的 Cisco ISE 服务器是集群的一部分，请登录主管理节点 (PAN)。

步骤 2 点击**菜单**图标 (☰)，然后点击**管理 > 部署**。

步骤 3 在“部署节点”下，点击部署节点的名称。

步骤 4 在下一页上，向下滚动以找到 **pxGrid** 节点。

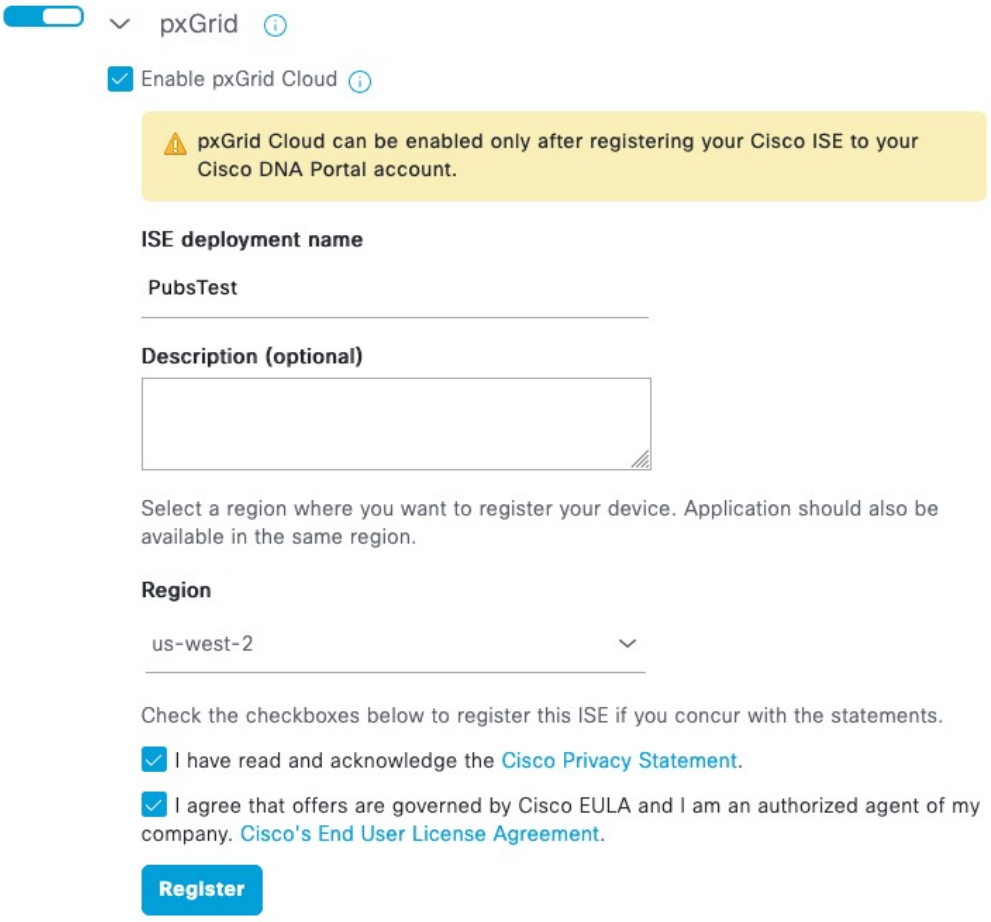
步骤 5 选择**启用 pxGrid Cloud** 复选框。

步骤 6 输入以下信息：

选项	说明
ISE 部署名称	输入唯一名称以标识您的 ISE 部署。
描述（选填）	输入可选的说明。
地区	点击您所在的区域（**us-west-2**、**eu-central-1** 或 **ap-southeast-1**）。 这是目前唯一有效的区域。
许可证协议	您需要同时选中这两个复选框才能继续。

步骤 7 点击**注册 (Register)**。

示例：



步骤 8 当系统提示输入 Catalyst 云门户 的激活代码时，请点击**下一步**。

步骤 9 出现提示时，登录到 Catalyst 云门户。

步骤 10 在“选择账户”对话框中，点击要注册到 Cisco ISE 的账户的名称：

步骤 11 点击**注册 ISE**。

下一步做什么

请参阅在 Catalyst 云门户 中验证 Cisco ISE 注册，第 2179 页。

在 Catalyst 云门户 中验证 Cisco ISE 注册

此任务说明如何验证 Cisco ISE 已向 Catalyst 云门户 注册。

开始之前

完成在 Cisco ISE 中启用 pxGrid 云 服务，第 2177 页中讨论的任务。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 如果出现提示，请选择账户。

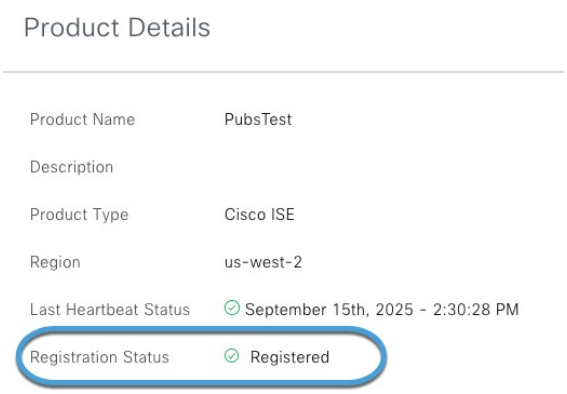
步骤 3 在左侧导航中，点击☰ > **应用和产品**。

步骤 4 在页面顶部，点击**产品**。

步骤 5 点击您之前创建的 Cisco ISE 部署的名称。

步骤 6 确保其状态显示为**已注册**。

示例：



下一步做什么

创建应用实例

此任务是您必须执行的多项任务之一，目的是创建一个 pxGrid 云身份源，以便将用户会话数据发送到 Secure Firewall Management Center。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

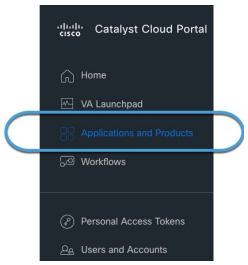
开始之前

在 Catalyst 云门户 中验证 Cisco ISE 注册 ，第 2179 页。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：



步骤 3 在页面顶部，点击**应用**。

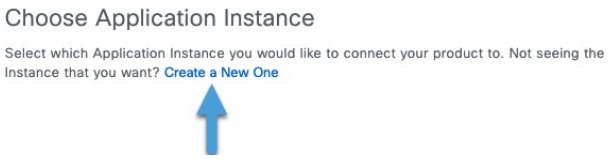
步骤 4 从**区域**列表中，点击 **us-west-2**、**eu-central-1** 或 **ap-southeast-1**。

步骤 5 点击 **Firepower 管理中心**旁边的**管理**（或**激活**）。

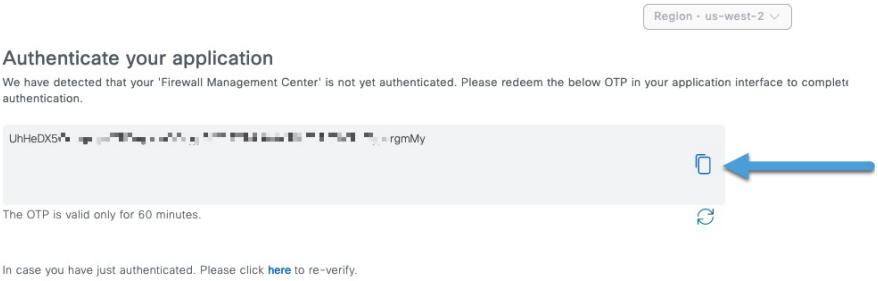
步骤 6 点击**添加 (Add)**。

步骤 7 点击**创建一个新的**。

下图显示了一个示例。



步骤 8 点击显示的 OTP 旁边的复制按钮，如下图所示：



步骤 9 将 OTP 复制到文本文件；它会在 60 分钟后过期。

步骤 10 继续执行创建身份源，第 2152 页。

创建身份源

此任务是创建 pxGrid 云身份源 以将用户会话数据发送到 Secure Firewall Management Center 的多项任务之一。

开始之前

完成 创建应用实例，第 2151 页中讨论的任务。

过程

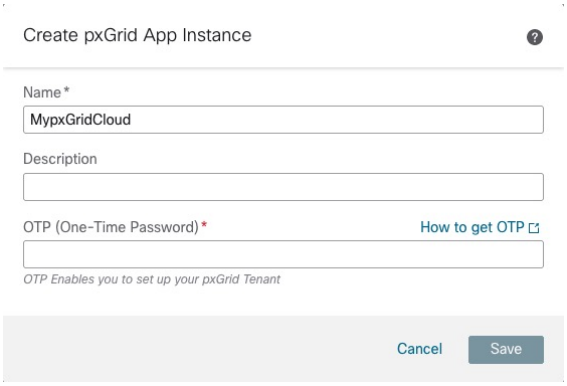
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击**创建 pxGrid 应用实例**。

下图显示了一个示例。



步骤 5 输入以下信息。

值	说明
名称	输入名称以唯一标识此连接器。
说明	可选说明。
OTP（一次性密码）	输入的 OTP。

步骤 6 点击**创建 (Create)**。

步骤 7 在该页面顶部，点击**保存**。

步骤 8 继续执行激活应用实例 ， 第 2153 页。

激活应用实例

本任务讨论如何创建 pxGrid 云身份源 向 Secure Firewall Management Center 发送用户会话数据。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

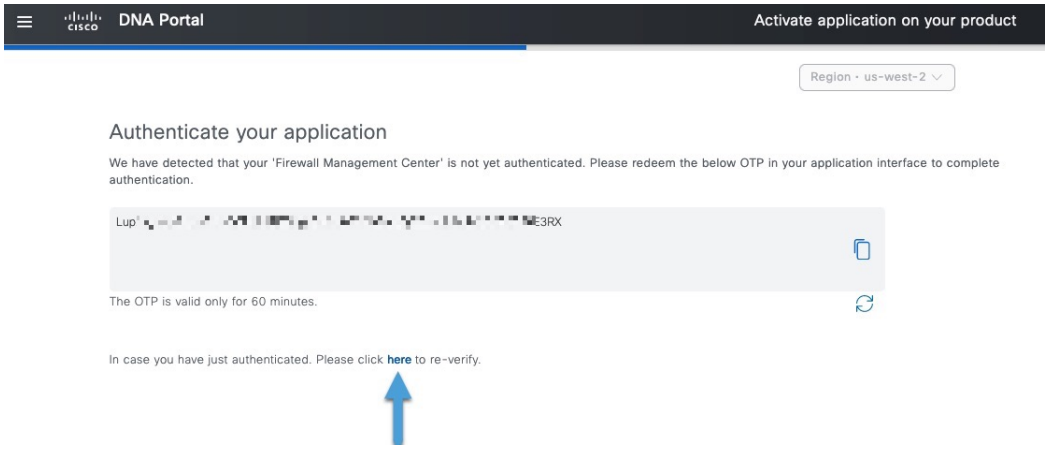
开始之前

完成 创建身份源， 第 2152 页中讨论的任务。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

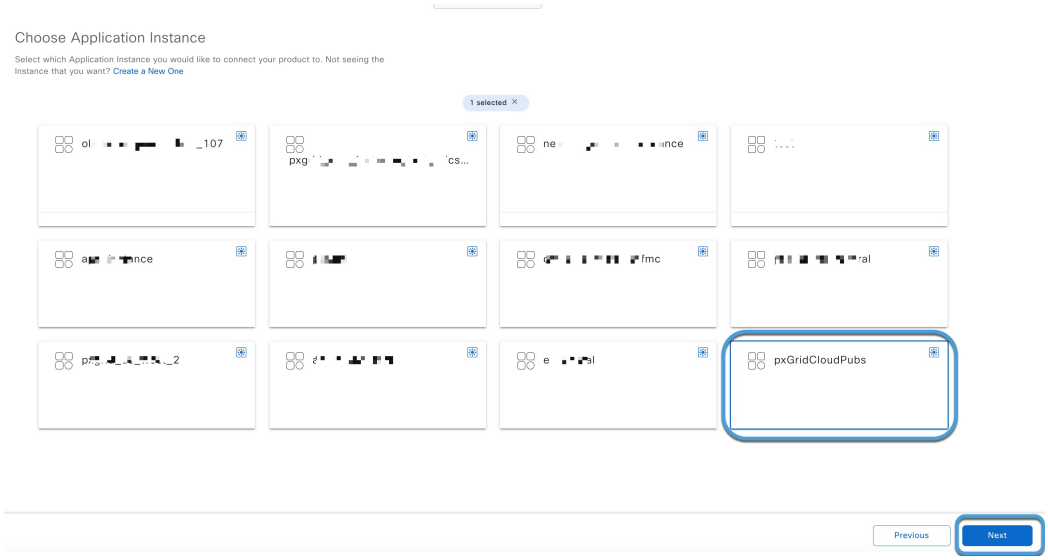
步骤 2 点击下图所示的单词**此处**，重新验证应用。



步骤 3 点击您刚刚在 Secure Firewall Management Center 中创建的应用实例的名称。

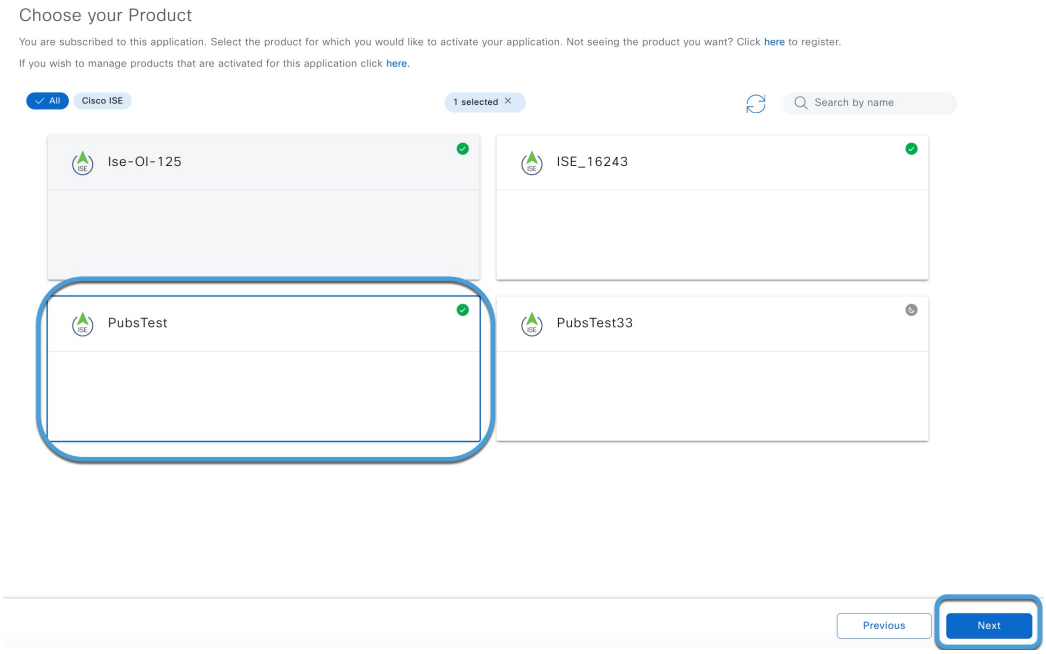
步骤 4 点击**下一步 (Next)**。

示例：

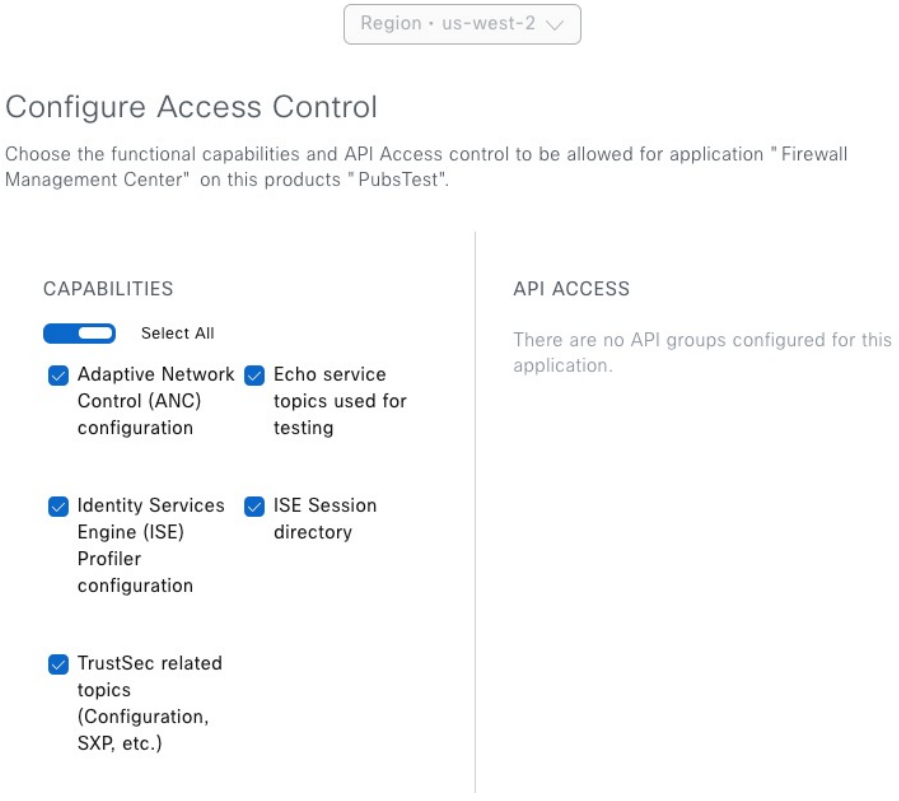


步骤 5 在“选择产品”页面上，点击 Cisco ISE 产品的名称，然后点击**下一步**。

示例：

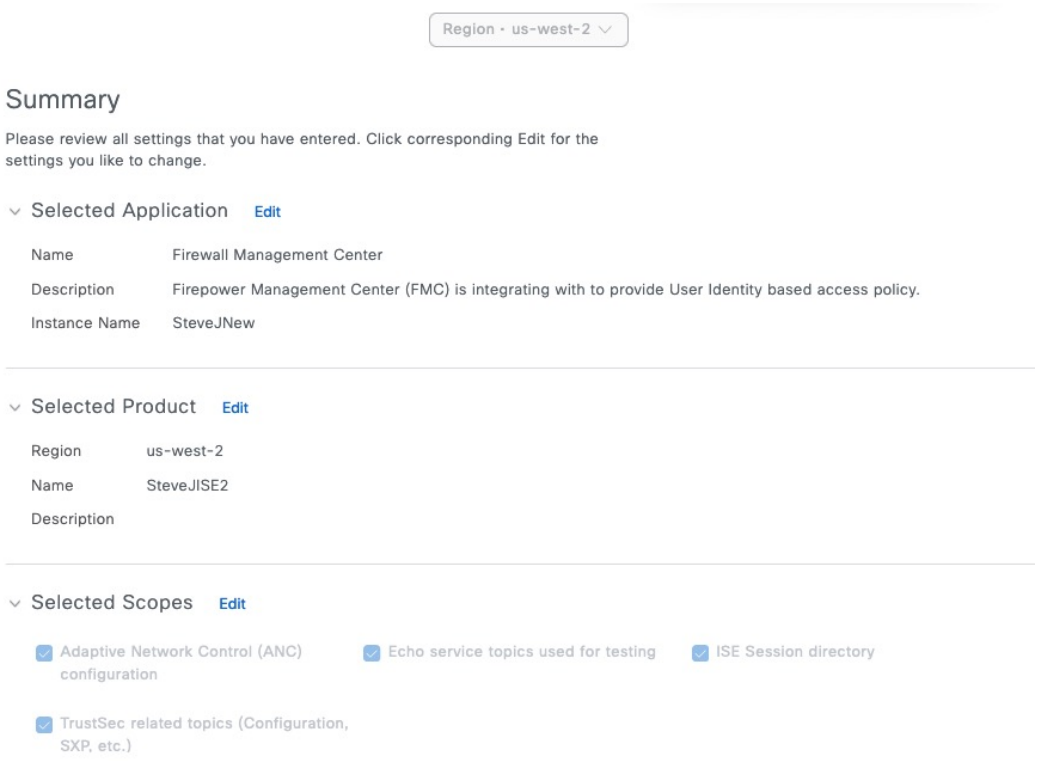


步骤 6 选中每个范围旁边的复选框。
下图显示了一个示例。



步骤 7 点击**下一步 (Next)**。

步骤 8 查看所显示信息的准确性。确保选中所有范围。
下图显示了一个示例。



步骤 9 点击**激活**。

激活应用实例可能需要几分钟时间。

步骤 10 继续执行激活 pxGrid 云身份源，第 2156 页。

激活 pxGrid 云身份源

此任务说明如何在 Secure Firewall Management Center 中激活 pxGrid 云身份源。

开始之前

完成激活应用实例，第 2153 页中讨论的任务。

注释 每次只能有一个 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录至 Secure Firewall Management Center

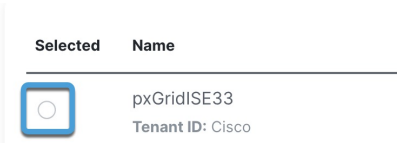
步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击页面顶部的**保存**。

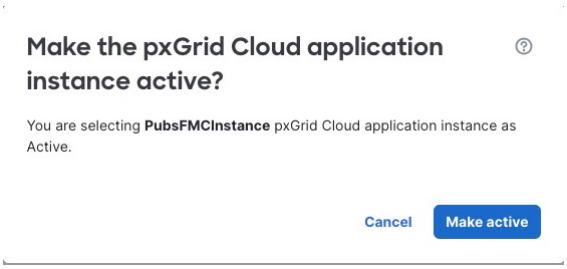
步骤 5 如果身份源名称旁边未显示绿色复选标记，请将其选中。

示例：



步骤 6 点击**设为主用**。

示例：



步骤 7 （可选。）如果需要，请选择以下选项：

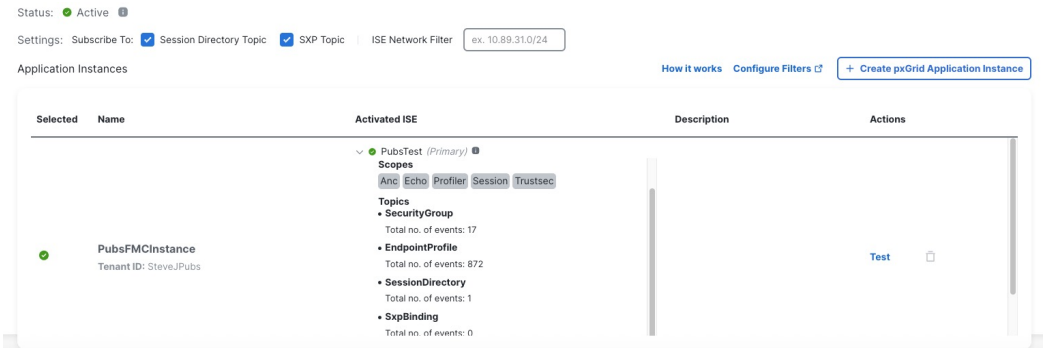
- **会话目录主题**：选中此复选框可从 Cisco ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**：选中此复选框，以便在 ISE 服务器提供 SGT 到 IP 映射的更新时接收更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。
- **ISE 网络过滤器**：您可以设置可选筛选条件来限制 Cisco ISE 报告的数据。如果提供网络过滤器，Cisco ISE 会报告来自该过滤器中的网络的数据。

  您有以下选择：

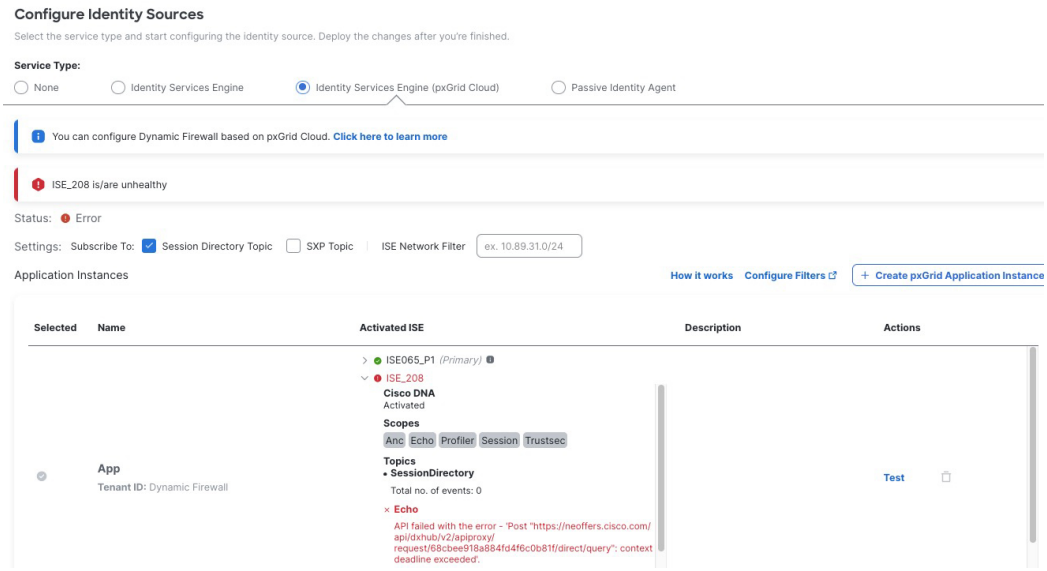
  - 将此字段留空以指定**任意 (any)** 值。
  - 使用 CIDR 符号输入单一 IPv4 地址块。
  - 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

步骤 8 在已激活的 ISE 下，展开身份源。

正常结果示例：



错误结果示例：



如有错误，请参阅测试 pxGrid 云身份源，第 2158 页。

步骤 9 验证状态是否为活动，以及是否已显示所有范围和主题。

步骤 10 等待几分钟以便下载数据。

下一步做什么

请参阅测试 pxGrid 云身份源，第 2158 页。

测试 pxGrid 云身份源

本主题讨论您可以使用 Secure Firewall Management Center 执行的诊断，以确定身份源是否正常工作。错误可能包括与 Cisco ISE 的通信，或与 Catalyst 云门户 的 Cisco ISE 配置问题。

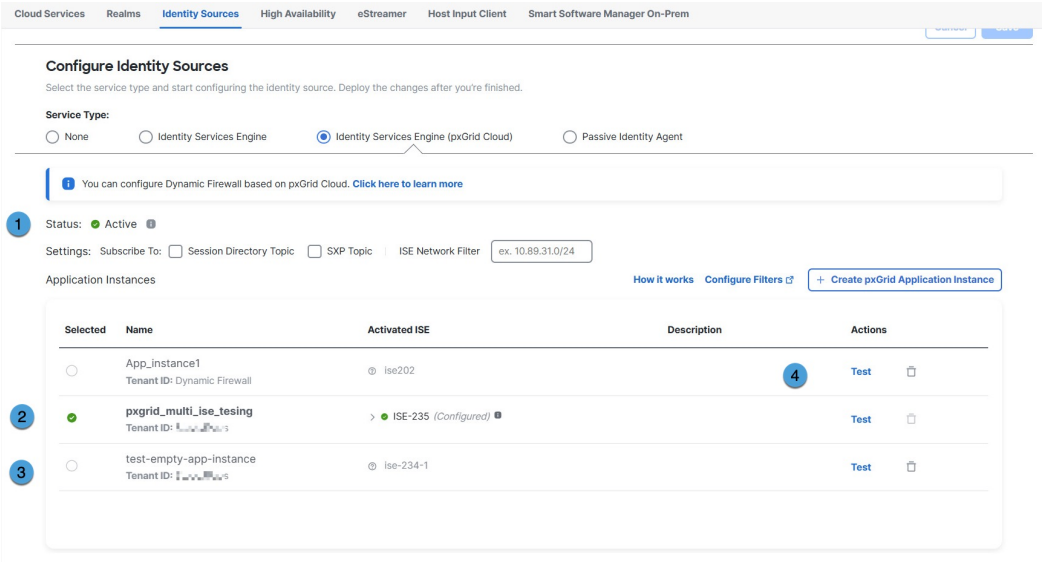
查看当前配置

如需了解入门信息：

1. 登录Secure Firewall Management Center。
2. 点击 **集成** > **身份** > **身份源**
3. 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

配置状态示例

下图所示为一个配置示例。

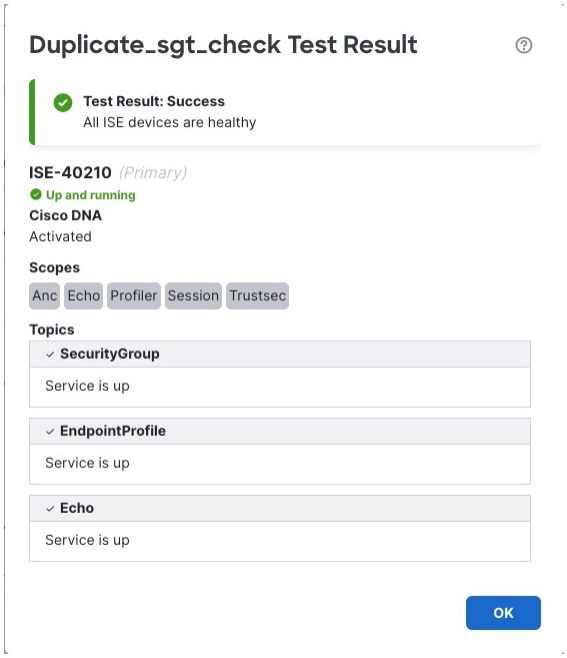


下表提供了有关图中编号区域的详细信息。

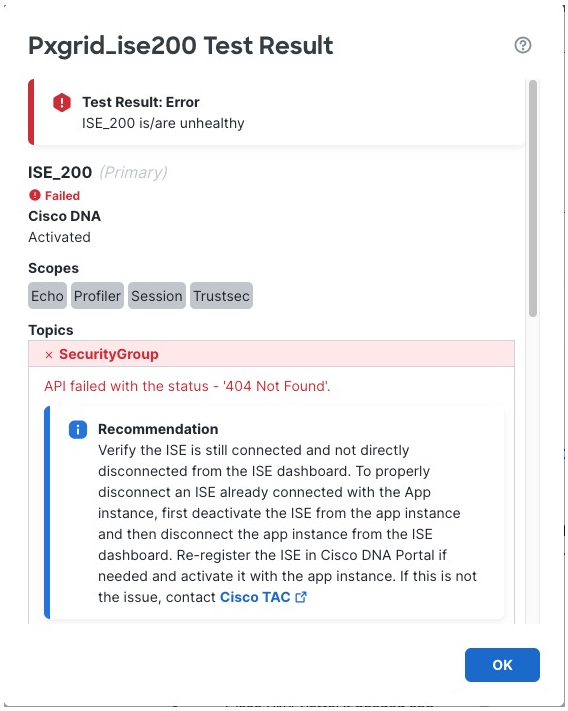
数字	含义
1	总体状态 系统会显示 Cisco ISE 应用实例的整体状态中的任何错误。在这种情况下，请滚动到该实例，然后展开错误消息或点击**测试**以了解更多信息。
2	主用 绿色复选标记表示应用处于活动状态。
3	非活动 灰显的应用实例处于非活动状态。您可以通过选中其名称旁边的复选框，然后点击**设为主用**来将其激活。

数字	含义
4	**测试**按钮 点击**测试**以执行显示更详细的应用实例状态的诊断测试。有关详细信息，请参阅下一节。

下图显示了一条示例成功消息。



下图为搜索结果的示例。



以下部分提供可能的错误的参考。

错误代码参考

提供以下信息可帮助您诊断和解决 Cisco ISE、pxGrid 云 和 Catalyst 云门户 的问题。如果这些建议不起作用，或者您遇到其他问题，请联系思科 TAC。

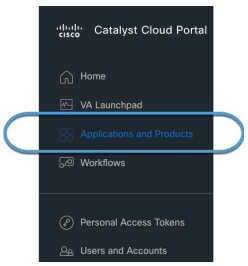
403 – Forbidden

请验证 Cisco ISE 产品在 Catalyst 云门户 中未处于**待处理**或**已中止**状态。如果设备已暂停，请按照在 Cisco ISE 中启用 pxGrid Cloud 服务并注册设备的步骤，验证 Cisco ISE 是否已注册。

此外，请验 pxGrid 云 证服务是否公开可用。

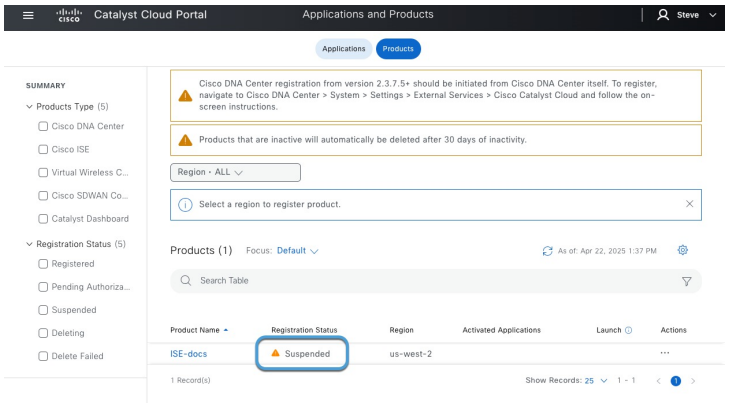
要验证您的产品是否处于活动状态，请执行以下操作：

1. 登录Catalyst 云门户。
2. 在 Catalyst 云门户 中，转到☰ > **应用程序和产品**，如下图所示：



3. 点击 **产品** 选项卡。

下图显示了已终止产品的示例。



4. 要更正此问题，请在操作列中点击 ⋯ ，然后点击**生成 OTP**。
5. 按照创建身份源，第 2152 页中所述使用 OTP。

404 – Not Found

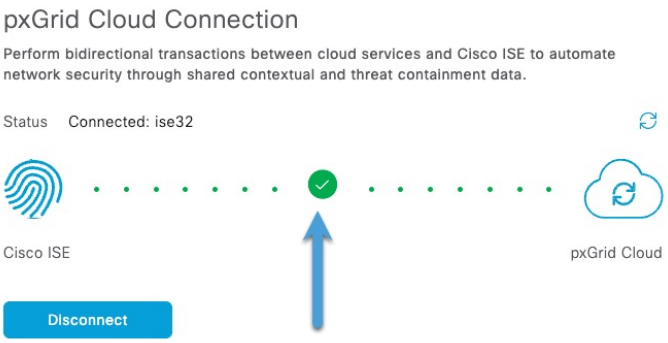
验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

408 – Request Timeout

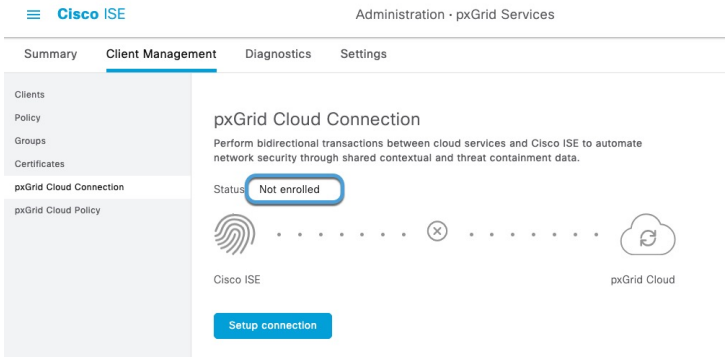
一般连接

检查 Cisco ISE是否存在任何常规连接问题，并在 ISE 面板中的 ☰ > **管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接** 下验证 pxGrid 云 连接状态是否为**已连接**。

下图显示了已连接的系统示例。



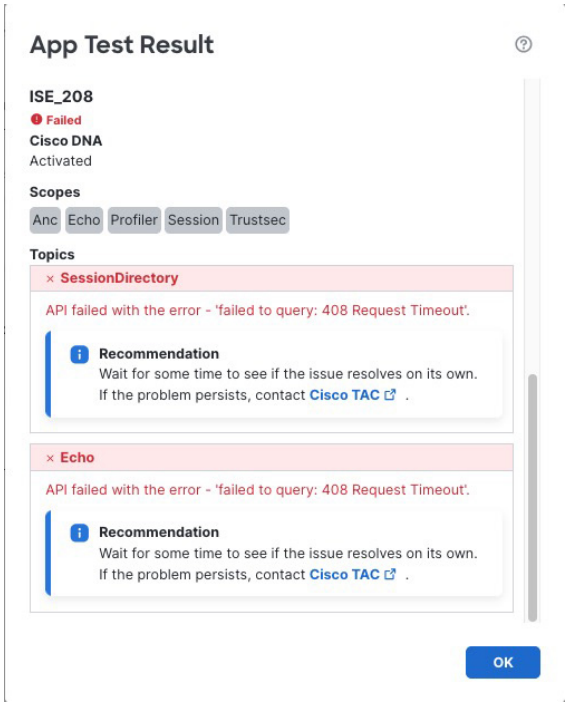
下图显示的是未注册（即未连接）的系统示例。



验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

集群成员无法访问

如果无法访问 Cisco ISE 集群的一个成员，系统将显示如下页面：



要查找无法访问的节点，请以管理员身份登录 Cisco ISE 主管理节点，然后点击 点击**菜单**图标 (☰)，然后选择 **管理** > **系统** > **部署**，查看 Cisco ISE 部署中的节点状态。

413 – 内容过大

我们建议您查看 GitHub 上的 pxGrid Cloud API 限制。如果需要，请考虑升级您的 Cisco ISE 版本，以充分利用 pxGrid 云 支持。

500 – Internal Server Error

检查 Cisco ISE 服务器是否正常运行以及 pxGrid 云服务是否处于活动状态（验证 MNT、SXP、pxGrid 节点等）。

有关更多信息，请参阅《思科身份识别服务引擎管理员指南》中 Cisco pxGrid 章节的“监控和调试”。

pxGrid 云身份源 故障排除

这些主题介绍如何对 pxGrid 云身份源 进行故障排除。

相关主题

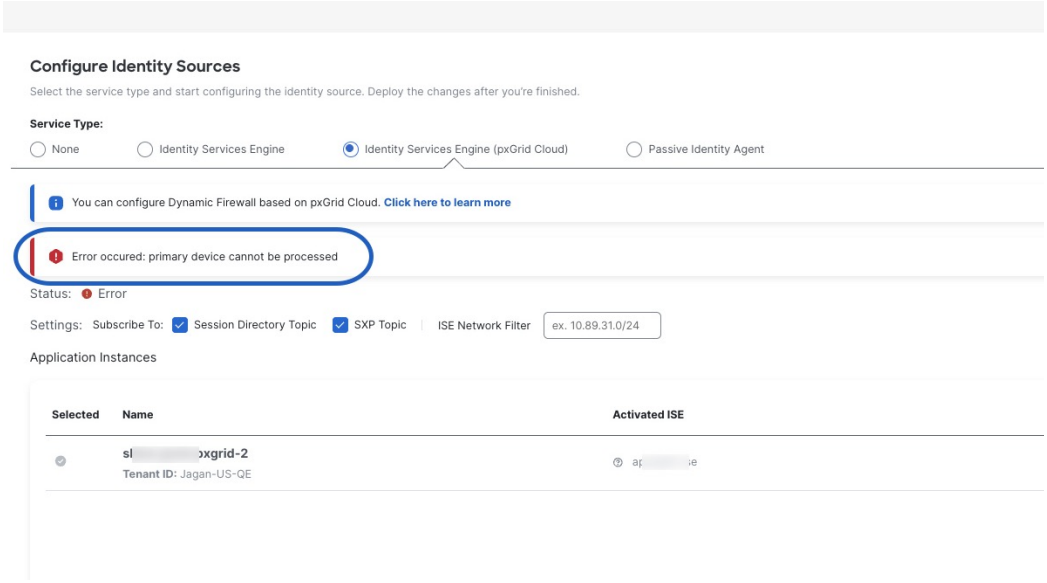
无法处理主设备，第 2167 页

无法处理主设备

每个 Cisco ISE 集群必须与且仅与一个应用实例相关联，且通常位于一个专用租户中。

如果将一个 Cisco ISE 与多个应用实例相关联，身份源将显示错误，例如`错误：无法处理主设备`或 `ISE 运行状况不正常。`

示例：



解决方案是，在将该租户用于任何其他租户或应用实例之前，先从该租户的其他应用实例中正确停用 ISE。

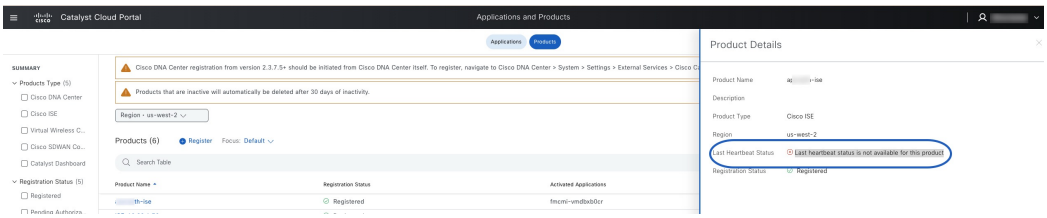
过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在页面顶部，点击**应用**。

步骤 3 找到一款已激活的 Cisco ISE 产品，并确认是该产品导致了相关问题。

示例：



步骤 4 等待产品被删除。

步骤 5 停用应用实例，如停用 pxGrid 云 应用实例，第 2168 页中所述。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

开始之前

创建连接器，第 2340 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ()。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

您创建的动态属性查询应显示为动态对象。

使用动态属性过滤器来创建访问控制规则或 DNS 规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

要向 DNS 策略添加动态属性过滤器，请参阅创建基本 DNS 策略。

要将动态属性过滤器添加到 DNS 策略，请参阅创建基本 DNS 策略。

开始之前

按照创建动态属性过滤器，第 2164 页中所述，创建动态属性筛选器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录至 Secure Firewall Management Center

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

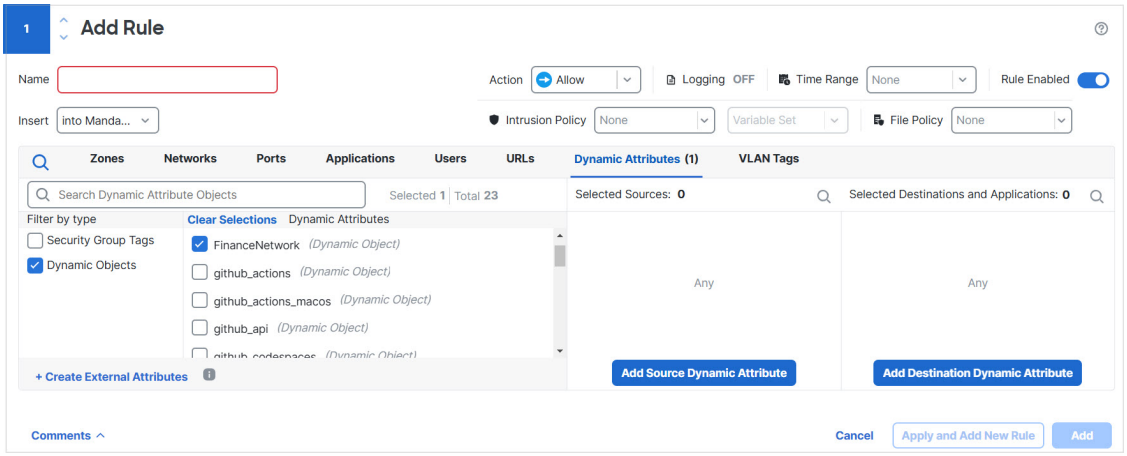
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



本示例显示一个名为 `APIC 动态属性`的动态对象，它对应于 dynamic attributes connector 中创建的动态属性筛选器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

请参阅动态属性规则条件，第 2383 页。

停用并删除 pxGrid 云身份源

这些主题讨论了如何选择性地：

- 在 Catalyst 云门户 中停用 FMC 应用实例。

  您可以执行此可选任务来排除 Cisco ISE 集成问题。

- 从 Secure Firewall Management Center 中删除 pxGrid 云身份源。

  只有在确定不再使用身份源时，才应将其删除。

相关主题

停用 pxGrid 云 应用实例，第 2168 页
删除 pxGrid 云身份源，第 2171 页

停用 pxGrid 云 应用实例

（可选。）此任务介绍如何使用 Catalyst 云门户 停用 pxGrid 云 应用实例。只有当您的 Cisco ISE 或 pxGrid 云 停止工作或您需要更新时，才应执行此操作。

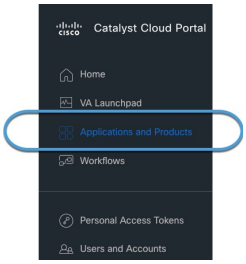
开始之前

如激活 pxGrid 云身份源，第 2156 页中所述，请确保当前的 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：

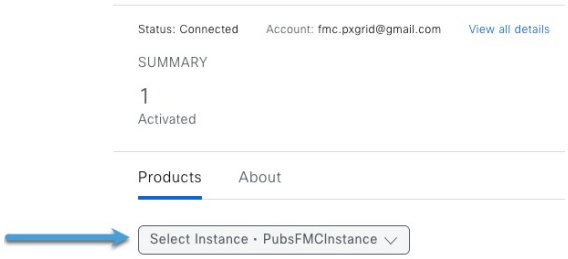


步骤 3 点击 **应用**。

步骤 4 点击防火墙管理中心的**管理**。

步骤 5 从**选择实例**列表中，点击您之前创建的防火墙应用的名称。

示例：



步骤 6 在“操作”列中，点击更多图标 （ ··· ） > **停用**。

步骤 7 等待直至移除产品。

如有必要，您可以点击 **刷新** ( ) 以查看更新后的状态。

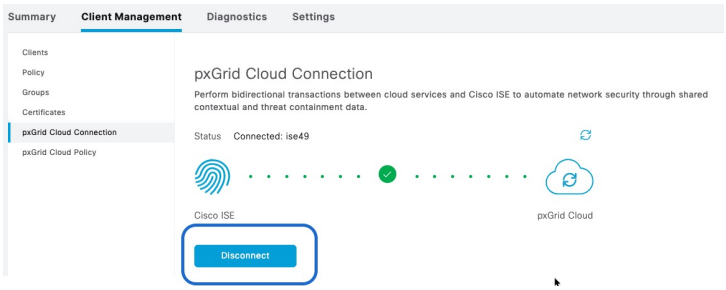
步骤 8 ISE 3.3 或更低版本：断开应用实例的连接：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接**。

c) 点击**断开连接**。

示例：



步骤 9 ISE 3.4 或更高版本：取消注册应用实例：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **系统** > **部署**。

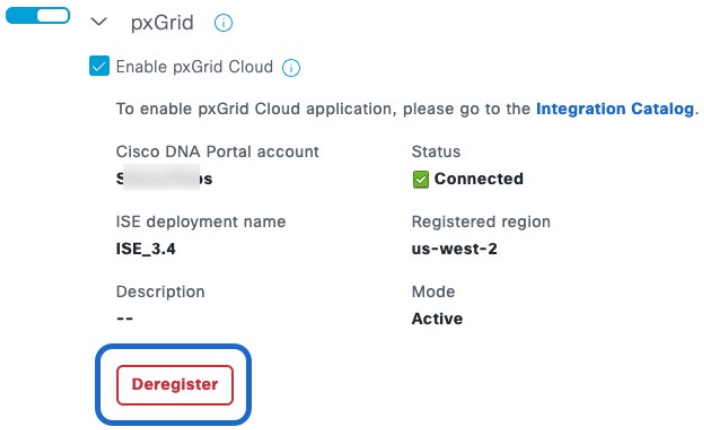
c) 展开**部署**。

d) 点击 ISE 节点的名称。

e) 在**常规设置**选项卡页面中，滚动至找到 **pxGrid**。

f) 点击**取消注册**。

示例：



步骤 10 要验证已在 Secure Firewall Management Center 中停用应用实例：

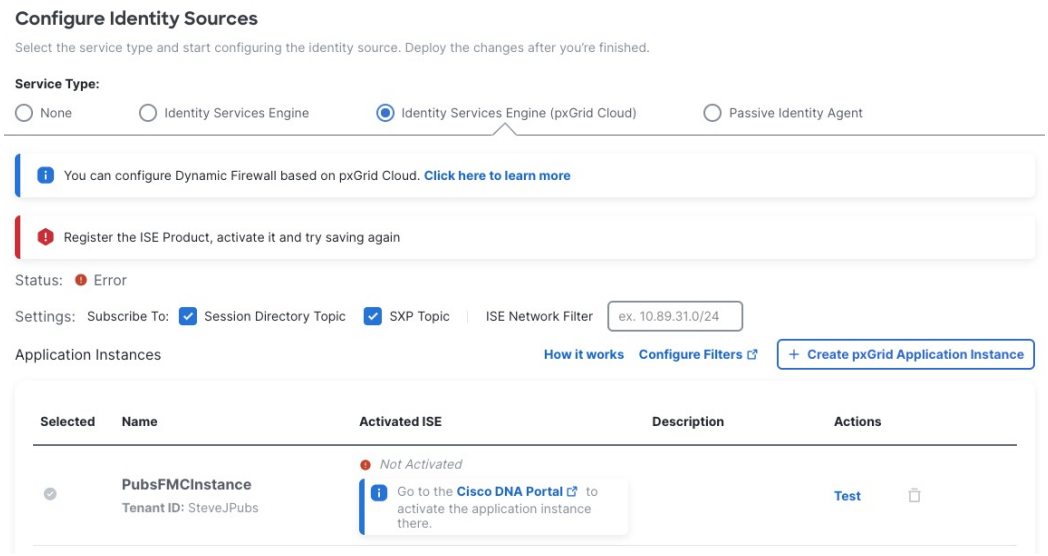
a) 登录 Secure Firewall Management Center。

b) 点击 **集成** > **身份** > **身份源**

c) 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

d) 验证已激活 ISE 列中是否显示**未激活**。

示例：



下一步做什么

- 要向 pxGrid 云 注册 Cisco ISE 并激活应用实例，请参阅：
  - ISE 3.3 及更早版本：使用 Catalyst 云门户 注册 Cisco ISE，第 2146 页。
  - ISE 3.4 及更高版本：创建应用实例，第 2180 页。

- 要彻底删除身份源，请参阅删除 pxGrid 云身份源 ， 第 2171 页。

删除 pxGrid 云身份源

（可选。）此任务说明如何从 Secure Firewall Management Center 中删除不想再次使用的 pxGrid 云身份源。

开始之前

按照停用 pxGrid 云 应用实例 ， 第 2168 页中所述，从 Catalyst 云门户 中停用 FMC 应用实例。

过程

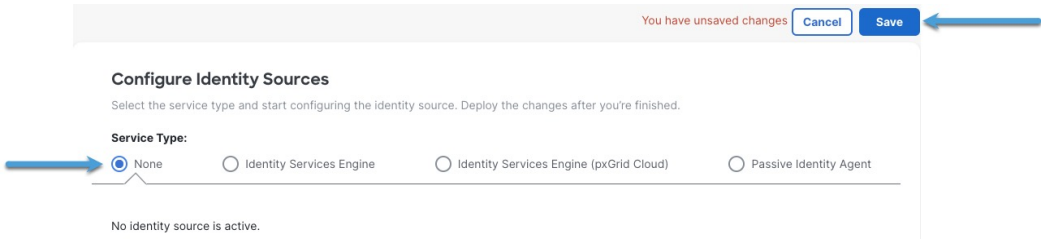
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 对于服务类型，请点击**无**。

示例：



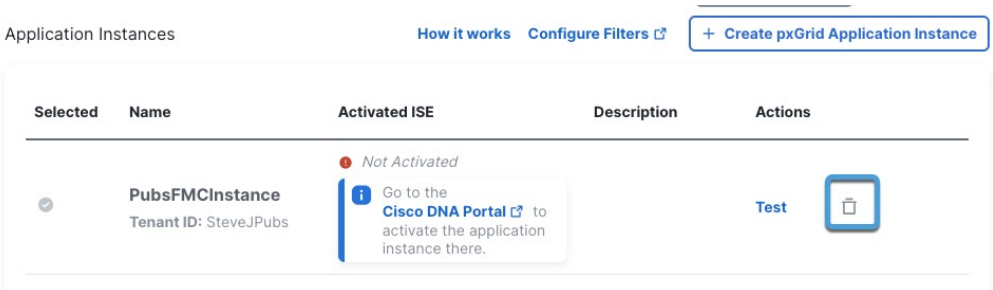
步骤 5 点击**保存**。

步骤 6 您需要确认您的选择。

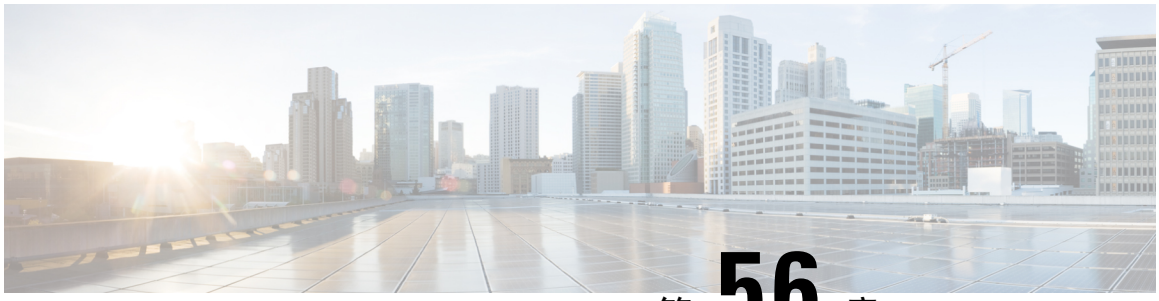
步骤 7 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 8 请点击 **删除** ( )。

示例：



步骤 9 您需要确认操作。



第 56 章

身份源：远程访问 VPN

以下主题讨论如何通过远程接入 VPN 执行用户感知和用户控制：

- 远程访问 VPN 身份源， 第 2203 页
- 配置用户控制 RA VPN， 第 2204 页
- 远程访问 VPN 身份源的故障排除准则， 第 2205 页
- 远程接入 VPN 的历史记录， 第 2206 页

远程访问 VPN 身份源

远程访问VPN身份源在建立至网络的安全远程连接前对用户进行身份验证。要求用户通过客户端提供凭据以核验身份。

身份源配置

Secure Client 是终端设备上通过远程 VPN 连接至 Firewall Threat Defense 设备唯一受支持的客户端。

按照创建新的远程访问 VPN 策略， 第 1542 页中的描述设置安全 VPN 网关时，您可以为这些用户设置一个身份策略，并将该身份策略与访问控制策略关联，前提是您的用户位于 Active Directory 存储库中。

注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则必须配置领域（**对象** > **AAA 服务器** > **RADIUS 服务器组**）。

远程用户提供的登录信息由 LDAP 或 AD 领域或 RADIUS 服务器组进行验证。这些实体与 Cisco Secure Firewall Threat Defense 安全网关集成。

注释 如果用户使用 Active Directory 作为身份验证源通过远程访问 VPN 进行身份验证，则用户必须使用其用户名登录；domain\username 或 username@domain 格式无效。（Active Directory 将此用户名视为 logon 名称，有时也视为 sAMAccountName。）有关详细信息，请参阅 MSDN 上的用户命名属性。

如果使用 Radius 进行身份验证，用户可以使用上述任何一种格式登录。

通过 VPN 连接身份验证后，远程用户获得 VPN 身份。安全网关上的身份策略使用该 VPN 身份识别并过滤属于此远程用户的网络流量。

身份策略与访问控制策略相关联，后者用于确定哪些人有权访问网络资源。访问控制策略据此阻止或允许远程用户访问您的网络资源。

相关主题

安全连接概览，第 1427 页
远程访问 VPN 概述，第 1531 页
VPN 基础知识，第 1428 页
远程访问 VPN 功能，第 1532 页
远程访问 VPN 的准则和限制，第 1538 页
创建新的远程访问 VPN 策略，第 1542 页

配置用户控制 RA VPN

配置 RA VPN 进行用户控制，以管理远程访问 VPN 连接并应用基于身份的策略来控制用户访问和流量过滤。

通过远程访问 VPN 用户控制，可以实施基于身份的策略来管理和监控 VPN 用户连接，从而为网络环境提供增强的安全性和访问控制。

Before you begin

- 按创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页中所述创建领域。
- 要使用身份验证、授权和审核 (AAA)，请按照添加 RADIUS 服务器组，第 2620 页中的讨论设置 RADIUS 服务器组。

请按照以下步骤配置 RA VPN 以实现用户控制：

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **安全连接** > **远程访问 VPN**。

步骤 3 请参阅创建新的远程访问 VPN 策略，第 1542 页。

下一步做什么

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。

- 按 VPN 会话和用户信息，第 1643 页中所述，监视 VPN 用户流量 。

远程访问 VPN 身份源的故障排除准则

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 2049 页和用户控制故障排除，第 2231 页。

如果遇到远程访问 VPN 问题，请检查 防火墙管理中心和托管设备之间的连接。如果连接失败，则无法在停机期间识别设备报告的所有远程访问VPN登录，除非以前查看过这些用户并已将他们下载到 防火墙管理中心。

无法识别的用户在 防火墙管理中心 上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。

托管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。

主动 FTP 会话在事件中显示为**未知**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关主动 FTP 的详细信息，请参阅 RFC 95。

未观察到 VPN 统计信息的正确设置

此任务可确保托管设备在修改 VPN 统计配置后接收正确的运行状况策略设置。

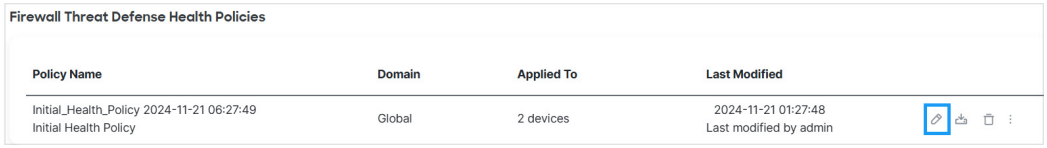
此任务讨论在运行状况策略中启用或禁用 **VPN 统计信息** 设置后必须执行的步骤。未能执行此任务意味着托管设备的运行状况策略设置不正确。

过程

步骤 1 如果尚未登录，请登录Secure Firewall Management Center。

步骤 2 请点击 **故障排除** > **+ 显示更多** > **运行状况** > **策略** 。

步骤 3 在防火墙威胁防御运行状况策略下，点击要编辑的策略旁边的 **编辑** (✎) 。



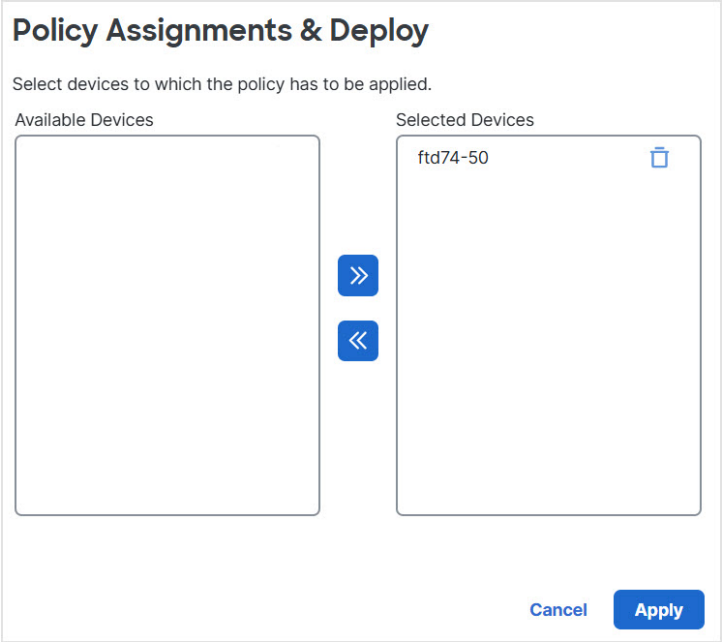
步骤 4 在 **运行状况** 模块选项卡页面上，向下滚动以找到 **VPN 统计信息**。

步骤 5 验证 VPN 统计信息设置是否正确，或根据需要进行更改。

步骤 6 如果您更改了设置，请点击 **保存**，然后点击 **取消** 以返回到运行状况策略。

步骤 7 在防火墙威胁防御运行状况策略下， **部署运行策略** (☁) 点击以应用策略。

步骤 8 在 **策略分配和部署** 对话框中，将要部署运行状况策略的设备移至 **所选设备** 字段。



步骤 9 点击**应用 (Apply)**。
部署运行状况策略时，系统会显示一条消息。

步骤 10 运行状况策略完成部署后，点击 **策略** > **安全策略** > **访问控制** 以编辑访问控制策略。

步骤 11 点击策略旁边的 **编辑** (✎) 进行编辑。

步骤 12 对策略进行细微更改，例如更改其名称。

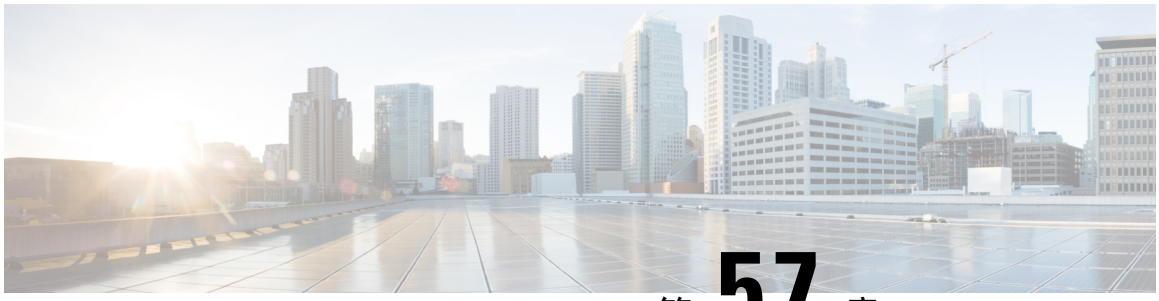
步骤 13 保存访问控制策略。

步骤 14 部署配置更改；请参阅 部署配置更改，第 180 页。。

远程接入 VPN 的历史记录

本参考提供各防火墙管理中心和 Firewall Threat Defense 版本的远程访问 VPN (RA VPN) 功能的版本历史记录和介绍详细信息。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
远程接入 VPN	6.2.1	任意	引入的功能。远程接入 VPN 允许个人用户使用连接到互联网的笔记本电脑或台式计算机或者使用 Android 或 Apple iOS 移动设备，从远程位置连接到专用企业网络。远程用户使用对于通过共享介质和互联网传输的数据至关重要的加密技术，安全且自信地传输数据。



第 57 章

身份源：TS 代理

要将 TS 代理用作用户感知和用户控制的身份源，请按照思科终端服务 (TS) 代理指南中所述安装和配置 TS 代理软件。

后续操作：

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动， 如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程 所述。

- 终端服务 (TS) 代理身份源，第 2207 页
- TS 代理准则，第 2208 页
- 身份源：TS 代理，第 2208 页
- TS 代理身份源故障排除，第 2208 页
- TS 代理的历史记录，第 2209 页

终端服务 (TS) 代理身份源

TS 代理是一种被动身份验证方式，并且是系统支持的授权身份源之一。Windows 终端服务器执行身份验证，然后 TS 代理将其报告给独立版或高可用性的 。

当安装在 Windows 终端服务器上时，TS 代理在个人用户登录或注销受监控网络时向其分配唯一端口范围。Secure Firewall Management Center使用唯一端口识别系统中的个人用户。您可以使用一个 TS 代理监控一台 Windows 终端服务器上的用户活动，并将加密数据发送到一个 Secure Firewall Management Center。

TS 代理不报告失败的登录尝试。从 TS 代理获取的数据可用于用户感知和用户控制。

TS 代理准则

TS 代理需要多步骤配置，并且包括以下内容：

1. 已安装并配置 TS 代理的 Windows 终端服务器。
2. 一个或多个针对服务器所监控用户的身份领域。

在 Microsoft Windows 终端服务器上安装 TS 代理。有关多步骤 TS 代理安装和配置的详细信息以及服务器和系统要求的全面介绍，请参阅思科终端服务 (TS) 代理指南。

TS 代理数据显示在“用户”、“用户活动”和“连接事件”表中，并可用于用户感知和用户控制。

注释 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 Secure Firewall Management Center 会划分 TS 代理数据的优先级。如果 TS 代理和另一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 Secure Firewall Management Center。

身份源：TS 代理

要将 TS 代理用作用户感知和用户控制的身份源，请按照思科终端服务 (TS) 代理指南中所述安装和配置 TS 代理软件。

后续操作：

- 使用创建身份策略，第 2213 页中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联，第 1719 页中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。
- 将身份和访问控制策略部署到托管设备，如部署配置更改，第 180 页中所述。
- 监控用户活动， 如 *Cisco Secure Firewall Management Center* 管理指南 中使用工作流程 所述。

TS 代理身份源故障排除

有关其他相关故障排除信息，请参阅领域和用户下载故障排除，第 2049 页和用户控制故障排除，第 2231 页。

如果您遇到 TS 代理集成问题，请检查：

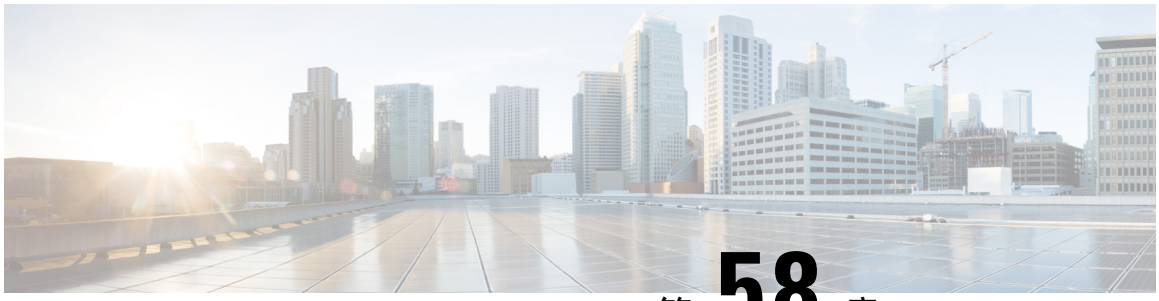
- 您必须将 TS 代理服务器上的时间与 Secure Firewall Management Center 上的时间进行同步。
- 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则 Secure Firewall Management Center 会划分 TS 代理数据的优先级。如果 TS 代理和一个被动身份源通过同一 IP 地址报告活动，则仅会将 TS 代理数据记录到 Secure Firewall Management Center。

- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

有关故障排除更多信息，请参阅 思科终端服务 (TS) 代理指南。

TS 代理的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
TS 代理用于用户控制。	7.2.0	6.2.0	引入的功能。Firepower现在提供更好地识别共享环境中各个用户的功能（例如 Citrix 的虚拟桌面基础架构 (VDI)），以便对防火墙准确地实施基于用户的策略规则。通过使用的端口识别用户。 TS 代理软件的更新与 Firepower 管理中心无关。有关详细信息，请参阅： • cisco.com 上提供的思科终端服务 *(TS)* 代理指南 • Cisco Firepower 兼容性指南



第 58 章

身份策略

以下主题讨论如何创建和管理身份规则及身份策略：

- 关于身份策略， 第 2211 页
- 身份策略的许可证要求， 第 2212 页
- 身份策略的要求和先决条件， 第 2212 页
- 创建身份策略， 第 2213 页
- 身份规则条件， 第 2215 页
- 创建身份规则， 第 2221 页
- 示例身份策略和规则， 第 2223 页
- 管理身份策略， 第 2230 页
- 管理身份规则， 第 2230 页
- 用户控制故障排除， 第 2231 页

关于身份策略

身份策略包含身份规则。身份规则会将流量集与领域和身份验证方法相关联：被动身份验证、主动身份验证或无身份验证。

除了下面段落提到的例外之外，您必须配置计划使用的领域和身份验证方法，然后才能在身份规则中进行调用：

- 在**集成** > **身份** > **领域** > **领域**中配置身份策略外的领域。有关详细信息，请参阅 创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页。
- 在**集成** > **身份** > **身份源**中，配置 ISE/ISE-PIC 被动身份验证身份源。有关详细信息，请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页。
- 在系统外，配置被动身份验证身份源：TS代理。有关详细信息，请参阅《思科终端服务*(TS)*代理指南》。
- 在身份策略中，配置主动身份验证身份源：强制网络门户。有关详细信息，请参阅如何为用户控制配置强制网络门户， 第 2063 页。

- 您可以在远程访问 VPN 策略中配置远程访问 VPN，即主动身份验证身份源。有关详细信息，请参阅远程访问 VPN 身份验证，第 1534 页。

向一个身份策略添加多个身份规则后，对规则排序。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一个规则是处理该流量的规则。

您也可以按网络对象过滤流量，从而在设备达到或接近其内存限制时限制每个设备监控的网络。

配置一个或多个身份策略后，必须将一个身份策略与访问控制策略相关联。当网络上的流量与身份规则中的条件匹配时，系统会将流量与指定领域相关联并使用指定身份源对流量中的用户进行身份验证。

如果不配置身份策略，则系统不会执行用户身份验证。

创建身份策略的例外

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

相关主题

如何设置身份策略，第 1982 页

身份策略的许可证要求

威胁防御 许可证

任意

身份策略的要求和先决条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

- 访问管理员
- 网络管理员

创建身份策略

此任务讨论如何创建身份策略。

开始之前

在访问控制策略内使用领域中的用户和组需要身份策略。创建并启用一个或多个领域，如创建LDAP领域或 Active Directory 领域和领域目录， 第 2019 页中所述。

（可选。）如果特定托管设备监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。如果设备运行的是版本 6.7 或更高版本，您可以将身份规则配置为仅按一个网络或网络组对象监控流量。要创建网络对象，请参阅创建网络对象， 第 2660 页。

如果满足以下所有条件，则不需要身份策略：

- 您使用 ISE/ISE-PIC 身份源。
- 您未在访问控制策略中使用用户或组。
- 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅ISE SGT 与自定义 SGT 规则条件。

过程

步骤 1 登录Firewall Management Center。

步骤 2 点击**策略** > **安全策略** > **身份**，然后点击**新建策略 (New Policy)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 4 点击**保存**。

步骤 5 要将规则添加到策略，请点击**添加规则 (Add Rule)**，如创建身份规则， 第 2221 页中所述。

步骤 6 要创建规则类别，请点击**添加类别 (Add Category)**。

步骤 7 要配置强制网络门户主动身份验证，请点击**主动身份验证 (Active Authentication)** 并查看创建身份策略和主动身份验证规则， 第 2066 页。

步骤 8 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加** (+) 以创建新的网络对象。

步骤 9 点击**保存** 保存身份策略。

下一步做什么

- 将规则添加到指定要匹配的用户和其他选项的身份策略；请参阅创建身份规则，第 2221 页。
- 将身份策略与访问控制策略相关联，以允许或阻止选定用户访问指定的资源；请参阅将其他策略与访问控制相关联，第 1719 页。
- （Microsoft Azure AD 领域不需要。）将配置更改部署到托管设备；请参阅部署配置更改，第 180 页。

如果您遇到问题，请参阅用户控制故障排除，第 2231 页。

相关主题

创建身份策略和主动身份验证规则，第 2066 页
强制网络门户字段，第 2073 页
用户控制故障排除，第 2231 页

创建身份映射过滤器

身份映射过滤器可用于限制应用身份规则的网络。例如，如果您的 Firewall Management Center 管理的 FTD 内存有限，则可以限制其监控的网络。

您必须为 IPv4 和 IPv6 地址分别创建身份映射过滤器。

您还可以选择从以下项目中排除子网：

- 接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网。
- 从 被动身份代理接收用户到 IP 映射。

您通常应对内存较低的托管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

开始之前

执行以下任务：

1. 创建以下任意项目：
   - LDAP 或 Microsoft Active Directory 领域。请参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页。
   - ISE/ISE-PIC 身份源。请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页。
   - 强制网络门户身份源。请参阅如何为用户控制配置强制网络门户，第 2063 页。
   - 被动身份代理身份源。请参阅如何创建 被动身份代理 身份源，第 2114 页。
   - TS 代理身份源。请参阅终端服务 (TS) 代理身份源，第 2207 页。
   - RA-VPN 身份源。请参阅配置用户控制 RA VPN，第 2204 页。
2. 创建网络对象或网络组对象，如网络，第 2658 页中所述。您创建的网络对象或组应定义您希望托管设备在身份策略中监控的网络。

过程

步骤 1 开始创建身份策略。

步骤 2 在**身份映射过滤器 (Identity Mapping Filter)** 列表中，执行以下任一操作：

- 点击列表中的网络对象。
- 点击 **添加** (+) 并按照屏幕上的提示创建网络对象或网络组对象。有关详细信息，请参阅 网络，第 2658 页。

下一步做什么

继续配置身份策略。

身份规则条件

通过规则条件，您可以微调身份策略，以您要控制的用户和网络为目标。有关详细信息，请参阅以下主题之一：

相关主题

安全区域规则条件，第 1921 页
网络规则条件，第 1420 页
VLAN 标记规则条件，第 1768 页
端口规则条件，第 1421 页
领域和设置规则条件，第 2219 页

安全区域规则条件

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

重定向到主机名的网络规则条件

（仅限 Snort 3.0）—你可以使用一个网络对象，其中包含强制网络门户可用于主动认证请求的接口的完全限定主机名（FQDN）。

FQDN 必须解析为托管设备上接口之一的 IP 地址。通过使用 FQDN，您可以为客户端将识别的主动身份验证分配证书，从而避免用户在被重定向到托管设备的 IP 地址时收到不受信任证书警告。

证书可以在证书的使用者替代名称 (SAN) 中指定一个 FQDN、通配符 FQDN 或多个 FQDN。

如果身份规则要求对用户进行主动身份验证，但您未指定重定向 FQDN，则用户将被重定向到他们连接的托管设备接口上的强制网络门户端口。

如果您不提供重定向到主机名 FQDN，HTTP Basic、HTTP 响应页面和 NTLM 身份验证方法会使用接口的 IP 地址将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.directory-server-domain-name*进行重定向。要在不提供重定向到主机名 FQDN 的情况下使用 HTTP 协商，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

建议您始终提供重定向到主机名 FQDN 以确保行为一致，而无论采用哪种身份验证方法。

VLAN 标记规则条件



注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

对于会动态打开独立通道以区分控制流和数据流的应用（如 Firewall Threat Defense），也建议使用应用过滤。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标记。此外，系统使用外部报头将访问控制策略中的**所有**流量与 GRE 限制的规则相匹配。对于 Firewall Threat Defense设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- 解密 规则 - SSL 规则仅支持 TCP 端口条件。

- IMCP 回应 - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

领域和设置规则条件

通过**领域和设置 (Realm & Settings)** 选项卡页面，您可以选择要应用身份规则的领域或领域序列。如果您使用的是强制网络门户，则还可以选择其他选项。

身份验证领域

从**领域**列表中，点击领域或领域序列。

包含要对其执行指定**操作 (Action)** 的用户的领域或领域序列。必须在选择作为身份规则中的领域或领域序列之前，对领域进行完全配置。

注释 如果启用了 VPN 远程访问，而且您的部署正在使用 RADIUS 服务器组进行 VPN 身份验证，请确保您指定的领域与此 RADIUS 服务器组相关联。

仅主动身份验证：其他选项

如果选择**主动身份验证 (Active Authentication)** 作为身份验证类型，或者选中**如果无法建立被动或 VPN 身份则使用主动身份验证 (Use active authentication if passive or VPN identity cannot be established)** 框，您将看到以下选项。

如果无法建立被动或 VPN 身份，请使用主动身份验证

（仅限被动身份验证规则。）如果被动身份验证或VPN身份验证无法标识用户，选择此选项将通过强制网络门户主动身份验证来验证用户。您必须在身份策略中配置主动身份验证规则，才能选择此选项。（即，用户必须使用强制网络门户进行身份验证。）

如果禁用此选项，没有 VPN 身份或被动身份验证不能标识的用户将被标识为“未知”。

另请参阅本主题后面对 **身份验证领域** 列表的讨论，

如果身份验证无法识别用户，则识别为特殊身份/访客

选择此选项允许执行强制网络门户主动身份验证时而失败指定次数的用户以访客身份访问您的网络。这些用户显示在以其用户名（如果 AD 或 LDAP 服务器中有他们的用户名）或**访客**（如果他们的用户名未知）标识的防火墙管理中心中。其领域是在身份规则中指定的领域。（默认情况下，失败的登录次数为 3。）

仅当您将**主动身份验证**（即，强制网络门户身份验证）配置为规则**操作**时，才会显示此字段。

身份验证协议

要用于执行强制网络门户主动身份验证的方法。用户在使用响应页面登录时看到的内容的示例如 使用主动身份验证规则创建示例身份策略，第 2226 页中所示。

选项因领域、LDAP 或 AD 的类型而有所不同。

- 如果要使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证，请选择 **HTTP 基本身份验证**。用户通过其浏览器的默认身份验证弹出窗口登录网络。

  大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。

- 选择 **NTLM** 以使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅在选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。
- 选择 **Kerberos** 以使用 Kerberos 连接对用户进行身份验证。仅在为已启用安全 LDAP (LDAPS) 的服务器选择 AD 领域时，此选项才可用。如果在用户的浏览器中配置了透明身份验证，则该用户自动登录。如果未配置透明身份验证，则用户使用其浏览器的默认身份验证弹出窗口进行登录。

注释 您选择的**领域**必须配置 **AD 加入用户名**和 **AD 加入密码**，才能执行 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 Kerberos 强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。

对于 Firewall Threat Defense 设备，FQDN 必须解析为用于强制网络门户的路由接口的 IP 地址。

- 选择 **HTTP 协商**以允许强制网络门户服务器选择“HTTP 基本”、“Kerberos”或“NTLM”进行身份验证连接。仅在选择 AD 领域时，此类型才可用。

注释 您选择的**领域**必须配置 **AD 加入用户名**和 **AD 加入密码**，这样一来，**HTTP 协商**才能选择 Kerberos 强制网络门户主动身份验证。

注释 如果您要创建身份规则来执行 **HTTP 协商**强制网络门户，并且已配置了 DNS 解析，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。用于强制网络门户的设备的 FQDN 必须与您配置 DNS 时提供的主机名匹配。

- 选择 **HTTP 响应页面**，使用户能够选择要登录的领域。

  您可以选择自定义响应页面；例如，符合公司风格标准。

主动身份验证领域

（仅限被动身份验证规则。）如果您点击了 **如果无法建立被动或 VPN 身份，则使用主动身份验证**，则必须点击领域或领域序列的名称。领域或领域序列的可用性取决于您对身份验证协议的选择，如下所示：

- **HTTP 基本** 或 **HTTP 响应页面** 身份验证协议：您可以选择领域或领域序列。
- **NTLM**、 **Kerberos**或 **HTTP 协商** 身份验证协议：只能选择领域。您 不能 选择领域序列。

创建身份规则

有关身份规则的配置选项的详细信息，请参阅身份规则字段 ， 第 2222 页。

开始之前

您必须创建并启用领域 或领域序列。

- 创建 Microsoft Active Directory 领域和领域目录，如创建 LDAP 领域或 Active Directory 领域和领域目录 ， 第 2019 页中所述。
- （仅限 Microsoft AD 领域。）下载用户和组并启用领域，如 同步用户和组 ， 第 2037 页中所述。
- 如创建Microsoft Azure AD (SAML)领域 ， 第 1994 页中所述，创建 Microsoft Azure AD (SAML) 领域。
- （可选。）按创建领域序列 ， 第 2039 页中所述创建领域序列。
- 规则自上而下进行评估。对于与给定规则的指定网络条件匹配的连接，系统将根据规则中指定的身份领域对用户进行评估。如果用户不属于该领域，他们将被标记为未知，并且不会评估身份策略中的其他规则。因此，如果有多个领域需要评估，请务必使用领域序列而不是单个领域。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 a 解密策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为 ， 第 174 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 点击要将身份规则添加到的身份策略旁边的 **编辑** (✎) 。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 输入 **Name**。

步骤 6 如果指定规则适用，请选中**已启用 (Enabled)** 复选框。

步骤 7 要将规则添加到现有类别，请指明要**插入**规则的位置。要添加新类别，请点击**添加类别 (Add Category)**。

步骤 8 从列表中选择一个规则**操作**。

步骤 9 如果您正在配置强制网络门户，请参阅如何为用户控制配置强制网络门户，第 2063 页。

步骤 10 （可选）要向身份规则中添加条件，请参阅身份规则条件，第 2215 页。

步骤 11 点击**添加 (Add)**。

步骤 12 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

步骤 13 点击**保存**。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

身份规则字段

使用以下字段配置身份规则。

启用

启用此选项可启用身份策略中的身份规则。取消选择此选项可禁用身份规则。

操作

指定要对指定领域中的用户执行的身份验证的类型：**被动身份验证**（默认）、**主动身份验证**或**无身份验证**。必须完全配置身份验证方法或身份源，然后再选择其作为身份规则中的操作。

此外，如果启用了 VPN（至少在一台托管设备上配置），远程访问 VPN 会话将通过 VPN 进行主动身份验证。其他会话使用规则操作。这意味着，如果启用了 VPN，会首先确定所有会话的 VPN 身份，而不考虑所选的操作。如果在指定领域发现 VPN 身份，将使用此身份源。不再执行任何其他强制网络门户主动身份验证，即便已选择。

如果未发现 VPN 身份源，该过程将根据指定操作继续。不能将身份策略仅限制为仅使用 VPN 身份验证，因为如果未找到 VPN 身份源，将根据所选的操作应用规则。



注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 SSL 策略时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

有关您的系统版本支持哪些被动和主动身份验证方法的信息，请参阅关于用户身份源，第1976页。

示例身份策略和规则

以下各节提供使用被动身份验证规则或主动身份验证规则配置身份策略的示例。此外，由于您可以使用领域或领域序列通过主动身份验证对用户进行身份验证，因此提供了单独的示例。

主动身份验证 意味着用户使用强制网络门户进行身份验证；用户在被允许访问允许的资源之前输入网络凭证。（RA-VPN 是另一种类型的主动身份验证，但它不能与强制网络门户身份验证一起使用。有关详细信息，请参阅远程访问 VPN 身份源，第 2203 页。）

被动身份验证 涵盖所有其他类型。被动身份验证包括使用 Microsoft Active Directory 领域、Microsoft Azure Active Directory 领域、思科身份服务引擎等。

您可以使用 Microsoft Azure Active Directory 领域以不同的方式对用户进行身份验证，此处未讨论。有关详细信息，请参阅创建Microsoft Azure AD (SAML)领域，第 1994 页。

假定条件

示例使用以下假设：

- Microsoft Active Directory (AD) 领域，名为 forest.example.com，其中两个子域配置为信任关系：
  - 美国西部
  - 美国东部地区
- 包含两个领域的名为 US 的领域序列
- 使用领域序列对用户进行身份验证的被动身份验证规则
- 两个主动身份验证规则：
  - 通过领域对用户进行身份验证并使用 NTLM 身份验证协议的一个规则
  - 使用领域序列对用户进行身份验证并使用 HTTP 响应页面身份验证协议的一个规则
- 每个示例身份规则与不同的身份策略相关联

被动身份验证身份规则

配置被动身份验证身份规则时，可以选择使用 LDAP（Microsoft Active Directory 领域），或 Microsoft AD 领域序列对用户进行身份验证。您可以使用领域对任何身份验证类型进行身份验证；领域序列限制您可以使用的身份验证类型。有关示例，请参阅创建带有被动身份验证规则的身份策略，第 2224 页。

主动身份验证身份规则

配置主动身份验证身份规则时，可以选择使用 LDAP（Microsoft Active Directory 领域），或 Microsoft AD 领域序列对用户进行身份验证。您可以使用领域对任何身份验证类型进行身份验证；领域序列限制您可以使用的身份验证类型。

您还可以使用 Microsoft Active Directory 领域序列对用户进行身份验证，但以下身份验证类型除外：

- NTLM
- Kerberos
- HTTP 协商

有关示例，请参阅使用主动身份验证规则创建示例身份策略，第 2226 页。

创建带有被动身份验证规则的身份策略

此任务讨论如何使用被动身份验证规则创建身份策略，该规则使用美国领域序列对用户进行身份验证。如果在序列中的第一个领域中未找到用户，系统将按领域序列中列出的顺序搜索序列中的其他领域。如果仍未在领域或领域序列找到用户，则会将该用户标识为“未知”。

如果在序列中的任何领域均未找到用户，则可以选择使用强制网络门户对用户进行身份验证（即主动身份验证）。有关详细信息，请参阅强制网络门户准则和限制，第 2060 页。

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 点击**新建策略 (New Policy)**。

步骤 4 输入策略的 **名称** 和可选 **说明**。

步骤 5 点击**保存**。

步骤 6 点击**添加规则 (Add Rule)**。

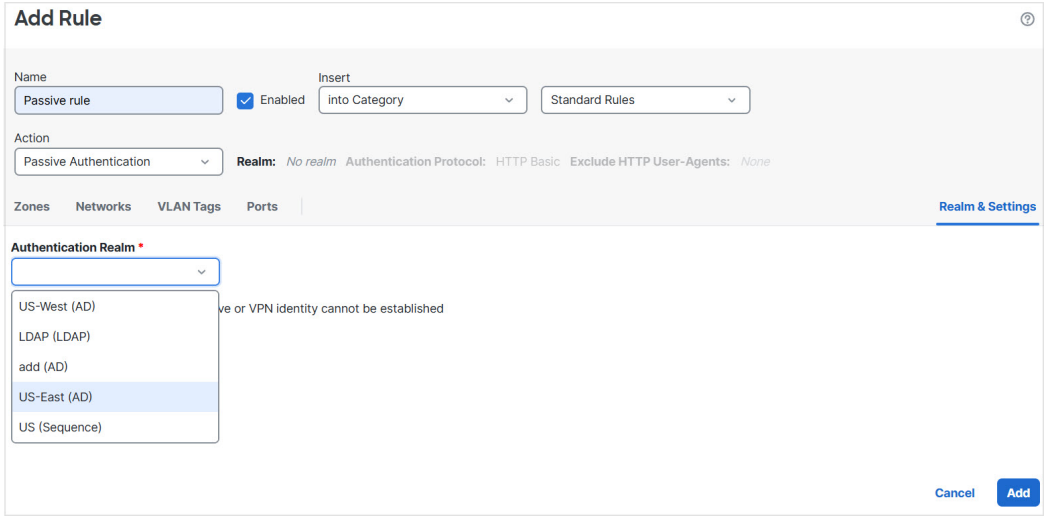
步骤 7 为规则输入**名称 (Name)**。

步骤 8 从“操作”列表中，点击 **被动身份验证**。

步骤 9 点击 **领域和设置** 选项卡页面。

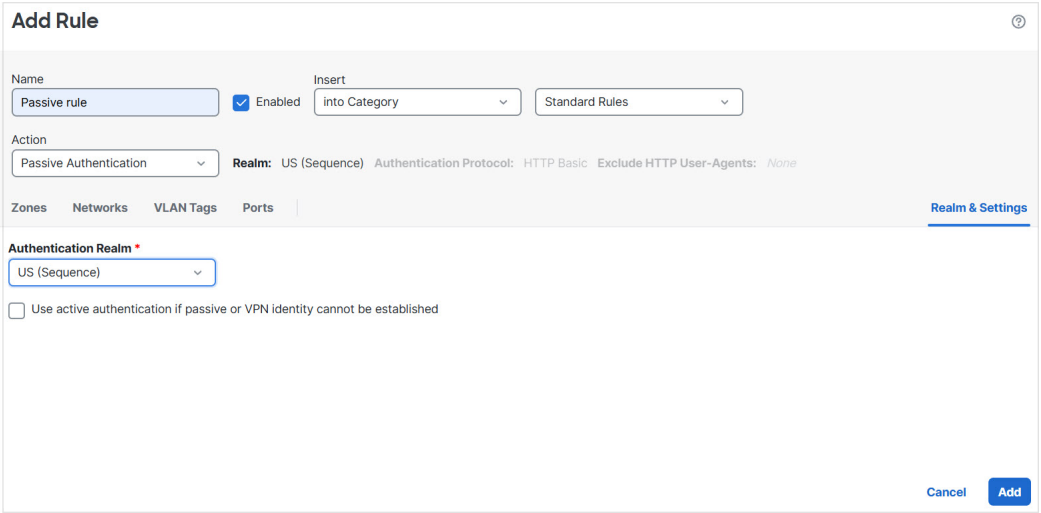
步骤 10 从列表中，点击领域或领域序列的名称。

下图显示了一个示例。



- 如果您选择一个领域（例如示例中的**美国东部**），则系统会搜索该领域以查找与规则匹配的用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。
- 如果选择领域序列（在示例中的**美国（序列）**），则系统将按照序列中指定的顺序在该序列中的每个领域搜索用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。
- 您还可以选择 LDAP 领域。
- 对于用户身份验证的额外方法，请选中**如果无法建立被动或 VPN 身份，请使用主动身份验证**。有关详细信息，请参阅 强制网络门户准则和限制，第 2060 页。

下图显示配置为在美国领域序列中搜索用户的被动身份策略示例。



步骤 11 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加** (+) 以创建新的网络对象。

步骤 12 设置身份规则条件，如中所述 身份规则条件，第 2215 页。

步骤 13 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联，第 1719 页中所述。

步骤 14 将配置更改部署到托管设备；请参阅部署配置更改，第 180 页。

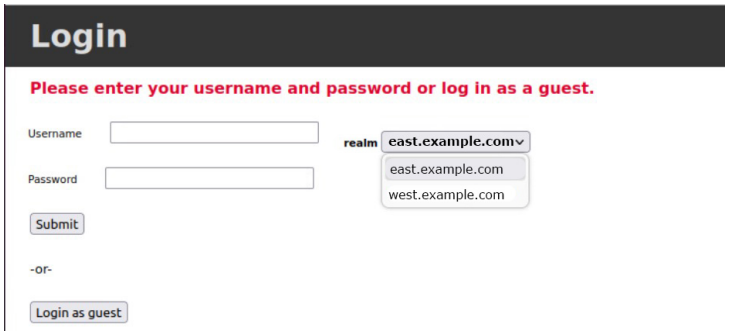
使用主动身份验证规则创建示例身份策略

关联的任务显示使用**主动身份验证**规则配置身份策略的示例，其中使用领域或领域序列执行身份验证。

差异如下：

- 领域 是您可以使用任何受支持的身份验证类型（当前， **HTTP Basic**、 **NTLM**、 **Kerberos**、**HTTP Negotiate**或 **HTTP Response Page**）。
- 领域序列 将您限制为仅 **HTTP Basic** 或 **HTTP 响应页面** 身份验证类型。

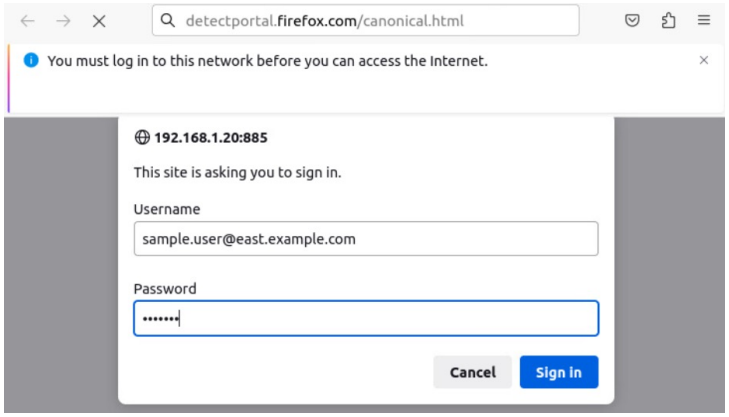
  使用领域序列和 HTTP 响应页面身份验证类型进行身份验证的用户默认会看到以下内容：



  用户可以通过以下任何一种方式进行身份验证：

  - 如果显示领域序列中的领域列表（如图所示），则用户必须在提供的字段中输入用户名和密码，然后从列表中点击其领域名称。
  - 如果领域未显示在列表中，则用户可以按照 `username@domain` 格式输入其凭证。

  使用领域和 HTTP 基本身份验证页面进行身份验证的用户会看到以下内容：



用户必须以 `username@domain` 格式来输入其用户名。

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 点击**新建策略 (New Policy)**。

步骤 4 输入策略的 **名称** 和可选 **说明**。

步骤 5 点击**保存**。

步骤 6 点击**主动身份验证**选项卡。

步骤 7 输入以下信息：

- **服务器证书**：从列表中，点击要用于与 Firewall Threat Defense 设备安全连接的内部证书对象，或点击 **添加** (+) 以添加一个。
- **要重定向到的主机名**：（可选。）从列表中，点击要将强制网络门户请求重定向到的网络对象。如果省略此值，请求将重定向到托管设备的 IP 地址。点击 **添加** (+) 以创建新的网络对象。有关详细信息，请参阅重定向到主机名的网络规则条件，第 2216 页。

  托管设备必须启用 Snort 3 才能使用此选项。
- **端口**：输入要供强制网络门户使用的端口。此端口对于强制网络门户必须是唯一的，并且必须与您设置的访问控制规则相匹配，如创建TCP端口访问控制规则，第2068页中所述。（默认值为 885。）
- **最大登录尝试次数**：输入登录失败前的最大登录尝试次数。（默认值为 3。）
- **跨防火墙共享主动身份验证**：取消选中以便让 Firewall Management Center 强制要求用户在每次使用与上次不同的托管设备访问您的网络时重新进行身份验证。

  有关此选项的详细信息，请参阅强制网络门户字段，第 2073 页。
- **主动身份验证响应页面**：为强制网络门户用户选择系统提供的或自定义的登录页面。有关您的选项的更多信息，请参阅强制网络门户字段，第 2073 页。

步骤 8 点击 **保存** 保存身份策略的更改。

步骤 9 点击**规则**选项卡。

步骤 10 点击**添加规则 (Add Rule)**。

步骤 11 为规则输入**名称 (Name)**。

步骤 12 从列表中，点击 **主动身份验证**。

步骤 13 点击 **领域和设置** 选项卡页面，然后继续以下部分之一。

下一步做什么

继续执行以下部分之一：

- 使用领域进行主动身份验证， 第 2228 页
- 使用领域序列的主动身份验证， 第 2229 页

使用领域进行主动身份验证

此任务讨论如何使用领域和任何可用的身份验证协议（当前为 **HTTP Basic**、**NTLM**、**Kerberos**、**HTTP Negotiate** 或 **HTTP Response Page**）对强制网络门户用户进行身份验证。

开始之前

完成 使用主动身份验证规则创建示例身份策略， 第 2226 页中讨论的任务。

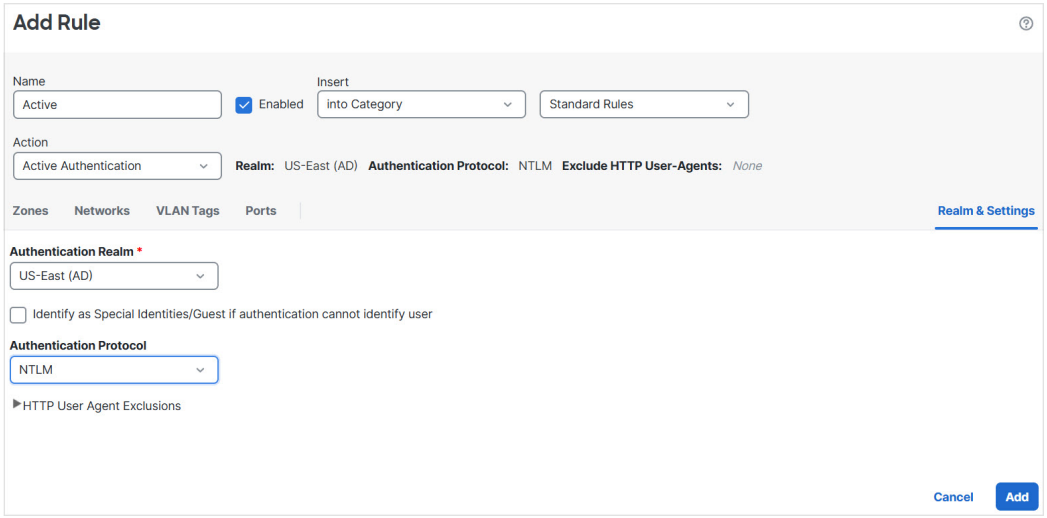
过程

步骤 1 继续 使用主动身份验证规则创建示例身份策略， 第 2226 页。

步骤 2 在**领域和设置 (Realms & Settings)** 选项卡页面中，点击**美国东部 (US-East)**。

步骤 3 在**身份验证协议 (Authentication Protocol)** 列表中，点击 **NTLM**。

下图显示了一个示例。



如果您选择一个领域（如示例中），则系统会搜索该领域以查找与规则匹配的用户。如果未找到用户，则会将该用户标识为“未知”(Unknown)。

步骤 4 点击**添加 (Add)**。

步骤 5 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加** (+) 以创建新的网络对象。

步骤 6 设置身份规则条件，如中所述 身份规则条件，第 2215 页。

步骤 7 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联，第 1719 页中所述。

步骤 8 将配置更改部署到托管设备；请参阅部署配置更改，第 180 页。

使用领域序列的主动身份验证

此任务讨论如何使用领域序列对强制网络门户用户进行身份验证，这会将您限制为 **HTTP 基本**或 **HTTP 响应页面**身份验证协议。

开始之前

完成 使用主动身份验证规则创建示例身份策略，第 2226 页中讨论的任务。

过程

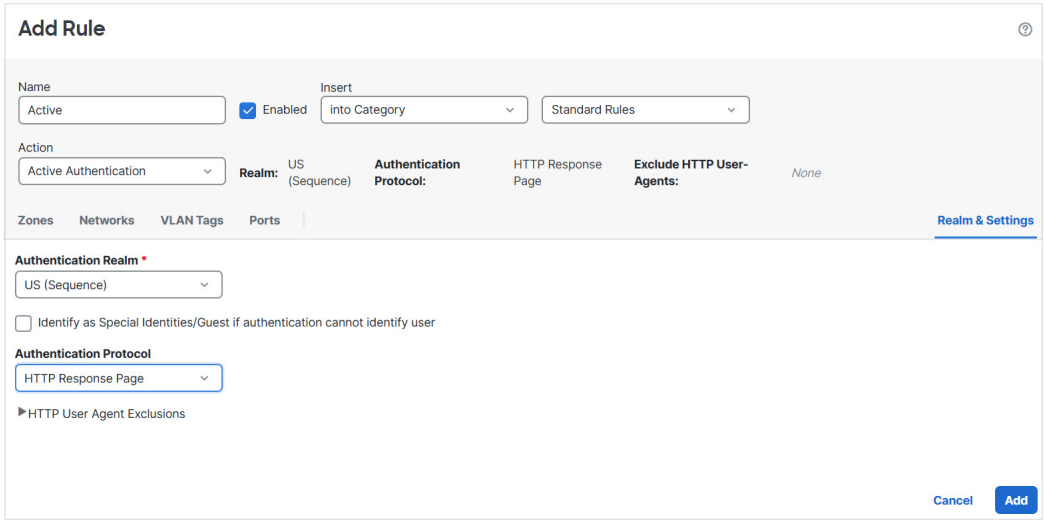
步骤 1 继续 使用主动身份验证规则创建示例身份策略，第 2226 页。

步骤 2 在 **领域和设置** 选项卡页面上，点击列表中的领域的名称。

步骤 3 从列表中，点击**美国东部 (US-East)**。

步骤 4 从**协议 (Protocol)** 列表中，点击 **HTTP 响应页面 (HTTP Response Page)**。

下图显示了一个示例。



如果选择了领域序列（如本例所示），系统会按照领域序列中指定的顺序来搜索序列中的领域。序列中的第一个领域可以称为默认领域；如果用户没有更改，则会使用该领域。如果未找到用户，则会将该用户标识为“未知”(Unknown)。

（仅当您从较早版本升级到版本 7.4.1 时。）编辑 HTTP 响应页面，使其显示序列中的领域列表，如更新自定义身份验证表单，第 2068 页中所述。

步骤 5 点击**添加 (Add)**。

步骤 6 （可选。）要按网络对象过滤流量，请点击**身份源 (Identity Source)** 选项卡。从列表中，点击要用于过滤此身份策略流量的网络对象。点击 **添加** (+) 以创建新的网络对象。

步骤 7 设置身份规则条件，如中所述 身份规则条件，第 2215 页。

步骤 8 将身份规则与访问控制规则相关联，如 将其他策略与访问控制相关联，第 1719 页中所述。

步骤 9 将配置更改部署到托管设备；请参阅部署配置更改，第 180 页。

管理身份策略

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 要删除策略，请点击 **删除** (🗑)。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 要编辑策略，请点击策略旁边的 **编辑** (✎) 并进行更改，如创建身份策略，第 2213 页中所述。 如果显示**视图** (👁)，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 5 要复制策略，请点击 **复制** (⧉)。

步骤 6 要生成该策略的报告，请点击 **报告** (📋)，如生成当前策略报告，第 198 页中所述。

步骤 7 要比较策略，请参阅比较策略，第 197 页。

步骤 8 要创建用于组织策略的文件夹，请点击**添加类别 (Add Category)**。

下一步做什么

部署配置更改；请参阅 部署配置更改，第 180 页。

管理身份规则

过程

步骤 1 登录Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **身份**。

步骤 3 点击您要编辑的策略旁边的**编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 如创建身份策略，第 2213 页中所述，要编辑身份规则，请点击 **编辑** () 并进行更改。

步骤 5 要删除身份规则，请点击 **删除** ()。

步骤 6 要创建规则类别，请点击**添加类别**并选择位置和规则。

步骤 7 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

用户控制故障排除

如果您发现意外的用户规则行为，请考虑调整规则、身份源或领域配置。有关其他相关故障排除信息，请参阅：

- 排除 Cisco ISE/ISE-PIC 或思科 TrustSec 问题，第 2101 页
- TS 代理身份源故障排除，第 2208 页
- 强制网络门户身份源故障排除，第 2075 页
- 领域和用户下载故障排除，第 2049 页

针对领域、用户或用户组的规则与流量不匹配

如果将 TS 代理或 ISE/ISE-PIC 设备配置为监控大量用户组，或者如果将大量用户映射到网络上的主机，则系统可能会由于防火墙管理中心用户限制而丢弃用户记录。因此，具有用户条件的规则可能不会按预期与流量匹配。

针对用户组或用户组内的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，则 LDAP 或 Active Directory 服务器必须配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。

针对辅助组中的用户的规则不是按预期与流量匹配

如果配置具有用户组条件的规则，并且该条件包含或排除属于 Active Directory 服务器中辅助组的成员的用户，则服务器可能会限制其报告的用户数。

默认情况下，Active Directory 服务器会限制它们从辅助群组报告的用户数量。您必须自定义此限制，以便辅助组中的所有用户都报告给 防火墙管理中心并可用于具有用户条件的规则中。

规则与首次发现的用户不匹配

在系统检测到先前未发现的用户的活动后，会从服务器检索其有关信息。直到系统成功检索此信息后，此用户发现的活动才不由匹配规则处理。相反，用户会话由其匹配的下一个规则（或适用时的策略默认操作）处理。

例如，这可能解释以下情形：

- 属于用户组成员的用户与具有用户组条件的规则不匹配。
- 当用于用户数据检索的服务器是 Active Directory 服务器时，由 TS 代理或 ISE 设备报告的用户与规则不匹配。

请注意，这可能会导致系统延迟显示事件视图和分析工具中的用户数据。

规则与所有 ISE/ISE-PIC 用户都不匹配

这是预期行为。可以对由 Active Directory 域控制器进行身份验证的 ISE/ISE-PIC 用户执行用户控制。不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE/ISE-PIC 用户执行用户控制。

使用过多内存的用户和组

如果处理用户和组使用的内存过多，则会显示运行状况警报。请记住，所有用户会话都会传播到 防火墙管理中心 管理的所有设备。如果 防火墙管理中心 管理具有不同内存量的设备，则内存量最少的设备将确定系统可以处理的无错误用户会话数。

无法调整分配给身份进程的内存；即使设备有可用内存，它也可以报告内存不足问题。如果问题仍然存在，您可以选择以下选项：

- 隔离子网上容量较低的托管设备，并将 ISE/ISE-PIC 配置为不向这些子网报告被动身份验证数据。

  请参阅 《*Cisco* 身份服务引擎管理员指南》中关于管理网络设备的章节。

- 取消订阅安全组标记（SGT）。

  有关详细信息，请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法 ， 第 2092 页。

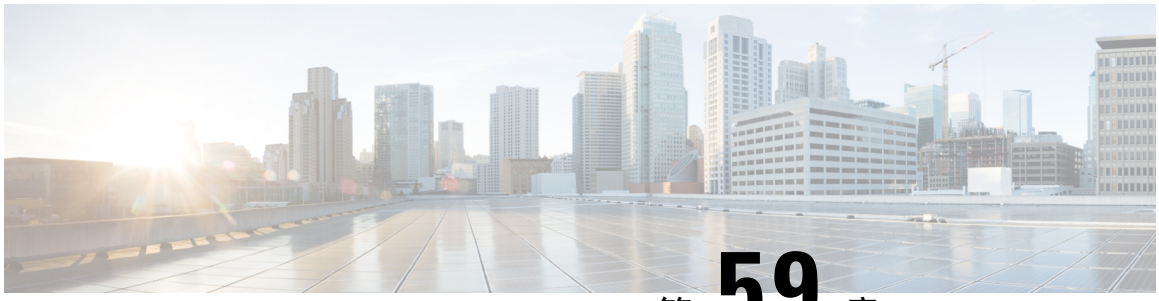
- 将托管设备升级为内存更高的型号。



第 XI 部分

访问控制的高级策略和设置

- 预过滤器策略 ， 第 2235 页
- 安全情报 DNS 策略， 第 2261 页
- 网络恶意软件防护的文件策略， 第 2283 页
- Dynamic Attributes Connector， 第 2325 页
- 威胁情报导向器， 第 2411 页
- 访问控制的高级设置， 第 2455 页
- 服务策略， 第 2473 页
- 威胁检测， 第 2491 页
- 大象流检测， 第 2501 页



第 59 章

预过滤器策略

预过滤策略是应用于传入连接的第一个安全策略。预过滤规则仅根据第 3/4 层条件评估流量，即协议以及源/目标 IP 地址和端口。它们让您有机会就连接做出早期决定，从而避免进一步处理并提高设备性能。

以下主题介绍预过滤策略。

- 关于预过滤器策略， 第 2235 页
- 预过滤策略 的要求和先决条件， 第 2243 页
- 预过滤策略 的准则和限制， 第 2244 页
- 封装流量处理的准则和限制， 第 2244 页
- 快速路径预过滤器的最佳实践， 第 2245 页
- 配置预过滤策略 ， 第 2246 页
- 预过滤器策略示例， 第 2255 页
- 预过滤策略的历史记录， 第 2259 页

关于预过滤器策略

预过滤策略是应用于传入连接的第一个安全策略。预过滤规则仅根据第 3/4 层条件评估流量，即协议以及源/目标 IP 地址和端口。它们让您有机会就连接做出早期决定，从而避免进一步处理并提高设备性能。

使用预过滤器策略实施以下主要操作：

- 提高性能 — 越早排除不需要检查的流量越好。具体而言，您将实现：
  - 分流受信任的流 — 如果设备支持流量分流，请使用预过滤器快速路径操作来识别您信任的、符合分流到 NIC 处理条件的流。这些连接不需要进一步处理，包括检查。请参阅快速路径预过滤器的最佳实践， 第 2245 页 和 大型流量分流， 第 2238 页。
  - 阻止不需要的连接 — 例如，如果您确定要阻止整个子网、整个协议或 TCP/UDP 端口，理想的做法是在预过滤器策略中完成此操作。
- 对纯文本封装隧道进行重新分区，以便可以将其作为访问控制策略中的一个单元进行处理。某些协议（例如 GRE）会创建在隧道内包含许多连接的明文隧道。通过对隧道进行重新分区，可

以为隧道提供一个标记，然后可以在访问控制规则中将该标记选择为源区域/目标区域，从而将自定义入侵规则或其他规则应用于隧道流量。这可以为纯文本隧道提供精细的洞察和控制。

注释 VPN 或其他加密隧道不是明文隧道，因此无法重新分区。

您必须为每个访问控制策略分配一个预过滤策略。但是，系统提供的预定义预过滤器策略可能适合您。

以下主题将详细介绍预过滤策略。

默认预过滤策略

每个访问控制策略都必须有一个分配的预过滤策略。为方便起见，系统包含一个默认预过滤策略，在您创建新的访问控制策略时会自动分配。您不能删除此策略。

默认预过滤策略只做一件事：分析明文封装隧道。这使得访问控制策略能够对隧道中包含的连接采取行动。

您可以改为将默认策略更改为阻止所有明文隧道。请参阅配置默认操作，第 2248 页。

如果您想进行任何其他自定义，包括添加预过滤或隧道规则，您必须创建自己的预过滤策略并将其分配给相应的访问控制策略，如将设备分配给访问控制策略，第 1717 页中所述。

预过滤策略规则顺序

在预过滤策略中，隧道规则、预过滤规则和默认操作处理网络流量：

- 隧道和预过滤规则 - 首先，预过滤策略中的规则按您指定的顺序处理流量。隧道规则仅匹配特定隧道。预过滤规则具有更广泛的约束范围。

  规则按从上到下的顺序匹配，最先匹配的规则获胜。因此，规则顺序至关重要。例如，您可能想要阻止整个子网，但允许该子网中的两个特定 IP 地址。在这种情况下：

  - 第一条规则应将这两个允许的 IP 地址指定为源网络，规则动作为分析。来自这两个 IP 地址的连接将匹配此规则，不会处理下一条规则。
  - 下一条规则应将整个子网指定为源网络，规则动作为“阻止”。

  有关详细信息，请参阅隧道与预过滤器规则，第 2237 页。

- 默认操作（仅限隧道）- 如果隧道不与任何规则匹配，则对隧道应用默认操作。默认动作可以阻止这些隧道，或继续对其各自的封装连接进行访问控制（分析动作）。

  没有用于未封装流量的默认操作。如果未封装的连接与任何预过滤规则都不匹配，系统将继续进行访问控制。这些连接随后可能会被其他策略阻止，或最终被允许。

更改规则顺序

如果您需要更改规则顺序，您可以：

- 将规则拖放到正确位置。
- 右键点击规则并**剪切**，然后找到正确位置，右键点击并选择**粘贴到上方**或**粘贴到下方**。
- 编辑规则并使用**插入**控件更改其位置。

隧道与预过滤器规则

配置隧道规则还是预过滤器规则取决于要匹配的特定流量类型和要执行的操作或进一步分析。

特征	隧道规则	预过滤器规则
主要功能	对明文传递隧道快速使用快速路径、加以阻止或重新分区。	对从早期处理中受益的其他任何连接快速使用快速路径或加以阻止。
封装和端口/协议条件	封装条件只与所选协议上的明文隧道匹配：GRE、IP-in-IP、IPv6-in-IP、Toredo。	与隧道规则相比，端口规则可以使用范围更广泛的端口和协议限制；请参阅端口、协议和 ICMP 代码规则条件，第 1422 页。
网络条件	隧道终端条件限制要处理的隧道的终端。	网络条件限制每个连接中的源主机和目标主机。
方向	双向或单向（可配置）。 默认情况下，隧道规则是双向的，这样便于它们处理隧道终端之间的所有流量。	仅单向（不可配置）。 预处理器规则只与源到目标流量匹配。还允许允许连接的返回流量。
对会话进行重新分区以便进一步分析	支持，使用隧道区域；请参阅使用隧道区域在隧道级别应用访问控制，第 2238 页。	不适用。

系统如何处理明文隧道

某些协议（如 GRE）会创建包含（或封装）多个内部连接的纯文本（未加密）隧道。这些连接可能在不连续的网络之间传输。这些隧道对通过 IP 网络的路由自定义协议、通过 Ipv4 网络的 IPv6 流量等尤其有用。

因此，明文隧道有两组 IP 报头：

- 外部报头 — 外部封装报头指定隧道端点（隧道两端网络设备的路由接口）的源 IP 地址和目标 IP 地址。

  预过滤策略使用外部报头处理流量。在此阶段，您可以阻止或通过快速路径放行整个明文直通隧道。

- 内部报头 — 内部负载报头指定封装连接实际端点的源 IP 地址和目标 IP 地址。隧道内的每个连接都有独立的报头。

  您分析的任何隧道（即未被阻止或使用快速路径）都会暴露这些内部报头，以供其余安全策略及其他功能（如 QoS）使用。这些功能使用最深可检测的报头层级，确保实现最精细的检测与处理。这可防止恶意行为者在明文隧道中隐藏非法流量。

对于常规非隧道连接，仅存在“外部”报头，因为连接不包含任何从属连接。

若您完全不允许明文隧道，可将预过滤策略的默认操作设为阻止所有明文隧道。此阻止不适用于 VPN 等加密隧道。

或者，您可使用隧道区域重新标记隧道流量，以便专门为该隧道编写访问控制规则。这样，您可以针对隧道内的连接定制入侵检测或其他第 7 层过滤。请参阅使用隧道区域在隧道级别应用访问控制，第 2238 页。

使用隧道区域在隧道级别应用访问控制

如系统如何处理明文隧道，第 2237 页中所述，一旦明文隧道连接通过预过滤策略，访问控制策略将对隧道内的每个连接应用其规则。

但是，您可能希望对隧道内的所有连接应用相同策略。例如，您可能有想要用于隧道连接的特殊入侵策略。

为使访问控制规则能应用于隧道内的所有连接，必须使用预过滤策略对隧道重新分区。重新分区会给明文隧道应用一个隧道区域标记。然后，在定义访问控制规则的源接口条件时，可以使用该隧道区域代替安全区域。

由于隧道区域不包含接口，隧道进入设备的源接口与之无关。您可以将隧道区域标记应用于通过不同接口进入设备的多个不同隧道，并让访问控制以相同方式处理它们。



注释 重新分区后的隧道中的连接不匹配访问控制规则中的安全区域约束。对隧道重新分区后，访问控制规则可根据其新分配的隧道区域匹配其封装的连接，但无法匹配任何原始安全区域。

请参阅如何为重定区域隧道进行自定义检测，第 2255 页，了解隧道区域实施逐步指导，以及在不显式处理重新分区流量时对重新分区的影响的讨论。

大型流量分流

对于以下型号，通过预过滤器策略配置为快速路径的部分流量将由硬件（具体为网卡）处理，而非由 Firewall Threat Defense 软件处理。

- Firepower 4100/9300
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

- Cisco Secure Firewall 6100

分流这些流量可获得更高吞吐量与更低延迟，尤其适用于大文件传输等数据密集型应用。此功能对于数据中心尤为有用。这称为静态数据流分流。

此外，默认情况下设备会根据包括信任在内的其他条件分流流量。这称为动态数据流分流。

已分流数据流会继续接收受限的状态检测，例如基础 TCP 标志和选项检查。如有必要，系统可以有选择地将数据包上报至防火墙系统以进行进一步处理。

可以从分流大流量中受益的应用示例如下：

- 高性能计算（HPC）研究站点，防火墙部署在存储设施与高性能计算站之间。当一个研究站点使用 NFS 上的 FTP 文件传输或文件同步进行备份时，大量数据流量会影响所有连接。对 NFS 上的 FTP 文件传输或文件同步分流可降低对其他流量的影响。
- 高频交易 (HFT) 站点，防火墙部署在工作站与交易所之间，主要出于合规目的。通常无需担心安全问题，但延迟是一个重大问题。

可以分流以下数据流：

- （仅限静态数据流分流。）按预过滤器策略使用快速路径的连接。
- 仅有标准或 802.1Q 标记的以太网帧。
- 集群非对称流 (Cisco Secure Firewall 4200)。对于不对称流，集群重定向允许转发节点将流量分流到硬件上。当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。
- （仅限动态数据流分流）：
  - 检测引擎认定无需再检测的已检测数据流。这些数据流包括：
    - 由应用“信任”操作且仅基于安全区域、源和目标网络以及端口匹配的访问控制规则处理的流。
    - 未选择使用 a 解密策略 进行解密的 TLS/SSL 流。
    - 明确受智能应用绕行 (IAB) 策略信任或由于超出数据流绕行阈值而受其信任的数据流。
    - 与文件或入侵策略相匹配而受其信任的数据流。
    - 不再需要检查的任何允许的流。
  - 以下 IPS 预处理器检测的数据流：
    - SSH 和 SMTP。
    - FTP 预处理器辅助连接。
    - 会话初始协议 (SIP) 预处理器辅助连接。
  - 使用关键字的入侵规则（也称为选项）



重要事项 有关上述内容的详细信息、例外情况和限制，请参阅流量卸载限制，第 2240 页。

使用静态流量分流

要将符合条件的流量卸载到硬件上，请创建应用**快速路径 (Fastpath)** 操作的预过滤器策略规则。为 TCP/UDP 使用预过滤器规则，并为 GRE 使用隧道规则。

(Not recommended.) 要禁用流量分流，请使用 FlexConfig：

- 禁用静态（及动态）流量分流：**no flow-offload enable**
- 重新启用流量分流：**flow-offload enable**
- 禁用集群重定向：**no flow-offload cluster-redirect**

有关详细信息，请参阅*Cisco Secure Firewall ASA 系列命令参考*。

使用动态流量分流

动态数据流分流默认启用。但是，无论是否配置预过滤，仅当启用静态流量分流时才会发生动态分流。

要禁用动态流量分流，请使用设备 CLI：

- 禁用动态分流：**configure flow-offload dynamic whitelist disable**
- 重新启用动态分流：**configure flow-offload dynamic whitelist enable**

流量卸载限制

并非所有数据流都可分流。即使在分流后，在某些情况下可取消对数据流的分流。以下是一些限制条件：

设备限制

以下设备支持此功能：

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100
- Firepower 4100/9300

无法分流的数据流

以下数据流类型无法分流。

- 任何不使用 IPv4 寻址的流，例如 IPv6 寻址。
- 除 TCP、UDP 和 GRE 之外的任意协议的数据流。



注释 无法分流 PPTP GRE 连接。

- 被动、内联或内联分流模式下配置的接口上的数据流。仅支持已路由和已交换的接口类型。
- （3100/4200/6100。）根据隧道流量的内部信头进行分流。
- （3100/4200。）多实例分流。
- 需要由Snort或其他检查引擎检查的数据流。在某些情况下（例如FTP），虽然无法分流控制通道，但可以分流次要数据通道。
- 在设备上终止的 IPsec 和 TLS/DTLS VPN 连接。
- 需要加密或解密的数据流。例如，由于 a 解密策略 而解密的连接。
- 路由模式下的组播数据流。如果桥接组中只有两个成员接口，则它们在透明模式下受支持。
- TCP 拦截数据流。
- TCP 状态绕过流。不能在同一流量上配置数据流分流和 TCP 状态绕行。
- 使用安全组标记的数据流。
- 从不同集群节点转发来的逆向数据流（在集群中数据流不对称的情况下）。
- 集群中的集中数据流（如果数据流的所有者不是控制设备）。
- 无法动态分流包含 IP 选项的数据流。

其他限制

- 流分流与死连接检测 (DCD) 不兼容。不要在可分流的连接上配置 DCD。
- 在 Firepower 4100 和 9300 上，如果多个与数据流分流条件匹配的数据流排队等待同时分流到硬件上的同一位置，则只会分流第一个数据流。其他数据流则会照常处理。这称为冲突。在 CLI 中使用 **show flow-offload flow** 命令显示此情况的统计信息。

  在 3100/4200/6100 上，Cuckoo 散列技术用于以更有效的方式在内部解决散列冲突，因此 **show flow-offload flow** 命令不会显示冲突计数器统计信息的任何增量。
- 动态数据流分流会禁用所有 TCP 规范器检查。
- 虽然分流的数据流通过FXOS接口，但这些数据流的统计信息不会显示在逻辑设备接口上。因此，逻辑设备接口计数器和数据包速率不会反映分流流量。

集群重定向

当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称流量会在集群控制链路上产生大量流量，因此分流这些流量可以提高性能，例如，对于分布式站点间 VPN 模式。此功能支持以下模式：

- Cisco Secure Firewall 4200

- 路由和透明模式
- 跨区以太网通道模式

逆向分流的条件

数据流被卸载后，如果流中的数据包满足以下条件，将被返回给防火墙操作系统进行进一步处理：

- 数据包包含时间戳以外的 TCP 选项。
- 数据包经过分段。
- 它们会进行等价多路径 (ECMP) 路由，并且入口数据包会从一个接口移至另一个接口。
- 路由表的变更会应用到该流。数据包返回设备以确定新的路由。

预过滤器与访问控制策略

预过滤和访问控制策略都允许您阻止和信任流量，但预过滤“信任”功能被称为“快速路径”，因为它会跳过更多检查。下表解释了预筛选策略和访问控制策略之间的这些区别以及其他区别，以帮助您决定是否配置自定义预筛选策略。

如果不配置自定义预过滤策略，则只能在访问控制策略中使用早期放置的“阻止”和“信任”规则来接近而非复制预过滤功能。

特征	预过滤器策略	访问控制策略
主要功能	对特定类型的明文、直通隧道快速使用快速路径或加以阻止，或针对其封装的流量定制后续检查。 对从早期处理中受益的其他任何连接使用快速路径或加以阻止。	使用简单或复杂的条件检查和控制所有网络流量，包括情景信息和深度检查结果。
访问控制中的序列	首先。 在所有其他访问控制配置之前，系统会将流量与预过滤条件匹配。 因此，预过滤器策略中的快速路径会跳过许多其他策略和检查。	最后。 在评估访问控制规则之前，会应用可能检查连接的其他策略，包括安全智能和解密。
规则操作	更少。 您可以停止进一步检查（快速路径和阻止），或对其余访问控制允许进一步分析（分析）。	更多。 访问控制规则有更广泛的操作，包括监控、深度检查、阻止并重置和交互式阻止。请参阅访问控制规则操作，第 1748 页。

特征	预过滤器策略	访问控制策略
绕过功能	快速路径规则操作。 在预过滤阶段为流量使用快速路径可绕过所有进一步检查和处理，包括： • 安全智能 • 用户身份发现（身份策略） • 解密 • 访问控制规则 • 对数据包负载的深度检验 • 发现 • 速率限制	信任规则操作。 受访问控制规则信任的流量只能免于入侵检查和发现。如果另一个需要检查的策略应用于最终被信任的连接，则无论如何都会对该连接进行检查。 信任其实只是意味着您没有对连接应用入侵或文件策略。
规则条件	限制版。 预过滤策略中的规则使用简单网络条件：IP 地址、VLAN 标记、端口和协议。 对于隧道，隧道终端条件会指定隧道任一端上网络设备的路由接口的 IP 地址。	强健。 访问控制规则使用网络条件，但同时也采用用户、应用、请求的 URL 和数据包负载中可用的其他情景信息。 网络条件指定源和目标主机的 IP 地址。
使用的 IP 报头（隧道处理）	最外层。 使用外部报头使您可以处理整个明文、直通隧道。 对于未封闭的流量，预过滤仍使用“外部”标头 - 在这种情况下，它们是唯一报头。	尽可能在内部。 对于未加密隧道，访问控制作用于其各个封装的连接，而不是作用于整个隧道。 请参阅系统如何处理明文隧道，第 2237 页。
对封装的连接重新分区以进行进一步分析	重新分区隧道传输的流量。 隧道区域允许您对预过滤的封装流量定制后续检查。	使用隧道区域。 访问控制使用在预过滤期间分配的隧道区域。请参阅使用隧道区域在隧道级别应用访问控制，第 2238 页。
连接日志记录	仅使用快速路径和阻止的流量。允许的连接仍然可由其他配置进行记录。	任何连接。

预过滤策略 的要求和先决条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

预过滤策略 的准则和限制

- 您可以记录被预过滤策略使用快速路径或阻止的连接。预过滤连接事件包含有关记录的连接（包括整个隧道）是否被预过滤以及如何预过滤的信息。但是，由于被快速路径和阻止的连接不进行深度检查，因此关联的连接事件包含的信息有限。
- 访问控制使用基于分层的实施，完善了多租户策略。除了其他高级设置之外，您还可以锁定预过滤策略关联，在所有子代访问控制策略中实施该关联。有关详细信息，请参阅访问控制策略继承，第 1704 页。
- 部署预过滤策略 时，其规则不会应用于现有连接。因此，现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用规则，请清除现有连接，然后部署策略。
- 对于操作为“快速路径”且日志记录选项已禁用的预过滤规则，您可能会发现系统中仍然会生成流程结束事件。但是，这些事件在管理中心事件页面上不可见。

封装流量处理的准则和限制

本主题讨论以下类型的封装流量的准则：

- 通用路由封装 (GRE)
- 点对点协议 (PPTP)。（预过滤策略 中的隧道规则不处理此协议。）
- IPinIP
- IPv6inIP
- Teredo

GRE 隧道限制

GRE 隧道处理仅限于 IPv4 和 IPv6 乘客流。GRE 隧道内不支持其他协议，例如 PPTP 和 WCCP。

GRE v1 和 PPTP 会绕过外部流处理

GRE v1（有时称为状态性 *GRE*）和 PPTP 流量会绕过外部流处理。

IPv6inIP 和 Teredo 支持客流处理，但存在以下限制：

- 会话位于未进行负载均衡的单个隧道上。
- 没有 HA 或集群复制。
- 不维护主要和辅助流关系。
- 不支持预过滤策略白名单和黑名单。

GRE v0 序列号字段必须为可选

在网络上发送流量的所有终端都必须发送带有可选序列号字段的GREv0流量；否则，序列号字段会被删除。RFC 1701 和 RFC 2784 都将序列字段指定为可选。

隧道如何与接口配合使用

预过滤器和访问控制策略规则适用于路由、透明、内联集、内联分流和被动接口上的所有隧道类型。

参考资料

有关 GRE 和 PPTP 协议的详细信息，请参阅以下内容：

- RFC 1701、RFC 2784 和 RFC 2890（GRE 协议 v0）
- RFC 2637（PPTP 和 GRE 协议 v1）

快速路径预过滤器的最佳实践

在预过滤器规则中使用快速路径操作时，匹配的流量会绕过检查并直接通过设备进行传输。请对您可以信任但不会受益于任何可用安全功能的流量使用此操作。

以下类型的流量是快速路径的理想选择。例如，您可以将规则配置为对来自或到达终端或服务器的 IP 地址的任何流量进行快速路径处理。您可以根据使用的端口来进一步限制规则。

- 通过设备的 VPN 流量。也就是说，该设备不是 VPN 拓扑中的终端。
- 内部网络上受信任终端之间的 SQL 流量。
- 扫描程序流量。扫描程序探测可以从入侵策略中创建大量误报响应。
- 语音/视频。
- 备份。
- 流经 Firewall Threat Defense 设备的管理流量 (sftunnel)。对管理流量执行深度检查（使用访问控制策略）可能会导致问题。您可以根据管理中心和托管设备之间的端口 TCP/8305 进行预过滤。

配置预过滤策略

要执行自定义预过滤，请配置预过滤策略并将策略分配给访问控制策略。预过滤器策略是通过访问控制策略分配给托管设备的。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

过程

步骤 1 选择**策略** > **安全策略** > **预过滤器**。

在页面顶部，有一些相关功能的便捷链接：对象管理和访问控制。

从预过滤页面或在编辑预过滤策略时无法判断它是否由访问控制策略使用或哪些策略在使用。

步骤 2 执行以下任一操作：

- 创建 — 点击**新建策略**以创建自定义预过滤策略 。系统会提示您输入名称，并可选择性地添加描述。点击**保存**后，系统将打开新策略进行编辑。新的预过滤器策略不包含规则及“分析所有隧道流量”(Analyze all tunnel traffic) 这一默认操作。
- 编辑 — 点击 **编辑** (✎) 打开策略，以便添加规则或以其他方式修改策略。
- 复制 - 点击 **复制** (⧉)。系统将提示您输入名称。点击**确定**时，副本将添加到列表中，但不会打开副本进行编辑。
- 删除 — 点击 **删除** (🗑) 可删除策略。不能删除当前正在用于访问控制策略的策略。

步骤 3 编辑预过滤策略时，您可以执行以下操作：

- 设定默认操作 — 在策略的底部设定隧道的默认操作。请参阅配置默认操作，第 2248 页。
- 添加预过滤器规则—点击**添加预过滤器规则**。规则会被添加到策略底部。请参阅配置预过滤规则，第 2248 页。
- 添加隧道规则—点击**添加隧道规则**。规则会被添加到策略底部。请参阅配置隧道规则，第 2251 页。
- 插入规则—右键点击之前要添加新规则的规则，然后根据需要选择**插入新预过滤规则**或**插入新隧道规则**。
- 复制/剪切并粘贴规则 — 要复制规则，请右键点击规则并选择**复制**。您还可以通过选择**剪切**来剪切（将其删除）规则。然后，选择要插入规则的位置，右键点击并选择**粘贴到上方**或**粘贴到下方**。复制时，系统会在规则名称中添加一个用括号括起来的数字；您应根据需要编辑规则并更改名称和其他条件。剪切规则保留原始名称。

- 编辑规则 — 点击 **编辑** (✎) 以打开规则编辑器。您还可以点击表中规则的任何元素。请参阅配置预过滤规则，第 2248 页 和 配置隧道规则，第 2251 页。
- 删除规则 — 点击 **删除** (🗑) 可删除规则。
- 移动规则 — 点击规则并将其拖放到正确的位置。或者，剪切规则，然后将其粘贴到正确的位置。您还可以在编辑规则时更改规则位置。

  正确创建规则并将其排序是一项复杂的任务，但却是构建有效部署的一项重要任务。如果您未缜密地计划，有些规则可能会抢占其他规则，或者包含无效的配置。有关详细信息，请参阅预过滤策略规则顺序，第 2236 页。
- 将预过滤规则移动到关联的访问控制策略 — 要将预过滤规则从预过滤策略移动到关联的访问控制策略，请右键点击规则并选择**移动到其他策略**。您不能将隧道规则移至访问控制策略。请参阅将预过滤器规则移至访问控制策略，第 2254 页。
- 命中计数 — 要查看有关与每个规则匹配的连接数的统计信息，请点击**分析命中计数**。请参阅查看规则命中计数，第 1721 页。
- 搜索规则 — 使用**搜索规则**框执行纯文本搜索。输入字符串并按 Enter 键。搜索框会显示匹配项数，以及用于在匹配项之间移动的上/下按钮。

  匹配项会在表中突出显示。匹配包括部分匹配，但仅限于显式设置的项目。例如，输入“any”与默认网络不匹配，但输入“any-ipv4”将会匹配，因为它是网络对象，而不是被动默认网络。操作和规则类型与搜索字符串不匹配。
- 查看对象详细信息 — 要查看规则中使用的对象的内容，请右键点击该对象，然后选择**对象详细信息**。
- 更改策略说明 — 要修改策略的说明，请点击页面顶部策略名称下方的说明文本。点击离开说明以保存更改。

确保点击**保存**以保存所做的任何更改。

步骤 4 在相应的访问控制策略中使用预过滤策略。

对于应使用自定义预过滤策略的每个访问控制策略：

- 编辑访问控制策略，并在**预过滤策略**链接或高级设置中选择预过滤策略。请参阅将其他策略与访问控制相关联，第 1719 页。
- 如果在任何隧道规则中应用了隧道区域标记，请创建将这些隧道区域用作源接口条件的访问控制规则。

下一步做什么

现在可以部署更改。

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅时区，第 1031 页。

配置默认操作

使用默认操作确定应如何处理不匹配任何隧道规则的明文封装隧道。

默认操作不适用于非隧道流量。不匹配预过滤器规则的任何其他连接将由后续策略进行处理。

过程

步骤 1 选择 **策略** > **安全策略** > **预过滤器** 并创建或编辑预过滤策略。

步骤 2 选择**默认操作：隧道流量**选项：

1. **分析所有隧道流量** — 允许这些隧道，并由访问控制和其他策略评估其封装连接。

   阻止所有隧道流量 — 将丢弃隧道，且不再评估隧道。

步骤 3 如果选择**阻止所有隧道流量**，请点击默认操作旁边的 **日志记录**（）。

请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用策略默认操作记录连接 您只能为被阻止的隧道配置默认操作日志记录。

配置预过滤规则

在非默认的预过滤策略中使用预过滤规则，为不需要的流量提供早期阻断，并为无法从访问控制检查中获益的流量提供快速路径。

如果您的设备支持流量卸载，快速路径流量在满足所有其他条件的情况下有资格进行流量卸载。请参阅大型流量分流，第 2238 页。

开始之前

您无法在默认预过滤策略中创建规则。如果尚未创建自定义预过滤策略，请立即创建。

过程

步骤 1 选择 **策略** > **安全策略** > **预过滤器** 并创建或编辑预过滤策略。

步骤 2 点击**添加预过滤规则**。

您也可以右键点击规则并选择**插入新预过滤规则**。

步骤 3 为规则输入**名称 (Name)**。

步骤 4 选择规则是否应**已启用**。必须启用规则才能影响通过设备的流量。

步骤 5 选择应用于匹配流量的**操作**。

- Fastpath - 让匹配流量免于进行进一步的各项检查和控制，包括访问控制、身份要求和速率限制。如果设备支持，这些连接符合流卸载条件。
- 阻止 - 阻止匹配流量，不进行任何类型的进一步检查。
- 分析 — 允许流量继续由其余访问控制策略进行分析。即使流量被访问控制和所有相关深度检查放行，也可能会受到速率限制。

步骤 6 选择**插入**规则的位置。

默认是在策略末尾插入规则，但您可以选择现有规则并在该规则之前或之后插入新规则。列表中与连接匹配的第一条规则将应用于该连接，因此顺序至关重要。

步骤 7 （可选。）选择定义规则**时间范围**的对象。

您可以限制规则在一天中的哪些时段或哪些天生效。例如，规则可以仅在工作时间内生效。选择现有的时间范围对象或创建新的时间范围对象。有关详细信息，请参阅创建时间范围对象，第 2702 页。

步骤 8 配置规则的流量匹配条件。

该规则适用于匹配所有条件的连接。在条件类型内，各元素之间是“或”(OR) 关系，即匹配任一选定项即视为匹配。对于整个规则，所有条件类型之间是“与”(AND) 关系：连接必须匹配每个选项卡上的至少一个项目才能匹配该规则。您可以使用以下类型的条件：

- **接口对象** — 选择包含应应用该规则的接口的安全区域或接口组。默认情况下（未选择对象），规则将应用于设备上的所有接口。
- **网络** — 选择定义源（**添加到源**）和/或目标（**添加到目标**）IP 地址或两者的网络对象。默认情况（未选择对象）匹配所有源和目标 IP 地址。
- **VLAN 标记** — 选择定义应应用该规则的 VLAN 的对象。有关详细信息，请参阅VLAN 标记规则条件，第 2250 页。
- **端口** — 选择用于连接的 TCP/UDP 端口或其他协议，并将其添加到源或目标条件。源条件仅限 TCP/UDP，但您可以为目标选择其他协议。有关详细信息，请参阅预过滤规则的端口规则条件，第 2250 页。

步骤 9 （仅限快速路径和阻断规则。）点击**日志记录**，并配置匹配连接的记录方式。

有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用隧道和预过滤器规则记录连接。

步骤 10 （可选。）点击**注释**，并向规则添加注释。使用注释来帮助您理解规则的用途及其变更历史。

步骤 11 点击**添加 (Add)**。如果需要移动规则，请立即执行。

步骤 12 点击**保存** 保存策略。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

预过滤规则的端口规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。仅支持 TCP 和 UDP 源端口。您也可以将它们指定为目标端口。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。当选择 ICMP 作为目标端口时，系统会提示您指定类型和代码。
- 协议-您可以借助于未使用端口的其他协议控制流量。并非所有协议都支持。您必须选择协议作为目标端口。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以配置端口条件以匹配预过滤器规则中的其他协议，但在匹配 GRE、IP in IP、IPv6 in IP 和 Toredo 端口 3544 时，应改为使用隧道规则。

配置隧道规则

在非默认预过滤策略中使用隧道规则：

- 为不需要的封装隧道流量提供早期阻断。
- 对无法从访问控制检查中获益的隧道进行快速路径处理。
- 将封装隧道放入隧道区域（称为重新分区），以便编写访问控制规则，将检测应用于隧道内的整体连接。

开始之前

预过滤策略的默认操作适用于封装隧道。因此，仅为隧道流量创建规则，以便对特定隧道应用不同的操作。

例如，如果默认操作是分析隧道，则意味着所有隧道都将传递给访问控制策略以及其他进行检查、允许并可能阻断连接的策略，这些策略将评估内层连接。如果该默认操作正是您对所有隧道的期望，则无需创建任何隧道规则。

反之：

- 如果默认操作是阻断封装隧道，请使用规则使特定隧道免于阻断，并将其传递给其他访问控制策略（分析操作）或绕过任何额外处理（快速路径）。
- 对于某些您希望对其中所有封装连接应用访问控制规则的隧道，请创建规则将隧道重新分区到相应的隧道区域标记，并在访问控制策略中为这些隧道区域标记编写规则。

过程

步骤 1 选择 **策略** > **安全策略** > **预过滤器** 并创建或编辑预过滤策略。

步骤 2 点击**添加隧道规则**。

您也可以右键点击现有规则并选择**插入新隧道规则**。

步骤 3 为规则输入**名称 (Name)**。

步骤 4 选择规则是否应**已启用**。必须启用规则才能影响通过设备的流量。

步骤 5 选择应用于匹配流量的**操作**。

- Fastpath - 让匹配流量免于进行进一步的各项检查和控制，包括访问控制、身份要求和速率限制。对隧道执行快速路径操作可为所有封装连接提供快速路径。如果设备支持，这些连接符合流卸载条件。

- 阻止 - 阻止匹配流量，不进行任何类型的进一步检查。阻止隧道将阻止所有封装连接。
- 分析 — 允许流量继续由其余访问控制功能使用内层报头进行分析。即使流量被访问控制和所有相关深度检查放行，也可能会受到速率限制。

步骤 6 选择**插入**规则的位置。

默认是在策略末尾插入规则，但您可以选择现有规则并在该规则之前或之后插入新规则。列表中与连接匹配的第一条规则将应用于该连接，因此顺序至关重要。

步骤 7 （仅限分析规则；仅在重新分区时。）如果您的目的是对隧道重新分区，请在**分配隧道区域**中选择隧道区域标记。

如果您希望对隧道内的封装连接应用访问控制而无需特殊处理，请将此选项留空。有关重新分区和隧道组标记的详细信息，请参阅：

- 使用隧道区域在隧道级别应用访问控制，第 2238 页
- 创建隧道区域，第 2253 页
- 如何为重定区域隧道进行自定义检测，第 2255 页

注意
分配隧道区域时应格外小心。在之后进行评估时，重新分区后的隧道中的连接可能与安全区域限制不匹配。请参阅如何为重定区域隧道进行自定义检测，第 2255 页，查看隧道区域实施的简要步骤，以及对在不明确处理重新分区流量的情况下进行重新分区的影响的说明。

步骤 8 （可选。）选择定义规则**时间范围**的对象。

您可以限制规则在一天中的哪些时段或哪些天生效。例如，规则可以仅在工作时间内生效。选择现有的时间范围对象或创建新的时间范围对象。有关详细信息，请参阅创建时间范围对象，第 2702 页。

步骤 9 选择以下选项之一来设置规则的方向：

- **仅从源匹配隧道**（单向）— 仅匹配源到目标的流量。匹配流量必须源自其中一个指定的源接口或隧道终端，并通过其中一个目标接口或隧道终端流出。还允许允许连接的返回流量。（注意：预过滤规则始终是单向的。）
- **从源和目标匹配隧道**（双向）— 同时匹配源到目标的流量和目标到源的流量。其效果与编写两个互为镜像的单向规则相同。这是默认值。

步骤 10 点击**封装和端口**选项卡，然后为此规则选择协议。

您必须在隧道规则中至少选择一个以下选项，以指定所使用的封装协议。该列表包含选项的 IP 协议编号。

- **GRE** (47)
- **IP-in-IP** (4)
- **IPv6-in-IP** (41)
- **Teredo** (UDP (17)/3455)

步骤 11 配置规则的流量匹配条件。

该规则适用于匹配所有条件的连接。在条件类型内，各元素之间是“或”(OR) 关系，即匹配任一选定项即视为匹配。对于整个规则，所有条件类型之间是“与”(AND) 关系：连接必须匹配每个选项卡上的至少一个项目才能匹配该规则。您可以使用以下类型的条件：

- **接口对象**—选择包含应应用该规则的接口的安全区域或接口组。默认情况下（未选择对象），规则将应用于设备上的所有接口。
- **隧道端点** — 定义隧道的源（**添加到源**）和目标（**添加到目标**）IP 地址的网络对象。默认情况（未选择对象）匹配所有源和目标 IP 地址。
- **VLAN 标记** — 选择定义应应用该规则的 VLAN 的对象。有关详细信息，请参阅VLAN 标记规则条件，第 2250 页。

步骤 12 （仅限快速路径和阻断规则。）点击**日志记录**，并配置匹配连接的记录方式。

有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用隧道和预过滤器规则记录连接。

步骤 13 （可选。）点击**注释**，并向规则添加注释。使用注释来帮助您理解规则的用途及其变更历史。

步骤 14 点击**添加 (Add)**。如果需要移动规则，请立即执行。

步骤 15 点击**保存** 保存策略。

创建隧道区域

隧道区域代表您为进行特殊分析而明确标记的特定类型的明文、传递隧道。尽管隧道区域可用作访问控制规则中的接口限制条件，但它并非接口对象，如使用隧道区域在隧道级别应用访问控制，第 2238 页中介绍。

以下步骤介绍如何在对象管理器中创建隧道区域。您还可以在编辑隧道规则时创建区域。

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中，选择**隧道区域**。

步骤 3 点击**添加隧道区域**。

您也可以编辑现有隧道，或删除未在隧道规则中使用的隧道区域。

步骤 4 输入**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

步骤 5 点击**保存**。

下一步做什么

- 作为隧道规则的一部分，将隧道区域分配给明文直通隧道。请参阅配置隧道规则，第 2251 页。
- 将隧道区域用作访问控制规则中的源接口条件。

将预过滤器规则移至访问控制策略

您可以将预过滤器规则从预过滤器策略移至关联的访问控制策略。

开始之前

请在继续之前注意以下条件：

- 只能将预过滤器规则移至访问控制策略。无法移动隧道规则。
- 预过滤规则只能移动到使用预过滤策略的访问控制策略中。由于您可以在多个访问控制策略中使用相同的预过滤策略，因此您需要选择规则应移至的策略。
- 无法移动使用接口组定义接口条件的预过滤器规则。您只能移动使用安全区域的规则或不包含接口条件的规则。
- 移动时，预过滤器规则中的**操作 (Action)** 参数将更改为访问控制规则中的适当操作。
  - 分析 (Analyze) 变为允许 (Allow)。
  - 阻止 (Block) 变为阻止 (Block)。
  - 快速路径 (Fastpath) 变为信任 (Trust)。
- 保留规则中的日志记录配置。
- 移动规则后，预过滤器规则配置中的注释会丢失。但是，新注释会被添加到提及源预过滤器策略的移动规则中。
- 从源策略迁移规则时，如果其他用户修改了这些规则，系统会发出警告。您可以在刷新页面后继续该过程。

过程

步骤 1 在预过滤器策略编辑器中，通过点击鼠标左键来选择要移动的规则。

提示
要选择多条规则，请使用 Shift + 点击。

步骤 2 右键点击所选规则，然后选择**移至另一个策略 (Move to another policy)**。

步骤 3 选择目标访问控制策略，然后点击**添加**以将其添加到所选策略的列表中。

步骤 4 从**放置规则 (Place Rules)** 下拉列表中，选择要放置移动规则的位置：

- 要将其定位为**默认 (Default)** 部分中的最后一组规则，请选择**底部（在“默认”部分中） (At the bottom [within the Default section])**。
- 要将其定位为**必填 (Mandatory)** 部分中的第一组规则，请选择**顶部（在“必填”部分中） (At the top [within the Mandatory section])**。

步骤 5 点击 **移动**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

预过滤器策略示例

以下主题提供了使用预筛选策略的示例。

如何为重定区域隧道进行自定义检测

此操作步骤示例总结了如何对GRE隧道进行重新分区，以便使用隧道区域执行进一步分析。您可以将此示例中描述的概念加以调整并应用到需要根据明文、传递隧道中封装的连接定制流量检查的其他情景中。

设想一种情形，在该情形中，您组织的内部流量流过受信任的安全区域。受信任的安全区域表示部署在不同地方的多个托管设备上的一组接口。您组织的安全策略要求您在对漏洞和恶意软件进行深度检查后允许内部流量。

内部流量有时包含特定终端之间的明文、传递及 GRE 隧道。由于此封装流量的流量配置文件与您“正常”的局间活动（可能为已知且为良性）不同，因此您可以在遵守安全策略的前提下限制对某些封装连接的检查。

在本示例中，部署配置更改后：

- 在受信任区域中检测到的明文、传递和GRE封装隧道各自的封装连接由一组入侵和文件策略评估。
- 受信任区域中的所有其他流量则由另外一组不同的入侵和文件策略评估。

您可以通过对 GRE 隧道进行重新分区来完成这项任务。重新分区可以确保访问控制将 GRE 封装连接与自定义隧道区域（而非其原始的受信任安全区域）关联。鉴于访问控制对封装流量的处理方式，需要进行重新分区；请参阅系统如何处理明文隧道，第 2237 页和使用隧道区域在隧道级别应用访问控制，第 2238 页。

过程

步骤 1 配置根据封装流量定制深度检查的自定义入侵和文件策略，以及专为非封装流量定制的另外一组入侵和文件策略。

步骤 2 配置自定义预过滤，以便对流过受信任安全区域的 GRE 隧道进行重新分区。

创建自定义预过滤器策略并将其与访问控制关联。在此自定义预过滤器策略中，创建隧道规则（在此示例中，隧道规则为 **GRE_tunnel_rezone**）和对应的隧道区域 (**GRE_tunnel**)。有关详细信息，请参阅配置隧道规则，第 2251 页。

表 *123: GRE_tunnel_rezone* 隧道规则

规则组件	说明
接口对象条件	通过将受信任的安全区域同时用作源接口对象和目标接口对象限制来匹配仅内部隧道。
隧道终端条件	为组织中使用的 GRE 隧道指定源终端和目标终端。 默认情况下，隧道规则是双向的。如果不更改**从...匹配隧道 (Match tunnels from...)** 选项，则您将哪些终端指定为源、哪些终端指定为目标都可以。
封装条件	匹配 GRE 流量。
分配隧道区域	创建 **GRE_tunnel** 隧道区域，并将其分配到与规则匹配的隧道。
操作	分析（借助其他访问控制）。

步骤 3 配置访问控制以处理重新分区后的隧道中的连接。

在部署到受管设备的访问控制策略中，确保使用了预过滤策略。然后，配置一条规则（在此示例中为 **GRE_inspection**），以处理您重定区域的流量。有关详细信息，请参阅创建和编辑访问控制规则，第 1764 页。

表 *124: GRE_inspection* 访问控制规则

规则组件	说明
安全区域条件	通过使用 GRE_tunnel 隧道区域作为源区域约束来匹配重定区域的隧道。
操作	允许（已启用深度检查） 选择专门用于检查封装内部流量的文件和入侵策略。

注意
如果您跳过此步骤，重新分区后的连接可能会与不受安全区域限制的**任何**访问控制规则匹配。如果重新分区后的连接与任何访问控制规则都不匹配，则由访问控制策略默认操作处理。请确定您想这么做。

步骤 4 配置访问控制以处理流过受信任安全区域的非封装连接。

在同一访问控制策略中，配置用于处理受信任安全区域中未重新分区的流量的规则（在此示例中，规则为 **internal_default_inspection**）。

***表 125: internal_default_inspection* 访问控制规则**

规则组件	说明
安全区域条件	通过将受信任的安全区域同时用作源区域和目标区域限制来匹配未重新分区的仅内部流量。
操作	允许（已启用深度检查） 选择专门用于检查非封装内部流量的文件和入侵策略。

步骤 5 评估新访问控制规则相对于预先存在的规则的位置。如有必要，请更改规则顺序。

如果将两个新的访问控制规则放在一起，则哪一个规则放在前面都可以。由于您对GRE隧道进行了重新分区，因此，这两个规则无法相互抢占。

步骤 6 保存所有更改。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

如何卸载大型流量

您可以使用预过滤策略来配置静态数据流分流。如果您的硬件型号支持，数据流分流会将符合条件的快速路径连接移交给 NIC 处理，从而避免性能密集型检查。

有些硬件型号会自动识别可分流连接，但您可以通过将连接与预过滤快速路径规则匹配来主动识别符合分流条件的连接。此静态配置可帮助您快速提高确定可以信任的大型连接的性能。

在以下示例中，假定两台服务器已得到充分保护，以便您可以信任它们之间的连接。可能一台服务器正在使用另一台服务器进行备份。因此，您可以为从主服务器 10.100.1.20/24 流向备份服务器 10.100.2.2/24 的任何流量编写快速路径规则。该示例假定可通过常规的物理路由接口访问服务器。

过程

步骤 1 选择 **策略** > **安全策略** > **预过滤器** 并创建或编辑自定义预过滤策略。

步骤 2 点击**添加预过滤规则**。

您也可以右键点击规则并选择**插入新预过滤规则**。

步骤 3 为规则输入**名称 (Name)**。例如，Offload_Server_A。

步骤 4 在**操作**中，选择**快速路径**。

步骤 5 在**插入**中，选择应在其上方或下方插入规则的规则。

您也可以在创建规则后移动规则。

步骤 6 点击**网络**选项卡并指定源服务器和目标服务器。

- 在**源网络**下方的编辑框中，键入 10.100.1.20，然后点击**添加**。
- 在**目标网络**下方的编辑框中，键入 10.100.2.2，然后点击**添加**。

步骤 7 （可选。）为该流量配置其他流量匹配特征。

点击以下选项卡以填写条件。在本示例中，只有“网络”选项卡需要配置，因此请仅当这些设置适合您的情况时才配置这些设置。

- **接口对象** — 定义源接口和/或目标接口的安全区域或接口对象。本示例不需要此规范。
- **VLAN** — 由于此示例使用路由物理接口而不是交换机接口，因此此设置不相关。即使在这些情况下，您也不需要基于 VLAN 限制规则。
- **端口** — 如果要将分流限制为特定 TCP/UDP 端口，则可以指定这些端口。这将规则的范围仅限于这些端口。

步骤 8 （可选。）点击**日志记录**并决定是否要查看匹配流量的系统日志事件。

步骤 9 点击**添加**以添加规则。

如果规则在策略中的正确位置不存在，请花些时间将其移至正确位置。

步骤 10 点击**保存** 保存策略。

下次部署配置时，该规则将应用于目标设备。

预过滤策略的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群重定向：支持Cisco Secure Firewall 4200非对称集群流量的流卸载	10.0.0	10.0.0	对于不对称流，集群重定向允许转发节点将流量分流到硬件上。此功能默认启用，但可以使用 FlexConfig 配置。 当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。 新增/经修改的命令：**flow-offload cluster-redirect** (FlexConfig)、**show conn**、**show flow-offload flow**、**show flow-offload info**。
将预过滤器规则移至访问控制策略	6.7	任意	您可以将预过滤器规则从预过滤器策略移至关联的访问控制策略。 新增/修改的页面：在预过滤器策略页面中，所选规则的右键点击菜单提供了新的**移至另一个策略 (Move to another policy)** 选项。 支持的平台： 防火墙管理中心
基于时间的规则	6.6	任意	能够根据设备的时区确定的日期和时间来应用预过滤器和隧道规则。
从预过滤器规则页面查看对象详细信息	6.6	任意	引入的功能：在查看预过滤器规则时，用于查看对象或对象组的详细信息的选项。 新选项：右键点击预过滤器规则列表中任何列中的值，可提供查看对象详细信息的选项：源网络 (Source Networks)、目标网络 (Destination Networks)、源端口 (Source Port)、目标端口 (Destination Port) 和 VLAN 标记。



第 60 章

安全情报 DNS 策略

以下主题介绍 DNS 策略、DNS 规则，以及向托管设备部署 DNS 策略的方法。

- DNS 策略概述， 第 2261 页
- Cisco Umbrella DNS 策略， 第 2262 页
- DNS 策略组件， 第 2262 页
- DNS 策略许可证要求， 第 2263 页
- DNS 策略的要求和前提条件， 第 2263 页
- 管理 DNS 和 Umbrella DNS 策略， 第 2264 页
- DNS 规则， 第 2266 页
- 如何创建 DNS 规则， 第 2271 页
- DNS 策略部署， 第 2276 页
- Cisco Umbrella DNS 策略， 第 2276 页

DNS 策略概述

基于DNS的安全智能允许你根据客户端请求的域名，使用安全智能阻止列表来阻止流量。思科提供可用于过滤流量的域名智能，您还可以根据部署配置自定义域名列表和源。

DNS策略阻止列表上的流量会立即被阻止，因此不会受到任何进一步的检查--不是为了入侵、利用、恶意软件等，但也不是为了网络发现。你可以使用安全智能的不阻止列表来覆盖阻止列表并强制评估访问控制规则，而且，在被动部署中建议你使用"仅监控"设置来进行安全智能过滤。这允许系统分析本会被阻止列表阻断的连接，但也会记录与阻止列表的匹配，并生成一个连接结束的安全智能事件。

注释 基于 DNS 的安全智能可能无法为域名实现预期功能，除非 DNS 服务器由于到期删除域缓存条目，或者客户端的 DNS 缓存或本地 DNS 服务器的缓存被清除或已到期。

您可使用 DNS 策略及关联的 DNS 规则配置基于 DNS 的安全智能。要将配置部署到设备，您必须将 DNS 策略与访问控制策略相关联，然后将配置部署到托管设备。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这允许 Cisco Umbrella 验证请求，并根据域名允许或阻止它们，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接（**集成 > 其他集成 > 云服务 > Cisco Umbrella 连接**），将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些条件来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

要将 DNS 请求从管理中心重定向到思科 Umbrella，请执行以下操作：

1. 配置思科 Umbrella 连接设置。
2. 创建并配置 Umbrella DNS 策略。
3. 将 Umbrella DNS 策略与访问控制策略相关联
4. 部署更改。

有关如何在管理中心设置Umbrella DNS 连接器的详细信息，请参阅 为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

DNS 策略组件

DNS 策略允许您使用阻止列表基于域名阻止连接，或使用“不阻止”列表来免除此类连接的此类阻止。以下列表介绍可在创建 DNS 策略后更改的配置。

名称和描述

每个 DSN 策略必须拥有唯一的名称。说明为可选项。

规则

规则提供一种基于域名处理网络流量的精细方法。DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。

创建 DNS 策略时，系统使用默认的全局 DNS 不阻止列表和默认的 DNS 全局阻止列表规则来填充该策略。两个规则均固定到其各自类别中的第一个位置。您无法修改这些规则，但是可以将其禁用。



注释 如果为 防火墙管理中心启用多租户，则系统组成域的层次结构，包括祖先域和后代域。这些域截然不同并独立于 DNS 管理中所使用的域名。

后代列表包含系统子域用户的阻止或不阻止列表上的域。从祖先域中，您无法查看后代列表的内容。如果您不希望子域用户将域添加到阻止或不阻止列表：

- 禁用后代列表规则，并且
- 使用访问控制策略继承设置执行安全智能

系统按照以下顺序评估规则：

- DNS 规则的全局不阻止列表（如果启用）
- 后代 DNS 不阻止列表规则（如果启用）
- 包含不阻止操作的的规则
- DNS 规则的全局阻止列表（如果启用）
- 后代 DNS 阻止列表规则（如果启用）
- 包含除不阻止以外的操作的规则

通常，系统根据第一个 DNS 规则（其中所有规则的条件都与流量匹配）处理基于 DN 的网络流量。如果没有任何 DNS 规则与流量匹配，则系统根据关联的访问控制策略规则继续评估流量。DNS 规则条件可以简单，也可以复杂。

DNS 策略许可证要求

威胁防御 许可证

IPS

DNS 策略的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

重要事项 您必须在设备上应用网络发现策略，才能成功对流量进行 DNS 验证。

管理 DNS 和 Umbrella DNS 策略

使用“DNS 策略”(DNS Policy) 页面（**策略** > **安全策略** > **DNS**）管理自定义 DNS 和 Umbrella DNS 策略。

除了您创建的自定义策略之外，系统还提供默认 DNS 策略和默认 Umbrella DNS 策略。默认 DNS 策略会使用默认阻止列表和不阻止列表。您可以编辑并使用系统提供的自定义策略。

过程

步骤 1 选择**策略** > **安全策略** > **DNS**。

步骤 2 要管理 DNS 策略，请执行以下操作：

- 比较 - 要比较 DNS 策略，请点击**比较策略 (Compare Policies)**，然后如比较策略，第 197 页中所述继续操作。
- “复制”(Copy) - 要复制 DNS 策略，请点击 **复制** ()，然后如编辑 DNS 策略，第 2265 页中所述继续操作。
- “创建”(Create) - 要创建新的 Umbrella DNS 策略，请点击**新建策略 (New Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**，然后如创建 Umbrella DNS 策略，第 2280 页中所述继续操作。
- “删除”(Delete) - 要删除 DSN 或 Umbrella DSN 策略，请点击 **删除** ()，然后确认要删除策略。
- “编辑”(Edit) - 要修改现有 DNS 策略，请点击 **编辑** ()，然后如编辑 DNS 策略，第 2265 页中所述继续操作。要修改现有 Umbrella DNS 策略，请点击 **编辑** ()，然后如编辑 Cisco Umbrella DNS 策略和规则，第 2280 页中所述继续操作。

创建基本 DNS 策略

当您创建新的 DNS 策略时，它包含默认设置。然后，您必须对其进行编辑以自定义行为。

过程

步骤 1 选择策略 > 安全策略 > DNS。

步骤 2 点击添加 DNS 策略 (Add DNS Policy) > DNS 策略 (DNS Policy)。

步骤 3 在 Name 和 Description 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击保存。

下一步做什么

配置策略。请参阅编辑 DNS 策略，第 2265 页。

编辑 DNS 策略

一个用户一次只能使用一个浏览器窗口编辑一个DNS策略。如果多个用户尝试保存同一策略，系统会仅保留第一组保存的更改。

为保护会话隐私，在策略编辑器上 30 分钟未执行任何操作之后，系统将显示警告。在 60 分钟后，系统将放弃更改。

过程

步骤 1 选择策略 > 安全策略 > DNS。

步骤 2 点击您要编辑的 DNS 策略旁边的编辑 ()。

如果显示视图 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要编辑 DNS 策略，请执行以下操作：

- 名称和说明 - 要更改名称或说明，请点击相应的字段并键入新信息。
- 规则 - 要添加、分类、启用、禁用或以其他方式管理 DNS 规则，请点击规则 (Rules)，然后如创建和编辑 DNS 规则，第 2266 页中所述继续操作。

步骤 4 点击保存。

下一步做什么

- 或者，进一步配置新策略，如*Cisco Secure Firewall Management Center* 管理指南中的使用安全智能记录连接中所述。
- 部署配置更改；请参阅部署配置更改，第 180 页。

DNS 规则

DNS 规则根据主机请求的域名处理流量。作为安全智能的一部分，此评估发生在所有流量解密之后以及访问控制评估之前。

系统按照您指定的顺序将流量与DNS规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中规则的所有条件都与流量匹配）处理网络流量。

除其唯一名称之外，每个 DNS 规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

DNS 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。DNS规则必须包含DNS源或列表条件，还可以按安全区域、网络、动态属性或 VLAN 匹配流量。

操作

规则的操作确定系统如何处理匹配流量：

- 允许包含**不阻止**操作的流量，需进一步进行访问控制检查。
- 受监控的流量将根据其余有关 DNS 阻止列表的规则进行进一步评估。如果流量不匹配 DNS 阻止列表规则，则将使用访问控制规则进行检查。系统会记录流量的安全智能事件。
- 阻止列表上的流量将被丢弃，无需进一步检查。您还可以返回“找不到域”(Domain Not Found)响应，或将 DNS 查询重定向到 Sinkhole 服务器。

相关主题

关于安全智能，第 1729 页

创建和编辑 DNS 规则

在 DNS 策略中，最多可以向阻止列表和不阻止列表规则中添加总共 32767 个 DNS 列表；即，DNS 策略中的列表数不能超过 32767。

过程

步骤 1 在 DNS 策略编辑器中，可进行以下选择：

- 要添加新规则，请点击**添加 DNS 规则 (Add DNS Rule)**。
- 要编辑现有规则，请点击 **编辑** (✎)。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分，或接受默认值：

- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅DNS 规则操作，第 2268 页。
- 条件 - 配置规则的条件；请参阅DNS 规则条件，第 2269 页。
- 已启用 - 指定规则是否为**已启用 (Enabled)**。

步骤 4 点击**保存**。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

DNS 规则管理

通过 DNS 策略编辑器的**规则 (Rules)** 选项卡，您可以添加、编辑、移动、启用、禁用、删除或以其他方式管理策略中的 DNS 规则。

对于每个规则，策略编辑器会显示其名称和条件摘要，以及规则操作。其他图标代表 **警告**（⚠）、**错误**（✖）和其他重要的 **信息**（ⓘ）。已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。

启用和禁用 DNS 规则

创建DNS规则时，默认情况下会启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。查看DNS策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。请注意，也可使用 DNS 规则编辑器启用或禁用 DNS 规则。

过程

步骤 1 在 DNS 策略编辑器中，右键点击规则并选择规则状态。

步骤 2 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

DNS 规则顺序评估

DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中所有规则的条件都与流量相匹配）处理网络流量。

- 对于“监控”(Monitor)规则，系统会记录流量，然后根据优先级较低的DNS黑名单规则继续评估流量。
- 对于“非监控”规则，在流量匹配规则后系统**不会**根据其他优先级较低的DNS规则继续评估流量。

对规则排序时，请注意：

- DNS 的全局不阻止列表 (Do-Not-Block List) 始终排在首位，优先于所有其他规则。
- “不阻止列表”(Do-Not-Block List)部分优先于“阻止列表”(Block List)部分；不阻止列表规则始终优先于其他规则。
- “全局阻止列表”(Global Block List) 始终排在“阻止列表” (Block List) 部分的第一个位置，并且优先于所有其他“监控”(Monitor) 和“阻止”(Block) 列表规则。
- “阻止列表”(Block List) 部分包含监控和阻止列表规则。
- 首次创建 DNS 规则时，如果分配**不阻止 (Do Not Block)** 操作，系统会将其放在“不阻止列表”(Do-Not-Block List)部分的最后；如果分配任何其他操作，模块会将其放在“阻止列表”(Block List) 部分的最后。

可以通过拖放规则来为规则重新排序。

DNS 规则操作

每个 DNS 规则都有确定匹配流量的以下过程的操作：

- 处理 - 首先，规则操作可管理系统是否会根据阻止或不阻止列表来阻止、不阻止或监控符合规则条件的流量。
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

如果已配置，则 TID 还会影响操作优先级。有关详细信息，请参阅 威胁智能导向器-防火墙管理中心 操作优先级。

不阻止操作

不阻止 (Do Not Block) 操作将允许流量传递到下一个检查阶段，即访问控制规则。

系统不会记录不阻止列表匹配项。是否记录这些连接取决于其最终的安全状态。

“监控”(Monitor) 操作

监控 (Monitor) 操作旨在强制执行连接日志记录；匹配的流量既不会被立即允许，也不会被阻止。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非“监控”(Monitor) DNS 规则可确定系统是否阻止流量。如果没有其他匹配的规则，流量会进行访问控制评估。

对于DNS策略监控的连接，系统会记录连接结束的安全智能和防火墙管理中心数据库的连接事件。

阻止操作

这些操作会阻止流量，无需任何类型的进一步检查：

- **丢弃 (Drop)** 操作会丢弃流量。
- **找不到域 (Domain Not Found)** 操作会针对 DNS 查询返回“不存在的互联网域”响应，防止客户端解析 DNS 请求。
- **Sinkhole** 操作会返回 Sinkhole 对象的 IPv4 或 IPv6 地址以响应 DNS 查询（仅限 A 和 AAAA 记录）。Sinkhole 服务器可以记录或记录并阻止 IP 地址的后续连接。如果配置 **Sinkhole** 操作，还必须配置 Sinkhole 对象。

对于根据**丢弃 (Drop)** 或**找不到域 (Domain Not Found)** 操作而被阻止的连接，系统会记录连接开始的安全智能和连接事件。因为被阻止的流量会被立即拒绝，无需进一步检测，所以，没有要记录的唯一连接终止。

对于根据 **Sinkhole** 操作阻止的连接，日志记录取决于 Sinkhole 对象配置。如果将 Sinkhole 对象配置为仅记录 Sinkhole 连接，则系统会记录后续连接的连接结束的连接事件。如果将 Sinkhole 对象配置为记录并阻止 Sinkhole 连接，则系统会记录后续连接的连接开始的连接事件，然后阻止该连接。

DNS 规则条件

DNS 规则的条件识别该规则处理的流量的类型。条件可以简单，也可以复杂。您必须在 DNS 规则中定义 DNS 源或列表条件。您也可以选择按安全区域、网络、动态属性或 VLAN 控制流量。

将条件添加到 DNS 规则时：

- 如果不为规则配置特定条件，系统将不基于此标准匹配流量。
- 您可以为每个规则配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，包含 DNS 源或列表条件和网络条件，但没有 VLAN 标记条件的规则会根据域名以及源或目标评估流量，无论会话采用任何 VLAN 标记。
- 最多可以为规则中的每个条件添加50个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单一规则根据最多 50 个 DNS 列表和源来阻止流量。

以下主题更详细地解释 DNS 规则条件。

安全区域规则条件

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

DNS 策略规则条件

如果 DNS 列表、源或类别包含客户端请求的域名，则 DNS 规则中的 DNS 条件可用于控制流量。您必须在 DNS 规则中定义 DNS 条件。

无论向DNS条件中添加全局或自定义阻止还是不阻止列表，系统都会将所配置的规则操作应用于流量。例如，如果向规则中添加全局不阻止列表，并配置**丢弃 (Drop)** 操作，则系统会阻止所有本应被允许进入下一阶段检查的流量。

动态属性规则条件

可以使用以下类型的动态属性来匹配 DNS 规则中的连接：

- （源或目标。）动态对象，其中包含 IP 地址。终端设备类型对象仅供源。有关更多信息，请参阅动态对象，第 2642 页一章Dynamic Attributes Connector。
- （仅源。）安全组标记 (SGT) 对象，包含手动定义或通过 ISE 定义的标记。有关详细信息，请参阅源和目标安全组标记 (SGT) 匹配，第 2080 页和安全组标记，第 2649 页。

为DNS规则配置动态属性时，同一源或目标列表中相同类型的对象将进行“或”运算，不同类型的对象将进行“与”运算。例如，如果同时选择安全组标记和列出IP地址的动态对象，如果带有 标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

最初，打开“**动态属性**”**(Dynamic Attributes)** 选项卡时，系统会列出所有 **动态对象** 和 **安全组标记**。您可以取消选择某个选项以从列表中删除这些对象。您还可以在搜索框中键入内容以查找所需的对象。

如何创建 DNS 规则

以下主题讨论如何创建 DNS 规则。

根据 DNS 和安全区域控制流量

通过DNS规则中的区域条件，您可以根据其源安全区域来控制流量。安全区域是一个或多个接口的分组，可位于多个设备之间。

过程

步骤 1 在 DNS 规则编辑器中，点击**区域 (Zones)**。

步骤 2 从 **Available Zones** 中查找并选择您想要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 3 点击选择一个区域，或右键点击，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 5 点击 **DNS** 选项卡，添加包含您要控制的 DNS 名称的列表或源。有关详细信息，请参阅根据 DNS 列表或源来控制流量，第 2274 页。

步骤 6 保存或继续编辑规则。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

根据 DNS 和网络控制流量

DNS 规则中的网络条件可以根据源 IP 地址控制流量。您可以为要控制的流量显式指定源 IP 地址。

过程

步骤 1 在 DNS 规则编辑器中，点击**网络 (Networks)**。

步骤 2 从 **Available Networks** 中查找并选择您想要添加的网络，如下所示：

- 要即时添加可随后添加到条件中的网络对象，请点击**可用网络 (Available Networks)** 列表上方的**添加** (+)，然后如创建网络对象，第 2660 页中所述继续操作。
- 要搜索要添加的网络对象，请点击**可用网络**列表上方的**按名称或值搜索**提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源 IP 地址或地址块。点击**源网络 (Source Networks)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示，然后键入 IP 地址或地址块，并点击**添加 (Add)**。

步骤 5 点击 **DNS** 选项卡，添加包含您要控制的 DNS 名称的列表或源。有关详细信息，请参阅根据 DNS 列表或源来控制流量，第 2274 页。

步骤 6 保存或继续编辑规则。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

根据 DNS 和 VLAN 控制流量

通过 DNS 规则中的 VLAN 条件，您可以控制 VLAN 标记流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。

构建基于 VLAN 的 DNS 规则条件时，可以手动指定 VLAN 标记。或者，也可以使用 VLAN 标记对象配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

过程

步骤 1 在 DNS 规则编辑器中，选择 **VLAN 标记 (VLAN Tags)**。

步骤 2 查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击“可用 VLAN 标记”(Available VLAN Tags) 列表上方的 **添加** (+) 并继续操作，如创建 VLAN 标记对象，第 2720 页中所述。
- 要搜索将添加的 VLAN 标记对象和组，请点击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 添加要手动指定的任何 VLAN 标记。点击**所选 VLAN 标记 (Selected VLAN Tags)** 列表下方的**输入 VLAN 标记 (Enter a VLAN Tag)** 提示，然后键入 VLAN 标记或范围并点击**添加 (Add)**。您可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

步骤 5 点击 **DNS** 选项卡，添加包含您要控制的 DNS 名称的列表或源。有关详细信息，请参阅根据 DNS 列表或源来控制流量，第 2274 页。

步骤 6 保存或继续编辑规则。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

根据 DNS 列表或源来控制流量

过程

步骤 1 在 DNS 规则编辑器中，点击 **DNS**。

步骤 2 从 **DNS 列表和源 (DNS Lists and Feeds)** 中查找并选择要添加的 DNS 列表和源，如下所示：

- 要动态添加可随后添加到条件中的 DNS 列表和源，请点击 **DNS 列表和源 (DNS Lists and Feeds)** 列表上方的 **添加** (+)，然后如创建安全智能源，第 2697 页中所述继续操作。
- 要搜索将添加的 DNS 列表、源或类别，请点击 **DNS 列表和源** 列表上方的 **按名称或值搜索** 提示，然后键入对象名称或其中一个对象的组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。
- 有关系统提供的威胁类别的说明，请参阅安全智能类别，第 1736 页。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 保存或继续编辑规则。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

根据安全组标记或动态属性控制流量

DNS 规则中的动态属性条件允许您根据安全组标记或其他动态属性来控制流量。要使用这些属性，必须将安全组标记应用于网络中的流量，或使用 API 或 Cisco Secure 动态属性连接器创建所需的动态属性对象。有关启用动态属性过滤器的详细信息，请参阅动态属性规则条件，第 2271 页。

为 DNS 规则配置动态属性时，同一源或目标列表中相同类型的对象将进行“或”运算，不同类型的对象将进行“与”运算。例如，如果同时选择安全组标记和列出 IP 地址的动态对象，如果带有标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

过程

步骤 1 在 DNS 规则编辑器中，点击**动态属性** 选项卡。

步骤 2 选择要使用的对象，然后点击 **添加源 (Add Sources)** 或 **添加目的 (Add Destinations)**。

最初，打开 “**动态属性**”**(Dynamic Attributes)** 选项卡时，系统会列出所有 **动态对象** 和 **安全组标记** 。您可以取消选择某个选项以从列表中删除这些对象。您还可以在搜索框中键入内容以查找所需的对象。

您可以使用这些对象来标识连接的源和/或目标。

注释
您只能使用 SGT 和终端设备类型对象作为源条件。

步骤 3 点击 **DNS** 选项卡，添加包含您要控制的 DNS 名称的列表或源。有关详细信息，请参阅根据 DNS 列表或源来控制流量，第 2274 页。

步骤 4 保存或继续编辑规则。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

使用 DNS Sinkhole 执行内容限制

通常，DNS Sinkhole 会将流量定向到特定的目标。此过程描述如何将 DNS Sinkhole 配置为将流量重定向到 Google 安全搜索虚拟 IP 地址 (VIP)，这会强制对 Google 和 YouTube 搜索结果应用内容过滤器。

由于 Google 安全搜索为 VIP 使用单个 IPv4 地址，因此主机必须使用 IPv4 寻址。

⚠

注意 如果您的网络包括代理服务器，则除非您在代理服务器和互联网之间放置 Firewall Threat Defense设备，否则此内容限制方法无效。

此过程仅强制执行对 Google 搜索的内容限制。它不适用于任何其他搜索引擎。

开始之前

此程序仅适用于 Firewall Threat Defense 并需要 IPS 许可证。

过程

步骤 1 通过以下 URL 获得支持的 Google 域列表：https://www.google.com/supported_domains。

步骤 2 在本地计算机上创建自定义 DNS 列表，并添加以下条目：

- 要执行 Google 安全搜索，为每个支持的 Google 域添加一个条目。
- 要实施 YouTube 限制模式，请添加一个“youtube.com”条目。

自定义 DNS 列表必须是文本文件 (.txt) 格式。文本文件的每一行都必须指定一个单独的域名，去掉任何前导句点。例如，支持的域“.google.com”必须显示为“google.com”。

步骤 3 将自定义 DNS 列表上传到 防火墙管理中心；请参阅将新的安全智能列表上传到 Secure Firewall Management Center，第 2698 页。

步骤 4 确定 Google 安全搜索 VIP 的 IPv4 地址。例如，在 forcesafesearch.google.com 上运行 `nslookup`。

步骤 5 为安全搜索 VIP 创建一个 Sinkhole 对象；请参阅创建 Sinkhole 对象，第 2700 页。

为此对象使用以下值：

- IPv4 地址 - 输入安全搜索 VIP 地址。
- IPv6 地址 - 输入 IPv6 环回地址 (`::1`)。
- 记录到 Sinkhole 的连接 - 点击“记录连接” (Log Connections)。
- 类型 - 选择**无**。

步骤 6 创建基本的 DNS 策略；请参见创建基本 DNS 策略，第 2264 页。

步骤 7 为 Sinkhole 添加 DNS 规则；请参阅创建和编辑 DNS 规则，第 2266 页。

对于此规则：

- 选中**已启用 (Enabled)** 复选框。
- 从操作下拉列表中选择 **Sinkhole**。
- 从 **Sinkhole** 下拉列表中选择您创建的 Sinkhole 对象。
- 将您创建的自定义 DNS 列表添加到 **DNS** 上的**所选项目 (Selected Items)** 列表中。
- （可选）在**网络 (Networks)** 中选择一个网络，以将内容约束限制为特定用户。例如，如果要将内容约束限制为学生用户，请将学生分配给不同于教员的子网，并在此规则中指定该子网。

步骤 8 将 DNS 策略与访问控制策略相关联；请参阅将其他策略与访问控制相关联，第 1719 页。

步骤 9 部署配置更改；请参阅 部署配置更改，第 180 页。

DNS 策略部署

完成 DNS 策略配置更新后，您必须将其部署为访问控制配置的一部分。

- 将 DNS 策略与访问控制策略相关联，如配置安全智能，第 1732 页中所述。
- 部署配置更改；请参阅 部署配置更改，第 180 页。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这允许 Cisco Umbrella 验证请求，并根据域名允许或阻止它们，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接（**集成 > 其他集成 > 云服务 > Cisco Umbrella 连接**），将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些条件来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

要将 DNS 请求从管理中心重定向到思科 Umbrella，请执行以下操作：

1. 配置思科 Umbrella 连接设置。
2. 创建并配置 Umbrella DNS 策略。
3. 将 Umbrella DNS 策略与访问控制策略相关联
4. 部署更改。

有关如何在管理中心设置 Umbrella DNS 连接器的详细信息，请参阅 为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

如何将 DNS 请求重定向到 Cisco Umbrella

本节提供使用 防火墙管理中心将 DNS 请求从设备重定向到思科 Umbrella 的说明。

步骤	相应操作	更多信息
1	确保您已满足前提条件。	配置 Umbrella DNS 连接器的前提条件， 第 2277 页
2	配置思科 Umbrella 连接设置。	配置 Cisco Umbrella 连接设置， 第 2279 页
3	创建 Umbrella DNS 策略	创建 Umbrella DNS 策略， 第 2280 页
4	配置 Umbrella DNS 策略	编辑 Cisco Umbrella DNS 策略和规则， 第 2280 页
5	将 Umbrella DNS 策略与访问控制策略相关联	将 Umbrella DNS 策略与访问控制策略相关联， 第 2281 页

配置 Umbrella DNS 连接器的前提条件

表 *126:* 支持的最低平台

产品	版本
Cisco Secure Firewall Threat Defense	6.6 及更高版本

产品	版本
Secure Firewall Management Center	7.2 及更高版本

- 在 https://umbrella.cisco.com上建立思科 Umbrella 账户，然后在 http://login.umbrella.com上登录 Umbrella。
- 将 CA 证书从思科 Umbrella 服务器导入 防火墙管理中心。在思科 Umbrella 中，依次选择 **部署 > 配置 > 根证书** 并下载证书。

  必须导入根证书，才能与思科 Umbrella 注册服务器建立 HTTPS 连接。证书需要受信任才能进行 SSL 服务器验证，这是 防火墙管理中心中的非默认选项。将以下设备证书复制并粘贴到 防火墙管理中心(**设备 > 证书**) 中。

  ```
  MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG
  EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw
  HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy
  MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp
  Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
  CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6aqXodgojl
  EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddng9/n00tnTCJRpt8OmRDt
  V1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuWraKImxW8oHzf6VGo1bDtN+I2tIJLYrVJ
  muzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGBAfr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkD
  Ka77SU+kFbnO8lwZV21reacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE
  FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G
  A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw
  BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0
  LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv
  YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v
  RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v
  RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG
  BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX
  3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z
  u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe
  50gG66sSmvKvhMNbg0qZgYOrAKHKCjxMoiWJKiKnpPMzTFuMLhoClw+dj20tlQj7T9rxkTgl4Zxu
  YRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KE
  SaZMkE4f97Q=
  ```

  在管理中心添加证书时，请确保选中 **仅 CA** 复选框。
- 在设备上安装证书。
- 从 Umbrella 获取以下数据：
  - 组织 ID
  - 网络设备密钥
  - 网络设备密钥
  - 旧版网络设备令牌
- 确保 防火墙管理中心 已连接到互联网。
- 确保已在 中启用具有出口控制功能选项的基础许可证。防火墙管理中心
- 确保 DNS 服务器配置为解析 api.opendns.com。

- 确保 防火墙管理中心 可以解析 management.api.umbrella.com 以进行策略配置。
- 配置到 api.opendns.com 的 Firewall Threat Defense 路由。

配置 Cisco Umbrella 连接设置

思科 Umbrella 连接设置定义了在思科 Umbrella 中注册设备时所需的 API 令牌。

开始之前

使用思科 Umbrella https://umbrella.cisco.com 建立账户，然后通过 https://dashboard.umbrella.com 登录 Umbrella，获取与思科 Umbrella 建立连接所需的信息。

过程

步骤 1 选择**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 2 获取以下详细信息并将其添加到**常规 (General)** 设置中：

- **组织 ID (Organization ID)** - 在思科 Umbrella 上标识您的组织的唯一编号。每个 Umbrella 组织都是一个单独的 Umbrella 实例，并且有自己的控制面板。组织通过其名称和组织 ID（组织 ID）进行标识。
- **网络设备密钥 (Network Device Key)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。
- **网络设备密钥 (Network Device Secret)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。
- **旧版网络设备令牌 (Legacy Network Device Token)** - 通过思科 Umbrella 控制面板颁发 Umbrella 旧版网络设备 API 令牌。Umbrella 需要 API 令牌才能注册网络设备。

步骤 3 在 **高级** 下，配置以下可选设置：

- **DNSCrypt 公钥**-DNSCrypt 对终端和 DNS 服务器之间的 DNS 查询进行身份验证和加密。要启用 DNScrypt，您可以为证书验证配置 DNScrypt 公钥。密钥是一个 32 字节的十六进制值，预配置为 B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79，即公钥的 Umbrella 任播服务器。
- **管理密钥 (Management Key)** - 从 Umbrella 云获取 VPN 策略的数据中心详细信息的密钥。
- **管理秘密 (Management Secret)** - 用于从 Umbrella 云获取 VPN 数据中心的秘密。

步骤 4 点击 **测试连接**-测试是否可从 防火墙管理中心访问 Cisco Umbrella Cloud。在提供所需的组织 ID 和网络设备详细信息时，您会创建 Umbrella 连接。

步骤 5 点击**保存**。

创建 Umbrella DNS 策略

过程

步骤 1 选择**策略** > **安全策略** > **DNS**。

步骤 2 点击**添加 DNS 策略 (Add DNS Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击**保存**。

下一步做什么

配置策略。请参阅编辑 Cisco Umbrella DNS 策略和规则，第 2280 页。

编辑 Cisco Umbrella DNS 策略和规则

过程

步骤 1 选择**策略** > **安全策略** > **DNS**。

步骤 2 在“DNS 策略”页面上，选择要编辑的 Umbrella DNS 策略，然后点击 **编辑** ()。

刷新 Umbrella 保护策略

如果要从思科 Umbrella 获取最新的 Umbrella 保护策略，请点击**上次更新 Umbrella 保护策略 (Umbrella Protection Policy Last Updated)** 旁边的**刷新 (Refresh)** 图标。

要配置或修改管理中心的 Umbrella 连接设置，请转至**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 3 在 Cisco Umbrella DNS 策略编辑器中，选择 Umbrella DNS 规则并点击 **编辑** ()。

步骤 4 配置规则组成部分，或接受默认值：

- **Umbrella 保护策略 (Umbrella Protection Policy)** - 指定要应用于设备的思科 Umbrella 策略的名称。
- **绕过域 (Bypass Domain)** - 指定 DNS 请求应绕过思科 Umbrella 直接转至所配置的 DNS 服务器的本地域。

  例如，假设允许所有内部连接，可以借助内部 DNS 服务器解析组织域名的所有名称。
- **DNSCrypt** - 启用 DNSCrypt，以便为设备和思科 Umbrella 之间的连接加密。

  启用 DNScrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNScrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。

- **空闲超时** - 配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。

步骤 5 点击**保存**。

下一步做什么

将 Umbrella DNS 策略与访问控制策略相关联有关详细信息，请参阅将 Umbrella DNS 策略与访问控制策略相关联，第 2281 页。

将 Umbrella DNS 策略与访问控制策略相关联

在设备上部署 Umbrella DNS 策略之前，必须将其与访问控制策略相关联。

过程

步骤 1 选择 **策略 > 访问控制**，然后选择要编辑的访问策略。

步骤 2 选择 **安全智能**。

步骤 3 从 **Cisco Umbrella DNS 策略** 下拉列表中，选择 Umbrella DNS 策略。

步骤 4 点击**保存**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 180 页。



第 61 章

网络恶意软件防护的文件策略

以下主题概述文件控制、文件策略、文件规则、高级恶意软件保护(AMP)、云连接和动态分析连接。

- 关于网络恶意软件防护和文件策略， 第 2283 页
- 文件策略的要求和前提条件， 第 2284 页
- 文件和恶意软件策略许可证要求， 第 2285 页
- 文件策略和恶意软件检测的最佳实践 ， 第 2285 页
- 如何配置恶意软件防护， 第 2288 页
- 恶意软件防护的云连接， 第 2293 页
- 文件策略和文件规则， 第 2302 页
- 追溯处置情况更改， 第 2316 页
- 文件和恶意软件检测性能和存储选项， 第 2317 页
- 调整文件和恶意软件检测性能和存储 ， 第 2318 页
- （可选）Secure Endpoint 的恶意软件防护， 第 2319 页
- 网络恶意软件保护和文件策略的历史记录， 第 2323 页

关于网络恶意软件防护和文件策略

要检测和阻止恶意软件，请使用文件策略。您还可以使用文件策略按文件类型来检测和控制流量。

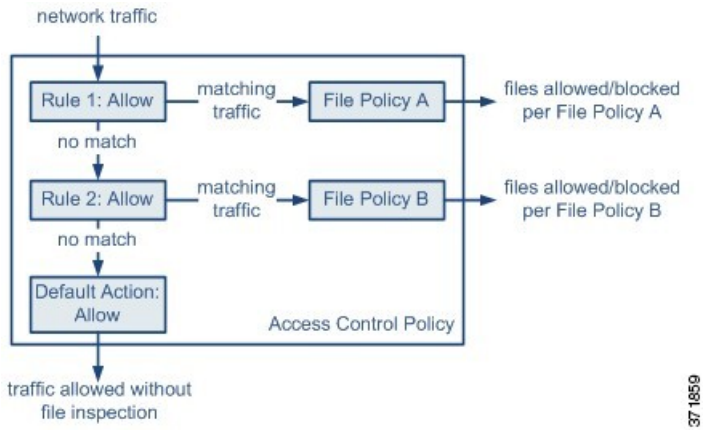
面向 Firepower 的高级恶意软件防护 (AMP) 可以检测、捕获、跟踪、分析、记录并选择性地阻止网络流量中恶意软件的传输。在 Secure Firewall Management Center Web 界面中，此功能称为恶意软件防护，以前称为面向 *Firepower* 的 *AMP*。思科高级恶意软件保护利用内联部署的托管设备和来自思科云的威胁数据来识别恶意软件。

您可以将文件策略与处理网络流量的访问控制规则作为整体访问控制配置的一部分关联起来。

当系统检测到网络上的恶意软件时，它会生成文件和恶意软件事件。要分析文件和恶意软件事件数据，请参阅*Cisco Secure Firewall Management Center* 管理指南 中的文件/恶意软件事件和网络文件轨迹一章。

文件策略

文件策略是作为整体访问控制配置的一部分供系统用于执行恶意软件保护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。在内联部署中，可考虑下图所示的简单访问控制策略。



策略有两个访问控制规则，两者都使用“允许”(Allow)操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在这种情况下，流量的处理方式如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。
- 与 `Rule 1` 不匹配的流量根据 `Rule 2` 进行评估。与 `Rule 2` 匹配的流量根据 `File Policy B` 进行检查。
- 允许与任一规则都不匹配的流量；不能将文件策略与默认操作关联。

通过将不同文件策略与不同访问控制规则相关联，可以精细控制如何识别并阻止网络上传输的文件。

文件策略的要求和前提条件

型号支持

任意

Cisco Secure Firewall 200 仅通过 AMP 云查找支持恶意软件分析。它不支持文件存储或提交文件以进行分析。这包括 Spero、本地恶意软件分析、文件捕获和 Clam AV。策略中配置的任何不受支持的功能，在部署到设备时会自动关闭。

支持的域

任意

用户角色

- 管理员

- 访问管理员

文件和恶意软件策略许可证要求

要执行此操作	所需许可证	文件规则操作
阻止或允许特定类型的所有文件（例如，阻止all.exe文件）	IPS （对于 Firewall Threat Defense 设备） 保护 （适用于传统设备）	允许、阻止、阻止并重置
根据文件包含或可能包含恶意软件的判断，选择性地允许或阻止文件	IPS （对于 Firewall Threat Defense 设备） 保护 （适用于传统设备） 恶意软件防御	恶意软件云查找、阻止恶意软件
存储文件	IPS （对于 Firewall Threat Defense 设备） 保护 （适用于传统设备） 恶意软件防御	选择了 **存储文件** 的任何文件规则操作

有关 恶意软件防御 许可证的详细信息，请参阅：

- *Cisco Secure Firewall Management Center* 管理指南中的恶意软件防御许可证

文件策略和恶意软件检测的最佳实践

除下述项目外，请按照 如何配置恶意软件防护，第 2288 页 和参考主题中的步骤操作。

文件规则最佳实践

在配置文件规则时，请注意以下准则和限制：

- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 一个策略可以包含多个规则。在创建规则时，请确保没有规则被先前的规则“隐藏”。

- 动态分析支持的文件类型是其他分析类型支持的文件类型的子集。要查看每种分析支持的文件类型，请导航至文件规则配置页面，选择**阻止恶意软件 (Block Malware)** 操作，然后选中所需的复选框。

  要确保系统检查所有的文件类型，请为动态分析和其他类型的分析创建单独的规则（在同一策略内）。

- 如果文件规则配置有**恶意软件云查找**或**阻止恶意软件**操作，并且 防火墙管理中心无法与 AMP 云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复连接为止。

- 思科建议启用**重置连接 (Reset Connection)**（适用于**阻止文件 [Block Files]** 和**阻止恶意软件 [Block Malware]** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话会保持打开，直到 TCP 连接重置为止。

- 如果监控大量流量，请**勿**存储所有捕获文件，或者将所有捕获文件提交进行动态分析。否则可能对系统性能产生不利影响。

- 不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

文件检测最佳实践

请考虑文件检测的以下注意事项和限制：

- 如果未启用自适应分析，则访问控制规则无法执行文件控制（包括 AMP）。
- 如果文件与带有应用协议条件的规则相匹配，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- FTP 通过不同信道传输命令和数据。在被动或内联分流模式部署中，来自 FTP 数据会话及其控制会话的流量可能不会均衡分摊到同一个内部资源。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。
- 当通过 SMTP 传输基于文本的文件时，某些邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些邮件客户端在处理无法识别的文件类型时默认进行换行。
- 要检测 ISO 文件，请将“限制执行文件类型检测时检查的字节数”选项设置为大于 36870 的值，如文件和恶意软件检测性能和存储选项，第 2317 页中所述。
- 无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。
- 如果文件处置为中性，则为未知处置。

文件阻止最佳实践

请考虑文件阻止的以下注意事项和限制：

- 无论使用何种传输协议，如果未检测到文件的文件结尾标记，**Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件（如文件结尾标记所指示），并在检测到该标记后阻止文件。
- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指示文件传输失败，但是文件实际上将完整传输到磁盘。
- 具有**阻止文件 (Block Files)** 和**阻止恶意软件 (Block Malware)** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量顺序错误，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用**阻止文件 (Block Files)** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果您创建文件规则来检测或阻止通过 NetBIOS-ssn 传输的文件（例如 SMB 文件传输），系统不会检测正在进行的文件传输。但是，系统会检测部署调用文件策略的访问控制策略后传输的新文件。
- SMB 的多通道功能可以创建 IP 地址相同但端口不同的多个并行会话。对于多通道上的给定事务，文件下载会在未由系统作为单个文件检测的这些会话之间多路复用。
- 系统不会检测单个 TCP 或 SMB 会话中同步传输的文件。
- 在集群环境中，如果现有 SMB 会话因集群角色更改或设备故障而移至新设备，则任何正在传输的文件可能无法得到检测。
- Microsoft Windows 系统之间的一些 SMB 文件传输使用非常高的 TCP 窗口大小来进行快速文件传输。要检测或阻止此类文件传输，建议您增大**网络分析策略 (Network Analysis Policy)** > **TCP 数据流配置 (TCP Stream Configuration)** > **故障排除选项 (Troubleshooting Options)** 下的**最大排队字节数 (Maximum Queued Bytes)** 和**最大排队分段数 (Maximum Queued Segments)** 的值。
- 如果配置了 Firepower 威胁防御高可用性，并且在原始主用设备识别文件时发生故障切换，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。

文件策略最佳实践

在配置文件策略时，请注意以下常规准则和限制：

- 可以将单个文件策略与其操作为**允许 (Allow)**、**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)** 的访问控制规则关联。
- 您**不能**使用文件策略检查由访问控制默认操作处理的流量。
- 对于新策略，Web 界面会指出该策略未在使用。如果编辑的是使用中的文件策略，则 Web 界面会告知您使用该文件策略的访问控制策略的数量。在任一情况下，可以点击文本以跳至“访问控制策略”(Access Control Policies) 页面。

- 要使文件阻止起作用，应用于访问控制策略的NAP策略必须在保护模式（也称为内联模式）下运行。
- 根据您的配置，您可以在系统首次检测到某个文件时对其进行检查并等待云查找结果，也可以在首次检测到文件时不等待云查找结果即对文件放行。
- 默认情况下，已加密负载的文件检查会被禁用。当已加密连接与已配置文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。



注意 默认情况下，为文件/恶意软件策略启用具有以下生成器 ID (GID) 的文件检查预处理器：GID: 146 和 GID: 147。

- 如果在使用恶意软件操作或存储文件选项的文件策略中启用访问控制策略，则会降低设备的计算能力和系统性能。

如何配置恶意软件防护

本主题总结设置系统以保护网络免受恶意软件侵害时必须执行的步骤。

过程

步骤 1 规划和准备恶意软件防护，第 2289 页

步骤 2 配置文件策略，第 2290 页

步骤 3 将文件策略添加到访问控制配置，第 2290 页

步骤 4 配置网络发现策略，将文件和恶意软件事件与网络上的主机相关联。

（不要简单地打开网络发现；您必须将其配置为发现网络上的主机，以构建组织的网络映射。）

请参阅网络发现策略，第 2583 页以及子主题。

步骤 5 将策略部署到托管设备。

请参阅部署配置更改，第 180 页。

步骤 6 测试您的系统，确保它按预期处理恶意文件。

步骤 7 设置恶意软件防护的维护和监控，第 2292 页

下一步做什么

- （可选）要进一步增强对网络中恶意软件的检测，请部署和集成思科Secure Endpoint。请参阅（可选）Secure Endpoint 的恶意软件防护，第 2319 页以及子主题。
- 了解如何调查文件和恶意软件事件。

请参阅 *Cisco Secure Firewall Management Center* 管理指南中文件/恶意软件事件和网络文件轨迹。

规划和准备恶意软件防护

此程序是配置系统以提供恶意软件防护的完整过程中的第一组步骤。

过程

步骤 1 购买和安装许可证。

请参阅 文件和恶意软件策略许可证要求，第 2285 页 和 *Cisco Secure Firewall Management Center* 管理指南中的 许可证。

步骤 2 了解文件策略和恶意软件防护如何融入您的访问控制计划。

请参阅章节访问控制策略，第 1701 页。

步骤 3 了解文件分析和恶意软件防护工具。

请参阅文件规则操作，第 2308 页以及子主题。

也可以考虑 高级和存档文件检查选项，第 2303 页。

步骤 4 确定您将使用公共云还是私有（本地）云进行恶意软件防护（文件分析和动态分析）。

请参阅恶意软件防护的云连接，第 2293 页以及子主题。

步骤 5 如果您将使用私有（本地）云进行恶意软件防护：购买、部署和测试这些产品。

有关信息，请联系思科客户代表或授权经销商。

步骤 6 配置防火墙以允许与您选择的云进行通信。

请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 安全、互联网接入和通信端口 。

步骤 7 配置 Firepower 和恶意软件防护云（公共或私有云）之间的连接。

- 有关 AMP 云，请参阅更改 AMP 选项，第 2298 页。
- 如果您部署了本地 Secure Secure Malware Analytics 设备，请参阅连接到内部动态分析设备，第 2299 页。（访问公共 Secure Secure Malware Analytics 云不需要配置。）

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 2288 页。

配置文件策略

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护 ， 第 2288 页。

过程

步骤 1 查看文件策略和文件规则限制。

请参阅文件策略和恶意软件检测的最佳实践 ， 第 2285 页以及子主题。

步骤 2 创建文件策略。

请参阅创建或编辑策略 ， 第 2302 页。

步骤 3 在文件策略中创建规则。

请参阅文件规则 ， 第 2307 页以及子主题。

步骤 4 配置高级选项。

请参阅高级和存档文件检查选项 ， 第 2303 页。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护 ， 第 2288 页。

将文件策略添加到访问控制配置

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护 ， 第 2288 页。

过程

步骤 1 查看访问控制政策中的文件策略准则。（这些准则与您之前查看的文件规则和文件策略准则不同。）

查看 文件和入侵检查顺序，第 1751 页。

步骤 2 将文件策略与访问控制策略关联。

请参阅配置访问控制规则以执行恶意软件保护，第 2291 页

步骤 3 将访问控制策略分配给被托管的设备。

请参阅将设备分配给访问控制策略，第 1717 页。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 2288 页。

配置访问控制规则以执行恶意软件保护

注意 在**检测文件**或**阻止文件**规则中启用启用或禁用**存储文件**，或添加包含**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）的第一个文件规则，或者删除最后一个这样的文件规则，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

注释 当访问控制规则中包含文件策略时，会自动启用内联规范化。有关详细信息，请参阅内联规范化预处理器https://www.cisco.com/go/snort3-inspectors。

开始之前

- 为了让访问控制规则执行文件控制（包括 AMP），**必须**启用自适应分析（默认已启用）。
- 您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制规则编辑器中（从**策略 (Policies) > 访问控制 (Access Control)**），从**操作 (Action)** 选择**允许 (Allow)**, **交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**。

步骤 2 （仅限旧版 UI。）点击**检测 (Inspection)**。

步骤 3 选择**文件策略 (File Policy)** 以检查与访问控制规则相匹配的流量，或选择**无 (None)** 禁用对匹配流量的文件检查。

步骤 4 （可选）通过点击**日志记录 (Logging)** 并取消选中**日志文件 (Log Files)** 为匹配连接禁用文件或恶意软件文件的日志记录。

注释
思科建议您保持启用文件和恶意软件日志记录。

步骤 5 保存规则。

步骤 6 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改， 第 180 页。

设置恶意软件防护的维护和监控

持续维护对于保护您的网络至关重要。

开始之前

配置您的系统以保护您的网络免受恶意软件的侵害。

请参阅如何配置恶意软件防护， 第 2288 页和引用的程序。

过程

步骤 1 确保您的系统始终具有最新、最有效的保护。

请参阅维护您的系统：符合动态分析条件的文件类型， 第 2301 页。

步骤 2 为恶意软件相关事件和运行状况监控配置警报。

有关配置 恶意软件防护 警报的信息以及有关以下模块的信息，请参阅*Cisco Secure Firewall Management Center* 管理指南：

- 本地恶意软件分析

- 安全智能
- 设备中威胁数据更新
- 入侵和文件事件率
- 面向 Firepower 的 AMP 状态
- Secure Endpoint状态

下一步做什么

查看恶意软件防护工作流程中的“后续操作”：

请参阅如何配置恶意软件防护，第 2288 页。

恶意软件防护的云连接

为了保护网络免受恶意软件，需要连接到公共云或私有云。

AMP 云

高级恶意软件防护 (AMP) 云是一种 Cisco 托管服务器，它使用大数据分析和持续分析提供系统用于检测和阻止网络中的恶意软件的情报。

AMP 云为由托管设备在网络流量中检测到的潜在恶意软件提供处置情况，并为本地恶意软件分析和文件预分类提供数据更新。

如果您的组织已部署Secure Endpoint 并且已配置 Firepower 以导入其数据，则系统会从 AMP 云导入这些数据，包括扫描记录、恶意软件检测、隔离和危害表现 (IOC)。

Cisco 提供以下选项，用于从 思科云获取有关已知恶意软件威胁的数据：

- **AMP 公共云**

  您的 Secure Firewall Management Center 直接与公共 思科云通信。有三个公共 AMP 云，分别位于美国、欧洲和亚洲。

- **AMP 私有云**

  AMP 私有云虚拟设备用作压缩的内部 AMP 云，以及用于连接到公共 AMP 云的匿名代理。有关详细信息，请参阅思科 AMP 私有云，第 2295 页。

  如果与Secure Endpoint 集成，则 AMPv 会有一些限制。请参阅Secure Endpoint 和 AMP 私有云，第 2321 页。

动态分析云

- **Secure Secure Malware Analytics 云**

公共云处理您提交进行动态分析的符合条件的文件，并提供威胁评分和动态分析报告。Firepower 支持 200 个样本/天进行 Secure Secure Malware Analytics 分析。

- **本地 Secure Secure Malware Analytics 设备**

  如果您的组织的安全策略不允许系统发送网络外部的文件，则您可以配置本地设备。此设备不会联系公共 Secure Secure Malware Analytics 云。

  有关详细信息，请参阅动态分析本地设备 (Cisco Secure Secure Malware Analytics)，第 2299 页。

配置与 AMP 和 Secure Secure Malware Analytics 云的连接

- AMP 云连接配置，第 2294 页
- 动态分析连接，第 2298 页

AMP 云连接配置

以下主题介绍不同场景的 AMP 云连接配置：

- 选择 AMP 云，第 2295 页
- 连接到 AMP 私有云，第 2296 页
- 集成 Firepower 和 Secure Endpoint，第 2321 页

以下主题也相关：

- 思科 AMP 私有云，第 2295 页
- AMP 云连接的要求和最佳实践，第 2294 页
- 管理与 AMP 云的连接（公共或私有），第 2297 页

AMP 云连接的要求和最佳实践

AMP 云连接的要求

您必须是管理员用户才能设置 AMP 云。

为保证 防火墙管理中心 可与 AMP 云通信，请参阅*Cisco Secure Firewall Management Center* 管理指南中安全、互联网接入和通信端口。

AMP 和高可用性

尽管高可用性对中的防火墙管理中心共享文件策略和相关配置，但它们不共享 AMP 云连接、捕获的文件、文件事件和恶意软件事件。为确保操作的连续性，并且使两台防火墙管理中心上的恶意软件处置相同，主用和备用防火墙管理中心都必须能够访问云。

这些要求适用于公共和私有 AMP 云。

AMP 云连接和多租户

在多域部署中，在全局级别配置 恶意软件防护 连接。每个 防火墙管理中心只能有一个恶意软件防护 连接。

选择 AMP 云

默认情况下，为您的系统配置并启用与美国 (US) AMP 公共云的连接。（此连接会在 Web 界面中显示为 恶意软件防护，有时会显示为面向 Firepower 的 AMP。）您无法删除或禁用 恶意软件防护 云连接，但您可以使用此程序在不同的地理 AMP 云之间切换，或者配置私有云 (AMPv) 连接。

开始之前

- 如果您将使用 AMP 私有云，请参阅连接到 AMP 私有云，第 2296 页而不是本主题。
- 除非 Firepower 与Secure Endpoint 集成，否则只能配置一个 AMP 云连接。此连接标记为 **面向网络的 AMP** 或 **面向 Firepower 的 AMP**。
- 如果您已部署Secure Endpoint，并且想要添加一个或多个 AMP 云以将该应用与 Firepower 集成，请参阅集成 Firepower 和 Secure Endpoint，第 2321 页。
- 请参阅AMP 云连接的要求和最佳实践，第 2294 页。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 点击铅笔以编辑现有云连接。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择离 Secure Firewall Management Center最近的区域云：

APJC 是指亚太地区/日本/中国。

步骤 4 点击**保存**。

下一步做什么

- 如果您的部署为高可用性配置，请参阅AMP 云连接的要求和最佳实践，第 2294 页。
- （可选）更改 AMP 选项，第 2298 页。

思科 AMP 私有云

防火墙管理中心必须连接到AMP云，才能对在网络流量中检测到的文件进行处置情况查询并接收追溯性恶意软件事件。此云可以是公共云，也可以是私有云。

您的组织可能会担心隐私或安全，以致在受监控网络和 AMP 云之间难以或无法进行频繁或直接连接。在这些情况下，您可以设置一个思科AMP私有云，它是一个思科专有的产品，用作压缩内部版

AMP 云，以及网络与 AMP 云之间的安全中介。将 防火墙管理中心连接到 AMP 私有云会禁用到公共 AMP 云的现有直接连接。

所有到 AMP 云的连接均通过 AMP 私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。此项筛选包括，对在网络流量中检测到的文件进行处置情况查询、接收追溯性恶意软件事件等等。AMP 私有云不通过外部连接共享任何终端数据。

注释 AMP 私有云既 **不** 执行动态分析，也不支持匿名检索其他依靠思科综合安全智能 (CSI)（例如，URL 和安全智能过滤）的功能的威胁情报。

有关 AMP 私有云（有时称为“AMPv”）的信息，请参阅 https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html。

连接到 AMP 私有云

开始之前

- 根据该产品的文档中的方向配置思科AMP私有云。在配置过程中，请记下私有云的主机名。配置 防火墙管理中心上的连接需要使用此主机名。
- 确保 防火墙管理中心 可与 AMP 私有云通信，并确认私有云可访问互联网，以便它可与公有 AMP 云通信。请参阅*Cisco Secure Firewall Management Center* 管理指南中安全、互联网接入和通信端口下的主题。
- 除非您的部署与Secure Endpoint 集成，否则每个 防火墙管理中心 只能有一个 AMP 云连接。此连接标记为 **面向网络的 AMP** 或 **面向 Firepower 的 AMP**。

  如果与 Secure Endpoint 集成，可以配置多个 Secure Endpoint 云连接。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择**私有云 (Private Cloud)**。

步骤 4 输入 **Name**。

此信息显示在 AMP 私有云生成或传输的恶意软件事件中。

步骤 5 在**主机 (Host)** 字段中，输入在设置私有云时配置的私有云主机名。

步骤 6 点击**证书上传路径 (Certificate Upload Path)** 旁边的**浏览 (Browse)**，浏览至私有云的有效 TLS 或 SSL 加密证书的位置。有关详细信息，请参阅 AMP 私有云文档。

步骤 7 如果要将此私有云用于 恶意软件防护 和Secure Endpoint，请选中 **用于面向 Firepower 的 AMP** 复选框。

如果配置其他私有云来处理 恶意软件防护 通信，则可以清除此复选框；如果这是唯一的 AMP 私有云连接，则无法清除。

在多域部署中，此复选框仅显示在全局域中。每个防火墙管理中心只能有一个恶意软件防护连接。

步骤 8 点击**注册 (Register)**，确认要禁用到 AMP 云的现有直接连接，并最终确认要继续至 AMP 私有云管理控制台以完成注册。

步骤 9 登录管理控制台并完成注册过程。有关进一步说明，请参阅 AMP 私有云文档。

下一步做什么

在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。

管理与 AMP 云的连接（公共或私有）

使用防火墙管理中心管理与用于恶意软件防护 或Secure Endpoint 或两者的公共和私有 AMP 云的连接。

如果不想再从云接收恶意软件相关信息，则可以删除与公共或私有 AMP 云的连接。请注意，使用 Secure Endpoint 或 AMP 私有云管理控制台取消注册连接不会从系统中删除连接。取消注册的连接会在Secure Firewall Management Center Web 界面上显示失败状态。

您还可以临时禁用连接。当重新启用云连接时，云恢复向系统发送数据，包括禁用期内的已排队数据。

⚠

注意 对于已禁用的连接，公共或私有 AMP 云可以存储恶意软件事件和危害表现等，直到重新启用连接。在极少数情况下（例如，事件率超高或连接长时间禁用），云可能无法存储在连接处于禁用状态时生成的所有信息。

在多域部署中，系统会显示在当前域中创建的连接，您可以对其进行编辑。系统还会显示在祖先域中创建的连接，您不可以对其进行管理。要管理较低域中的连接，请切换至该域。每个 防火墙管理中心只能具有一个属于全局域的恶意软件防护 连接。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 管理 AMP 云连接：

- 删除 - 点击 **删除** ( )，然后确认选择。
- 启用或禁用 - 点击滑块，然后确认选择。

下一步做什么

在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。

更改 AMP 选项

过程

步骤 1 选择**集成** > **云服务**。

步骤 2 选择选项：

表 *127:* 适用于网络的 *AMP* 的选项

选项	说明
启用自动本地恶意软件检测更新 (Enable Automatic Local Malware Detection Updates)	本地恶意软件检测引擎使用思科提供的签名对文件进行静态分析和预分类。如果启用此选项，则 防火墙管理中心每 30 分钟检查一次签名更新。
与思科共享恶意软件事件中的 URI (Share URI from Malware Events with Cisco)	系统可以向 AMP 云发送有关网络流量中检测到的文件的信息。此信息包括与被检测的文件相关联的 URI 信息及其 SHA-256 散列值。虽然共享功能是可选的，不过向思科传输此信息对未来的恶意软件识别和跟踪工作有帮助。

步骤 3 点击**保存**。

动态分析连接

动态分析的要求

您必须是管理员、访问管理员或网络管理员用户并且在全局域中，才能使用动态分析。

通过适当的许可证，系统会自动访问 Secure Secure Malware Analytics 云。

动态分析要求托管设备具有对 Secure Secure Malware Analytics 云或本地 Secure Secure Malware Analytics 设备的端口 443 的直接或代理访问权限。

另请参阅哪些文件符合动态分析的条件？，第 2312 页。

如果您将连接到本地 Secure Secure Malware Analytics 设备，另请参阅连接到内部动态分析设备，第 2299 页中的前提条件。

查看默认动态分析连接

默认情况下，Secure Firewall Management Center 可以连接到 Secure Secure Malware Analytics 公共云以提交文件并检索报告。您既不能配置也不能删除此连接。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 请点击 **编辑** ()。

注释

有关**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)** 页面上的 **关联** （） 的信息，请参阅启用对公共云中动态分析结果的访问权限，第 2300 页。

动态分析本地设备 (Cisco Secure Secure Malware Analytics)

如果您的组织担心提交文件到公共 Secure Secure Malware Analytics 云可能会造成隐私或安全问题，您可以部署内部 Secure Secure Malware Analytics 设备。如同公共云一样，内部设备在沙盒环境下运行合格文件，然后向系统传回威胁评分和动态分析报告。但是，内部设备不会与公共云或位于您的网络外部的任何其他系统通信。

有关本地 Secure Secure Malware Analytics 设备的详细信息，请参阅https://www.cisco.com/c/en/us/products/security/threat-grid/index.html。

连接到内部动态分析设备

如果在网络上安装内部 Secure Secure Malware Analytics 设备，则可以配置动态分析连接以提交文件并从该设备中检索报告。当配置内部设备动态分析连接时，可将 Secure Firewall Management Center 注册到内部设备。

开始之前

- 设置本地 Secure Secure Malware Analytics 应用。

  可从 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html获得应用的说明文档：

  请参阅 *Cisco Firepower* 兼容性指南。

- 如果您的 Secure Secure Malware Analytics 设备使用自签名公钥证书，请从 Secure Secure Malware Analytics 设备下载证书；有关您的 Secure Secure Malware Analytics 设备信息，请参阅设备管理员指南。

  如果使用证书颁发机构 (CA) 签名的证书，则证书必须满足以下要求：

  - 必须在 Secure Secure Malware Analytics 设备上安装服务器密钥和签名证书。按照 Secure Secure Malware Analytics 设备《管理员指南》中的上传说明进行操作。
  - 如果存在多级 CA 签名链，则所有必需的中间证书和根证书必须包含在 防火墙管理中心将上传到的单个文件中。
  - 所有证书都必须采用 PEM 编码。

- 文件的换行符必须是 UNIX，而不是 DOS。

- 如果要使用代理连接到内部设备，请配置代理；请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 修改防火墙管理中心 管理接口 。
- 托管设备必须在端口 443 上直接或代理访问 Secure Secure Malware Analytics 设备。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 点击**添加新连接 (Add New Connection)**。

步骤 3 输入 **Name**。

步骤 4 输入**主机**。

步骤 5 在**证书上传 (Certificate Upload)**旁，点击**浏览 (Browse)** 以上传本地设备的证书。

如果 Secure Secure Malware Analytics 设备将提供自签名证书，请上传您从该设备下载的证书。

如果 Secure Secure Malware Analytics 设备将提供 CA 签名证书，请上传包含证书签名链的文件。

步骤 6 如果要使用已配置的代理建立连接，选中 **在可用时使用代理**复选框。

步骤 7 点击 **Register**。

步骤 8 点击**是 (Yes)** 以显示本地 Secure Secure Malware Analytics 设备登录页面。

步骤 9 将用户名和密码输入到本地 Secure Secure Malware Analytics 设备。

步骤 10 点击 **Sign in**（登录）。

步骤 11 您有以下选择：

- 如果先前将 Secure Firewall Management Center注册到内部设备，请点击**返回**。
- 如果未注册 Secure Firewall Management Center，请点击**激活**。

启用对公共云中动态分析结果的访问权限

Secure Secure Malware Analytics 提供的有关已分析文件的报告比 防火墙管理中心提供的要详细。如果您的组织有 Secure Secure Malware Analytics 云账户，则您可以直接访问 Secure Secure Malware Analytics 门户，查看有关从托管设备发出的进行分析的文件的其他详细信息。但是，出于隐私方面的考虑，只有提交文件的组织才能查看文件分析详细信息。因此，在查看此信息之前，您必须将 防火墙管理中心 与其托管设备提交的文件相关联。

开始之前

您必须有一个 Secure Secure Malware Analytics 云账户，并准备好您的账户凭证。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 在 Secure Secure Malware Analytics 云对应的表行中点击 **关联** （ ） 。

将打开一个 Secure Secure Malware Analytics 门户窗口。

步骤 3 登录到 Secure Secure Malware Analytics 云。

步骤 4 点击**提交查询**。

注释
请勿更改**设备 (Devices)** 字段中的默认值。

如果在执行此流程时遇到困难，请与思科 TAC 的 Secure Secure Malware Analytics 代表联系。

此更改最多可能需要 24 小时才能生效。

下一步做什么

激活关联后，请参阅在 *Cisco Secure Firewall Management Center* 管理指南 中 查看思科云中的动态分析结果 。

维护您的系统：符合动态分析条件的文件类型

符合动态分析条件的文件类型列表由漏洞数据库 (VDB) 确定，该列表定期更新（但每天不超过一次）。如果您是管理员用户，则可以更新符合动态分析条件的文件类型。

每个版本中自动提交支持的文件类型可能不同。当前支持自动提交的文件包括：

- PE 可执行文件（仅 32 位）
- EXE
- DLL
- PDF
- MSOLE2（Microsoft 对象链接和嵌入复合文件）
- DOCX、PPTX、XLSX

注释 GZ 和 ZIP 文件类型不支持自动提交。

为确保您的系统拥有最新列表：

过程

步骤 1 执行以下操作之一：

- （推荐）请参阅 *Cisco Secure Firewall Management Center* 管理指南中所述的 漏洞数据库更新自动化
- 定期检查新的 VDB 更新，并根据需要 手动更新 *VDB*（如 *Cisco Secure Firewall Management Center* 管理指南 中所述）。

  如果您选择此选项，建议您安排定期提醒来执行此操作。

步骤 2 如果您的文件策略指定单个文件类型，而不是指定**支持动态分析**文件类型类别，请更新您的文件策略以使用新支持的文件类型。

步骤 3 如果符合条件文件类型列表发生更改，请部署到托管设备。

文件策略和文件规则

创建或编辑策略

开始之前

如果要配置恶意软件防护策略，请参阅 配置文件策略，第 2290 页中的所有必要程序。

过程

步骤 1 选择**策略** > **安全策略** > **恶意软件和文件** 。

步骤 2 创建新策略或编辑现有策略。

如果要编辑现有策略： 如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

提示
要复制现有文件策略，请点击 **复制** ( )，然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

步骤 3 如创建文件规则，第 2315 页中所述，向文件策略添加一个或多个规则。

步骤 4 或者，也可以选择“高级”，并如 高级和存档文件检查选项，第 2303 页中所述配置高级选项。

步骤 5 保存文件策略。

下一步做什么

- 如果要配置恶意软件防护策略，请参阅 配置文件策略，第 2290 页中的其他所需程序。
- 其他:
  - 如将文件策略添加到访问控制配置，第2290页中所述，将该文件策略添加到访问控制规则。
  - 部署配置更改；请参阅 部署配置更改，第 180 页。

高级和存档文件检查选项

文件策略编辑器中的“高级”设置具有以下常规选项：

- **首次文件分析**-选择此选项可在 AMP 云处置处于待定状态时分析首次看到的文件。该文件必须与配置为执行恶意软件云查找和Spero、本地恶意软件或动态分析的规则相匹配。如果取消选择此选项，则会将首次检测到的文件标记为具有“未知”处置情况。
- **启用自定义检测列表** - 阻止自定义检测列表上的文件。
- **启用干净列表**-如果启用，此策略将允许干净列表上的文件。
- **如果 AMP 云处置情况为未知，则根据威胁评分覆盖处置情况**-选择一个选项：
  - 如果您选择 **禁用**， 系统将不会覆盖 AMP 云提供的处置情况。
  - 如果设置了阈值威胁评分，则AMP云判定为“未知”的文件如果其动态分析评分等于或低于阈值，则会被视为恶意软件。
  - 如果选择更低的阈值，请增加被视为恶意软件的文件数。根据文件策略中选择的操作，这可能导致受阻文件数增加。
  - 有关威胁评分范围的数字，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的威胁评分和动态分析摘要报告 。

文件策略编辑器中的“高级”设置具有以下存档文件检查选项：

- **检测存档** - 对于大小可达**可存储的最大文件大小**高级访问控制设置的存档文件，启用内容检测。
- **阻止加密存档**-阻止受密码保护的存档。
- **阻止不可检测的存档** - 阻止系统并非因加密原因而无法检测其内容的存档文件。此类文件通常包括损坏的文件，或超过指定的最大存档深度的文件。
- **最大存档深度** - 阻止超过指定深度的嵌套存档文件。此计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

存档文件

存档文件是包含其他文件的文件，例如 `.zip` 或 `.rar` 文件。

如果存档中的任何单个文件与包含阻止操作的文件规则相匹配，系统将阻止整个存档而非该单个文件。

有关存档文件检查选项的详细信息，请参阅高级和存档文件检查选项，第 2303 页。

可进行检查的存档文件

- **文件类型**

  可检查存档文件类型的完整列表会显示在 FMC Web 接口中的文件规则配置页面上。要查看该页面，请参阅创建文件规则，第 2315 页。

  包含的可检查的文件显示在同一页面上。

- **文件大小**

  您可以检查的存档文件大小可达**可存储的最大文件大小**文件策略高级访问控制设置。

- **嵌套存档**

  存档文件可以包含其他存档文件，而其他存档文件反过来又可以包含所述存档文件。文件嵌套的级别是其存档文件深度。请注意，深度计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

  系统可以检查最外层存档文件（级别 0）以下的最多三级嵌套文件。您可以将文件策略配置为阻止超过该深度（或指定的较低最大文件深度）的存档文件。

  如果您选择不阻止超过最大存档文件深度 3 的文件，当受监控流量中出现包含某些可提取内容和某些嵌套深度为 3 或更大值的内容的存档文件时，系统仅检查其能够检查的文件并报告相关数据。

  所有适用于未压缩的文件的功能（例如，动态分析和文件存储）也适用于存档文件中的嵌套文件。

- **加密文件**

  您可以将系统配置为阻止内容已加密或无法检查的存档。

- **不会检查的存档**

  如果包含存档文件的流量在安全智能阻止列表或不阻止列表中，或者，如果顶级存档文件的 SHA - 256 值在自定义检测列表中，则系统将不检查该存档文件的内容。

  如果嵌套文件被阻止，则整个存档也将被阻止；但是，如果嵌套文件被允许，则存档不会自动通过（取决于任何其他嵌套文件和特性）。

  无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。

存档文件处置情况

存档文件处置情况基于分配给存档内文件的处置情况。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 `Malware` 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 `Unknown`；如果其仅包含安全文件，则其性质为 `Clean`。

表 *128:* 按内容划分的存档文件处置情况

存档文件性质	未知文件数	干净文件数	恶意软件文件数
未知	1 个或更多	任意	0
干净 (Clean)	0	1 个或更多	0
恶意软件 (Malware)	任意	任意	1 或更多

存档文件与其他文件一样可以具有自定义检测 (Custom Detection) 或不可用 (Unavailable) 处置情况（如果符合这些处置情况的条件）。

查看存档内容和详细信息

如果将文件策略配置为检查存档文件内容，当存档文件出现在文件事件、恶意软件事件或捕获的文件中时，您可以使用“分析 > 文件”菜单下页面上表格中的上下文菜单，及网络文件轨迹查看器查看有关存档内文件的信息。

存档的所有文件内容均以表形式列出，同时显示其相关信息的摘要：名称、SHA-256 散列值、类型、类别和存档深度。每个文件旁边都会显示一个网络文件轨迹图标，点击该图标即可查看有关该特定文件的详细信息。

使用自定义列表覆盖文件处置情况

如果文件在 AMP 云中的处置情况据您所知不正确，您可向覆盖云中处置情况的文件列表中添加该文件的 SHA-256 值：

- 要好像 AMP 云已为文件分配了干净的处置一样对其进行处理，请将文件添加到干净列表。
- 要好像 AMP 云已为文件分配了恶意软件处置一样对其进行处理，请将文件添加到自定义检测列表。

在后续检测中，设备无需重新评估文件处置情况即可允许或阻止该文件。您可以按文件策略使用干净的列表或自定义检测列表。

注释 要计算文件的 SHA-256 值，您必须将文件策略中的一条规则配置为对匹配的文件执行恶意软件云查找或阻止恶意软件。

有关在 Firepower 中使用文件列表的完整信息，请参阅文件列表，第 2650 页。

或者，如果适用，请使用来自Secure Endpoint 的集中文件列表，第 2305 页。

来自 *Secure Endpoint* 的集中文件列表

如果您的组织已部署Secure Endpoint，则在 Firepower 查询 AMP 云获取文件处置情况时，它可以使用在Secure Endpoint 中创建的阻止名单和允许名单。

要求：

- 您的组织使用的必须是 AMP 公共云。
- 您的组织已部署 Secure Endpoint。
- 已使用 集成 Firepower 和 Secure Endpoint， 第 2321 页 中的过程将系统注册到 Secure Endpoint。

要创建和部署这些列表，请参阅Secure Endpoint 的相关文档或在线帮助。



注释 在 Firepower 中创建的文件列表会覆盖在Secure Endpoint 中创建的文件列表。

管理文件策略

“文件策略”(File Policies) 页面显示现有文件策略的列表及其上次修改日期。您可以使用此页面来管理文件策略。



注释 系统会检查符合动态分析条件的文件类型列表的更新（每天不超过一次）。如果合格文件类型列表更改，这会构成文件策略发生更改；任何使用该文件策略的访问控制策略在部署于任何设备时都会标记为过期。在更新的文件策略可在设备上生效之前，必须先部署策略。请参阅维护您的系统：符合动态分析条件的文件类型， 第 2301 页。

过程

步骤 1 选择**策略** > **安全策略** > **恶意软件和文件** 。

步骤 2 管理文件策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略。
- 创建 - 要创建文件策略，请点击**新建文件策略 (New File Policy)**，然后如创建或编辑策略， 第 2302 页中所述继续操作。
- 复制 - 要复制文件策略，请点击 **复制** ()。

  如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 如果要删除文件策略，请点击 **删除** ()，然后按照提示点击**是**和**确定**。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 部署 - 选择 **部署** > **部署**；请参阅 部署配置更改， 第 180 页。
- 编辑 - 如果要修改现有文件策略，请点击 **编辑** ()。

- 报告 - 点击**报告** ( )；请参阅生成当前策略报告，第 198 页。

文件规则

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

例如，如果某个文件匹配某个规则，则该规则可以：

- 根据简单的文件类型匹配允许或阻止文件
- 根据处置情况阻止文件（无论评估是否表明它是恶意的）
- 将文件存储到设备（有关信息，请参阅捕获的文件和文件存储，第 2313 页）
- 提交储存的（捕获的）文件以进行本地恶意软件、Spero 或动态分析

此外，文件策略还可以：

- 根据干净的列表或自定义检测列表中的条目自动将文件视为干净的文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件（例如，`.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大存档深度或因其他原因无法检查的存档文件

文件规则组成部分

表 *129:* 文件规则组成部分

文件规则组成部分	说明
应用协议	系统可以检测和检查通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。**Any**（默认值）检测 HTTP、SMTP、IMAP、POP3、FTP 和 NetBIOS-ssn (SMB) 流量中的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、HTTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、HTTP、SMTP 和 NetBIOS-ssn (SMB) 传出的流量。 **提示** 无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。

文件规则组成部分	说明
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 请注意，可执行文件包括可以运行宏和脚本的文件类型，因为它们可能包含恶意软件。 有关系统可检测的文件类型列表，请选择**策略**>**安全策略**>**恶意软件和文件**，创建一个临时的新文件策略，然后点击**添加规则**。选择文件类型类别，系统可以检查的文件类型会显示在**文件类型**列表中。 **注释** 频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量（例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 根据所选操作，您可以配置系统是存储文件还是对文件执行 Spero、本地恶意软件或动态分析。如果选择“阻止”(Block) 操作，还可以配置系统是否还重置受阻连接。 有关这些操作和选项的说明，请参阅文件规则操作，第 2308 页。 文件规则是以规则操作顺序而非数字顺序进行评估。有关详细信息，请参阅文件规则操作：评估顺序，第 2314 页。

文件规则操作

借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。文件策略必须包含一个或多个规则才能生效。您可以在文件策略中使用单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件规则操作

- 检测文件规则允许将特定文件类型的检测记录到数据库，同时仍允许其传输。
- 阻止文件规则允许阻止特定文件类型。您可以配置选项，以在阻止文件传输时重置连接并将已捕获的文件存储到托管设备。
- 恶意软件云查找 *(Malware Cloud Lookup)* 规则允许您获取并记录通过网络传输的文件的处置情况，同时仍允许文件传输。

- 阻止恶意软件 *(Block Malware)* 规则允许您计算特定文件类型的 SHA-256 散列值，查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止表示为威胁的文件。

文件规则操作选项

根据所选择的操作，有不同的选项：

文件规则操作选项	能否阻止文件？	能否阻止恶意软件？	能否检测文件？	能否进行恶意软件云查找？
MSEXE 的 Spero 分析*	否	是，可以提交可执行文件	否	是，可以提交可执行文件
动态分析*	否	是，可以提交具有未知文件处置情况的可执行文件	否	是，可以提交具有未知文件处置情况的可执行文件
容量处理	否	是	否	是
本地恶意软件分析*	否	是	否	是
重置连接	是（推荐）	是（推荐）	否	否
存储文件	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型

* 有关这些选项的完整信息，请参阅恶意软件保护选项（在文件规则操作中），第 2309 页及其子主题。



注意 启用或禁用**检测文件**或**阻止文件**规则中的**存储文件**，或者添加第一条或删除最后一条将**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）、在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。结合起来的文件规则

恶意软件保护选项（在文件规则操作中）

系统运用多种文件检测和分析方法来确定文件是否包含恶意软件。

根据您在文件规则中启用的选项，系统将按顺序使用以下工具检查文件：

1. Spero 分析，第 2311 页 和 AMP 云查找，第 2311 页
2. 本地恶意软件分析，第 2312 页
3. 动态分析，第 2312 页

有关这些工具的比较，请参阅恶意软件防护选项的比较，第 2310 页。

（如果您愿意的话，还可以根据文件类型阻止所有文件。有关详细信息，请参阅按类型阻止所有文件，第 2314 页。）

另请参阅（可选）Secure Endpoint 的恶意软件防护，第 2319 页和子主题中有关思科Secure Endpoint产品的信息。

恶意软件防护选项的比较

下表详细介绍每种类型的文件分析的优缺点，以及每种恶意软件防护方法确定文件处置的方式。

分析类型	优点	限制	恶意软件识别
斯佩罗分析	可执行文件的结构分析，将 Spero 签名提交到AMP 云进行分析	没有本地恶意软件分析或动态分析彻底，仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
本地恶意软件分析	比动态分析消耗的资源少，返回结果更快，尤其当检测到的恶意软件较常见时	分析结果没有动态分析的结果彻底	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
动态分析	使用 Secure Secure Malware Analytics对未知文件的彻底分析	符合条件的文件将上传到公共云或本地设备。完成分析需要一些时间	威胁评分确定文件的恶意程度。处置情况根据文件策略中配置的威胁评分阈值。
Spero 分析结合本地恶意软件分析	比配置本地恶意软件分析和动态分析消耗的资源少，仍使用 AMP 云资源识别恶意软件	没有动态分析彻底，Spero 分析仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
Spero 分析结合动态分析	在提交文件和 Spero 签名时使用完整的 AMP 云功能	获取结果的速度没有使用本地恶意软件分析获取结果的速度快	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况根据文件策略中配置的威胁评分阈值更改，并在 Spero 分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)。

分析类型	优点	限制	恶意软件识别
本地恶意软件分析结合动态分析	使用两种类型的文件分析使分析结果更彻底	比单独使用任一种分析消耗的资源多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
Spero 分析、本地恶意软件分析结合动态分析	分析结果最彻底	运行所有三种类型的文件分析消耗的资源最多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在 Spero 分析或本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
（阻止传输指定文件类型的所有文件）	不需要 恶意软件防御许可证 （从技术上讲此选项不是恶意软件防护选项。）	合法文件也将被阻止	（不执行任何分析。）

注释 预分类本身并不确定文件的处置情况；它只是确定文件是否符合动态分析条件的一个因素。

Spero 分析

Spero 分析检查结构特征，例如可执行文件中的元数据和报头信息。根据此信息生成 Spero 签名后，若文件是合法可执行文件，则设备会将其提交到 AMP 云中的 Spero 启发式引擎。基于 Spero 签名，Spero 引擎确定文件是否为恶意软件。您还可以配置以下规则：提交文件以进行 Spero 分析，而不将其提交到 AMP 云。

请注意，您无法手动提交文件以进行 Spero 分析。

AMP 云查找

对于符合条件使用高级恶意软件防护进行评估的文件，防火墙管理中心执行恶意软件云查找，根据其 SHA-256 散列值在 AMP 云中查询文件的处置情况。

为了提高性能，系统会缓存由云返回的处置情况，并为已知文件使用缓存的处置情况而不是查询 AMP 云。有关此缓存的详细信息，请参阅缓存处置情况持久性 ，第 2312 页。

本地恶意软件分析

本地恶意软件分析允许托管设备使用由Talos 智能小组 提供的检测规则集，在本地检查可执行文件、PDF、办公文档以及其他类型的文件是否存在最常见的恶意软件类型。由于本地恶意软件分析不需要查询 AMP 云，也不运行该文件，因此节约了时间和系统资源。

如果系统通过本地恶意软件分析识别恶意软件，则它会将现有文件处置情况从“未知”(Unknown) 更改为“恶意软件”(Malware)。然后，系统会生成一个新恶意软件事件。如果系统未识别恶意软件，则它不会将文件处置情况从“未知”(Unknown) 更改为“干净”(Clean)。系统运行本地恶意软件分析后，会缓存 SHA-256 散列值、时间戳以及处置情况等文件信息，以便在特定时间段内再次检测时，系统可以在不进行其他分析的情况下识别恶意软件。有关缓存的详细信息，请参阅缓存处置情况持久性，第 2312 页。

本地恶意软件分析不需要与 Secure Secure Malware Analytics 云建立通信。但是，您必须配置与云的通信，以提交文件以进行动态分析，并将更新下载到本地恶意软件分析规则集。

缓存处置情况持久性

从 AMP 云查询返回的处置情况、关联的威胁评分以及本地恶意软件分析分配的处置情况都具有生存时间 (TTL) 值。保持某种处置情况而无更新达到 TTL 值中指定的持续时间后，系统会清除缓存的信息。安全状态及相关的威胁评分具有以下 TTL 值：

- “干净”(Clean) - 4 小时
- “未知”(Unknown) - 1 小时
- “恶意软件”(Malware) - 1 小时

如果对缓存进行查询发现已超时的缓存处置情况，系统会向 本地恶意软件分析数据库和 AMP 云重新查询新的处置情况。

动态分析

您可以将文件策略配置为使用思科的文件分析和威胁情报平台 Secure Secure Malware Analytics （以前称为 Threat Grid）自动提交文件以进行动态分析。

设备将符合条件的文件提交到 Secure Secure Malware Analytics （公共云或本地设备，以您指定的为准），无论设备是否存储文件。

Secure Secure Malware Analytics 在沙盒环境中运行该文件，分析文件的行为以确定该文件是否为恶意文件，然后返回威胁评分，指明文件包含恶意软件的可能性。您可以通过威胁评分查看动态分析摘要报告，该报告包含分配该威胁评分的原因。您还可以查看 Secure Secure Malware Analytics 以查看您的组织提交的文件的详细报告，以及您的组织未提交的文件的有限数据的清理报告。

有关思科 Secure Secure Malware Analytics的详细信息，请参阅 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

要配置系统以执行动态分析，请参阅动态分析连接，第 2298 页下面的主题。

哪些文件符合动态分析的条件？

文件是否符合动态分析的条件取决于：

- 文件类型
- 文件大小
- 文件规则的操作

此外：

- 系统只会提交与您配置的文件规则匹配的文件。
- 在发送文件进行分析时，该文件的恶意软件云查找性质必须为“未知”(Unknown) 或“不可用”(Unavailable)。
- 系统必须将文件预分类为潜在的恶意软件。

动态分析和容量处理

在设备无法与云通信或已达到最大提交次数而系统暂时无法将文件提交到云时，容量处理允许您暂时地存储符合动态分析条件的文件。当阻碍条件消除后，系统会提交存储的文件。

一些设备可以将文件存储在设备硬盘驱动器或恶意软件存储包中。另请参阅恶意软件存储包，第2314页。

捕获的文件和文件存储

通过文件存储功能，您可以捕获在流量中检测到的选定文件，并自动将文件副本暂时存储至设备硬盘驱动器（如果已安装）或恶意软件存储包内。

在设备捕获文件后，您可以：

- 将捕获文件存储至设备硬盘驱动器中供后期分析使用。
- 将存储的文件下载至本地计算机，以便进一步实施人工分析或存档。
- 手动提交符合条件的捕获文件，以进行 AMP 云查找或动态分析。

请注意，文件存储在设备中之后，如果未来检测到该文件且设备仍存有该文件，则不会再捕获该文件。

注释 在网络上第一次检测到某个文件时，您可以生成代表文件检测情况的文件事件。但如果您的文件规则执行恶意软件云查找，则系统需要额外的时间来查询AMP云并返回处置情况。由于这种延迟，在网络上第二次出现此文件之前，系统无法存储此文件，并且系统可以立即确定此文件的处置情况。

无论系统捕获还是存储文件，您都可以：

- 从“分析“>”文件“>”捕获的文件”审查捕获文件的信息，包括文件是否存储或提交用于动态分析、文件性质和威胁评分，以便迅速查看网络中检测到的恶意软件潜在威胁。
- 查看文件轨迹，确定其如何穿过网络以及哪些主机有副本。
- 向清空列表或自定义检测列表添加文件，以便在未来检测过程中始终将该文件作为清空或恶意软件性质。

您可以在文件策略中配置文件规则，以便捕获并存储特定类型或者具有特定文件性质的文件（如有）。如果将该文件策略与访问控制策略相关联，并将其部署到设备上，则系统将捕获并存储流量中的匹配文件。还可以限制要存储的最小和最大文件大小。

存储的文件不包含在系统备份中。

您可以在“分析”>“文件”>“捕获的文件”下查看捕获的文件信息，并下载副本进行离线分析。

恶意软件存储包

根据您的文件策略配置，设备可能会将大量文件数据存储到硬盘驱动器。您可以在设备中安装一个恶意软件存储包，系统则会将文件存储到该恶意软件存储包，从而使主硬盘驱动器中有更多空间来存储事件和配置文件。系统会定期删除较早的文件。如果设备的主硬盘驱动器没有足够的可用空间，也未安装恶意软件存储包，则无法存储文件。

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。

如果未安装恶意软件存储包，则在配置设备以存储文件时，该设备会将主硬盘驱动器空间的设定部分分配用于存储捕获文件。如果将容量处理配置为暂时存储文件以进行动态分析，则系统会使用相同的硬盘驱动器分配来存储这些文件，直至可以将这些文件重新提交到云。

在设备中安装恶意软件存储包并配置文件存储或容量处理时，该设备会分配整个恶意软件存储包来用于存储这些文件。设备无法在恶意软件存储包中存储任何其他信息。

在分配的用于存储捕获文件的空间容量填满时，系统将删除最早存储的文件，直到分配的空间达到系统定义的阈值。根据存储的文件数量，在系统删除文件后，您可能会看到磁盘已用空间明显下降。

如果在安装恶意软件存储包时，设备已经存储文件，则下次重新启动设备时，存储在主硬盘驱动器上的任何捕获文件或容量处理文件都会移至恶意软件存储包。设备未来存储的文件都将存储至恶意软件存储包。

有关在 Firepower 设备上使用 MSP 的详细信息，请参阅您的设备的 Firepower 硬件安装指南 。

按类型阻止所有文件

如果您的组织不仅要阻止恶意软件文件的传输，还要阻止某个特定类型的所有文件的传输（无论文件是否包含恶意软件），您可以做到这一点。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，例如多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。

从技术上来说，根据类型阻止所有文件不是恶意软件防护功能；它不需要恶意软件防御许可证，也不会查询 AMP 云。

文件规则操作：评估顺序

文件策略有可能包含针对不同情况的不同操作的多个规则。如果多个规则同时适用于某个特定情况，则将适用本主题中所述的评估顺序。一般来说，简单阻止优先于恶意软件检查和阻止，后者优先于简单检测和日志记录。

文件规则操作的优先顺序为：

- 阻止文件 *(Block Files)*
- 阻止恶意软件
- 恶意软件云查找
- 检测文件

如果已配置，则TID还会影响操作优先级。有关详细信息，请参阅威胁智能导向器-防火墙管理中心操作优先级，第 2433 页。

创建文件规则

注意 启用或禁用**检测文件**或**阻止文件**规则中的**存储文件**，或者添加第一条或删除最后一条将**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）、在部署配置更改时重新启动Snort进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。结合起来的文件规则

开始之前

如果要配置恶意软件防护规则，请参阅配置文件策略，第 2290 页。

过程

步骤 1 选择**策略** > **安全策略** > **恶意软件和文件** 。

步骤 2 点击编辑图标以编辑现有文件策略。

步骤 3 在文件策略编辑器中，点击 **添加规则**。

步骤 4 选择**应用协议 (Application Protocol)** 和**传输方向 (Direction of Transfer)**，如文件规则组成部分，第 2307 页中所述。

步骤 5 选择一个或多个**文件类型**。

显示的文件类型取决于所选的应用协议、传输方向和操作。

可以通过以下方式过滤文件类型列表：

- 在**文件类型类别 (File Type Categories)** 中选择一个或多个文件类型类别，然后点击**所选类别中的所有类型 (All types in selected Categories)**。
- 按名称或说明搜索文件类型。例如，在**搜索名称和说明 (Search name and description)** 字段中键入 **`Windows`** 将会显示 Microsoft Windows 专用文件的列表。

提示
将指针悬停在文件类型上方可查看其描述。

步骤 6 按照文件规则操作，第2308 页中的描述选择文件规则**操作**，并考虑文件规则操作：评估顺序，第2314 页。

可用的操作取决于您所安装的许可证。请参阅文件和恶意软件策略许可证要求，第 2285 页。

步骤 7 根据您选择的操作，配置选项：

- 在阻止文件后重置连接
- 存储与规则匹配的文件
- 启用 Spero 分析*
- 启用本地恶意软件分析*
- 启用动态分析*和容量处理

*有关这些选项的信息，请参阅文件规则操作，第2308 页和恶意软件保护选项（在文件规则操作中），第 2309 页及其子主题。

步骤 8 点击**添加 (Add)**。

步骤 9 点击 **Save** 保存策略。

下一步做什么

- 如果要配置恶意软件防护策略，请返回配置文件策略，第 2290 页。
- 部署配置更改；请参阅 部署配置更改，第 180 页。

用于恶意软件防护的访问控制规则日志记录

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录到Secure Firewall Management Center数据库中。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。

无论调用访问控制规则的日志记录配置如何，系统均会将关联连接的末端记录到 Secure Firewall Management Center数据库。

追溯处置情况更改

文件处置情况可以更改。例如，当发现新信息时，AMP 云可以确定先前被视为安全的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是安全的。如果上周查询过的文件的处置情况发生变化，AMP 云会通知系统，使其在下次检测到该文件进行传输时可以自动采取措施。已更改的处置情况称为追溯性处置情况。

文件和恶意软件检测性能和存储选项

提高文件大小会影响系统的性能。

表 *130:* 高级访问控制文件和恶意软件防护检测选项

字段	说明	准则和限制
限制进行文件类型检测时检查的字节数 (Limit the number of bytes inspected when doing file type detection)	指定执行文件类型检测时检查的字节数。	0 - 4294967295 (4GB) 0 可消除限制。 默认值是 TCP 数据包的最大分片大小（1460 个字节）。在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。 要检测 ISO 文件，请输入大于 36870 的值。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	指定进行恶意软件云查找时，没有缓存的处置情况，系统将会保持匹配**阻止恶意软件 (Block Malware)** 规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	0 - 30 秒 如未联系支持部门，请勿将此选项设置为 0。 由于连接故障，思科建议使用默认值以避免阻止流量。
Do not calculate SHA-256 hash values for files larger than (in bytes)	禁止系统存储大于特定大小的文件，对文件进行恶意软件云查找或阻止文件（如果已添加到自定义检测列表）。	0 - 4294967295 (4GB) 0 可消除限制。 该值必须大于或等于**可存储的最大文件大小（字节）**和**用于动态分析测试的最大文件大小（字节）**。

高级文件检查和存储的最大文件大小（字节）	这些设置指定：
	• 系统可以使用以下检测器检测的文件大小：
	  • 斯佩罗分析
	  • 沙盒和预分类
	  • 本地恶意软件分析/ClamAV
	  • 存档检测
	• 系统可以使用文件规则存储的文件大小。
		0 - 10485760 (10MB)
		0 可禁用文件存储。
		必须小于或等于**可存储的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。

高级文件检查和存储的最小文件大小（字节）		0 - 10485760 (10MB) 0 可禁用文件存储。 必须大于或等于**可存储的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。

字段	说明	准则和限制
用于动态分析测试的最大文件大小（字节）**(Maximum file size for dynamic analysis testing (bytes))**	指定系统可以提交到 AMP 云以供动态分析的最小文件大小。	0 - 10485760 (10MB) 必须小于或等于**用于动态分析测试的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最小文件大小（一天不超过一次）。如果新的最小值大于当前值，当前值会更新为新的最小值，而且策略会标记为过期。
用于动态分析测试的最小文件大小（字节）**(Minimum file size for dynamic analysis testing [bytes])**	指定系统可以提交到 AMP 云以供动态分析的最大文件大小。	0 - 10485760 (10MB) 必须大于或等于**用于动态分析测试的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最大文件大小（一天不超过一次）。如果新的最大值小于当前值，当前值会更新为新的最大值，而且策略会标记为过期。

调整文件和恶意软件检测性能和存储

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，点击**高级设置 (Advanced Settings)**。

步骤 2 点击**文件和恶意软件设置 (Files and Malware Settings)** 旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 设置文件和恶意软件检测性能和存储选项，第 2317 页中所述的任何选项。

步骤 4 点击**确定**。

步骤 5 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

（可选）Secure Endpoint 的恶意软件防护

思科的Secure Endpoint 是一款独立的恶意软件防护产品，它可以补充系统提供的恶意软件防护并与您的 Firepower 部署进行集成。

Secure Endpoint 是思科的企业级高级恶意软件防护解决方案，它在个人用户的终端（计算机和移动设备）上作为轻量级连接器运行，用于发现、了解和阻止高级恶意软件爆发、高级持续威胁和针对性攻击。

Secure Endpoint 的优势包括：

- 为整个组织配置自定义恶意软件检测策略和配置文件，以及对所有用户的文件执行快速扫描和全面扫描
- 执行恶意软件分析，包括查看热图、详细文件信息、网络文件轨迹和威胁根本原因
- 配置爆发控制的多个方面，包括自动隔离、用于阻止运行非隔离可执行文件的应用阻止，以及排除列表
- 创建自定义保护，根据组策略阻止某些应用的执行，并创建自定义允许的应用列表
- 使用Secure Endpoint 管理控制台帮助您减轻恶意软件的影响。管理控制台提供稳健灵活的 Web 界面，您可以通过该界面控制Secure Endpoint 部署的所有方面并管理爆发的所有阶段。

有关Secure Endpoint的详细信息，请参阅：

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- Secure Endpoint 管理控制台中的在线帮助。
- 可从以下位置获取 Secure Endpoint 文档：http://docs.amp.cisco.com。

恶意软件防护比较：Firepower 与Secure Endpoint

表 *131:* 按检测产品进行比较的高级恶意软件防护差异

特性	Firepower 恶意软件防护（恶意软件防护）	Secure Endpoint
文件类型检测和阻止方法（文件控制）	在网络流量中，使用访问控制和文件策略	不支持
恶意软件检测和阻止方法	在网络流量中，使用访问控制和文件策略	在单个终端（最终用户计算机和移动设备）上，使用与 AMP 云进行通信的连接器
检查的网络流量	流量传递通过托管设备	无；终端上安装的连接器直接检查文件

特性	Firepower 恶意软件防护（恶意软件防护）	Secure Endpoint
恶意软件情报数据源	AMP 云（公共或私有）	AMP 云（公共或私有）
恶意软件检测稳健性	有限的文件类型	所有文件类型
恶意软件分析方案	防火墙管理中心为基础的分析，以及在 AMP 云中的分析	防火墙管理中心为基础的分析，以及Secure Endpoint 管理控制台上的其他选项
恶意软件缓解	网络流量中的恶意软件阻止， 防火墙管理中心 发起的补救	基于 Secure Endpoint 的隔离和爆发控制方案，防火墙管理中心发起的纠错
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于防火墙管理中心	防火墙管理中心 和 Secure Endpoint 管理控制台均具有网络文件轨迹。两者均很有用。
所需许可证或订用	执行文件控制和所需的许可证 恶意软件防护	Secure Endpoint 订用。将 Secure Endpoint 数据导入 防火墙管理中心 无需许可证。

关于将 Firepower 与Secure Endpoint 进行集成

如果您的组织已部署Secure Endpoint，您可以选择将该产品与 Firepower 部署进行集成。

与Secure Endpoint 进行集成不需要专用 Firepower 许可证。

集成 Firepower 和Secure Endpoint 的优势

将Secure Endpoint 部署与系统集成具有以下优势：

- Secure Endpoint 中配置的集中屏蔽应用和允许应用可确定从 Firepower 发送到 AMP 云用于处置的文件 SHA 的判定。

  请参阅来自Secure Endpoint 的集中文件列表， 第 2305 页。

- 系统可以将Secure Endpoint 检测到的恶意软件事件导入到 Secure Firewall Management Center，这样您便可以管理这些事件以及系统生成的恶意软件事件。这些事件的导入数据包括扫描、恶意软件检测、隔离、阻止的执行和云召回，以及防火墙管理中心为其监控的主机显示的危害表现 (IOC)。

  有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用*Secure Endpoint* 进行恶意软件事件分析 。

- 您可以在Secure Endpoint 控制台中查看文件轨迹和其他详细信息。

有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用*Secure Endpoint* 控制台中的事件数据 。

重要事项 如果您使用思科 AMP 私有云虚拟设备 (AMPv)，请参阅 Secure Endpoint 和 AMP 私有云，第 2321 页中的限制。

Secure Endpoint 和 AMP 私有云

如果您配置思科 AMP 私有云以收集您的网络的 Secure Endpoint数据，则所有Secure Endpoint 连接器都会将数据都发送到私有云，然后私有云会将这些数据转发到 Secure Firewall Management Center。私有云不通过外部连接共享任何终端数据。

如果您的组织已部署 AMP 私有云，则所有到 AMP 云的连接均通过私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。这包括导入Secure Endpoint 数据。私有云不通过外部连接共享任何终端数据。

如果您使用 AMP 私有云，以下集成功能将不可用：

- 使用Secure Endpoint 中配置的“阻止的应用”和“允许的应用”列表。（这些列表用于阻止或允许文件。）
- Firepower 生成的恶意软件事件在Secure Endpoint 中的可视性。

您可以配置多个私有云来支持所需的容量。

集成 Firepower 和 Secure Endpoint

如果您的组织已部署思科的 Secure Endpoint 产品，您可以将该应用与 Firepower 进行集成以实现集成 Firepower 和Secure Endpoint 的优势，第 2320 页中所述的优势。

在与 Secure Endpoint集成时，即使已配置了 恶意软件防护 （面向 Firepower 的 AMP）连接，也必须配置 Secure Endpoint 连接。您可以配置多个 Secure Endpoint 云连接。

注释 未成功注册的 Secure Endpoint 连接不会影响 恶意软件防护。

开始之前

- 您必须是管理员用户才能执行此任务。
- 如果您的部署使用思科 AMP 私有云虚拟设备，请参阅 Secure Endpoint 和 AMP 私有云，第 2321 页中的限制。
- Secure Endpoint必须在您的网络中正确设置并正常工作。
- 防火墙管理中心 必须具有互联网访问权限。

- 确保您的 防火墙管理中心 和 Secure Endpoint 可以互相通信。请参阅*Cisco Secure Firewall Management Center* 管理指南中安全、互联网接入和通信端口下的主题。
- 如果在重新映像或从备份恢复 防火墙管理中心 之后连接到 AMP 云，请使用 Secure Endpoint 管理控制台移除之前的连接。
- 在此程序期间，您需要使用 Secure Endpoint 凭证来登录 Secure Endpoint 控制台。

过程

步骤 1 选择**集成** > **+ 显示更多** > **AMP** > **AMP 管理**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称**下拉菜单中，选择要使用的云。

- AMP 云最接近 防火墙管理中心的地理位置。

  APJC 是指亚太地区/日本/中国。

- 对于 AMP 私有云 (AMPv)，选择 **私有云** ，然后如 思科 AMP 私有云 ，第 2295 页中所述继续操作。

步骤 4 如果要将此云用于 恶意软件防护 和 Secure Endpoint，请选中**用于面向 Firepower 的 AMP** 复选框。

如果配置其他云来处理 恶意软件防护（面向 Firepower 的 AMP）通信，则可以清除此复选框；如果这是唯一的 AMP 云连接，则无法清除。

步骤 5 点击 **Register**。

旋转状态 （ ） 图标指示连接处于待处理状态，例如，在 防火墙管理中心 上配置连接后，但在使用 Secure Endpoint 控制台对其进行授权之前。**已拒绝**（ ） 图标表示云已拒绝连接，或者连接因其他原因而失败。

步骤 6 确认是否要继续访问 Secure Endpoint 管理控制台，然后登录管理控制台中。

步骤 7 使用管理控制台，授权 AMP 云以将 Secure Endpoint 数据发送到 防火墙管理中心。

步骤 8 如果要限制 防火墙管理中心 接收的数据，请选择您的组织中要为其接收信息的特定组。

默认情况下，AMP 云发送所有组的数据。要管理组，请在 Secure Endpoint 管理控制台上选择 **管理** > **组** 。有关详细信息，请参阅设备管理器联机帮助。

步骤 9 点击**允许 (Allow)** 以启用连接并开始传输数据。

点击**拒绝**会将您返回到 防火墙管理中心，其中连接标记为已拒绝。如果离开 Secure Endpoint 管理控制台上的“应用”页面，并且既未拒绝也未允许连接，则连接在 防火墙管理中心 的 Web 界面上标记为待处理。运行状况监控器在其中任一情况下**不**提示您连接失败。如果稍后要连接到AMP 云，请删除失败或待处理的连接，然后重新创建连接。

未完成 Secure Endpoint 连接注册不会禁用 恶意软件防护 连接。

步骤 10 要验证连接是否已正确配置，请执行以下操作：

a) 在 **集成** > **+ 显示更多** > **AMP** > **AMP 管理** 页面上，点击**思科 AMP 解决方案类型**列中包含Secure Endpoint 的“云名称”。
b) 在显示的Secure Endpoint 控制台窗口中，选择**账户 > 应用**。
c) 验证您的 防火墙管理中心在列表中。
d) 在Secure Endpoint 控制台窗口中，选择**管理 > 计算机**。
e) 验证您的 防火墙管理中心在列表中。

下一步做什么

- 在Secure Endpoint 控制台窗口中，根据需要配置设置。例如，定义您的管理中心的组成员，并分配策略。有关信息，请参阅Secure Endpoint 在线帮助或其他文档。
- 在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。
- 如果防火墙管理中心在初始成功连接后无法连接到Secure Endpoint 门户，或者如果使用 AMP 门户取消注册了连接，则默认运行状况策略会向您发出警告。

  验证是否在**故障排除** > **+ 显示更多** > **运行状况** > **策略** 下启用了**Secure Endpoint 状态**监控器。

网络恶意软件保护和文件策略的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
与 AMP 云的通信	7.0	任意	不再支持使用传统端口 32137 与 AMP 公共云或私有云进行通信。 新增/修改的屏幕：在**系统** > **集成** > **云服务**页面上，对网络的 **AMP 使用旧版端口 32137**选项不再可用。
章节重组	虽然是在第 6.4 版时间段内做出的更改，但是这些更改将会出现在重新发布的所有版本中	任意	重组了本章节的内容以减少混淆。 *Cisco Secure Firewall Management Center* 管理指南 中的某些内容已移至文件/恶意软件事件和网络文件轨迹一章或从中移出。
将 URL 过滤信息移动到了新的“URL过滤”章节	6.3	任意	将有关为 URL 过滤配置云通信的信息移动至新的“URL 过滤”章节。在本章节中对思科 CSI 主题的结构进行了相关更改。



第 62 章

Dynamic Attributes Connector

以下主题讨论如何配置和使用Dynamic Attributes Connector。

- 关于 dynamic attributes connector， 第 2325 页
- Dynamic Attributes Connector 的系统要求， 第 2330 页
- 启用 dynamic attributes connector， 第 2330 页
- 关于控制面板， 第 2333 页
- 创建连接器， 第 2340 页
- 创建动态属性过滤器， 第 2375 页
- 手动获取证书颁发机构 (CA) 链， 第 2378 页
- 在访问控制策略或 DNS 策略中使用动态对象， 第 2381 页
- 动态防火墙， 第 2386 页
- 禁用 dynamic attributes connector， 第 2403 页
- 使用 Secure Firewall Management Center 进行故障排除， 第 2403 页
- 手动获取证书颁发机构 (CA) 链， 第 2403 页
- 安全要求， 第 2406 页
- 互联网接入要求， 第 2407 页
- dynamic attributes connector 的历史记录， 第 2408 页

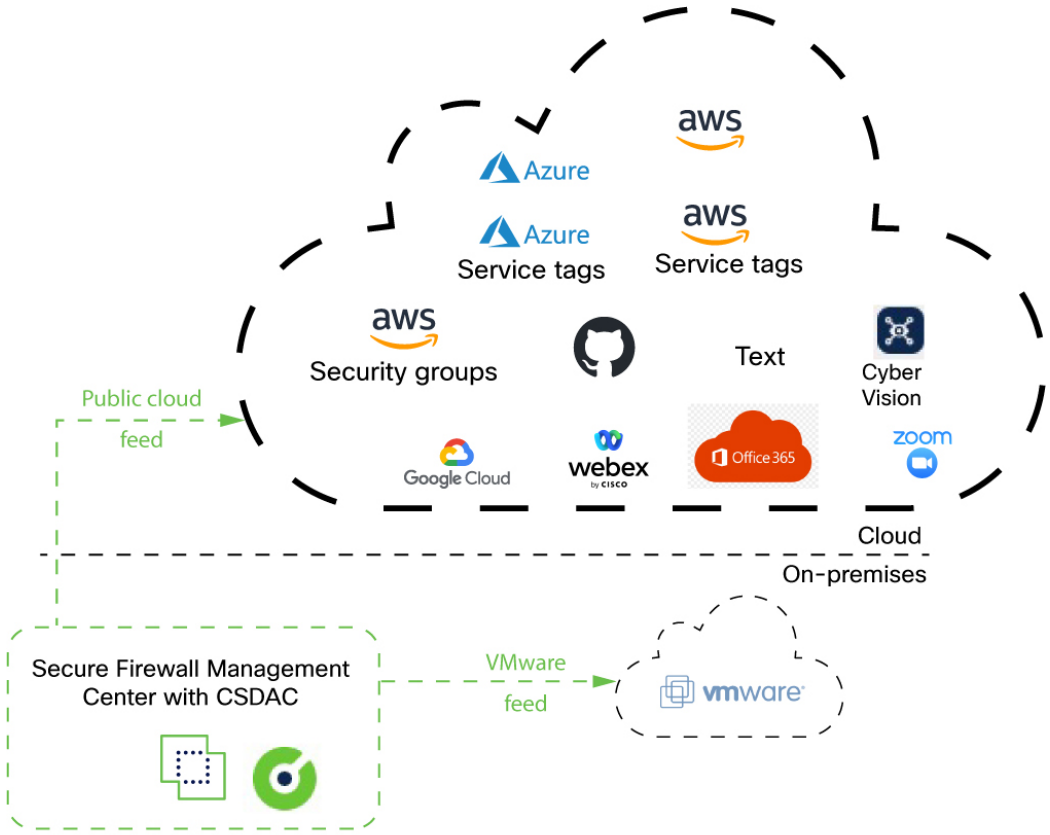
关于 dynamic attributes connector

dynamic attributes connector使您的访问控制策略和 DNS 策略能够实时适应公有云和私有云工作负载以及业务关键型软件即服务 (SaaS) 应用的变化。它通过保持规则最新（无需繁琐的手动更新和策略部署）来简化策略管理。客户需要根据非网络结构（例如虚拟机名称或安全组）定义策略规则，以便即使 IP 地址或 VLAN 发生更改，防火墙策略也能保持不变。

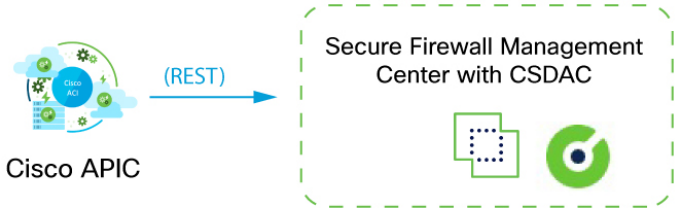
运作方式

本主题讨论 dynamic attributes connector 的架构。

下图显示了系统的总体运行情况。



Cisco APIC integration with the Secure Firewall Management Center



- 系统支持某些公共云提供商。

  本主题讨论受支持的 连接器 （即与这些提供程序的连接）。

- dynamic attributes connector 随 Secure Firewall Management Center 一起提供。

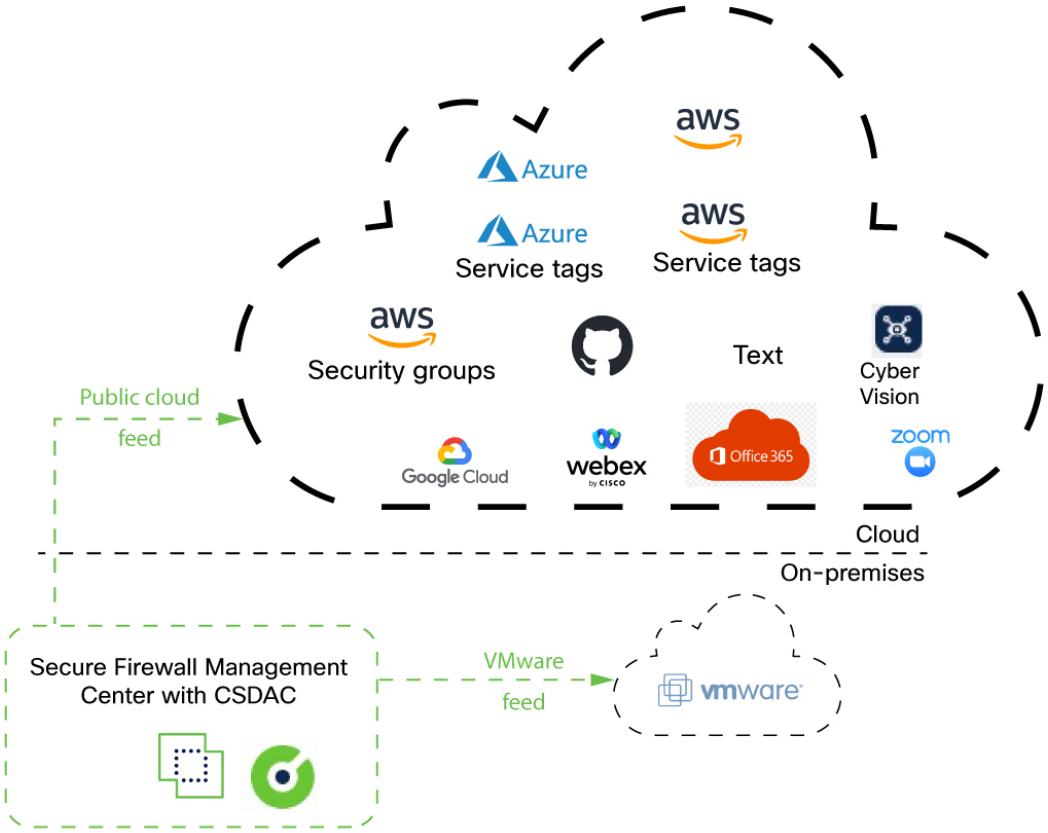
相关主题

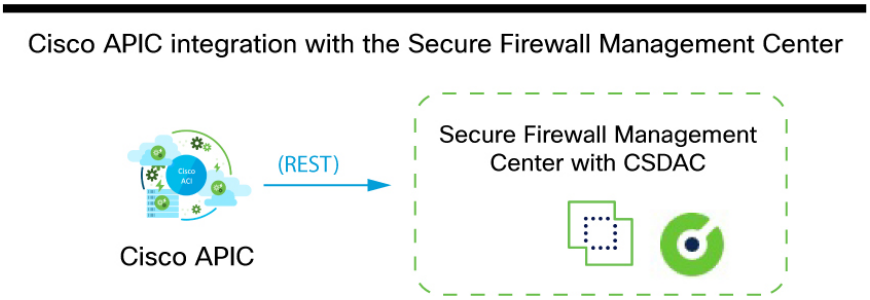
- 启用 dynamic attributes connector， 第 2116 页
- 关于控制面板， 第 2333 页

网络下载模式

dynamic attributes connector 一直在网络下载模式下运行，我们需要从互联网下载其工作所需的映像。如果您有更严格的安全要求，可以考虑气隙模式。

架构概述：





网络下载模式支持：

表 *132:* 按 ***dynamic attributes connector*** 版本和 平台列出的受支持连接器列表

CSDAC 版本	**AWS**	**AWS** 安全组	**AWS** 服务标记	**Azure**	**Azure** 服务标签	思科 **APIC**	**Cisco Cyber Vision**	思科多集群 **Defense**	通用文本	**GitHub**	**Google Cloud**	**Microsoft Office 365**	**Tenable**	**vCenter**	**Webex**	**Zoom**
版本 1.1（本地）	支持	否	否	支持	支持	否	否	否	否	否	否	支持	否	支持	否	否
版本 2.0（本地）	支持	否	否	支持	支持	否	否	否	否	否	支持	支持	否	支持	否	否
版本 2.2（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	否	否
版本 2.3（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	支持	支持
版本 3.0（本地）	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
版本 3.1（本地）	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持
云交付 (Security Cloud Control)	支持	否	否	支持	支持	否	否	支持	否	支持	支持	支持	支持	否	否	否
Secure Firewall Management Center 7.4.1	支持	否	否	支持	支持	否	否	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.6	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.7	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 10.0.0	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持	支持	否	支持	支持	支持

dynamic attributes connector 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DNS规则对动态对象和安全组标记的支持。	10.0.0	10.0.0	您可以在 DNS 策略中配置 DNS 规则以使用动态对象或安全组标记 (SGT)。如果您已经在访问控制规则中使用这些类型的对象，现在可以将其使用扩展到您的 DNS 策略。 我们在添加/编辑 DNS 规则对话框中添加了“动态属性”选项卡。
动态防火墙	10.0.0	10.0.0	以前，Secure Firewall Management CenterSecure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。 借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。 **新增/修改的屏幕：** • 请点击 **集成** > **动态属性连接器**。然后点击身份源名称旁的 ，点击**创建动态防火墙**。
思科 APIC 连接器	10.0.0	10.0.0	dynamic attributes connector 使您能够将 思科 APIC 动态终端组 (EPG) 和终端安全组 (ESG) 数据从 思科 APIC 租户发送到 。 **新增/更新的屏幕：** • **集成** > **动态属性连接器** > **连接器** > **新建连接器**
新连接器	7.6	20241127	AWS 安全组、AWS 服务标签和 Cisco Cyber Vision 这些连接器可以像 Security Cloud Control 一样发送本地 Secure Firewall Management Center 动态对象。 要从本地 dynamic attributes connector 接收动态对象，需要使用 3.0 版本的本地动态属性连接器。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Dynamic Attributes Connector	7.4.0	7.4.0	引入了此功能。 Dynamic Attributes Connector 现在包含在 Secure Firewall Management Center中。您可以在访问控制规则中使用 dynamic attributes connector 从基于云的平台（例如 Microsoft Azure）获取 IP 地址，而无需部署到托管设备。 详细信息： • 此产品随附的 dynamic attributes connector： 关于 dynamic attributes connector，第 2325 页 • 独立 dynamic attributes connector： 《*Cisco Secure Dynamic Attributes Connector* 配置指南》 新的/修改后的屏幕： **集成 > 动态属性连接器**

Dynamic Attributes Connector 的系统要求

Dynamic Attributes Connector 具有以下内存要求：

FMCv：RAM 大小	Secure Firewall Management Center 硬件型号	最大数量（连接器 + Azure AD 领域）
至少 32 GB	Firepower 1000、Firepower 1600、vFMC	10
至少 64 GB	Firepower 2500、Firepower 2600、vFMC 300	20
至少 128 GB	Firepower 4500、Firepower 4600	30

上述限制适用于虚拟机和物理机。

系统会阻止您超出这些限制，以避免部署问题。

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器 ， 第 2340 页。

相关主题

关于 动态防火墙 ， 第 2387 页
如何配置 动态防火墙 ， 第 2387 页

为 Docker 容器配置网络和子网

Dynamic Attributes Connector 使用 Docker 容器检索 Secure Firewall Management Center中的连接器数据。为避免与网络中使用的 Secure Firewall Management Center 管理接口和其他 IP 地址冲突，您可以选择使用本节中讨论的 命令来更改 Docker IP 地址和范围。

关于 Docker 网络

dynamic attributes connector 使用 Docker 守护程序需要以下网络：

- Docker 后台守护程序在内部使用的`docker0` 。
- 一系列名为 `veth`*`number`*的 IPv6 网络。

  这些是 dynamic attributes connector使用的内部网桥网络。
- dynamic attributes connector 连接器使用的 Docker 网桥网络，名为 `br-`*`number`*。

在启用 dynamic attributes connector 之前，只有一个名为 `Docker0` 的 Docker 接口，设置为 172.18.0.1/16（对于 Cisco Secure Firewall Management Center Virtual；本地管理器使用不同的 IP 地址范围）。示例部分的表格提供了详细信息。

更改 Docker 网络和子网

首先启用 dynamic attributes connector，如 启用 dynamic attributes connector ， 第 2116 页中所述。

要更改 Docker 网络和子网，请以具有 `root` 权限的用户身份运行 `/usr/local/sf/bin/change_docker_subnet.sh -b` *`CIDR-network`*`-s` *`address-pool-size`* ，其中：

- `-b CIDR-network` 以 CIDR 表示法设置网络基址池。
- `-s address-pool-size` 设置网络基址的网络掩码。如果网络范围与现有网络范围重叠，可以使用此选项限制基址范围内的地址数量；特别是，我们建议 Secure Firewall Management Center 型号的某些 `-s` 值，以确保不会超过计算机中的可用 RAM。（Docker 容器由 dynamic attributes connector 连接器使用，这些限制显示在 Dynamic Attributes Connector 的系统要求，第 2330 页中。）

重要事项 分配给 Docker 的网络必须在内部网络范围内，并且 不得 与 Secure Firewall Management Center 或内部网络中的其他设备使用的网络冲突。

示例

下表显示示例。

Secure Firewall Management Center 型号	推荐 -s 值	示例 -b 值	Dynamic Attributes Connector 使用的容器地址
Firepower 1000、Firepower 1600、vFMC	27（子网掩码 255.255.255.224）	172.19.0.0/16	30 个 IP 地址 `docker0`: 172.19.0.1 网桥网络 `br-编号` 网关 `172.19.0.33`，子网 为 `172.19.0.32/27` 在 `172.19.0.38/27`、`172.19.0.39/27`等网络中创建的连接器
Firepower 2500、Firepower 2600、vFMC 300	26（子网掩码 255.255.255.192）	192.168.0.0/16	62 个 IP 地址 `docker0`: 192.168.1.1 网桥网络 `br-编号` 网关 `192.168.1.65`，子网为 `192.168.1.64/26` 在 `192.168.1.71/26`、`192.168.1.72/26`等网络中创建的连接器
Firepower 4500、Firepower 4600	25（子网掩码 255.255.255.128）	192.168.0.0/16	126 个 IP 地址 `docker0`: 192.168.1.1 网桥网络 `br-编号` 网关 `192.168.1.129`，子网为 `192.168.1.128/25` 在 `192.168.1.136/25`、`192.168.1.135/25` 等网络中创建的连接器

作为参考，完整的命令如下：

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

检验网络

要验证网络设置，请输入 `sudo docker network inspect muster-net`。命令结果以 JSON 格式显示。

故障排除

以下是使用此命令可能遇到的常见错误的一些解决方案。

错误： `拉取子网值不能大于大小`

解决方案：更改 `-s` 的值，使其小于 CIDR 网络值。

例如，

错误： `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

正确： `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

错误：运行命令后，Docker 网络错误。

解决方案：重新启动 Docker 后台守护程序： `sudo pmtool restartbyid docker`

错误： `无法连接到位于 unix:///var/run/docker.sock 的 Docker 后台守护程序。Docker 守护程序是否正在运行？`

解决方案：重新启动 Docker： `pmtool restartbyid docker`

错误：输入不能为空

`-s` 需要此参数。

错误： `提取大小 - 32 - 不能大于 32 或小于 0`

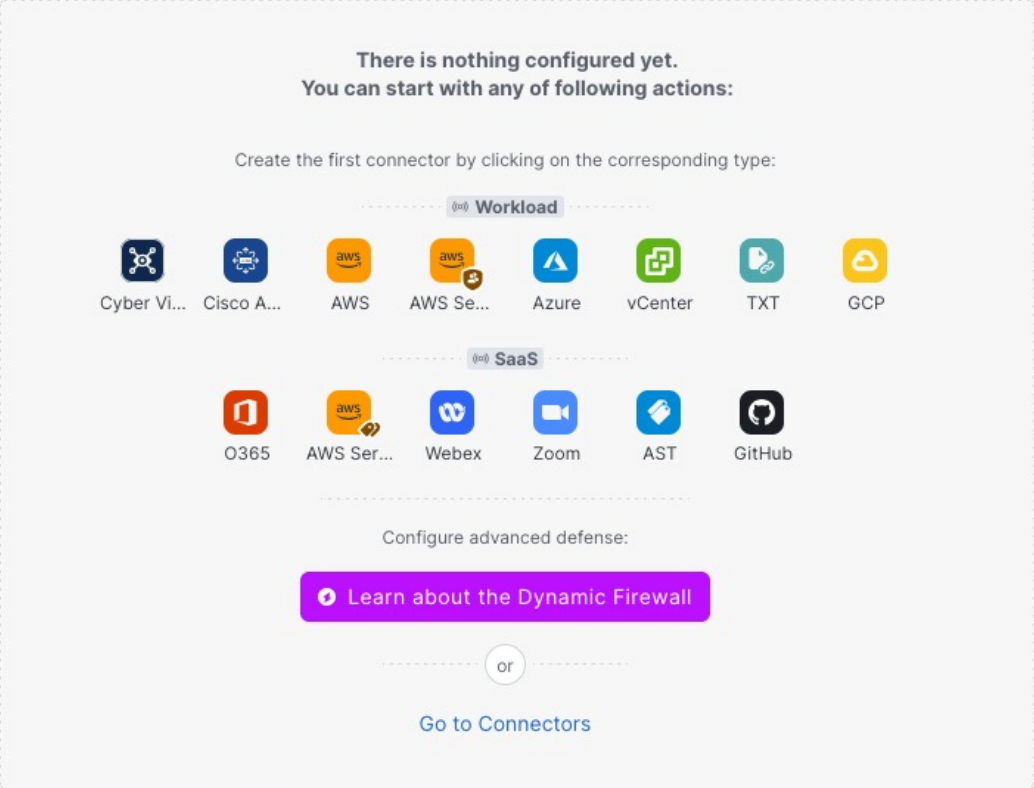
解决方案：更改 `-s` 的值，使其大于 0 且小于 32。

关于控制面板

要访问 dynamic attributes connector 控制面板，请登录 Cisco Secure Firewall 管理器并点击页面顶部的**集成** > **动态属性连接器**。

如果 dynamic attributes connector 未启用，请移动滑块将其启用。此过程需要几分钟时间才能完成。

dynamic attributes connector 控制面板页面会显示连接器、适配器和过滤器的状态。以下是未配置系统的控制面板示例：



您可以通过控制面板来执行的操作包括：

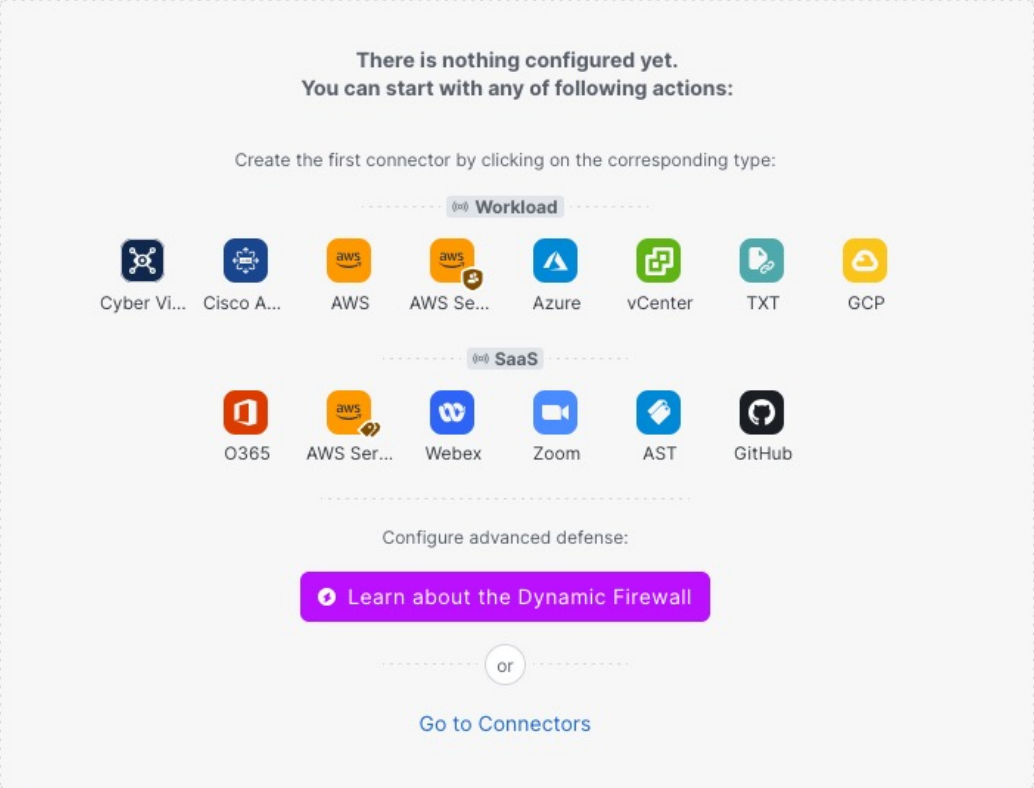
- 添加、编辑和删除连接器和动态属性过滤器。
- 了解连接器和动态属性过滤器之间的关系。
- 查看警告和错误。

相关主题

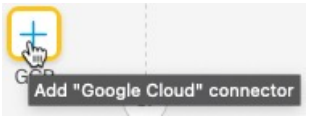
- 未配置系统的控制面板， 第 2334 页
- 已配置系统的控制面板， 第 2335 页
- 添加、编辑或删除连接器， 第 2337 页
- 添加、编辑或删除动态属性过滤器， 第 2338 页

未配置系统的控制面板

未配置系统的 dynamic attributes connector 控制面板页面示例：



控制面板最初显示您可以为系统配置的所有类型的连接器。您可以执行以下任何操作：

- 将鼠标指针悬停在连接器上，然后点击 

新建一个。
- 点击**转到连接器 (Go to Connectors)** 以添加、编辑或删除连接器（适用于同时创建、编辑或删除多个连接器）。

  有关详细信息，请参阅创建连接器，第 2340 页。

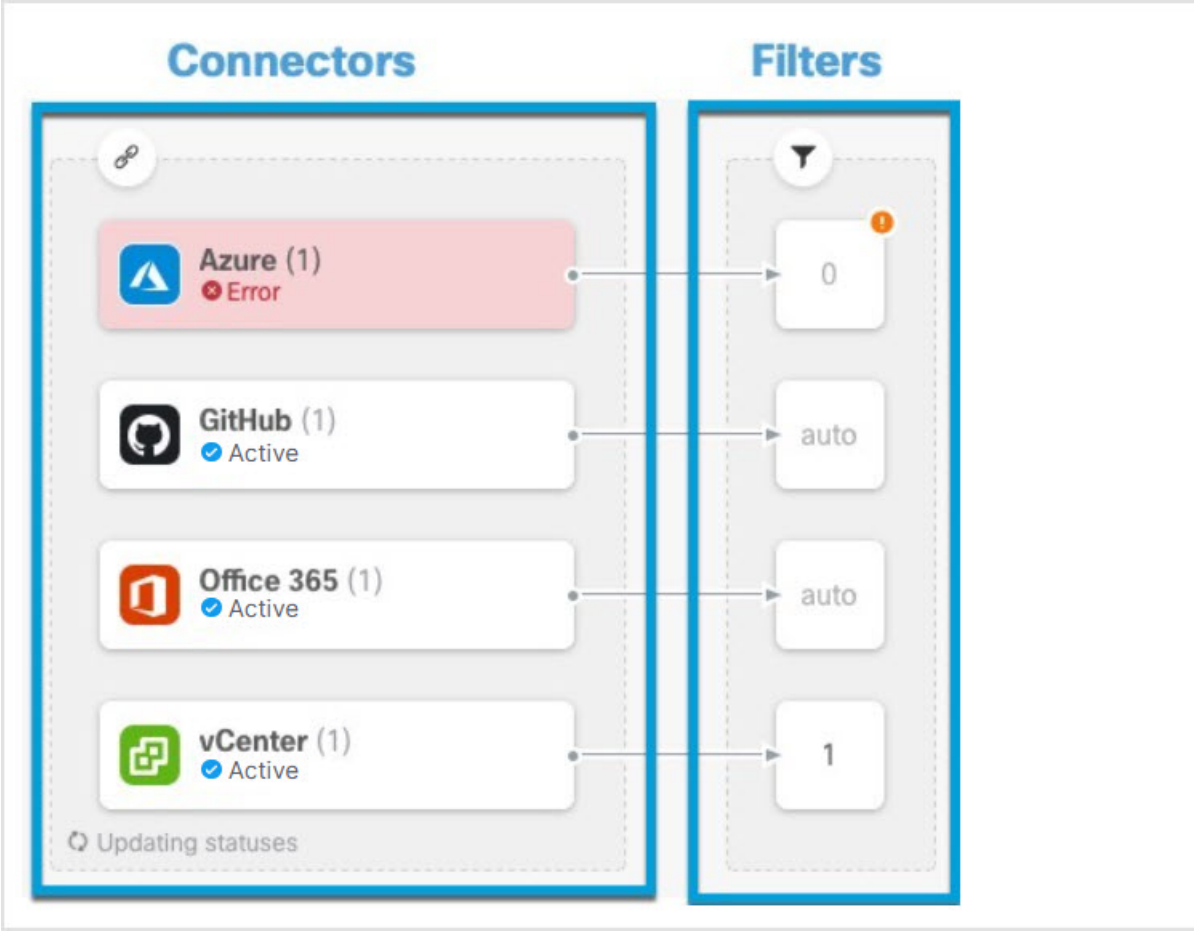
相关主题

- 已配置系统的控制面板，第 2335 页
- 添加、编辑或删除连接器，第 2337 页
- 添加、编辑或删除动态属性过滤器，第 2338 页

已配置系统的控制面板

已配置系统的 dynamic attributes connector 控制面板页面示例：

点击图中的某个区域以了解详细信息，或点击该图后面的链接之一。



1 创建连接器，第 2340 页
2 创建动态属性过滤器，第 2164 页

控制面板显示以下内容（从左到右）：

“连接器”(Connectors) 列	“过滤器”(Filters) 列
连接器列表，其中包含指示每种类型的配置数量的编号。连接器会收集可以发送到 Cisco Secure Firewall 管理器的动态属性。动态属性过滤器会指定要发送的数据。 点击 以查看有关所有已配置连接器的详细信息。您还可以点击连接器的名称来添加、编辑或删除连接器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除连接器，第 2337 页。	与每个连接器关联的动态属性过滤器列表，其中带有一个数字，表示每个过滤器与连接器关联的数量。 点击 以查看有关所有已配置过滤器的详细信息。您还可以点击过滤器的名称来添加、编辑或删除过滤器；或者查看有关它们的详细信息。有关详细信息，请参阅添加、编辑或删除动态属性过滤器，第 2338 页。

注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

控制面板会指明对象是否可用。控制面板页面会每 15 秒刷新一次，但您可以随时点击页面顶部的**刷新** （ ） 来立即刷新。如果问题仍然存在，请检查网络连接。

相关主题

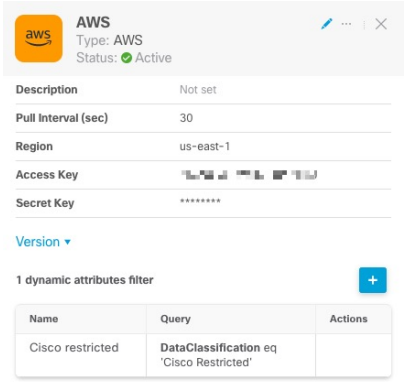
- 添加、编辑或删除连接器 ， 第 2337 页
- 添加、编辑或删除动态属性过滤器 ， 第 2338 页

添加、编辑或删除连接器

通过控制面板，您可以查看或编辑连接器。您可以点击连接器的名称以查看该连接器的所有实例，也可以点击 以查看以下其他选项：

- **转到连接器**可同时查看所有连接器；您可以在此处添加、编辑和删除连接器。
- **添加连接器 (Add Connector)** > **类型**以添加指定类型的连接器。

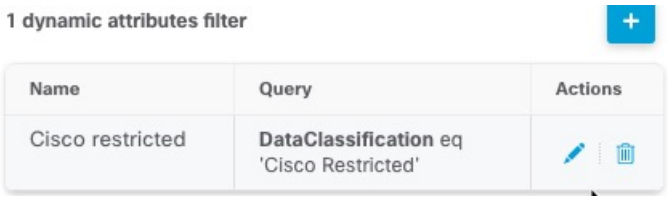
点击连接器列 ( ) 中的任意连接器可显示更多相关信息；示例如下：



您有以下选择：

- 点击 编辑图标 （ ） 以编辑此连接器。
- 点击 更多图标 （ ） 以查看其他选项。
- 点击 关闭面板。
- 点击 **版本**以显示版本。如果思科 TAC 需要，您可以选择将版本复制到剪贴板。

通过面板底部的表格，您可以添加动态属性过滤器；或编辑或 dynamic attributes connector 删除连接器。示例如下：



点击 添加图标 （ ） 以便为此连接器添加动态属性过滤器。有关详细信息，请参阅创建动态属性过滤器，第 2164 页。

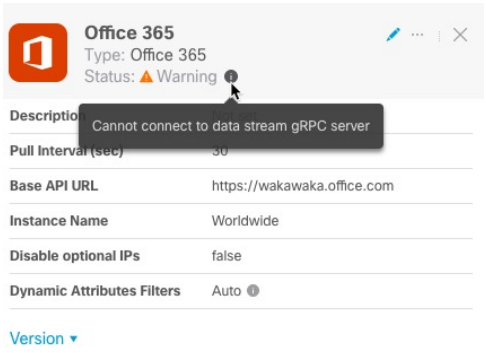
将鼠标指针悬停在“操作”(Actions) 列上，以编辑或删除指示的连接器。

查看错误信息

要查看连接器的错误信息，请执行以下操作：

1. 在控制面板上，点击显示错误的连接器的名称。
2. 在右侧窗格中，点击 **信息** （ ）。

   示例如下。



3. 要解决此问题，请按照创建 Office 365 连接器，第 2368 页中所述编辑连接器设置。
4. 如果您无法解决问题，请点击**版本 (Version)** 并将版本复制到文本文件。
5. 向思科 TAC 提供所有这些信息。https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

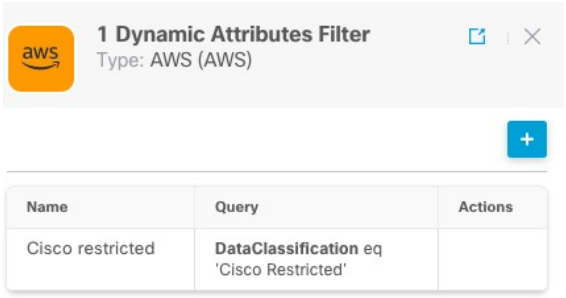
添加、编辑或删除动态属性过滤器

控制面板让您能够添加、编辑或删除动态属性过滤器。您可以点击过滤器的名称以查看该过滤器的所有实例，也可以点击 以查看下列附加选项：

- **转至动态属性过滤器** 以查看所有已配置的动态属性过滤器。您可以从这里添加、编辑或删除动态属性过滤器。
- **添加动态属性过滤器**以添加过滤器。

有关添加动态属性过滤器的详细信息，请参阅创建动态属性过滤器，第 2164 页。

如下所示：



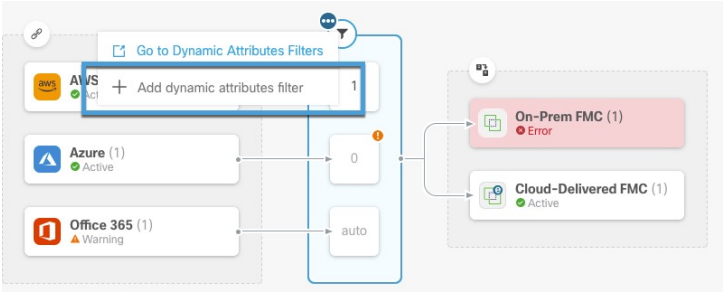
注释 某些连接器（例如 Outlook 365 和 Azure 服务标记）会自动提取可用的动态对象，而无需使用动态属性过滤器。这些连接器在 列中显示为**自动 (Auto)**。

您有以下选择：

- 点击过滤器实例可查看与连接器关联的动态属性过滤器的摘要信息。
- 点击 添加图标 （ ） 以添加新的动态属性过滤器。

  有关详细信息，请参阅创建动态属性过滤器，第 2164 页。
- 在表示指明的连接器没有关联的动态属性过滤器的过滤器列 ( ) 中点击 。如果没有关联的过滤器，连接器将无法向 防火墙管理中心 发送任何内容。

  解决此问题的一种方法是点击过滤器列中的 ，然后点击**添加动态属性过滤器 (Add Dynamic Attributes Filter)**。示例如下。



- 点击 以添加、编辑或删除过滤器。

- 点击 × 关闭面板。

创建连接器

连接器是云服务的接口。连接器从云服务检索网络信息，以便网络信息可用于 Secure Firewall Management Center上的策略。

我们支持以下内容：

表 *133:* 按 *dynamic attributes connector* 版本和 平台列出的受支持连接器列表

CSDAC 版本	AWS	AWS 安全组	AWS 服务标记	Azure	Azure 服务标签	思科 APIC	Cisco Cyber Vision	思科多集群 Defense	通用文本	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
版本 1.1（本地）	支持	否	否	支持	支持	否	否	否	否	否	否	支持	否	支持	否	否
版本 2.0（本地）	支持	否	否	支持	支持	否	否	否	否	否	支持	支持	否	支持	否	否
版本 2.2（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	否	否
版本 2.3（本地）	支持	否	否	支持	支持	否	否	否	否	支持	支持	支持	否	支持	支持	支持
版本 3.0（本地）	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
版本 3.1（本地）	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持
云交付 (Security Cloud Control)	支持	否	否	支持	支持	否	否	支持	否	支持	支持	支持	支持	否	否	否
Secure Firewall Management Center 7.4.1	支持	否	否	支持	支持	否	否	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.6	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 7.7	支持	支持	支持	支持	支持	否	支持	否	支持	支持	支持	支持	否	支持	支持	支持
Secure Firewall Management Center 10.0.0	支持	支持	支持	支持	支持	支持	支持	否	支持	支持	支持	支持	否	支持	支持	支持

Amazon Web Services 连接器 — 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 AWS 导入 Secure Firewall Management Center，以便用于策略。

动态属性已导入

我们从 AWS 导入以下动态属性：

- 标签，可用于组织 AWS EC2 资源的用户定义的键值对。

  有关更多信息，请参阅 AWS 文档中的 标记 EC2 资源

- AWS 中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求用户至少具有允许 `ec2:DescribeTags`、`ec2:DescribeVpcs` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

为 dynamic attributes connector 创建具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Amazon Web Services 连接器 — 关于用户权限和导入的数据，第 2341 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。可以稍后授予用户访问权限。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

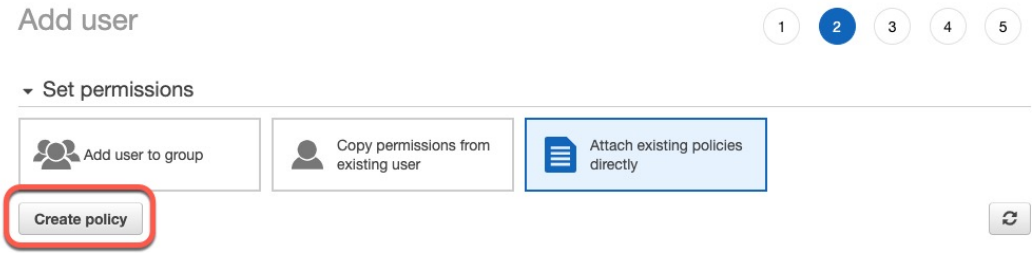
注释
这是您检索用户密钥的唯一机会。

步骤 11 点击关闭 (Close)。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击访问管理 (Access Management) > 策略 (Policies)。

步骤 13 点击创建策略 (Create Policy)。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 JSON。



步骤 15 在字段中输入以下策略：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

步骤 16 点击下一步 (Next)。

步骤 17 点击审核 (Review)。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击创建策略 (Create Policy)。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击操作 (Actions) > 附加 (Attach)。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击附加策略 (Attach Policy)。

下一步做什么

创建 AWS 连接器，第 2343 页。

创建 AWS 连接器

此任务讨论如何配置将数据从 AWS 发送到 Secure Firewall Management Center 以用于访策略的连接器。

开始之前

创建至少具有为 dynamic attributes connector 创建具有最小权限的 AWS 用户，第 2341 页中所述权限的用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标（），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。
地区	（必需。）输入您的 AWS 区域代码。
访问密钥	（必需。）输入访问密钥。
加密密钥	（必需。）输入加密密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

Amazon Web 服务安全组连接器 - 关于用户权限

dynamic attributes connector 会将动态属性从 AWS 导入 Secure Firewall Management Center，以便用于策略。

所需的最低权限

dynamic attributes connector 要求用户至少具有允许 `ec2:DescribeTags`、`ec2:DescribeVpcs` 和 `ec2:DescribeInstances` 以便能够导入动态属性的策略。

为 dynamic attributes connector 创建具有最小权限的 AWS 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Amazon Web Services 连接器 — 关于用户权限和导入的数据，第 2341 页。

开始之前

您必须已设置 Amazon Web 服务 (AWS) 帐户。有关执行此操作的更多信息，请参阅 AWS 文档中的此文章。

过程

步骤 1 以具有网络管理员角色的用户身份登录 AWS 控制台。

步骤 2 在控制面板中，点击**安全、身份和合规性 (Security, Identity & Compliance)** > **IAM**。

步骤 3 点击**访问管理 (Access Management)** > **用户 (Users)**。

步骤 4 点击**添加用户 (Add Users)**。

步骤 5 在**用户名 (User Name)** 字段中，输入用于标识用户的名称。

步骤 6 点击**访问密钥 - 编程访问 (Access Key - Programmatic Access)**。

步骤 7 在“设置权限”(Set permissions) 页面中，点击**下一步 (Next)** 而不授予用户任何访问权限；稍后执行此操作。可以稍后授予用户访问权限。

步骤 8 如果需要，向用户添加标签。

步骤 9 点击**创建用户**。

步骤 10 点击 **Download.csv**，将用户的密钥下载到计算机。

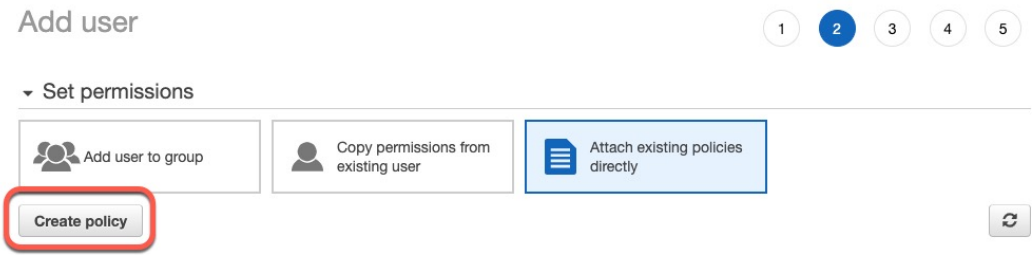
注释
这是您检索用户密钥的唯一机会。

步骤 11 点击**关闭 (Close)**。

步骤 12 在身份和访问管理 (IAM) 页面的左侧列中，点击**访问管理 (Access Management)** > **策略 (Policies)**。

步骤 13 点击**创建策略 (Create Policy)**。

步骤 14 在“创建策略”(Create Policy) 页面中，点击 **JSON**。



步骤 15 在字段中输入以下策略：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
   ],
   "Resource": "*"
  }
 ]
}
```

步骤 16 点击**下一步 (Next)**。

步骤 17 点击**审核 (Review)**。

步骤 18 在“查看策略”(Review Policy) 页面中输入请求的信息，然后点击**创建策略 (Create Policy)**。

步骤 19 在“策略”(Policies) 页面上，在搜索字段中输入全部或部分策略名称，然后按 Enter 键。

步骤 20 点击您刚刚创建的策略。

步骤 21 点击**操作 (Actions)** > **附加 (Attach)**。

步骤 22 如有必要，请在搜索字段中输入全部或部分用户名，然后按 Enter 键。

步骤 23 点击**附加策略 (Attach Policy)**。

下一步做什么

创建 AWS 连接器，第 2343 页。

创建 AWS 安全组连接器

本任务讨论如何配置将 AWS 安全组数据发送到 Secure Firewall Management Center 以在策略中使用的连接器。

开始之前

执行以下所有操作：

- 按照 AWS 文档站点上的 使用安全组 中的说明创建 AWS 安全组。

- 创建至少具有为 dynamic attributes connector 创建具有最小权限的 AWS 用户，第 2341 页中所述权限的用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
地区	（必需。）输入您的 AWS 区域代码。
AWS 访问密钥	（必需。）输入访问密钥。
AWS 加密密钥	（必需。）输入加密密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 AWS 服务标签连接器

本主题讨论了如何为 Amazon Web 服务 (AWS) 标签创建到 Secure Firewall Management Center 的连接器，以供在策略中使用。

有关详细信息，请参阅 AWS 文档网站上的以下资源：

- 什么是标签？
- AWS IP 地址范围
- 标记 AWS 资源
- AWS 上的标记指南
- AWS 服务点

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
URL	（必需。）除非建议，否则请勿更改URL。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

Azure 连接器 - 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 Azure 导入 Secure Firewall Management Center ， 以便用于策略。

动态属性已导入

我们从 Azure 导入以下动态属性：

- 标签，与资源、资源组和订用关联的键值对。

有关详细信息，请参阅 Microsoft 文档中的本页面。

- Azure 中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求至少具有**读者 (Reader)** 权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 Azure 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Azure 连接器 - 关于用户权限和导入的数据，第 2347 页。

开始之前

您必须已经拥有 Microsoft Azure 帐户。要进行设置，请参阅 Azure 文档站点上的本页面。

过程

步骤 1 以订用所有者的身份登录到 Azure 门户 。

步骤 2 点击 **Azure Active Directory**。

步骤 3 查找要设置的应用的 Azure Active Directory 实例。

步骤 4 点击**添加 (Add)** > **应用注册 (App registration)**。

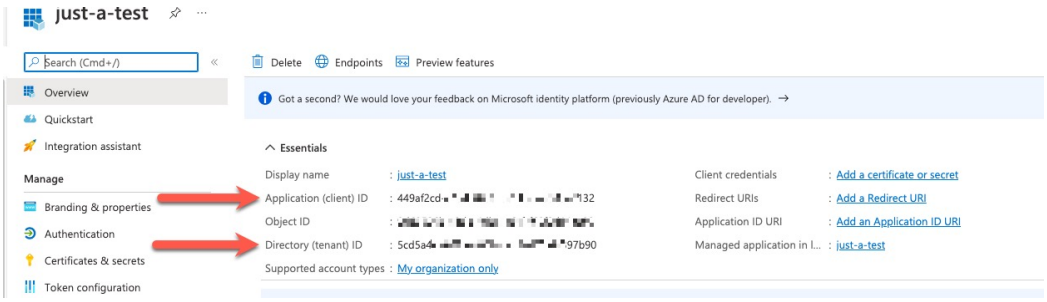
步骤 5 在 **名称 (Name)** 字段中，输入用于标识此应用的名称。

步骤 6 在此页面上输入贵组织所要求的其他信息。

步骤 7 点击**注册 (Register)**。

步骤 8 在下一页上，写下或复制客户端 ID（也称为应用 *ID*）和租户 ID（也称为目录 *ID*）。

示例如下。

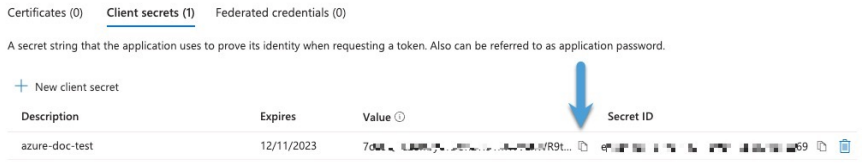


步骤 9 点击客户端凭证旁边的 **添加证书或密钥**。

步骤 10 点击**新建客户端密钥 (New Client Secret)**。

步骤 11 输入请求的信息，然后点击**添加 (Add)**。

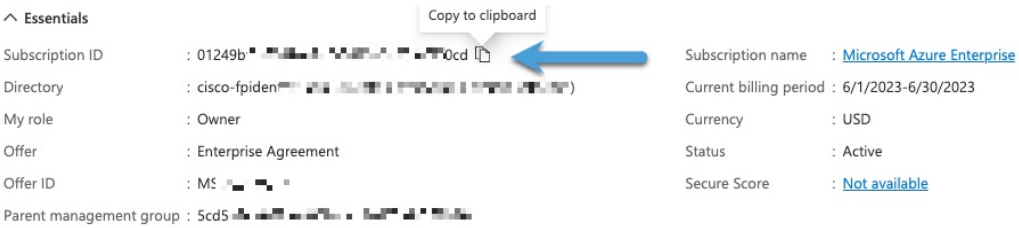
步骤 12 将 **值** 字段的值复制到剪贴板。此值是客户端密钥， 而不是 **密钥** ***ID***。



步骤 13 返回到 Azure 门户主页面，然后点击**订用 (Subscriptions)**。

步骤 14 点击您的订用的名称。

步骤 15 将订用 ID 复制到剪贴板。



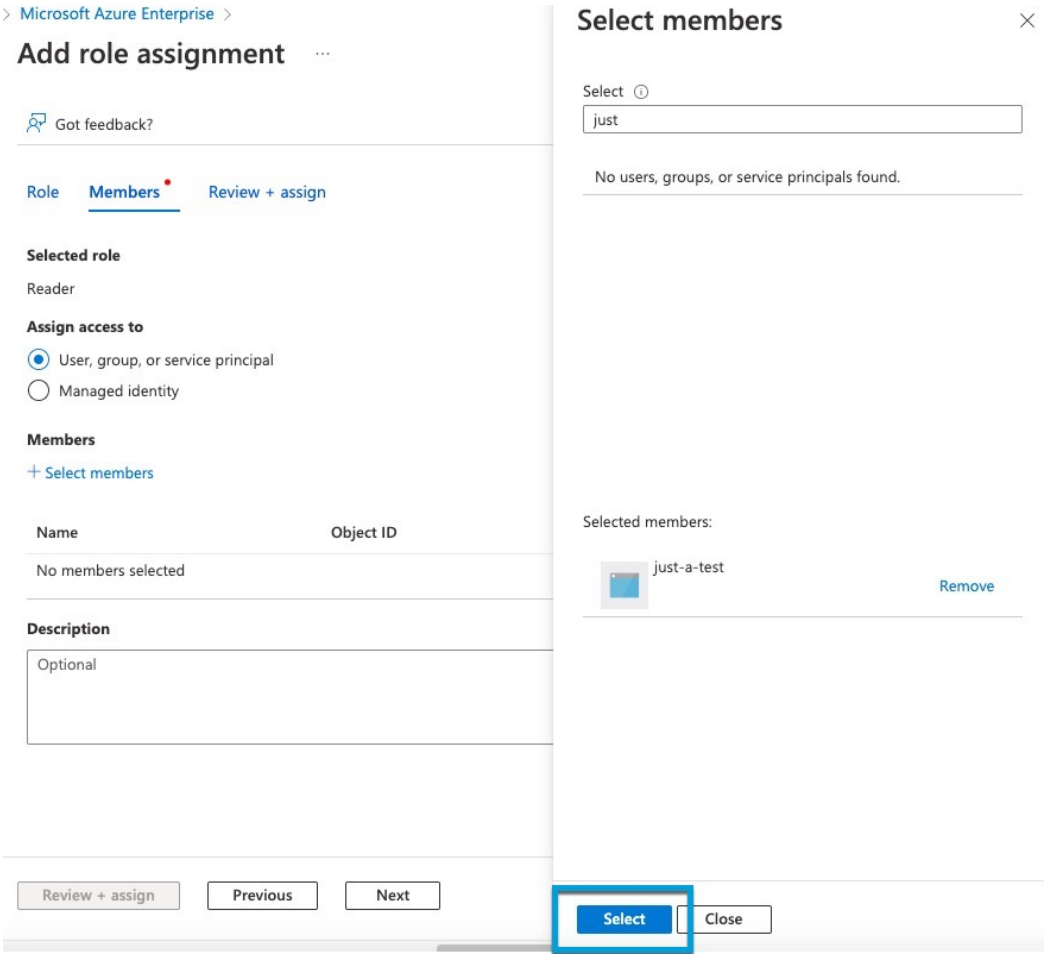
步骤 16 点击**访问控制 (IAM) (Access Control [IAM])**。

步骤 17 点击**添加 (Add)** > **添加角色分配 (Add role assignment)**。

步骤 18 点击**读者 (Reader)**，然后点击**下一步 (Next)**。

步骤 19 点击**选择成员 (Select Members)**。

步骤 20 在页面右侧，点击您注册的应用的名称，然后点击**选择 (Select)**。



步骤 21 点击查看 + 分配 **(Review + Assign)**，然后按照提示完成操作。

下一步做什么

请参阅创建 Azure 连接器， 第 2350 页。

创建 Azure 连接器

此任务讨论如何创建从 Azure 向 Secure Firewall Management Center 发送数据的连接器，以用于策略中。

开始之前

创建至少具有 创建对 dynamic attributes connector 具有最小权限的 Azure 用户， 第 2348 页 中所述权限的 Azure 用户。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标（），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 Azure 服务标签连接器

本主题讨论了如何为 Azure 服务标签创建到 Secure Firewall Management Center 的连接器，以供在策略中使用。Microsoft 会每周更新与这些标记的 IP 地址关联。

有关详细信息，请参阅 Microsoft TechNet 上的虚拟网络服务标签。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
订用 ID	（必需。）输入 Azure 订用 ID。
租户 ID	（必需。）输入租户 ID。
客户端 ID	（必需。）输入您的客户端 ID。
客户端密钥	（必需。）输入您的客户端密钥。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

思科 APIC 连接器

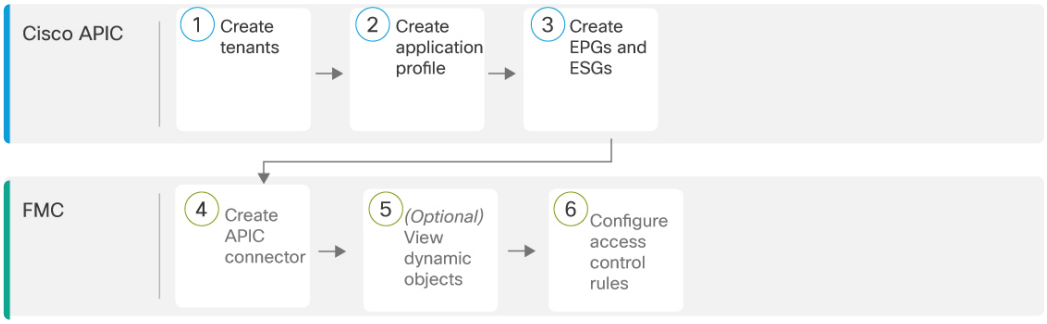
以下主题讨论如何配置 思科 APIC 与 Secure Firewall Management Center 的集成。

相关主题

与 思科 APIC 集成的系统要求，第 2354 页
获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页

如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页

如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象



1 基本用户租户配置
2 基本用户租户配置
3 EPG
4 创建连接器思科 APIC，第 2358 页
5 在 Secure Firewall Management Center 中查看动态对象，第 2383 页
6 使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页

表 *134:* 使用网络对象组配置 ***Secure Firewall Management Center*** 访问控制规则或 ***DNS*** 规则

1	思科 APIC	租户允许 思科 APIC 管理员设置基于域的访问控制。 请参阅基本用户租户配置
2	思科 APIC	应用配置文件是其他对象（例如终端组 (EPG)）的容器。 请参阅基本用户租户配置
3	思科 APIC	EPG 是网络对象的容器，是设备连接到网络的方式。ESG 是包含物理或虚拟网络终端集合的逻辑实体。 请参阅 EPG 和 ESG
	Secure Firewall Management Center	如果您尚未这样做，请启用 dynamic attributes connector，第 2116 页。
4	Secure Firewall Management Center	创建从 思科 APIC 检索 EPG 和 ESG 的 思科 APIC 连接器，并使其可用于 Secure Firewall Management Center 访问控制策略或 DNS 策略。 请参阅 创建连接器思科 APIC，第 2358 页。
5	Secure Firewall Management Center	（可选。）查看从 思科 APIC 获取的动态对象。 请参阅在 Secure Firewall Management Center 中查看动态对象，第 2383 页。

6	Secure Firewall Management Center	要在访问控制策略 或 DNS 策略中使用动态对象，您必须将它们作为动态对象添加到这些规则中。 请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

相关主题

与 思科 APIC 集成的系统要求，第 2354 页
获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页
思科 APIC 连接器，第 2352 页

与 思科 APIC 集成的系统要求

您的系统必须满足以下要求：

- Secure Firewall Management Center 版本：10.0.0 及更高版本。

  需要 Essentials 或更高级别的许可证；支持高可用性。

- Firewall Threat Defense 版本：7.2 及更高版本。
- 思科 APIC 版本：3.0(1k) 或更高版本。
- 如果您使用 ACI 终端更新应用程序，其版本必须为 2.6。

相关主题

与 思科 APIC 集成的系统要求，第 2354 页
获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页

获取集成所需的信息

本部分讨论以下内容：

- 配置集成所需的信息
- 动态对象名称中使用的信息

思科 ACI 终端更新应用 站点前缀和更新间隔

仅当您当前使用思科 ACI 终端更新应用时，此信息才适用于您；否则，您可以跳过。

要查找 思科 ACI 终端更新应用 站点前缀和更新间隔，请执行以下操作：

1. 以具有管理员权限的用户身份登录 思科 APIC。

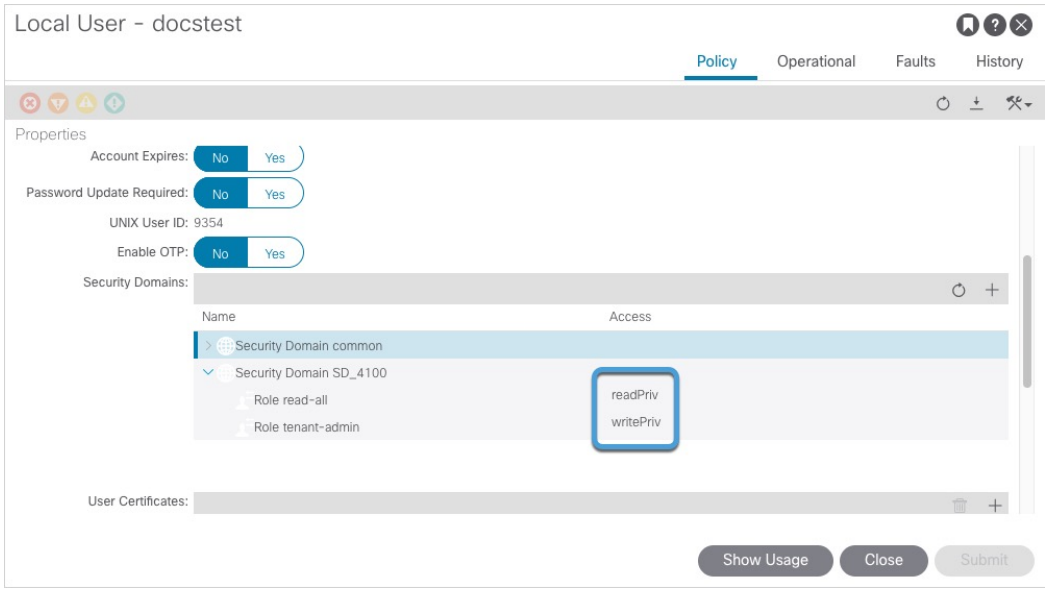
   有关详细信息，请参阅 *APIC* 角色和权限表。

2. 点击**应用 (Apps)**。
3. 在“ACI 终端更新应用”(ACI Endpoint Update app)，点击**打开 (Open)**。
4. 请点击 **编辑** ()。
5. 记下**更新间隔（以秒为单位）Update Interval [In seconds])** 和**站点前缀 (Site Prefix)** 的值。

配置集成所需：找到具有适当访问权限的用户

要查找包含 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色 的用户，请执行以下操作：

1. 登录 思科 APIC。
2. 点击**管理员 (Admin)**。
3. 在左侧窗格中，点击**用户 (Users)**。
4. 在右侧窗格中，双击用户的名称。
5. 滚动到“安全域”(Security Domains)。
6. 对于相关安全域，请确保用户具有 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色，如下图所示。



思科 APIC 租户名称

此集成创建的动态对象的名称中会使用思科 APIC租户名称。查找方法如下：

1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 记下包含要发送到 的对象的租户名称。

思科 APIC 应用配置文件名称

此集成创建的动态对象的名称中会使用思科 APIC应用配置文件名称。查找方法如下：

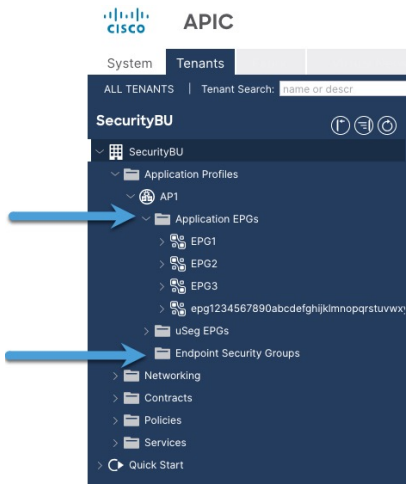
1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 双击您的租户的名称。
4. 展开您的租户。
5. 展开**应用配置文件 (Application Profiles)**。
6. 记下包含要与 ASA 集成的 EPG 和 ESG 的应用配置文件的名称。

EPG 名称

此集成创建的动态对象的名称中会使用思科 APIC EPG 名称。查找方法如下：

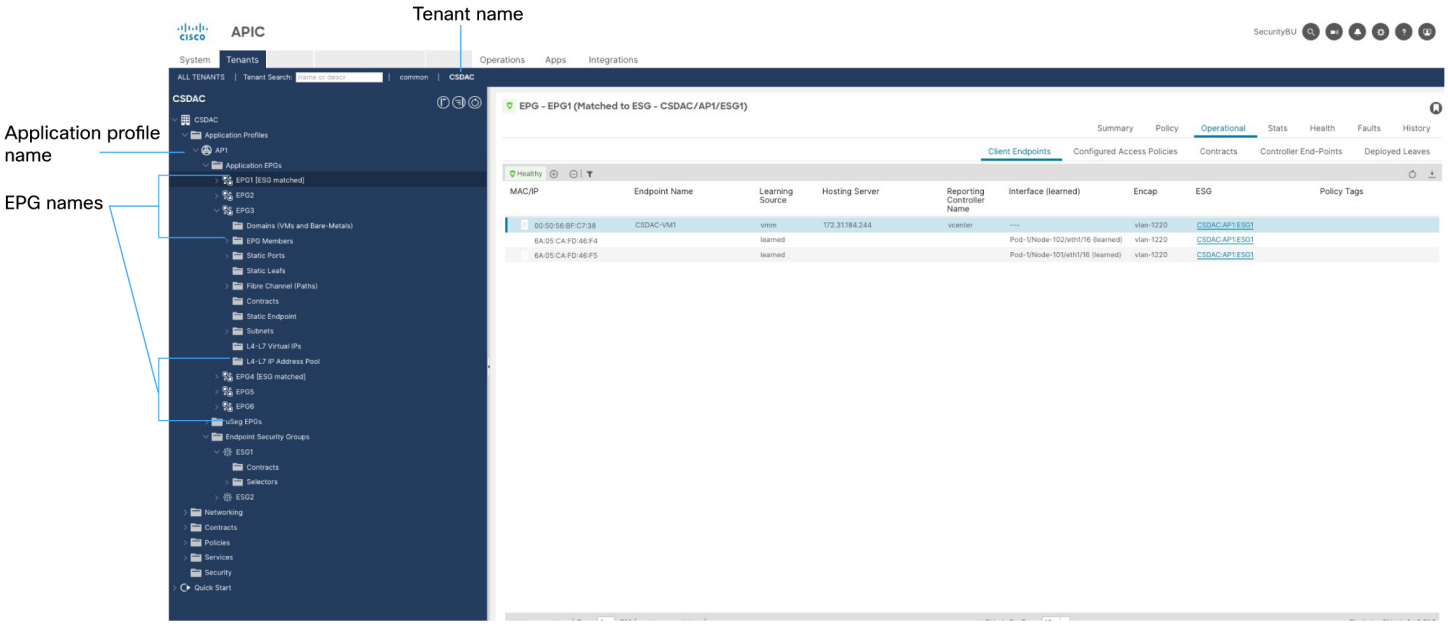
1. 登录 思科 APIC。
2. 点击**租户 (Tenants)**。
3. 双击您的租户的名称。
4. 展开您的租户。
5. 展开**应用配置文件 (Application Profiles)**。
6. 展开应用配置文件的名称。
7. 展开**应用 EPG**。
8. 记下有网络对象组要发送到 ASA 的EPG 或 ESG 的名称。

   下图显示了一个示例。



示例

下图显示了 思科 APIC 中的值。



相关主题

与 思科 APIC 集成的系统要求，第 2354 页
获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页

创建连接器思科 APIC

本主题讨论了如何创建 思科 APIC 连接器，以便从 思科 APIC 上已配置的终端组 (EPG) 获取网络对象组。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认值为 60 秒。）从 思科 APIC 检索 IP 映射的间隔。 建议将此值设置为 15 秒。
IP 或主机名	输入 思科 APIC 服务器的全称域名或 IP 地址，以便从 EPG 和 ESG 中检索网络对象组。 不要输入方案（如 **https://**），也不要包含尾部斜杠。
添加另一个集群 IP	（可选。）输入 思科 APIC 集群中其他服务器的 IP 地址。
用户名	输入至少包含 安全域至少具有 `readPriv` 访问权限的 `read-all` 角色和具有 `writePriv` 访问权限的 `tenant-admin` 角色 的 思科 APIC 用户的名称。 用户拥有权限的所有租户的对象都可以推送到 。
密码	输入用户的密码。

值	说明
服务器证书	（如果使用完全限定域名，则建议使用。） 您有以下选择： • 粘贴您找到的证书授权 (CA) 链，如手动获取证书颁发机构 (CA) 链，第 2359 页中所述。 • 点击**获取证书** > **获取**以自动获取证书，或者，如果无法获取证书，请按照手动获取证书颁发机构 (CA) 链，第 2359 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

相关主题

与 思科 APIC 集成的系统要求，第 2354 页
获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页

手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心
- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

```
security verify-cert -P url[:port]
```

其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

```
security verify-cert -P https://myvcenter.example.com
```

如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

```
security verify-cert -P https://myvcenter.example.com:12345
```

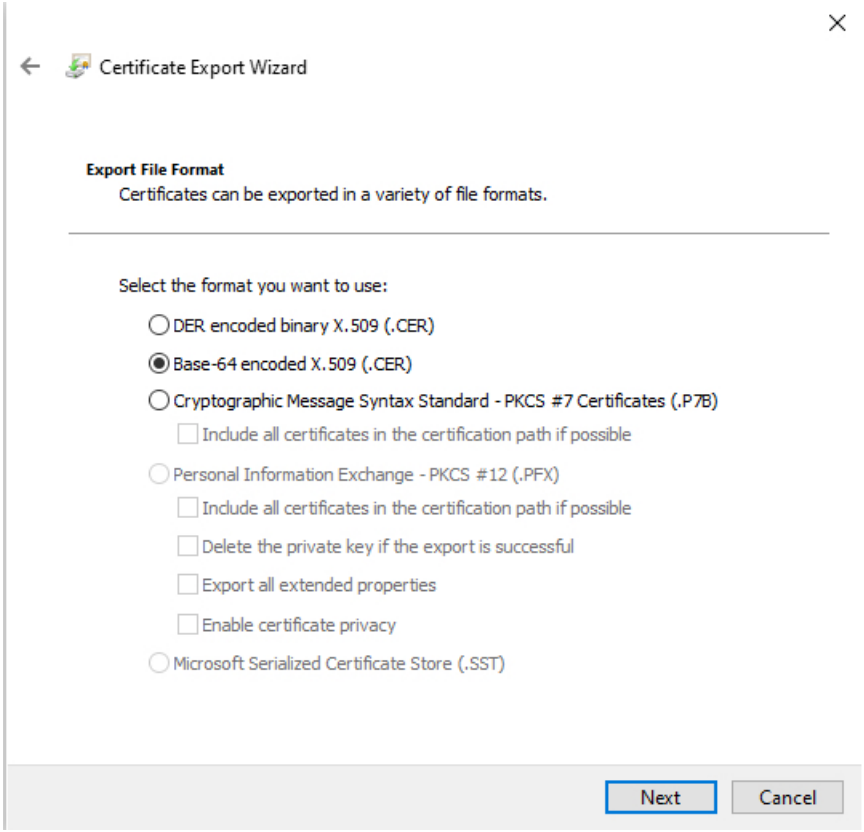
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



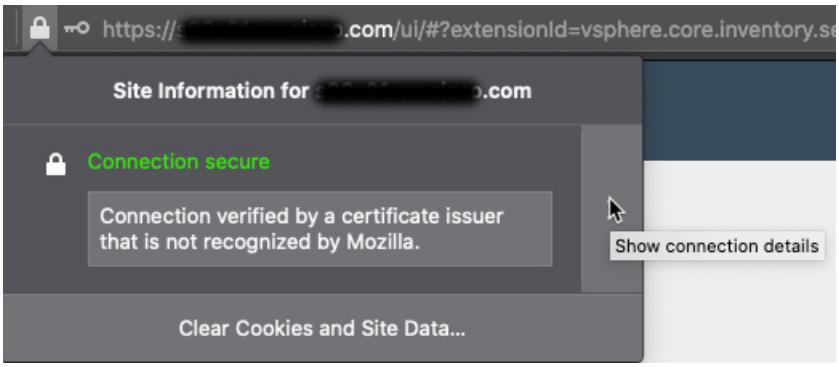
10. 按照提示完成导出。
11. 在文本编辑器中打开证书。
12. 对证书链中的所有证书重复此过程。

    您必须先按顺序将每个证书粘贴到文本编辑器中。
13. 对 vCenter、 防火墙管理中心 重复这些任务。

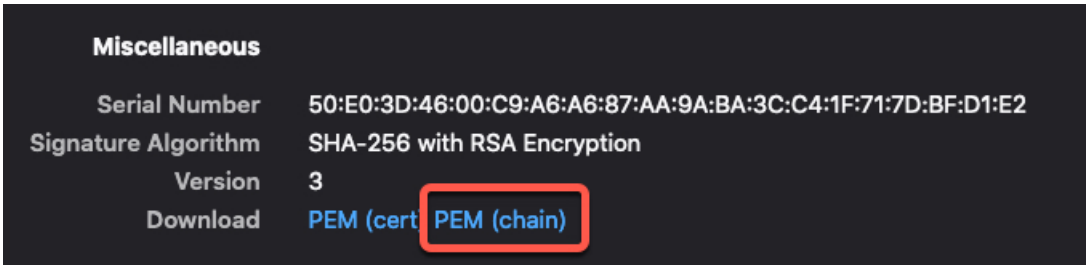
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击更多信息 **(More Information)**。
5. 点击查看证书 **(View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM**（链）**(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求， 第 2354 页
获取集成所需的信息， 第 2354 页
创建连接器思科 APIC， 第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象， 第 2353 页
手动获取证书颁发机构 (CA) 链， 第 2359 页
思科 APIC 连接器， 第 2352 页

创建 Cisco Cyber Vision 连接器

此任务讨论如何将数据从 Cisco Cyber Vision 发送到 Secure Firewall Management Center 。

开始之前

必须可从运行 dynamic attributes connector 的计算机访问 Cisco Cyber Vision。您必须知道其 IP 地址、端口和 API 密钥。

要在 Cyber Vision 管理控制台中查找 API 密钥，请点击**管理 (Admin)** > **API** > **令牌 (Token)**，然后点击**显示 (Show)** 以显示令牌，并点击  以将令牌复制到剪贴板。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
Cyber Vision 前缀	输入一个字母数字字符串，以便在将对象发送到 Secure Firewall Management Center 时标识来自此 Cyber Vision IP 地址的动态对象。 如果您有一个 Cyber Vision IP 地址，则可以输入任何值，例如 **1**。
提取间隔	（默认值为 60 秒。）从 Cyber Vision 获取数据映射的时间间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
主机	（必需。）输入 Cyber Vision 的完全限定主机名或 IP 地址。
端口	（必需。）输入 Cyber Vision 侦听端口。
令牌	（必需。）输入 API 令牌。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建通用文本连接器

此任务讨论如何创建手动维护的 IP 地址临时列表，并按您选择的时间间隔（默认情况下为 30 秒）进行检索。您可以随时更新地址列表。

开始之前

创建包含 IP 地址的文本文件，并将其放在可从 Secure Firewall Management Center 访问的 Web 服务器上。IP 地址可以包含 CIDR 表示法。文本文件每行只能有一个 IP 地址。

例如，访问控制规则中的“允许列表”可能有一个 IP 地址列表，访问控制规则中的“阻止列表”可能有另一个 IP 地址列表。

每个文本文件最多可以指定 10,000 个 IP 地址。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息：

项目	说明
名称	输入名称以唯一标识此连接器。
说明	（可选。）输入说明。
提取间隔	在提取间隔 (Pull Interval) 字段中，更改动态属性连接器从 text 文件检索 IP 地址的频率（以秒为单位）。默认值为 30 秒。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
URL	输入要从中检索 IP 地址的 URL。
添加其他 URL	（可选。）点击链接可向现有列表中添加更多 URL。
用户名	（可选。）如果文本文件所在的服务器使用身份验证，请在此字段中输入用户名。 基本身份验证

项目	说明
密码	（可选。）输入用户的密码。
证书	（可选。）如果安全连接到 Web 服务器需要证书链，您有以下选择： • 点击 **获取证书** > **获取** 以自动获取证书，或者，如果无法获取证书，请按照 手动获取证书颁发机构 (CA) 链，第 2359 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建 GitHub 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 GitHub 连接器。与这些标签关联的 IP 地址由 GitHub 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅关于 GitHub 的 IP 地址。

注释 请勿更改 URL，否则将无法检索任何 IP 地址。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入**名称**和可选说明。

步骤 5 （可选。）在**提取间隔 (Pull Interval)** 字段中，更改动态属性连接器从 GitHub 检索 IP 地址的频率（以秒为单位）。默认值为 21,600 秒（6 小时）。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

Google 云连接器 - 关于用户权限和导入的数据

dynamic attributes connector 会将动态属性从 Google Cloud 导入 Secure Firewall Management Center，以便用于策略。

动态属性已导入

我们会从 Google 云导入以下动态属性：

- 标签，可用于组织 Google 云资源的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- 网络标记，与组织、文件夹或项目关联的键值对。

  有关详细信息，请参阅 Google 云文档中的创建和管理标签。

- Google 云中虚拟机的 *IP* 地址。

所需的最低权限

dynamic attributes connector 要求至少具有**基本** > **查看者**权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 Google 云用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 Google 云连接器 - 关于用户权限和导入的数据，第 2366 页。

开始之前

您必须已设置 Google 云帐户。有关执行此操作的详细信息，请参阅 Google 云文档中的设置环境。

过程

步骤 1 以所有者角色的用户身份登录您的 Google 云帐户。

步骤 2 点击**IAM 和管理 (IAM & Admin)** > **服务帐户 (Service Accounts)** > **创建服务帐户 (Create Service Account)**。

步骤 3 输入以下信息：

- **服务帐户名称**：用于标识此帐户的名称；例如，**CSDAC**。
- **服务帐户 ID**：应在您输入服务帐户名称后填写唯一值。
- **服务帐户说明**：输入可选说明。

有关服务帐户的详细信息，请参阅 Google 云文档中的了解服务帐户。

步骤 4 点击**创建并继续 (Create and Continue)**。

步骤 5 按照屏幕上的提示操作，直到显示“授予用户对此服务帐户的访问权限”部分。

步骤 6 授予用户**基本** > **查看者**角色。

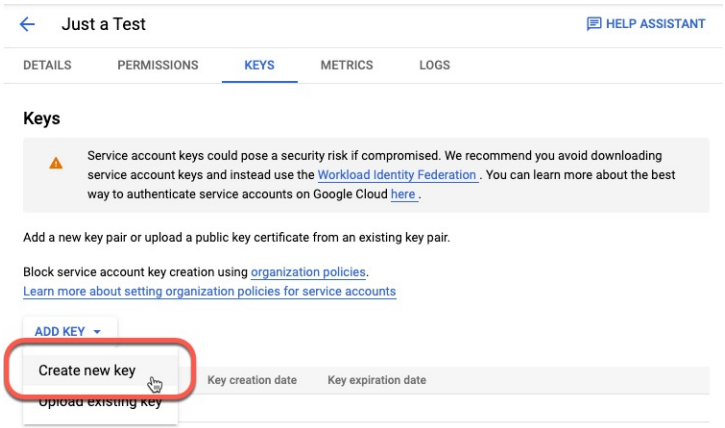
步骤 7 点击**完成**。

系统将显示服务帐户列表。

步骤 8 点击您所创建的服务帐户一行末尾的 **更多** (⋮)。

步骤 9 点击**管理密钥 (Manage Keys)**。

步骤 10 点击**添加密钥 (Add Key)** > **创建新密钥 (Create New Key)**。



步骤 11 点击 **JSON**。

步骤 12 点击**创建 (Create)**。

JSON 密钥将下载到您的计算机。

步骤 13 配置 GCP 连接器时，请将密钥放在手边。

下一步做什么

请参阅创建 Google Cloud 连接器，第 2367 页。

创建 Google Cloud 连接器

开始之前

准备好 Google 云 JSON 格式的服务帐户数据；它是设置连接器所必需的。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 AWS 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
GCP 区域	（必需。）输入您的 Google 云所在的 GCP 区域。有关详细信息，请参阅 Google 云文档中的区域和地区。
服务帐户	粘贴 Google 云服务帐户的 JSON 代码。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

创建 Office 365 连接器

此任务讨论如何为 Office 365 标记创建连接器，从而将数据发送到 Secure Firewall Management Center 以便用于策略。Microsoft 会每周更新与这些标记的 IP 地址关联。您不必创建动态属性过滤器即可使用数据。

有关详细信息，请参阅 docs.microsoft.com 上的 Office 365 URL 和 IP 地址范围。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Azure 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
基本 **API URL**	（必需。）输入要从中检索 Office 365 信息的 URL（如果其与默认值不同）。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
实例名称	（必需。）从列表中，点击实例名称。有关详细信息，请参阅 Microsoft 文档站点上的 Office 365 IP 地址和 URL Web 服务。
禁用可选 **IP**	（必需。）输入 **true** 或 **false**。

步骤 5 点击**保存**。

步骤 6 确保“状态”(Status) 列中显示**确定**。

vCenter 连接器 - 关于用户权限和导入的数据

Dynamic Attributes Connector 会将动态属性从 vCenter 导入 Secure Firewall Management Center，以便用于访问控制策略。

动态属性已导入

我们会从 vCenter 导入以下动态属性：

- 操作系统
- *MAC* 地址
- *IP* 地址
- *NSX* 标记

所需的最低权限

Dynamic Attributes Connector 要求至少具有**只读**权限的用户才能导入动态属性。

创建对 dynamic attributes connector 具有最小权限的 vCenter 用户

此任务讨论如何设置具有最低权限的服务帐户，以向 Secure Firewall Management Center 发送动态属性。有关这些属性的列表，请参阅 vCenter 连接器 - 关于用户权限和导入的数据，第 2369 页。

开始之前

您必须已设置 vCenter 服务器帐户。有关执行此操作的详细信息，请参阅 vCenter 文档中的关于 vCenter 服务器安装和设置。

过程

步骤 1 以管理员身份登录 vCenter。

步骤 2 点击**菜单 (Menu)** > **管理 (Administration)**。

步骤 3 在左侧窗格中，点击**单点登录 (Single Sign On)** > **用户和组 (Users and Groups)**。

步骤 4 从**域 (Domain)** 列表中，点击域的名称以添加用户。

步骤 5 点击**添加用户**。

步骤 6 输入请求的信息，然后点击**添加 (Add)**。

步骤 7 在左侧窗格中，点击**访问控制 (Access Control)** > **全局权限 (Global Permissions)**。

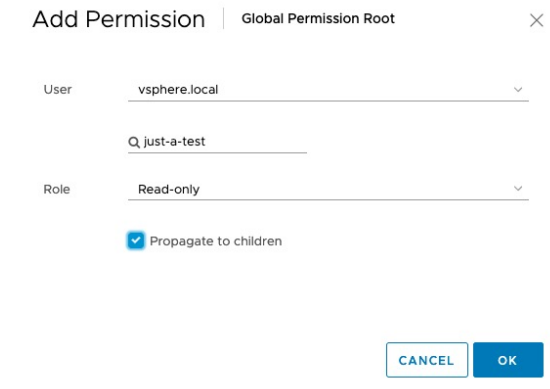
步骤 8 点击**添加** (+)。

步骤 9 在**用户**字段中，点击您在其中创建用户的 vCenter 域的名称。

步骤 10 在搜索字段中，输入用户名的一部分。

步骤 11 从**角色 (Role)** 列表中，点击**只读 (Read-only)**。

步骤 12 选择 **传播到子项** 复选框。



步骤 13 点击**确定**。

下一步做什么

请参阅创建 vCenter 连接器，第 2371 页。

创建 vCenter 连接器

此任务讨论如何为 VMware vCenter 创建连接器，从而将数据发送到 Secure Firewall Management Center 以用于策略。

开始之前

如果使用不受信任的证书与 vCenter 通信，请参阅手动获取证书颁发机构 (CA) 链，第 2359 页。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

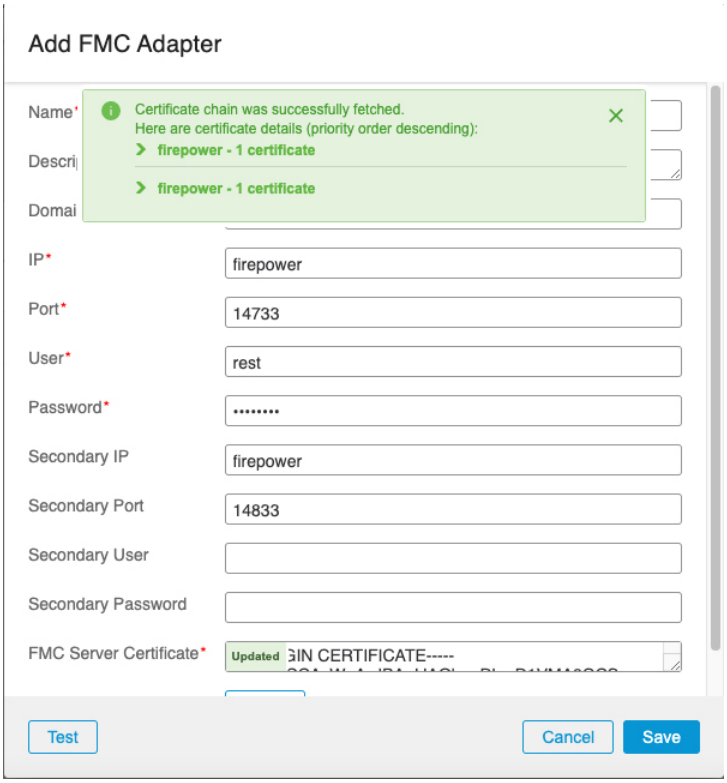
- 添加新连接器：点击添加图标（），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	输入可选的说明。
提取间隔	（默认为 30 秒。）从 vCenter 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
主机	（必需。）输入以下任意命令： • vCenter 的完全限定主机名 • vCenter 的 IP 地址 • （可选。）A 端口 请勿输入方案（例如 **`https://`**）或末尾斜杠。 例如，**`myvcenter.example.com`** 或 **`192.0.2.100:9090`**
用户	（必需。）输入至少具有只读角色的用户的用户名。用户名区分大小写。

值	说明
密码	（必需。）输入用户的密码。
NSX IP	如果使用 vCenter 网络安全可视化 (NSX)，请输入其 IP 地址。
NSX 用户	输入至少具有审核员角色的 NSX 用户的用户名。
NSX 类型	输入 **NSX-T**。
NSX 密码	输入 NSX 用户的密码。
vCenter 证书	您有以下选择： • 粘贴您找到的证书授权 (CA) 链，如 手动获取证书颁发机构 (CA) 链，第 2359 页中所述。 • 点击**获取 (Fetch)** 以自动获取证书，或者，如果无法获取证书，请按照手动获取证书颁发机构 (CA) 链，第 2359 页中所述手动获取证书。 • 点击 **获取证书** > **获取** 以自动获取证书，或者，如果无法获取证书，请按照 手动获取证书颁发机构 (CA) 链，第 2359 页中所述手动获取证书。 • 点击 **获取证书** > **从文件浏览** 以上传您之前下载的证书链。

以下是成功获取证书链的示例：



展开对话框顶部的证书 CA 链会显示类似于以下内容的证书。



如果无法通过这种方式获取证书，您可以手动获取证书链，如 手动获取证书颁发机构 (CA) 链，第 2359 页中所述。

步骤 5 点击**保存**。

创建 Webex 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 Webex 连接器。与这些标签关联的 IP 地址由 Webex 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅 Webex Calling 的端口参考。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标（），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Webex 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
运营商预留 IP	（必需。）（必需。）滑动至已启用以检索任何保留的 IP 地址。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建 Zoom 连接器

此部分讨论如何创建将数据发送到 Secure Firewall Management Center 以用于策略的 Zoom 连接器。与这些标签关联的 IP 地址由 Zoom 进行维护。您不必创建动态属性过滤器。

有关详细信息，请参阅 Zoom 网络防火墙或代理服务器设置。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新连接器：点击添加图标 （），然后点击连接器名称。
- 编辑或删除连接器：点击**更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

值	说明
名称	（必需。）输入名称以唯一标识此连接器。
说明	可选说明。
提取间隔	（默认为 30 秒。）从 Zoom 检索 IP 映射的间隔。 最小**拉取间隔时间 (Pull Interval)** 值为 1 秒。您可以将最大值设置为任何想要的值。我们建议不要将最小值设得太低，因为这会产生大量流量，而且在适用情况下，可能会导致您为流量付费。
运营商预留 IP	（必需。）滑动至已启用以检索任何保留的 IP 地址。

步骤 5 点击**测试 (Test)** 并确保测试成功后再保存连接器。

步骤 6 点击**保存**。

步骤 7 确保“状态”(Status) 列中显示**确定**。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

开始之前

创建连接器，第 2340 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ( )。
- 编辑或删除过滤器：点击 **更多**（ ），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加 。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。

项目	说明
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

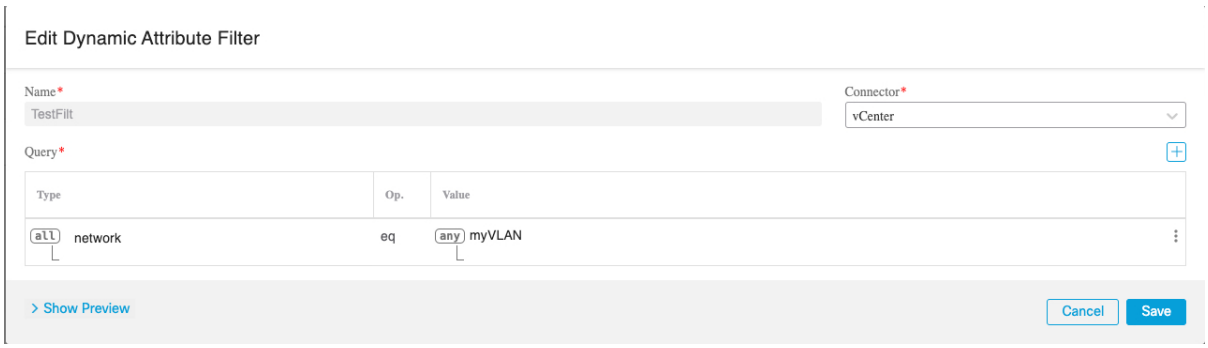
您创建的动态属性查询应显示为动态对象。

动态属性过滤器示例

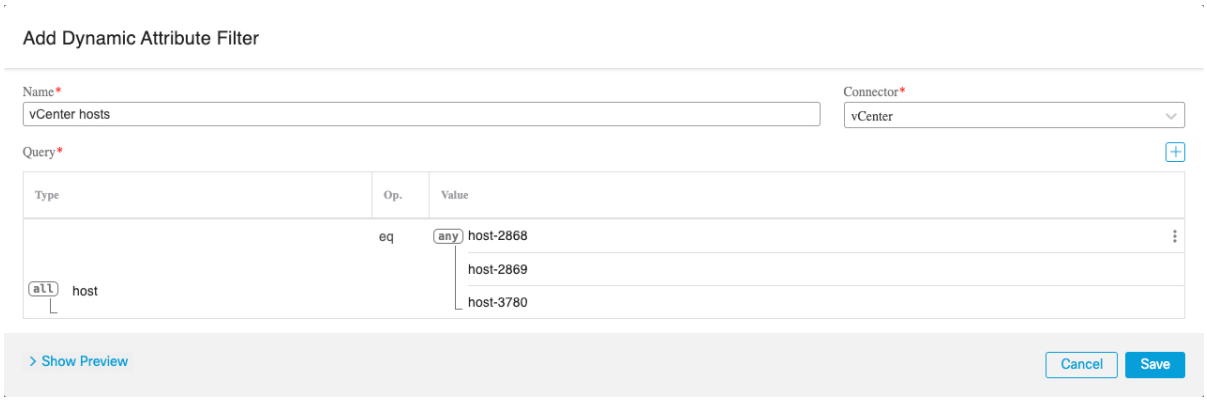
本主题提供了设置动态属性过滤器的一些示例。

示例：vCenter

以下示例显示了一个条件：VLAN。

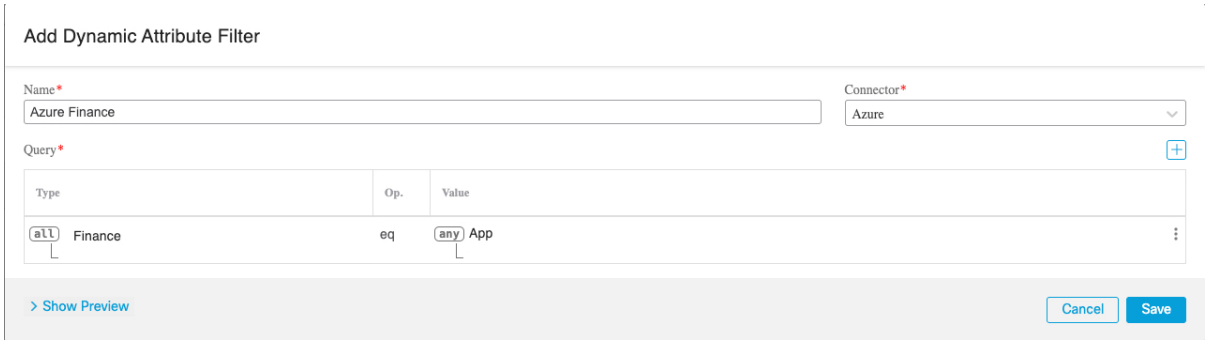


以下示例显示了使用 OR 连接的三个条件：查询匹配三个主机中的任何一个。



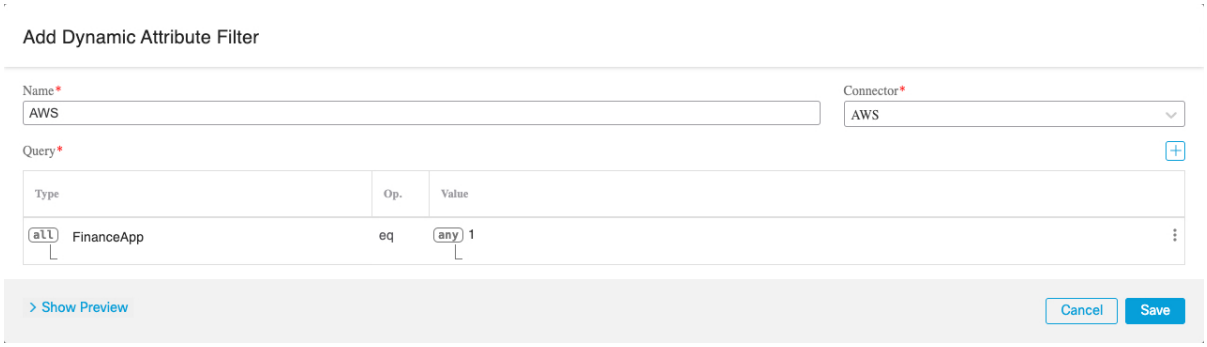
示例：Azure

以下示例显示了一个条件：标记为财务应用的服务器。



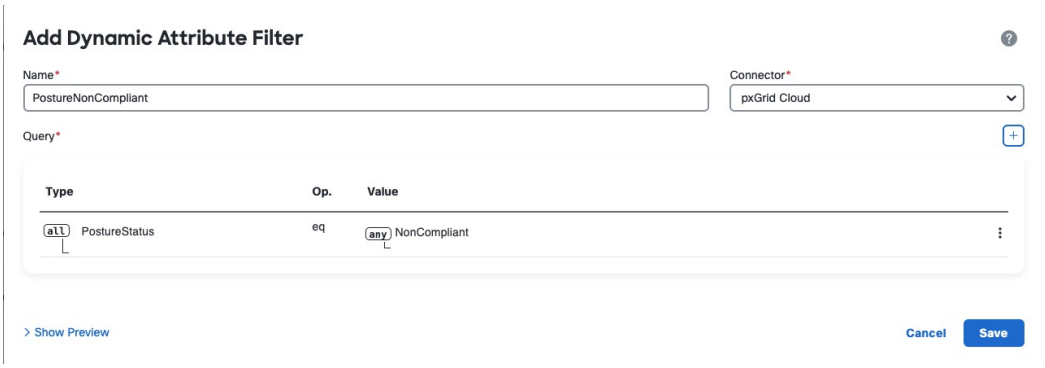
示例：AWS

以下示例显示了一个条件：值为 1 的 FinanceApp。



示例：pxGrid 云

以下示例显示一个条件：PostureStatus 为 NonCompliant。



手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心
- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

   ```
   security verify-cert -P url[:port]
   ```

   其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

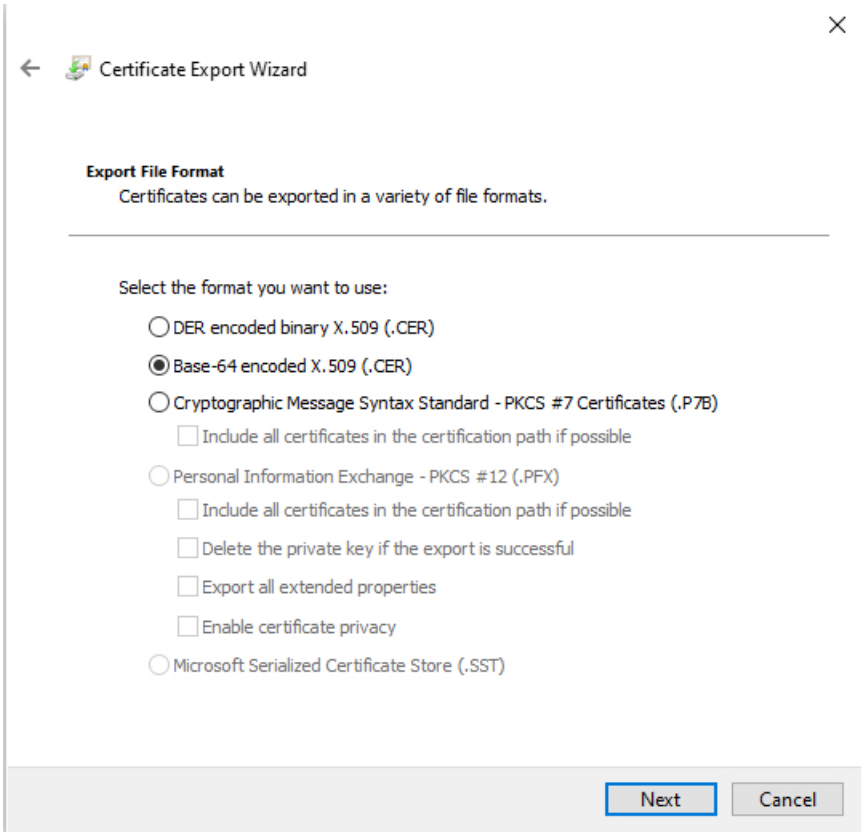
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



10. 按照提示完成导出。
11. 在文本编辑器中打开证书。

12. 对证书链中的所有证书重复此过程。

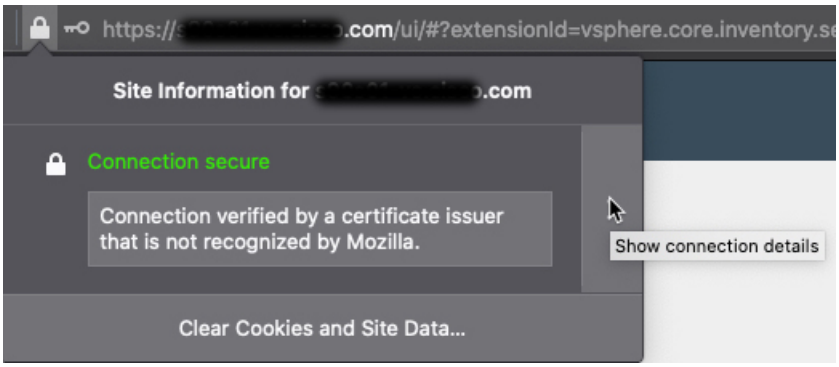
    您必须先按顺序将每个证书粘贴到文本编辑器中。

13. 对 vCenter、 防火墙管理中心 重复这些任务。

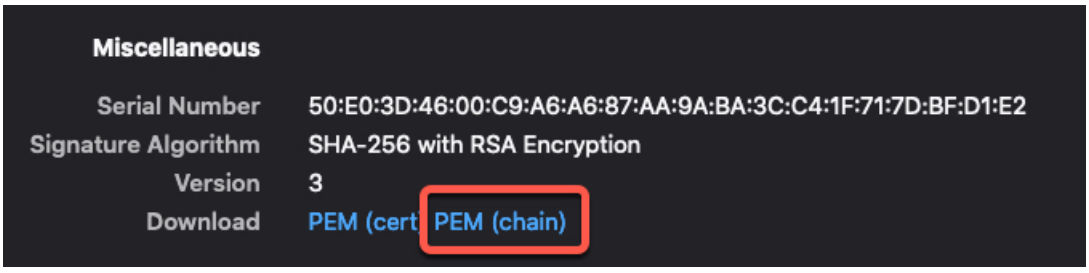
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击**更多信息 (More Information)**。
5. 点击**查看证书 (View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM（链）(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求 ， 第 2354 页

获取集成所需的信息，第 2354 页
创建连接器思科 APIC，第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象，第 2353 页
手动获取证书颁发机构 (CA) 链，第 2359 页
思科 APIC 连接器，第 2352 页

在访问控制策略或 DNS 策略中使用动态对象

通过 dynamic attributes connector，您可以在访问控制规则或 DNS 策略中配置动态属性过滤器（在 Secure Firewall Management Center 中可视为动态对象）。

关于访问控制规则或 DNS 规则中的动态对象

在创建连接器并在连接器上保存动态属性过滤器之后，动态对象会自动从 dynamic attributes connector 推送到 Cisco Secure Firewall 管理器。

您可以在访问控制规则的或DNS规则的**动态属性**选项卡页面使用这些动态对象。您可以将动态对象添加为源或目标属性；例如，在访问控制阻止规则中，您可以将财务动态对象添加为目标属性，以阻止通过匹配规则中其他条件的对象访问财务服务器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

开始之前

创建连接器，第 2340 页

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ()。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

您创建的动态属性查询应显示为动态对象。

动态属性规则条件

动态属性包括：

- （源或目标。）动态对象（例如来自 dynamic attributes connector）

  dynamic attributes connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Secure Firewall Management Center 以便将它们用于访问控制规则中。

  有关dynamic attributes connector的详细信息，请参阅《关于 dynamic attributes connector，第 2325 页》。

- （仅源。）安全组标记 (SGT) 对象，包含手动定义或通过 ISE 定义的标记。有关更多信息，请参阅《源和目标安全组标记 (SGT) 匹配，第 2080 页》和《安全组标记，第 2649 页》。
- （仅源。）位置 IP 对象 由Cisco ISE定义
- （仅源。）设备类型对象，由（也称为终端配置文件）Cisco ISE定义。

动态属性可用作访问控制规则中的源条件和目标条件。使用以下准则：

- 不同类型的对象通过 AND 连接在一起
- 将相似类型的对象一起进行 ORd 运算

例如，如果选择源目标条件 SGT 1、SGT 2 和设备类型 1；如果在 SGT 1 或 SGT 2 上检测到设备类型 1，则规则匹配。例如，如果同时选择安全组标记和列出 IP 地址的动态对象，如果带有 标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

在 Secure Firewall Management Center 中查看动态对象

（可选。）以下任务讨论如何在 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)** 中查看 思科 APIC 网络对象。

开始之前

完成之前所有 思科 APIC 与 Secure Firewall Management Center 集成相关的任务。

过程

步骤 1 登录至 Secure Firewall Management Center

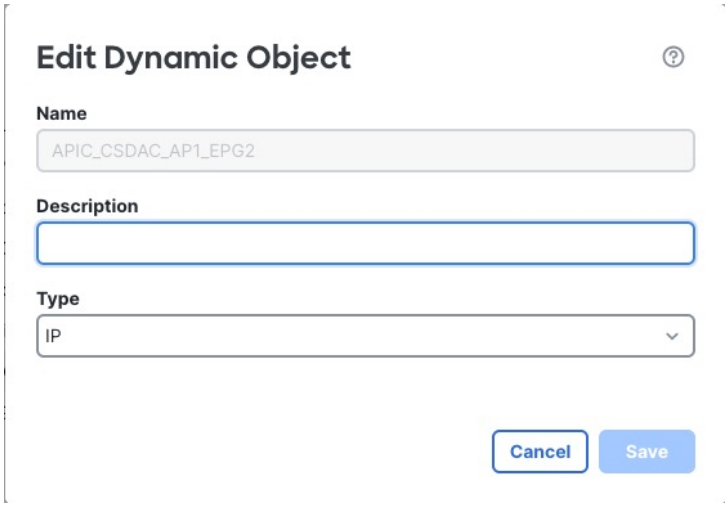
步骤 2 展开 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

动态对象有其自己的命名约定；例如，AWS 动态对象的名称类似于 `aws_AMAZON`。

通过与 思科 APIC 集成而创建的动态对象，其名称符合以下模式：

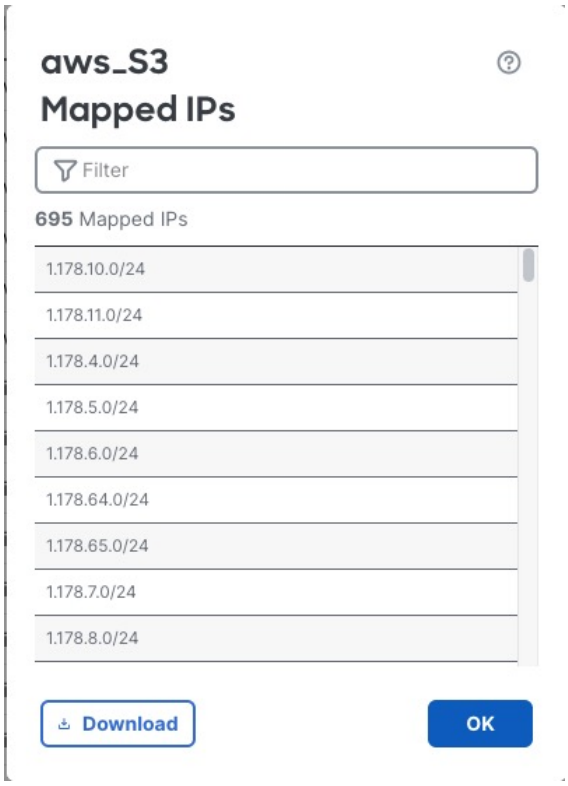
```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```

示例：



步骤 3 要查看与每个动态对象关联的 IP 地址，请点击行末的 (IP)。

示例：



下一步做什么

请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

使用动态属性过滤器来创建访问控制规则或 DNS 规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

要向 DNS 策略添加动态属性过滤器，请参阅创建基本 DNS 策略。

要将动态属性过滤器添加到 DNS 策略，请参阅创建基本 DNS 策略。

开始之前

按照创建动态属性过滤器，第 2164 页中所述，创建动态属性筛选器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录至 Secure Firewall Management Center

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

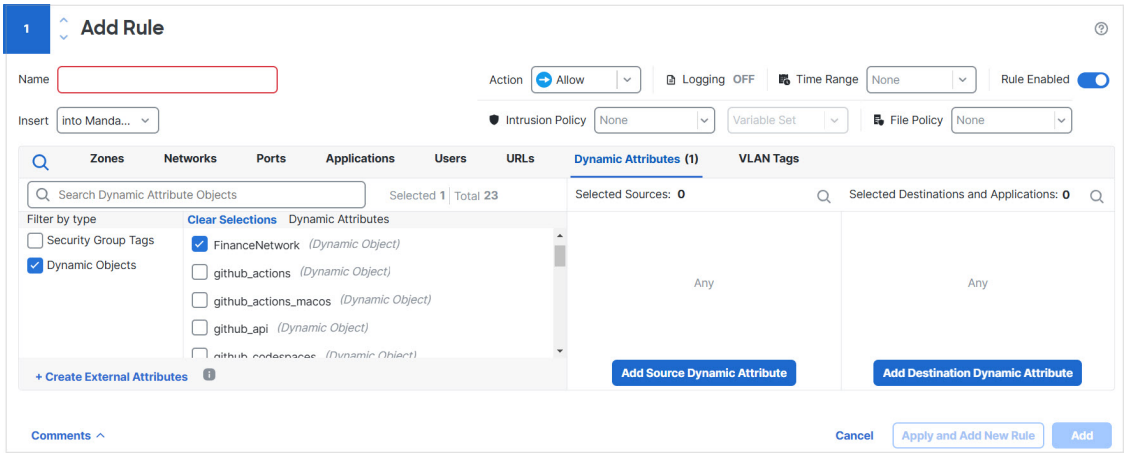
步骤 3 点击访问控制策略旁边的 **编辑**（ ）。

步骤 4 点击**添加规则 (Add Rule)**。

步骤 5 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的**动态对象 (Dynamic Objects)**。

下图显示了一个示例。



本示例显示一个名为 APIC 动态属性的动态对象，它对应于 dynamic attributes connector 中创建的动态属性筛选器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

请参阅动态属性规则条件，第 2383 页。

在 DNS 策略中使用动态对象

动态属性连接器使您能够在 DNS 规则中配置动态筛选器（在 Secure Firewall Management Center 中视为动态对象）。有关 DNS 策略的信息，请参阅安全情报 DNS 策略，第 2261 页。

在连接器上创建连接器并保存动态属性筛选器后，动态对象会自动从动态属性连接器推送到 Secure Firewall Management Center。

可以在 DNS 规则的“动态属性”选项卡页面上使用这些动态对象，类似于使用安全组标记 (SGT) 的方式。可以将动态对象添加为源或目标属性，但终端设备类型对象除外，它们仅作为源。

过程

步骤 1 点击 **策略** > **安全策略** > **DNS** 并创建或编辑 DNS 策略。

步骤 2 添加或编辑规则。

步骤 3 点击**动态属性 (Dynamic Attributes)** 选项卡。

步骤 4 在**动态属性**列表中，选择要使用的对象，然后将它们添加到相应的源列表或目标列表。最初，会列出所有安全组和动态对象，但可以取消选中“安全组”选项以仅查看动态对象。

步骤 5 在 **DNS** 选项卡上，选择与目标 DNS 请求匹配的相应列表或源。

步骤 6 根据需要向规则添加其他条件并设置操作。

步骤 7 点击**保存**。

动态防火墙

这些主题介绍如何将用户身份数据（包括 Microsoft AD 和 ISE）与 身份情报 提供的用户信任数据相集成，以增强您在网络中检测基于身份的漏洞的能力。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

关于 动态防火墙

以前，Secure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。

借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。

要使用 动态防火墙，您必须：

- 拥有一个 身份情报 租户

  请参阅具有 Cisco Identity Intelligence 的 Duo Identity Security。

- 启用 Dynamic Attributes Connector
- 设置身份源：
  - 思科身份服务引擎 (Cisco ISE)
  - pxGrid 云

    pxGrid 云 在同一源中结合身份和终端安全评估

    详细信息：什么是 pxGrid?

  除了提供身份验证信息外，Cisco ISE 和 pxGrid 云 还可以提供以下信息（如果需要）：
  - 基于 TCP 的 SGT 交换协议 (SXP) 绑定和目录会话信息。有关详细信息，请参阅《思科身份识别服务引擎管理员指南》。
  - 终端安全评估和移动设备管理合规性。有关详细信息，请参阅合规。
- 设置身份领域：
  - 创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页
  - 为被动身份验证创建Microsoft Azure AD (SAML)领域， 第 2002 页

身份源提供身份验证信息（登录、注销）以及终端安全评估。如果需要，身份源还可以提供 SXP 绑定和会话目录信息。

身份领域提供用户、组和 IP 地址信息。

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

如何配置 动态防火墙

本主题有助于您了解关于 动态防火墙， 第 2387 页中讨论的配置 动态防火墙 相关概念和选项

process_summary

动态防火墙 将身份源（如 Cisco ISE）与思科身份智能集成，以向 Secure Firewall Management Center 提供用户信任信息。

1. 配置思科身份智能以收集用户信任信息。
2. 配置受支持的 Secure Firewall Management Center 身份源。
3. 配置支持的身份领域。
4. 启用dynamic attributes connector。
5. 配置动态防火墙。

process_workflow

以下过程概述了如何配置 动态防火墙。

1. 作为具有所有者角色的 Duo 用户，配置思科 身份情报 租户。

   您可以按照调配思科身份智能租户中的说明，从 Duo Advantage 调配租户。

2. 在思科 身份情报 中，创建 API 集成，并使用相关信息来设置 动态防火墙。

   我们使用思科 身份情报 在您的网络中查找用户和设备风险信息。

   有关思科 身份情报 的详细信息，请参阅《操作指南》。

   有关此任务的详细信息，请参阅获取所需的 身份情报 信息，第 2390 页。

3. （仅限 Microsoft Azure AD 领域。）在 身份情报 中，创建 Microsoft Entra ID 集成。

   有关详细信息，请参阅《Microsoft Entra ID (Azure AD) 数据集成》。

4. 创建身份源。（如果您已有身份源，请继续执行下一步。）

   您可以通过以下任何一种方式执行此操作：

   - 配置动态防火墙对话框会显示**配置**链接，用于开始设置您的身份源。
   - 请点击 **集成** > **身份** > **身份源**。

   有关创建身份源的详细信息，请参阅：

   - 配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页
   - 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 2143 页
   - 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本），第 2175 页

5. 创建身份领域。

   我们支持以下领域：

   - 创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页

     仅支持 Microsoft AD；不支持 LDAP 领域。

- 为被动身份验证创建Microsoft Azure AD (SAML)领域， 第 2002 页

6. 启用dynamic attributes connector。

   使用 动态防火墙 需借助 dynamic attributes connector。它使您的身份源能够与 身份情报 集成，从而提供有关用户活动的增强洞察。

   请参阅启用 dynamic attributes connector， 第 2116 页。

7. 创建 动态防火墙 实例。（如果您已有 动态防火墙 实例，请继续执行下一步。）

   点击 **集成** > **动态属性连接器**，然后点击**配置动态防火墙**。

   请参阅创建 动态防火墙 实例， 第 2392 页。

8. 将您的身份源与思科 身份情报 相关联。

   请参阅将身份源与 身份情报 相关联， 第 2393 页。

9. 查看系统定义的过滤器。

   我们为以下内容创建动态属性过滤器：

   - 不可信设备
   - 可信设备
   - 不可信用户
   - 可疑用户

   您可以按照创建动态属性过滤器， 第 2401 页中的说明编辑或替换这些动态属性过滤器。

10. 查看系统定义的访问控制规则。

    我们会创建一个名为“动态防火墙策略”（或类似名称）的访问控制策略，其中包含以下规则：

    - 阻止不可信用户从任何源网络访问任何目标网络。
    - 监控可疑用户从任何源网络访问任何目标网络。
    - 阻止不可信设备从任何源网络访问任何目标网络。

    您可以按照查看和编辑系统创建的访问控制策略， 第2400 页中的说明编辑或删除访问控制策略和规则。

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

启用 dynamic attributes connector

此任务讨论如何在 Secure Firewall Management Center启用 dynamic attributes connector 。 dynamic attributes connector是一种集成，它使得来自云网络产品的对象能够用于Secure Firewall Management Center访问控制和 DNS 规则。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到**已启用 (Enabled)**。

步骤 4 启用 dynamic attributes connector 时，系统会显示消息。

如果出现错误，请重试。如果错误仍然存在，请联系思科 TAC。

下一步做什么

请参阅创建连接器，第 2340 页。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

获取所需的 身份情报 信息

此任务讨论如何创建 API 客户端，该客户端提供在动态防火墙中设置身份情报所需的所有信息。

如果您已有 API 客户端，并且知道以下所有值，则可以跳过此过程并继续执行创建 动态防火墙 实例，第 2392 页：

- **客户 ID**
- **API URL**
- **令牌 URL**
- **客户端密钥**

开始之前

与 动态防火墙 集成要求您在 身份情报 中创建 *API* 客户端集成。

您必须了解的关于 API 客户端集成的值包括客户端密钥，该密钥仅在创建 API 客户端时显示。因此，您可能需要先创建 API 集成。

有关创建 API 客户端集成的详细信息，请参阅公共 API。

过程

步骤 1 登录到您的 身份情报 租户。

步骤 2 点击 （**集成**）。

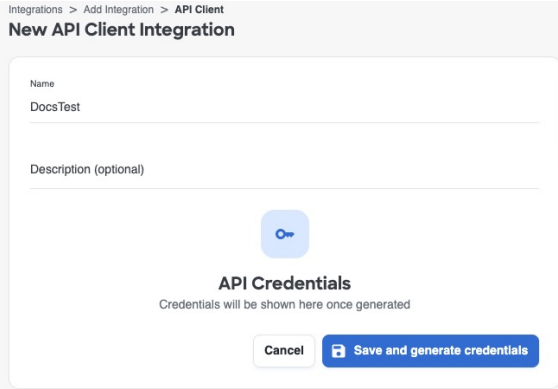
步骤 3 点击**添加集成**。

步骤 4 在下一页上，在“API 客户端”下，点击**添加 API 客户端**。

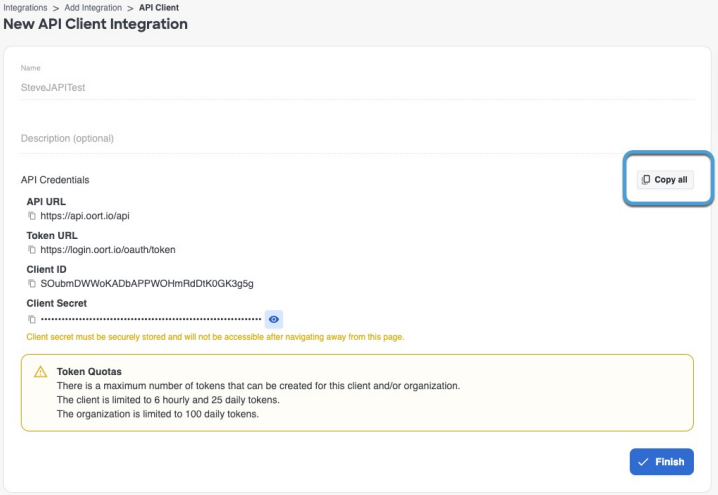
步骤 5 输入**名称**和可选的**说明**。

步骤 6 点击**保存并生成凭证**。

下图显示了一个示例。



步骤 7 在下一页上，如以下图所示，点击**全部复制**。



步骤 8 保存凭证以供稍后使用。

步骤 9 点击**完成 (Finish)**。

下一步做什么

请参阅创建 动态防火墙 实例， 第 2392 页。

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

为 动态防火墙 创建身份源和领域

在配置 动态防火墙 之前，您必须配置受支持的身份领域和身份源。

配置身份领域

支持以下身份领域：

- 创建 LDAP 领域或 Active Directory 领域和领域目录， 第 2019 页

  仅支持 Microsoft AD；不支持 LDAP 领域。

- 为被动身份验证创建Microsoft Azure AD (SAML)领域， 第 2002 页

配置身份源

支持以下身份源：

- 本地 Cisco ISE：配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页
- 单个或多个 Cisco ISE 集群：
  - 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）， 第 2175 页
  - 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）， 第 2143 页

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

创建 动态防火墙 实例

此任务讨论如何创建 动态防火墙 的新实例，该实例是身份源与 身份情报 之间的关联。

开始之前

执行以下所有操作：

- 启用 dynamic attributes connector，如启用 dynamic attributes connector， 第 2116 页中所述。
- 创建身份源：
  - 配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页。
  - 创建一个 pxGrid 云身份源， 第 2150 页。

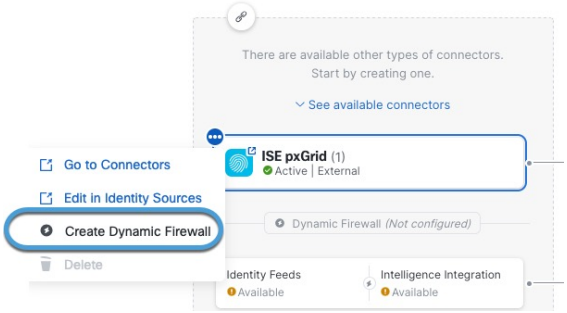
过程

步骤 1 如果尚未执行此操作，请登录 Secure Firewall Management Center。

步骤 2 点击**集成** > **动态属性连接器**。

步骤 3 点击身份源名称旁边的 ，通过它可以添加 动态防火墙。

下图显示了一个示例。



注释

如果未看到身份源，请先创建一个身份源，然后再继续：

- 配置思科身份服务引擎 (Cisco ISE)身份源的方法， 第 2092 页
- 如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）， 第 2143 页
- 如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）， 第 2175 页

步骤 4 点击**创建动态防火墙**。

步骤 5 继续将身份源与 身份情报 相关联， 第 2393 页。

相关主题

关于 动态防火墙， 第 2387 页

如何配置 动态防火墙， 第 2387 页

将身份源与 身份情报 相关联

此任务讨论如何将身份源与 身份情报 相关联， 会向 Secure Firewall Management Center 提供用户和设备信任评分。

有关详细信息，请参阅用户信任级别。

开始之前

开始之前，请确保您：

- 了解关于 动态防火墙， 第 2387 页中讨论的身份领域、身份源和 身份情报 如何协同工作。

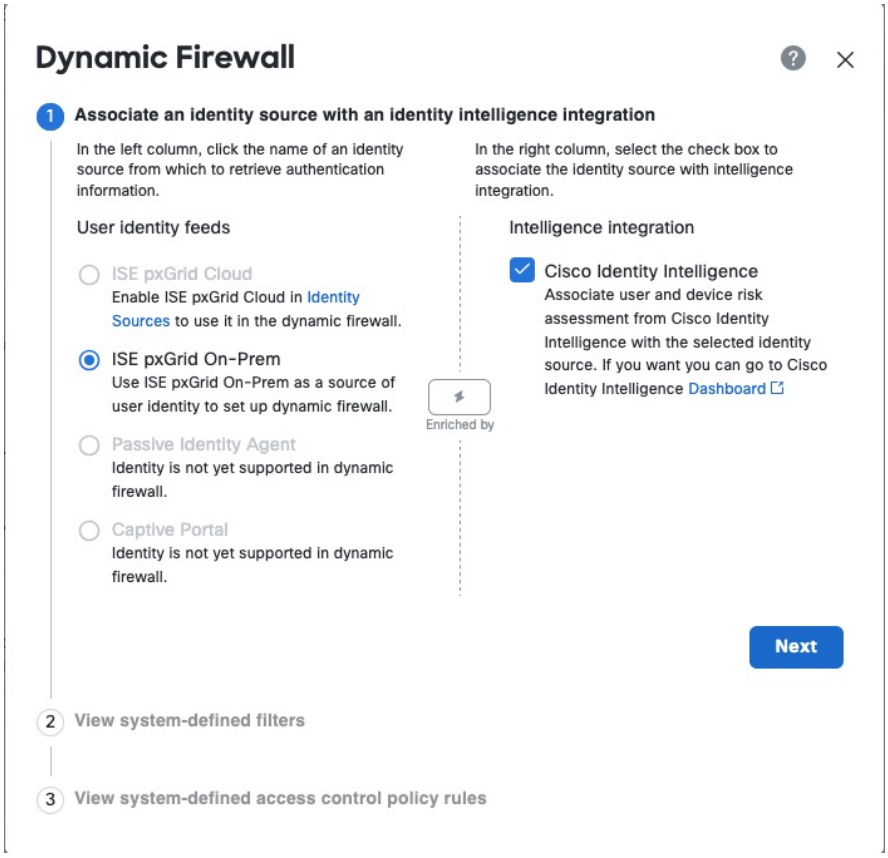
- 完成创建 动态防火墙 实例， 第 2392 页中讨论的任务。

过程

步骤 1 首先创建 动态防火墙 实例， 第 2392 页。

步骤 2 在下一页的左列中，点击您的身份源。然后，从右列选中**思科身份智能**复选框，以添加用户智能（包括用户和设备风险）。

下图显示了一个示例。



步骤 3 点击**下一步 (Next)**。

步骤 4 继续执行配置 身份情报， 第 2395 页。

相关主题

关于 动态防火墙， 第 2387 页
如何配置 动态防火墙， 第 2387 页

配置 身份情报

此任务讨论如何将身份源与 身份情报 相关联，后者会向 Secure Firewall Management Center 提供用户和设备风险评分。

开始之前

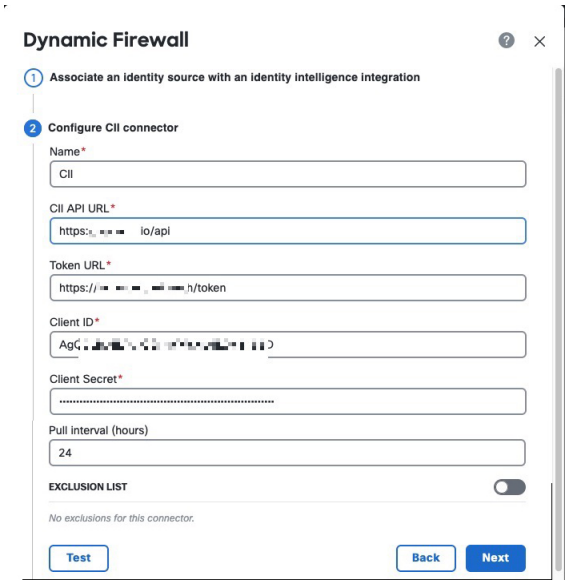
完成 将身份源与 身份情报 相关联， 第 2393 页中讨论的任务。

过程

步骤 1 完成 将身份源与 身份情报 相关联， 第 2393 页中讨论的任务。

步骤 2 如果您选中了**思科身份智能**复选框，请输入您找到的 身份情报 相关信息，如获取所需的 身份情报 信息， 第 2390 页中所述。

下图显示了一个示例。



步骤 3 （可选。）要让 身份情报 将特定用户组视为可信用户，请将**排除列表**滑动至**滑块已启用** ( )。

按 **username@domain.com** 格式每行输入一个用户名。此列表中的用户会被 身份情报 视为可信用户。

步骤 4 点击**测试**。

仅当测试成功时，才继续执行下一步。

如果显示任何错误，请检查所有 身份情报 值并重试。

步骤 5 点击**下一步 (Next)**。

步骤 6 继续执行查看系统定义的过滤器，第 2396 页。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

查看系统定义的过滤器

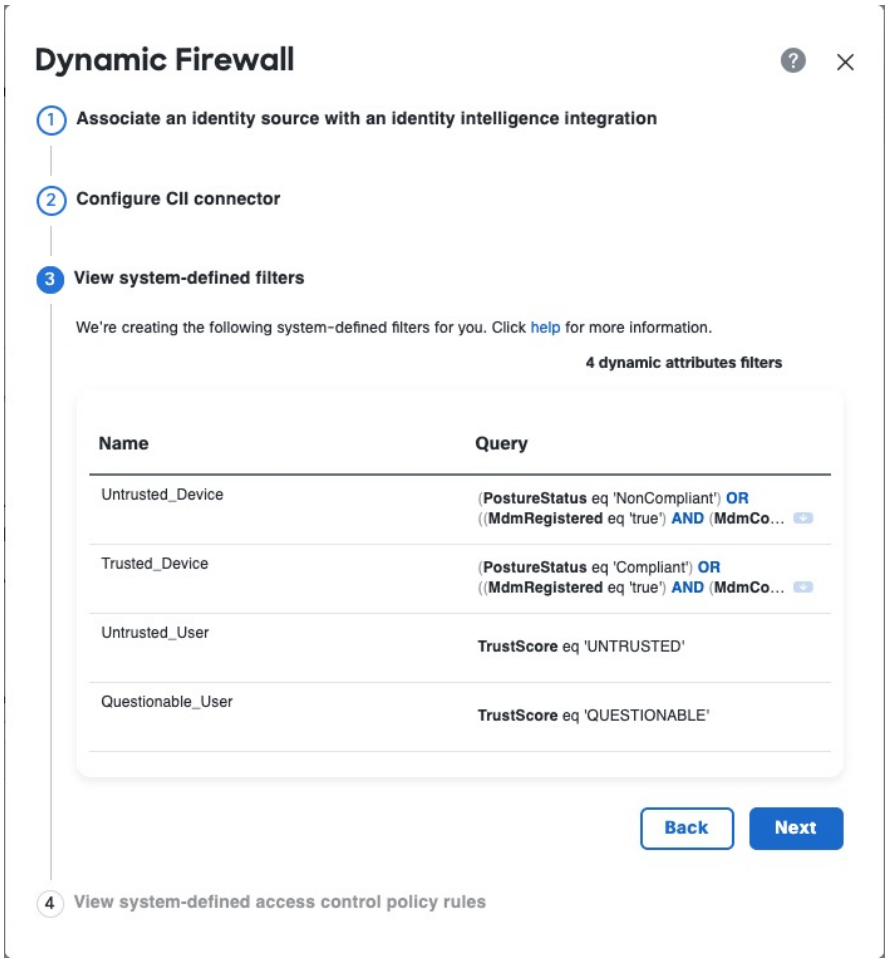
此任务讨论如何将身份源与思科 身份情报 相关联，后者会向 Secure Firewall Management Center 提供用户和设备风险评分。

开始之前

请参阅配置 身份情报，第 2395 页。

过程

步骤 1 系统显示一组系统定义的动态属性过滤器，如下图所示。



步骤 2 查看系统创建的过滤器。点击任意行上的 即可展开过滤器，以便查看过滤器及其详细信息。

步骤 3 点击**下一步 (Next)**。

步骤 4 继续执行查看系统定义的访问控制规则，第 2397 页。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

查看系统定义的访问控制规则

本任务讨论由 动态防火墙 创建的访问控制规则。

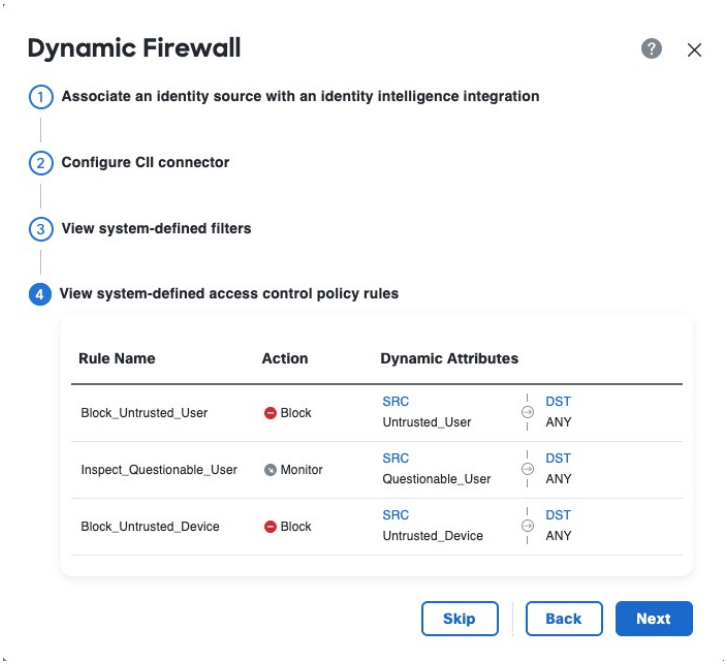
开始之前

请参阅查看系统定义的过滤器，第 2396 页。

过程

步骤 1 查看系统创建的访问控制规则。

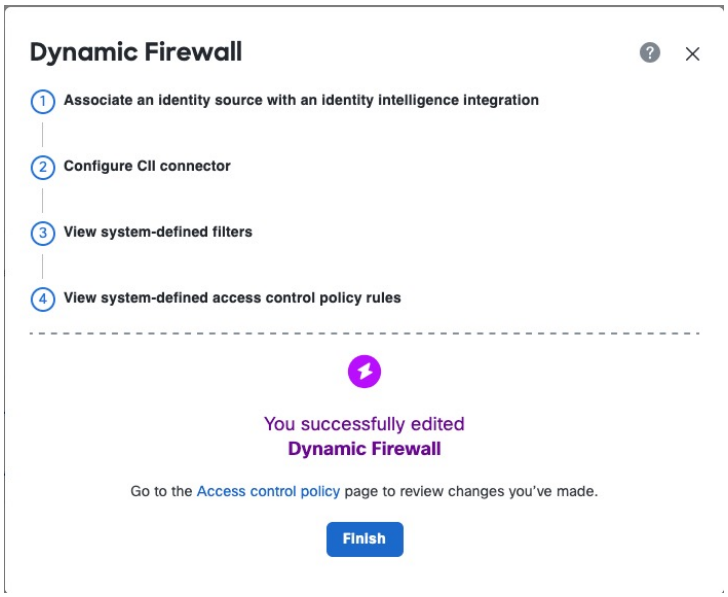
下图显示了一个示例。



步骤 2 选择以下选项之一：

- 点击**跳过**以跳过创建这些访问控制规则。您可以随时创建自己的规则。
- 点击**下一步**，创建一个名为“动态防火墙策略”的访问控制策略，其中包含上图所示的规则。
- 点击**返回**可返回到系统创建的过滤器。

步骤 3 点击**下一步**后，如果成功创建了访问控制规则，将显示以下页面：



相关主题

关于 动态防火墙 ， 第 2387 页
如何配置 动态防火墙 ， 第 2387 页

编辑用户排除列表

（可选。）您可以指示 身份情报 将特定用户视为可信用户。

开始之前

按照创建 动态防火墙 实例 ， 第 2392 页中所述配置 动态防火墙。

过程

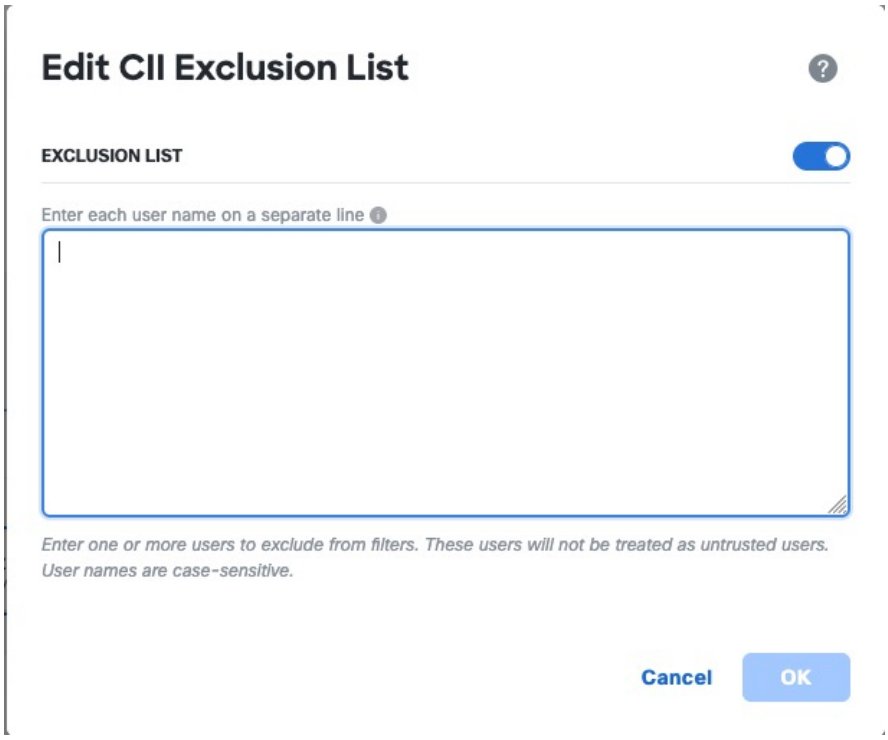
步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 点击身份源名称旁边的 。

步骤 4 点击**编辑 CII 排除列表**。

系统将显示以下对话框。



步骤 5 在提供的字段中，按 `username@domain.com` 格式在一行中输入一个用户名，按 Enter 键，然后输入另一个用户名。

每个用户名都会被 身份情报 视为可信用户。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

查看和编辑系统创建的访问控制策略

本主题讨论如何编辑系统创建的访问控制规则和策略。最初，该策略未与任何设备关联，但如果要使用它，可添加设备、更改规则、重新排序规则或删除规则。

开始之前

完成查看系统定义的访问控制规则，第 2397 页中所述的任务。

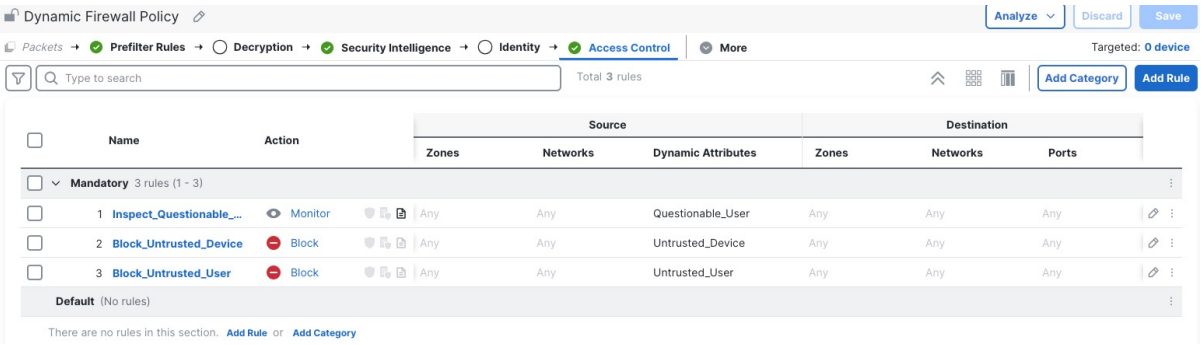
过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center。

步骤 2 请点击 **策略** > **安全策略** > **访问控制**。

步骤 3 点击名为“动态防火墙策略”（或类似名称）的策略旁边的 **编辑** ()。

下图显示了一个示例访问控制策略。



请注意，在此访问控制策略中，只有设置为监控可疑用户的规则会记录日志。要调整日志记录设置，请参阅访问控制策略的日志记录设置，第 1718 页。

步骤 4 执行以下任一操作：

- 将访问控制策略定位到设备：将设备分配给访问控制策略，第 1717 页。
- 编辑策略，包括添加日志记录：管理访问控制策略，第 1707 页。
- 编辑访问控制规则：管理访问控制规则，第 1763 页。
- 设置高级策略选项：为访问控制策略配置高级设置，第 2456 页。
- 将其他策略与该访问控制策略关联：将其他策略与访问控制相关联，第 1719 页。

相关主题

关于 动态防火墙，第 2387 页
如何配置 动态防火墙，第 2387 页

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

有关访问控制规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 2165 页。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **连接器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** ()。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在访问控制策略和 Secure Firewall Management Center 对象管理器（**外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。
查询	请点击 添加。

步骤 5 要添加查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。
您创建的动态属性查询应显示为动态对象。

相关主题

关于 动态防火墙 ， 第 2387 页
如何配置 动态防火墙 ， 第 2387 页

禁用 dynamic attributes connector

如果您不想再从云源收集动态对象，可以禁用 Dynamic Attributes Connector 中的 Secure Firewall Management Center ，如以下任务中所述。

过程

步骤 1 如果尚未登录，请登录 Secure Firewall Management Center 。

步骤 2 请点击 **集成** > **动态属性连接器**。

步骤 3 滑动到 **已禁用**。

使用 Secure Firewall Management Center 进行故障排除

此任务讨论如何为 Secure Firewall Management Center生成故障排除文件。

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 > **运行状况** > **监控器故障排除** 。

步骤 3 在左侧窗格中，点击 **防火墙管理中心**。

步骤 4 点击顶部的 **系统和故障排除详细信息**。

步骤 5 点击 **Generate Troubleshooting Files**。

步骤 6 将文件提供给思科 TAC 或您的 Beta 版协调员。

手动获取证书颁发机构 (CA) 链

在事件中无法自动获取证书颁发机构链，使用以下浏览器特定程序之一获取用于安全连接到vCenter、防火墙管理中心。

证书链是根证书和所有从属证书。

您可以选择使用以下程序之一连接到以下设备：

- vCenter 或 NSX
- 防火墙管理中心

- 思科 APIC

获取证书链 - Mac（Chrome 和 Firefox）

使用此程序在 Mac OS 上使用 Chrome 和 Firefox 浏览器来获取证书链。

1. 打开终端窗口。
2. 输入以下命令。

   ```
   security verify-cert -P url[:port]
   ```

   其中 *url* 是 vCenter、 防火墙管理中心 的 URL（包括方案）。例如：

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   如果使用 NAT 或 PAT 访问 vCenter、 防火墙管理中心，可以按如下方式添加端口：

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

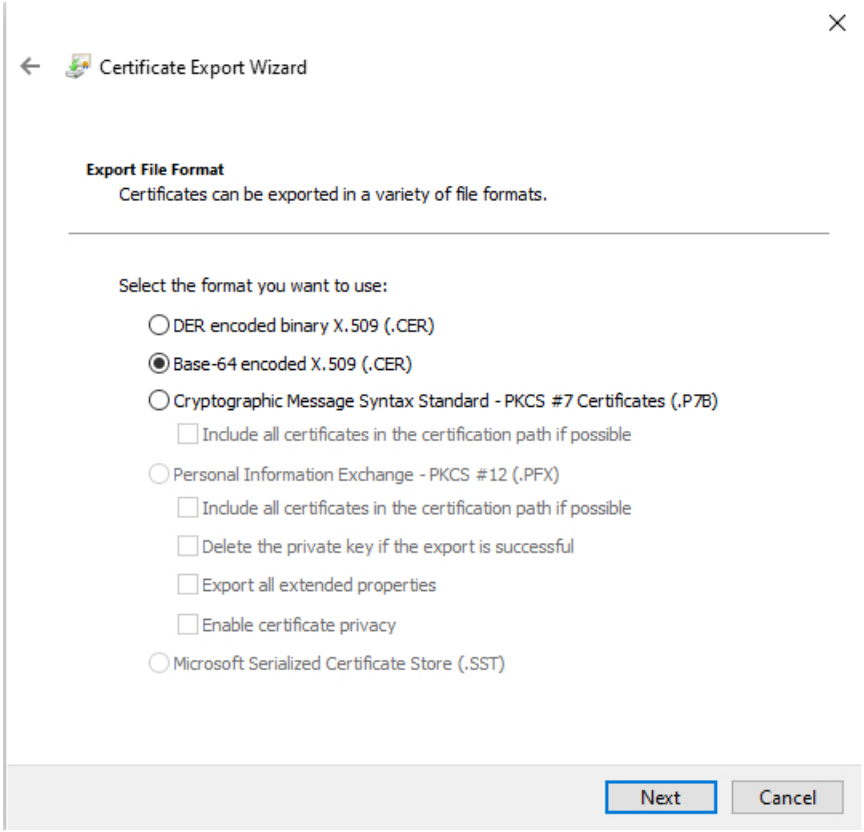
3. 将整个证书链保存到纯文本文件中。
   - 包括所有 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 分隔符。
   - 排除任何无关的文本（例如，证书的名称和尖括号 (< and >) 中包含的任何文本以及尖括号本身。
4. 对 vCenter 防火墙管理中心 重复这些任务。

获取证书链 - Windows Chrome

使用此程序在 Windows 上使用 Chrome 浏览器来获取证书链。

1. 使用 Chrome 登录 vCenter、 防火墙管理中心。
2. 在浏览器地址栏中点击主机名左侧的锁图标。
3. 点击**证书 (Certificate)**。
4. 点击**认证路径 (Certification Path)** 选项卡。
5. 点击证书链中顶部的（即第一个）证书。
6. 点击**查看证书 (View Certificates)**。
7. 点击**详细信息 (Details)** 选项卡。
8. 点击**复制到文件 (Copy to File)**。
9. 按照提示创建包含整个证书链的 CER 格式证书文件。

   当系统提示您选择导出文件格式时，点击 **Base 64-Encoded X.509 (.CER)**，如下图所示。



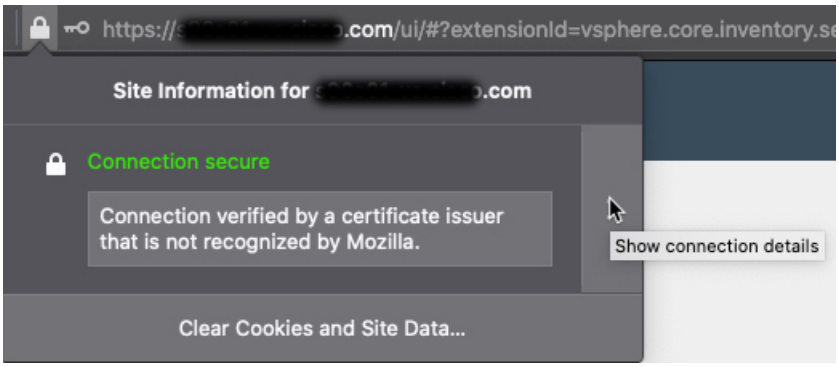
10. 按照提示完成导出。
11. 在文本编辑器中打开证书。
12. 对证书链中的所有证书重复此过程。

    您必须先按顺序将每个证书粘贴到文本编辑器中。
13. 对 vCenter、 防火墙管理中心 重复这些任务。

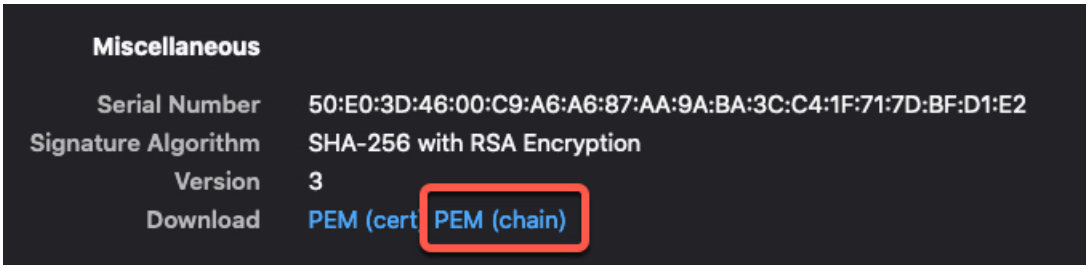
获取证书链 - Windows Firefox

使用以下程序为 Windows 或 Mac OS 上的 Firefox 浏览器来获取证书链。

1. 使用 Firefox 登录 vCenter、 防火墙管理中心。
2. 点击主机名左侧的锁图标。
3. 点击右箭头（**显示连接详细信息**）。下图显示了一个示例。



4. 点击**更多信息 (More Information)**。
5. 点击**查看证书 (View Certificates)**。
6. 如果生成的对话框包含选项卡页面，请点击与顶层 CA 对应的选项卡页面。
7. 滚动到“其他”(Miscellaneous) 部分。
8. 点击下载行中的 **PEM（链）(PEM [chain])**。下图显示了一个示例。



9. 保存文件。
10. 对 vCenter、 防火墙管理中心 重复这些任务。

相关主题

与 思科 APIC 集成的系统要求 ， 第 2354 页
获取集成所需的信息 ， 第 2354 页
创建连接器思科 APIC ， 第 2358 页
如何在访问控制规则或 DNS 规则中使用 Secure Firewall Management Center 中 思科 APIC 的动态对象 ， 第 2353 页
手动获取证书颁发机构 (CA) 链 ， 第 2359 页
思科 APIC 连接器 ， 第 2352 页

安全要求

为了保护dynamic attributes connector，应将其安装在受保护的内部网络中。虽然dynamic attributes connector被配置为仅提供必要的服务和端口，但您必须确保该防御中心不会受到攻击。

如果 dynamic attributes connector 和 Secure Firewall Management Center 位于同一个网络，您可以将 Secure Firewall Management Center 连接到与 dynamic attributes connector 相同的受保护内部网络。

无论如何部署设备，内部系统通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

互联网接入要求

默认情况下，dynamic attributes connector 会被配置为使用端口 443/tcp (HTTPS) 上的 HTTPS 通过互联网与 Firepower 系统通信。如果您不希望 dynamic attributes connector 直接访问互联网，则可以配置代理服务器。

以下信息会告知您 dynamic attributes connector 用来与 Secure Firewall Management Center 和外部服务器通信的 URL。

表 *135: Dynamic Attributes Connector* 访问要求

URL	原因
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	身份验证
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET 和 POST 动态对象
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	添加映射
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id*** /object/dynamicobjects/***object-id***/mappings?action=remove**	删除映射

表 *136: Dynamic Attributes Connector vCenter* 访问要求

URL	原因
https://*vcenter-ip***/rest/com/vmware/cis/session**	身份验证
https://*vcenter-ip***/rest/vcenter/vm**	获取 VM 信息
https://*nsx-ip***/api/v1/fabric/virtual-machines/***vm-id***	获取与虚拟机关联的 NSX-T 标记

从 DockerHub 迁移到 Amazon ECR

Dynamic Attributes Connector 的 Docker 映像正在从 Docker Hub 迁移到 Amazon Elastic Container Registry (Amazon ECR)。

要使用新的字段包，必须允许通过防火墙或代理访问以下所有 URL：

- https://public.ecr.aws
- https://csdac-cosign.s3.us-west-1.amazonaws.com
- https://d2glxqk2uabbnd.cloudfront.net
- https://d5l0dvt14r5h8.cloudfront.net

有关 Amazon CloudFront URL 的更多信息，请参阅 EKS Anywhere 文档。

Dynamic Attributes Connector Azure 访问要求

dynamic attributes connector 会调用内置 SDK 方法获取实例信息。这些方法会在内部调用 https://login.microsoft.com（用于身份验证）和 https://management.azure.com（用于获取实例信息）。

dynamic attributes connector 的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DNS 规则对动态对象和安全组标记的支持。	10.0.0	10.0.0	您可以在 DNS 策略中配置 DNS 规则以使用动态对象或安全组标记 (SGT)。如果您已经在访问控制规则中使用这些类型的对象，现在可以将其使用扩展到您的 DNS 策略。 我们在添加/编辑 DNS 规则对话框中添加了“动态属性”选项卡。
动态防火墙	10.0.0	10.0.0	以前，Secure Firewall Management CenterSecure Firewall Management Center 仅从配置的身份源（如 Microsoft Active Directory、被动身份代理、思科身份服务引擎 (Cisco ISE) 等）收集有关用户的信息。此信息通常包括用户名、组和 IP 地址。 借助 动态防火墙，您可以将来自思科 身份情报 的用户风险评分添加到身份源提供的信息中，以便根据始终最新的用户终端安全评估和风险设置策略。我们支持您将用户身份与智能配对，并在报告和访问控制策略中使用该信息。 **新增/修改的屏幕：** • 请点击 **集成** > **动态属性连接器**。然后点击身份源名称旁的 ，点击**创建动态防火墙**。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
思科 APIC 连接器	10.0.0	10.0.0	dynamic attributes connector 使您能够将 思科 APIC 动态终端组 (EPG) 和终端安全组 (ESG) 数据从 思科 APIC 租户发送到 。 **新增/更新的屏幕：** • **集成** > **动态属性连接器** > **连接器** > **新建连接器**
新连接器	7.6	20241127	AWS 安全组、AWS 服务标签和 Cisco Cyber Vision 这些连接器可以像 Security Cloud Control 一样发送本地 Secure Firewall Management Center 动态对象。 要从本地 dynamic attributes connector 接收动态对象，需要使用 3.0 版本的本地动态属性连接器。
Dynamic Attributes Connector	7.4.0	7.4.0	引入了此功能。 Dynamic Attributes Connector 现在包含在 Secure Firewall Management Center中。您可以在访问控制规则中使用 dynamic attributes connector 从基于云的平台（例如 Microsoft Azure）获取 IP 地址，而无需部署到托管设备。 详细信息： • 此产品随附的 dynamic attributes connector： 关于 dynamic attributes connector，第 2325 页 • 独立 dynamic attributes connector： *《Cisco Secure Dynamic Attributes Connector 配置指南》* 新的/修改后的屏幕： **集成** > **动态属性连接器**



第 63 章

威胁情报导向器

本章中的主题介绍如何配置和使用 威胁智能导向器。

- Cisco Secure Firewall 威胁智能导向器 概述， 第 2411 页
- 威胁情报导向器要求和前提条件， 第 2414 页
- 如何设置威胁智能导向器， 第 2416 页
- 分析 威胁智能导向器 事件和观察数据， 第 2425 页
- 查看和更改威胁智能导向器 配置， 第 2437 页
- 对威胁智能导向器进行故障排除， 第 2451 页
- 的历史记录威胁智能导向器， 第 2453 页

Cisco Secure Firewall 威胁智能导向器 概述

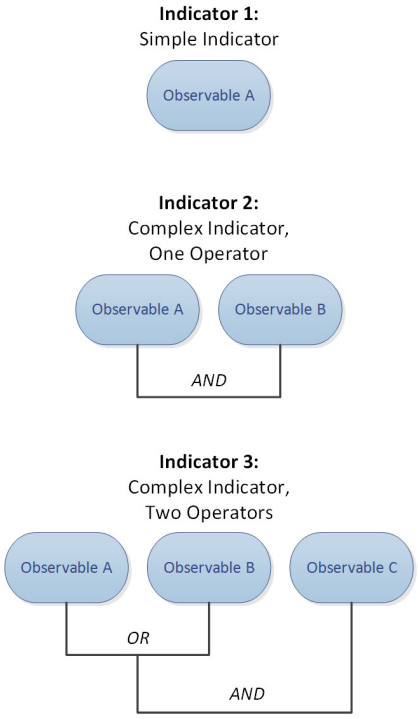
Cisco Secure Firewall 威胁智能导向器使用威胁情报数据进行操作，从而帮助您聚合情报数据，配置防御操作，并分析环境中的威胁。此功能旨在补充其他 Firepower 功能，可进一步加强对威胁的防御。

当在托管平台上配置 威胁智能导向器时，它会从威胁情报源摄取数据，并将数据发布到所有配置的托管设备（元素）。有关此版本中支持的托管平台和元素的更多信息，请参阅平台、元素和许可证要求， 第 2414 页。

源包含指示器，其中包含可观察对象。指示器传递与威胁相关的所有特征，而单个可观察对象表示与威胁相关的单个特征（例如 SHA-256 值）。简单指示器包含单个可观察对象，而复杂指示器包含两个或更多可观察对象。

可观察对象以及它们之间的 AND/OR 运算符构成指示器的模式，如下面的示例所示。

图 *450:* 示例：指示器模式



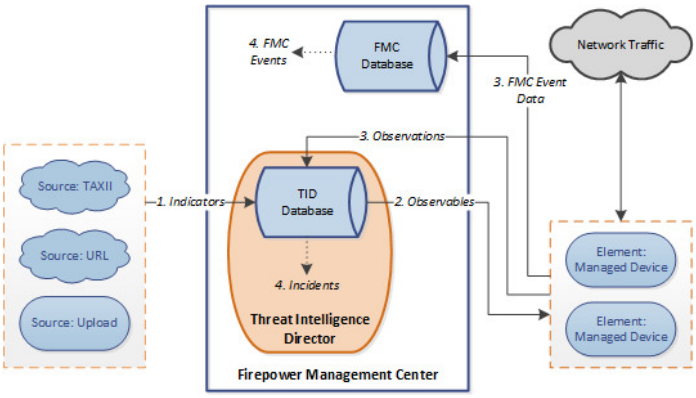
将可观察对象发布到元素后，在系统识别流量中的可观察对象时，元素会监控流量并将观察结果报告到 防火墙管理中心。

防火墙管理中心会从所有元素收集观察结果，根据 威胁智能导向器指示器评估观察结果，以及生成或更新与可观察对象的父指示器相关的事故。

当指示器的模式完成时，事件即完全实现。如果流量与指示器中的一个或多个可观察对象相匹配但未匹配整个模式，事故会部分实现。有关详细信息，请参阅观察和事故生成，第 2425 页。

下图显示了系统配置示例中的数据流。

图 *451:* 防火墙管理中心 数据流



当 威胁智能导向器事故完全或部分实现时，系统会执行配置的操作（监控、阻止、部分阻止或无操作）。有关详细信息，请参阅影响所执行操作的因素，第 2433 页。

威胁智能导向器和安全智能

作为访问控制策略的一部分，安全智能使用信誉情报来快速阻止与IP地址、URL和域之间的往来连接。安全智能唯一地提供通过 Talos 智能小组 对业界领先的威胁情报的访问。有关安全智能的详细信息，请参阅关于安全智能，第 1729 页。

威胁智能导向器增强了系统根据来自第三方来源的安全智能阻止连接的能力，如下所示：

- **威胁智能导向器 支持其他流量过滤条件** - 安全智能使您可以根据 IP 地址、URL 和（如果已启用 DNS 策略）域名来过滤流量。威胁智能导向器 还支持按这些条件进行过滤，并增加了对 SHA-256 散列值进行过滤的支持。
- **威胁智能导向器 支持其他情报注入方法** - 使用安全智能和 威胁智能导向器，可以通过手动上传平面文件或配置系统以从第三方主机检索平面文件，从而将威胁情报导入系统。威胁智能导向器 增强了管理这些平面文件的灵活性。此外，威胁智能导向器可以检索和摄取以结构化威胁信息表达式 (STIX™) 格式提供的情报。
- **威胁智能导向器提供对过滤操作的精细控制** - 使用安全智能，可以按网络、URL 或 DNS 对象指定过滤条件。安全智能对象（特别是列表和源）可以包含多个 IP 地址、URL 或 DNS 域名，但您只能根据整个对象来阻止或不阻止，而不是根据一个对象的单个组件来阻止。使用 威胁智能导向器，可以为单个条件（即简单指示器或单个可观察对象）配置过滤操作。
- **威胁智能导向器配置更改不需要重新部署** - 在访问控制策略中修改安全智能设置后，必须将更改的配置重新部署到托管设备。使用 威胁智能导向器，将访问控制策略初始部署到托管设备后，可以配置源、指示器和可观察对象而无需重新部署，系统会自动将新的 威胁智能导向器数据发布到这些元素。

有关安全智能或威胁智能导向器可以处理特定事件时系统操作的相关信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 2433 页。

威胁情报导向器的性能影响

Secure Firewall Management Center

在某些情况下，您可能会发现存在以下情况：

- 在摄取特别大的 STIX 源时，系统可能会遇到一些小的性能问题，而且摄取完成时间可能会比预期的要长。
- 系统可能需要 15 分钟才能将新的或修改后的威胁智能导向器数据向下发布到元素。

托管设备

对性能没有特殊影响。威胁智能导向器 对性能的影响与 Secure Firewall Management Center安全智能功能完全相同。

威胁情报导向器要求和前提条件

型号支持

任意

支持的域

任意

用户角色

管理员

威胁智能导向器用户

其它要求

以下主题介绍了使用威胁情报导向器的其他要求。

平台、元素和许可证要求

托管平台

可以在物理和虚拟 Secure Firewall Management Center上托管 威胁智能导向器：

- 运行版本 6.2.2 或更高版本。
- 配置至少 15 GB 的内存。
- 配置为已启用 REST API 访问。请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 启用 *REST API* 访问。

元素

如果设备运行的是 6.2.2 或更高版本，则可以使用任何 Secure Firewall Management Center托管设备作为 威胁智能导向器 元素。

许可

要为 SHA-256 可观察对象发布配置文件策略，您需要以下许可设备：

- 对于智能许可设备：
  - IPS 许可证 - 适用于 IPv4、IPv6、URL 和 DNS 检测和可观察对象
  - 恶意软件防御 许可证 - 用于 SHA-256 检测和可观察对象

有关详细信息，请参阅配置策略以支持威胁智能导向器，第 2417 页和 *Cisco Secure Firewall Management Center* 管理指南中的 。

源要求

源类型要求

STIX

文件必须是 STIX 版本 1.0、1.1、1.1.1 或 1.2，并且遵守 STIX 文档中的准则：http://stixproject.github.io/documentation/suggested-practices/。

STIX 文件可以包括复杂的指示器。

通过 URL 下载或文件上传进行配置时，STIX 文件的最大大小为 40MB。如果您的 STIX 文件大于此值，我们建议使用 TAXII 服务器。

平面文件

文件必须是每行包含一个可观察值的 ASCII 文本文件。

平面文件仅包括简单的指示器（每个指示器一个可观察对象）。

平面文件上传的文件最大可达 500 MB。

威胁智能导向器 不支持：

- 分隔可观察值的分隔符字符（例如 `observable,` 无效）。
- 围绕可观察值的封闭字符（例如 `"observable"` 无效）。

每个文件应仅包含一种类型的内容：

- `SHA-256` - SHA-256 散列值。
- `域` - RFC 1035 中定义的域名。
- `URL` - RFC 1738 中定义的 URL。

注释 威胁智能导向器 会规范化包含端口、协议或身份验证信息的任何 URL，并在检测指示器时使用规范化的版本。例如，威胁智能导向器 会将以下任一 URL：

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

规范化为：

```
example.com/index.htm
```

再例如，威胁智能导向器 会将以下 URL：

```
http://abc@example.com:8080/index.htm
```

规范化为

```
abc@example.com/index.htm/
```

- `IPv4` - RFC 791 中定义的 IPv4 地址。

  威胁智能导向器 不接受 CIDR 块。

- `IPv6` - RFC 4291 中定义的 IPv6 地址。

  威胁智能导向器 不接受前缀长度。

源内容限制

系统仅会注入并匹配 URL 可观察对象的前 1000 个字符。

如何设置威胁智能导向器

注释 如果在 威胁智能导向器配置或操作期间遇到问题，请参阅对威胁智能导向器进行故障排除，第 2451 页。

过程

步骤 1 确保您的安装符合 威胁智能导向器 运行要求。

请参阅 平台、元素和许可证要求，第 2414 页

步骤 2 对于每个托管设备，配置支持 威胁智能导向器 所需的策略，并将这些策略部署到设备。

请参阅配置策略以支持威胁智能导向器，第 2417 页。

可以在采集情报数据源之前或之后配置元素。

步骤 3 配置您希望 威胁智能导向器 采集的情报源。

请参阅源要求，第 2415 页和采集数据源的选项，第 2418 页下的主题。

步骤 4 如果尚未将数据发布到元素，请执行此操作。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。

下一步做什么

- 将 威胁智能导向器 纳入定期计划备份。请参阅关于备份和恢复 威胁智能导向器 数据，第 2424 页。

  如果您的 Secure Firewall Management Center 部署是高可用性配置，另请参阅 *Cisco Secure Firewall Management Center* 管理指南中的 防火墙管理中心 高可用性灾难恢复 。

- （可选）根据需要为 威胁智能导向器 功能授予管理访问权限。请参阅 具有 威胁智能导向器 访问权限的用户角色，第 2424 页 和 *Cisco Secure Firewall Management Center* 管理指南中的 用户 章节。

- 在运行期间，根据需要精细调节配置。例如，生成误报事件的白名单可观察对象。请参阅查看和更改威胁智能导向器 配置，第 2437 页。

配置策略以支持威胁智能导向器

您必须配置访问控制策略，以将 威胁智能导向器 数据从防火墙管理中心发布到托管设备（元素）。此外，我们还建议配置访问控制策略，以最大化观察结果和 防火墙管理中心事件生成。

对于您要支持 威胁智能导向器 的每个托管设备，请执行以下步骤以配置相关联的访问控制策略。

配置为在已发布数据后使用 威胁智能导向器 的元素将自动接收所有当前已发布的可观察对象。

过程

步骤 1 验证并确保已选中访问控制策略的 **常规设置** 中的 **启用威胁情报导向器** 复选框。要导航到**常规设置**，请选择 **策略** > **安全策略** > **访问控制**，然后点击**编辑** > **更多** > **高级设置**。默认情况下，此选项已启用。

有关详细信息，请参阅常规设置，第 2458 页。

步骤 2 如果尚不存在规则，请向访问控制策略添加规则。威胁智能导向器要求访问控制策略必须指定至少一个规则。

由于威胁智能导向器取决于检测，请确保允许流量而不是信任流量，因为信任流量的目的是绕过检测。有关详细信息，请参阅创建基本访问控制策略，第 1708 页。

步骤 3 如果选择**入侵防御** 作为访问控制策略的默认操作，请将解密策略与该访问控制策略相关联；请参阅将其他策略与访问控制相关联，第 1719 页。

步骤 4 如果您希望 `SHA-256` 可观察对象生成观察结果和 Secure Firewall Management Center事件：

a) 创建包含一个或多个**恶意软件云查找 (Malware Cloud Lookup)** 或**阻止恶意软件 (Block Malware)** 文件规则的文件策略。

有关详细信息，请参阅配置文件策略，第 2290 页。

b) 将此文件策略与访问控制策略中的一个或多个规则相关联。

步骤 5 如果希望 `IPv4`、`IPv6`、`URL` 或域名观察结果生成连接和安全智能事件，则请在访问控制策略中启用连接和安全智能日志记录：

a) 在调用文件策略的访问控制规则中，启用**在连接结束时记录日志**和**文件事件：日志文件**（如果尚未启用）。

有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中 的使用访问控制规则记录连接。

b) 验证并确保已在“安全智能”设置中启用了默认日志记录（**DNS 策略**、**网络**和 **URL**）。

有关详细信息，请 *Cisco Secure Firewall Management Center* 管理指南中的 参阅 中使用安全智能记录连接 。

步骤 6 部署配置更改；请参阅 部署配置更改，第 180 页。

下一步做什么

完成如何设置威胁智能导向器，第 2416 页中的剩余项目。

采集数据源的选项

请根据要使用的数据类型和传送机制选择配置选项。

有关这些数据类型的详细信息，请参阅源要求，第 2415 页。

表 *137:* 采集数据源的选项

数据类型	采集选项
STIX	• 从 TAXII 服务器采集 STIX 源： 请参阅 获取要用作源的 TAXII 源，第 2419 页 • 从 URL 下载 STIX 数据： 请参阅 从 URL 获取源，第 2420 页 • 上传 STIX 文件： 请参阅 上传本地文件以用作源，第 2421 页

数据类型	采集选项
平面文件	• 从 URL 下载数据： 请参阅 从 URL 获取源， 第 2420 页 • 上传平面文件： 请参阅上传本地文件以用作源， 第 2421 页

获取要用作源的 TAXII 源

如果在 TID 配置或操作期间遇到问题，请参阅 对威胁智能导向器进行故障排除， 第 2451 页

过程

步骤 1 请确保源满足以下部分中的要求 源要求， 第 2415 页

步骤 2 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 3 请点击 **添加**（+）。

步骤 4 选择 TAXII 作为源的**传递**方法。

步骤 5 输入信息。

- 如果主机服务器需要加密连接，请按照为 威胁智能导向器 源配置 TLS/SSL 设置， 第 2423 页中所述配置 **SSL 设置**。
- 不能更改 TAXII 源的**操作**选择。

  块不是 TAXII 源的**操作**选项，因为 STIX 数据可能包含复杂的指标，这是系统所无法阻止的。设备（元素）根据单个可观察对象存储和采取操作，无法根据多个可观察对象采取操作。

  但注入后，可以阻止从源获取的各个可观察对象和简单的指标。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作， 第 2447 页。
- 加载源列表可能需要一些时间。
- **更新间隔**指定 威胁智能导向器 从TAXII 检索更新的频率。

  更新频率应设置为对于数据源的更新频率有意义的值。例如，如果源每天更新 3 次，则将更新间隔设置为 1440/3 或 480 分钟，以定期捕获最新数据。
- 指定的 **TTL** 天数过后，威胁智能导向器 将删除：
  - 不包括在后续源更新中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

  注释
  如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（ ）。

启用此选项后，系统将自动发布初始源数据和任何后续更改。

有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。

步骤 7 点击**保存**。

下一步做什么

- TAXII 源可能包含大量数据，全部注入这些数据可能需要花费系统一些时间。要查看注入状态，请刷新“源”页面。
- 如果您看到此源的错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器，第 2416 页。

从 URL 获取源

如果希望 威胁智能导向器 从主机获取文件，请配置 URL 源。

如果在 TID 配置或操作期间遇到问题，请参阅 对威胁智能导向器进行故障排除，第 2451 页

过程

步骤 1 请确保源满足以下部分中的要求 源要求，第 2415 页

步骤 2 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 3 请点击 **添加**（ ）。

步骤 4 选择 `URL` 作为源的**传递**方法。

步骤 5 完成表格。

- 如果要采集平面文件，请选择描述源中所包含数据的**类型 (Type)**。
- 如果主机服务器需要加密连接，请按照为 威胁智能导向器 源配置 TLS/SSL 设置，第 2423 页中所述配置 **SSL 设置**。
- 对于名称：要基于威胁智能导向器简化分类和事故处理指标简化事故的排序和处理，请在所有源中使用一致的命名方案。例如， <source>-<type> 。

  包括源名称可简化返回到源，以获取进一步的信息或反馈。

  请确保按照一致的方式输入名称。例如，对于具有 IPv4 地址的源，您可能始终使用 IPV4（而不是 IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4 或 IP-V4 等。）
- 如果要采集 STIX 文件，`Block` 不是**操作**选项，因为 STIX 数据可能包含系统无法阻止的复杂指标。设备（元素）根据单个可观察对象存储和采取操作，无法根据多个可观察对象采取操作。

但注入后，可以阻止从源获取的各个可观察对象和简单的指标。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。

- 更新频率应设置为对于数据源的更新频率有意义的值。例如，如果源每天更新 3 次，则将更新间隔设置为 1440/3 或 480 分钟，以定期捕获最新数据。
- 为 **TTL** 间隔指定的天数过后，威胁智能导向器 将删除：
  - 不包括在后续源更新中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

注释
如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（）。

启用此选项后，系统将自动发布初始源数据和任何后续更改。

有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。

步骤 7 点击**保存**。

下一步做什么

- 要查看注入状态，请刷新“源”页面。如果您看到错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器，第 2416 页。

上传本地文件以用作源

使用此程序一次性手动上传本地文件。

注入 STIX 文件时，威胁智能导向器将从 STIX 文件的内容创建一个简单或复杂的指示器。

注入平面文件时，威胁智能导向器将为平面文件中的每个可观察对象值创建一个简单指示器。

如果在 威胁智能导向器 配置或操作期间遇到问题，请参阅对威胁智能导向器进行故障排除，第 2451 页

过程

步骤 1 请确保您的文件满足以下部分中的要求 源要求，第 2415 页

步骤 2 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 3 请点击 **添加**（）。

步骤 4 选择上传作为源的**交付**方法。

步骤 5 完成表格。

- 如果要上传平面文件，请选择描述源中所包含数据的 **内容** 类型。
- 对于名称：要基于威胁智能导向器简化分类和事故处理指标简化事故的排序和处理，请在所有源中使用一致的命名方案。例如， <source>-<type> 。

  包括源名称可简化返回到源，以获取进一步的信息或反馈。

  请确保按照一致的方式输入名称。例如，对于具有 IPv4 地址的源，您可能始终使用 IPV4（而不是 IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4 或 IP-V4 等。）
- 如果您上传的是 STIX 文件，阻止不是一个**操作**选项，因为 STIX 数据可能包含比较复杂的指示器。设备（元素）基于单个可观察对象存储并执行操作；无法基于多个可观察对象执行操作。

  但是，您可以在指示器或可观察对象级别阻止简单指示器。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作 ， 第 2447 页。
- 为 **TTL** 间隔指定的天数过后，威胁智能导向器 将会删除：
  - 不包括在后续源上传中的所有源指示器。
  - 保留下来的指标未引用的所有可观察对象。

  注释
  如果源在为 TTL 指定的天数内没有更新，且源校验和保持不变，则下载将被视为没有更新的源。要让可观察对象接收新的 TTL 值，源必须包含一些更新。

步骤 6 如果要立即开始发布到元素，请确认已启用 **发布 滑块**（ ） 。

如果没有在注入时发布源，则以后无法再发布所有源指示器；只能单独发布每个可观察对象。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ， 第 2449 页。

步骤 7 点击**保存**。

下一步做什么

- 要查看注入状态，请刷新“源”页面。如果您看到错误，请将鼠标悬停在状态上获取详细信息。
- 如果您执行的是初始 威胁智能导向器 配置，请返回到如何设置威胁智能导向器 ， 第 2416 页。

处理重复指示器

如果单个指示器包括在多个源中：

每个指示器实例都会生成一个事故，因此遇到一次特定威胁可能会生成多个事故。

为避免未来出现重复事故，请暂停发布除一个重复指示器之外的所有指示器。请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ， 第 2449 页。

为 威胁智能导向器 源配置 TLS/SSL 设置

如果主机服务器需要加密连接，则配置 **SSL 设置**。

开始之前

- 开始配置 TAXII 或 URL 源，如获取要用作源的 TAXII 源，第 2419 页或从 URL 获取源，第 2420 页中所述。

过程

步骤 1 在 **编辑源** 对话框中，展开 **SSL 设置** 部分。

步骤 2 如果您的服务器证书是自签名证书：

a) 启用**自签名证书**。

b) 选择 **SSL 主机名验证**方法。

- 严格 - 威胁智能导向器 要求源 **URL** 与服务器证书中提供的主机名相匹配。

  如果主机名包含通配符，则 TID 不能匹配多个子域。

- 浏览器兼容 - 威胁智能导向器 要求源 **URL** 与服务器证书中提供的主机名相匹配。

  如果主机名包含通配符，则 TID 匹配所有子域。

- 允许所有 - 威胁智能导向器 不要求源 **URL** 与服务器证书中提供的主机名相匹配。

例如，如果 `subdomain1.subdomain2.cisco.com` 是您的源 **URL** 并且 `*.cisco.com` 是服务器证书中提供的主机名：

- 严格主机名验证失败。
- 浏览器兼容主机名验证成功。
- 允许所有主机名验证完全忽略主机名值。

c) 对于**服务器证书**：

- 如果您有权访问 PEM 编码的自签名服务器证书，请在文本编辑器中打开该证书，并复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。在字段中输入此整个字符串。
- 如果您无权访问自签名服务器证书，请将该字段保留为空。保存源后，威胁智能导向器 将从服务器检索证书。

步骤 3 如果您的服务器需要用户证书：

a) 输入**用户证书**。

在文本编辑器中打开 PEM 编码的证书，复制整个文本块，包括 `BEGIN CERTIFICATE` 和 `END CERTIFICATE` 行。在字段中输入此整个字符串。

b) 输入**用户私有密钥**：

在文本编辑器中打开私有密钥文件并复制整个文本块，包括`BEGIN RSA PRIVATE KEY`和`END RSA PRIVATE KEY`行。在字段中输入此整个字符串。

下一步做什么

- 记下证书的到期日期。您可能希望设置日历提醒，在当前证书到期后输入新的服务器证书。
- 继续配置源：
  - 获取要用作源的 TAXII 源， 第 2419 页
  - 从 URL 获取源， 第 2420 页

具有 威胁智能导向器 访问权限的用户角色

可以使用 防火墙管理中心用户帐户访问 威胁智能导向器 菜单和页面：

- 具有**管理员**或**威胁情报导向器用户**用户角色的帐户。
- 具有包含**情报**权限的自定义用户角色的帐户。

此外，还可使用具有**管理员**、**访问管理员**或**网络管理员**用户角色的 防火墙管理中心用户帐户可在访问控制策略中启用或禁用 威胁智能导向器。

有关用户账户的详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的 防火墙管理中心 的用户一章。

关于备份和恢复 威胁智能导向器 数据

您可以使用 防火墙管理中心备份和恢复 威胁智能导向器 所需的所有数据：元素数据、安全智能事件、连接事件、威胁智能导向器 配置和 威胁智能导向器 数据。有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的备份/恢复章节。

注释 如果使用高可用性配置在主用 防火墙管理中心上托管 威胁智能导向器，则系统不会将 威胁智能导向器配置与 威胁智能导向器数据同步到备用 防火墙管理中心。我们建议对主用 防火墙管理中心上的 威胁智能导向器数据定期执行备份，以便您可以在故障转移后恢复数据。

在尝试恢复主用 防火墙管理中心上的 威胁智能导向器 数据之前，请暂停主用对等设备上的同步。关于更多信息，请参阅在 *Cisco Secure Firewall Management Center* 管理指南中的 暂停已配对 *Firepower* 管理中心之间的通信 。

表 *138:* 威胁智能导向器相关的备份和恢复文件内容

威胁智能导向器相关的文件内容	备份选择	恢复选择
元素数据	备份配置	恢复配置数据
Secure Firewall Management Center事件数据	备份事件	恢复事件数据
威胁智能导向器配置和威胁智能导向器数据	备份威胁智能导向器	恢复威胁情报导向器数据

分析 威胁智能导向器 事件和观察数据

要分析 威胁智能导向器 元素生成的事件和观察数据，请使用“事件表和事件详细信息”页。

观察和事故生成

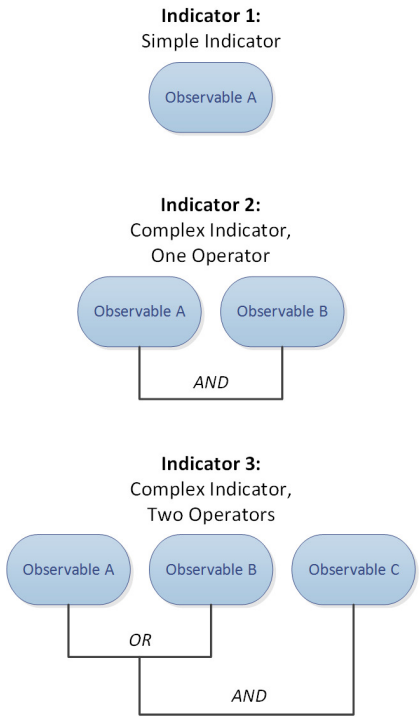
威胁智能导向器在流量中发现指示器的第一个可观察对象时生成事故。简单指示器在单个观察之后完全实现。复杂指示器直到一个或多个其他观察履行了其模式才会部分实现。在单个事务期间，不必满足复杂指示器的需要；随着时间推移，每个可观察对象均可通过不同事务单独完成。



注释 威胁智能导向器 在评估指示器模式时将忽略不支持的、无效的和已列入不阻止列表的可观察对象。

事故完全实现之后，后续观察将会触发新事故。

图 *452:* 示例：指示器模式



如果 威胁智能导向器从上面的示例中获取了可观察对象，并且可观察对象井然有序，则事故生成将按如下所示继续：

1. 当系统在流量中识别到可观察对象 A 时，威胁智能导向器：
   - 为指示器 1 生成完全实现的事故。
   - 为指示器 2 和指示器 3 生成部分实现的事故。
2. 当系统在流量中识别到可观察对象 B 时，威胁智能导向器：
   - 将事故更新为对指示器 2 完全实现，因为该模式已履行。
   - 将事件更新为对指示器 3 部分实现。
3. 当系统在流量中识别到可观察对象 C 时，威胁智能导向器：
   - 将事故更新为对指示器 3 完全实现，因为该模式已履行。
4. 当系统在流量中再次识别到可观察对象 A 时，威胁智能导向器：
   - 为指示器 1 生成完全实现的事故。
   - 为指示器 2 和指示器 3 生成部分实现的新事故。

如果特定指示器存在于多个源中，则您可能会看到重复事故。有关详细信息，请参阅对威胁智能导向器进行故障排除，第 2451 页。

请注意，只会通过实际流量生成事故。如果对于URL B存在一个可观察对象，并且某个用户访问显示指向 URL B 的链接的 URL A，则除非该用户点击 URL B 链接，否则不会发生事故。

查看和管理事故

“事故”页面显示最多 110 万个最新 威胁智能导向器 事故的摘要信息；请参阅事故摘要信息，第 2428 页。

开始之前

- 配置功能，如如何设置威胁智能导向器，第 2416 页中所述。
- 了解观察和事件生成，如观察和事故生成，第 2425 页中所述。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **事件**。

步骤 2 查看您的事故：

- 点击 **过滤器**（）以添加一个或多个过滤器。默认过滤器是6个小时。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 2444 页。
- 要查看上次由 威胁智能导向器 更新事故的日期和时间，请将光标悬停在**最后更新时间**列中的值上。
- 要查看与事件关联的指示器的详细信息，请点击**指示器名称**列中的文本；请参阅查看和管理指示器，第 2440 页。

步骤 3 请通过点击**事故 ID (Incident ID)** 列中的值来查看其他详细信息。

有关您查看的详细信息的说明，请参阅事件详细信息，第 2428 页。

- 要查看指示器详细信息，请点击窗口下半部分中**指示器 (Indicator)** 标题下的指示器值（例如，IP 地址或 SHA-256 值）。
- 要查看观察结果详细信息，请点击紧邻**观察结果 (Observations)** 标题下的观察结果左侧的箭头。
- 要在“安全智能事件”(Security Intelligence Events) 页面上查看此事故，请点击观察结果详细信息部分中的**事件 (Events)** 链接。

步骤 4 （可选）请在事故详细信息页面上输入描述性信息：

提示：要最大化一致性和下面的选项的作用，请提前规划和记录您的命名约定、类别选择和置信度级别条件。

- 在以下字段中输入您喜欢的任意值：**名称 (Name)**、**说明 (Description)** 和**类别 (Category)**。
- 点击**置信度 (Confidence)** 的评价级别。

- 请通过从**状态 (Status)** 字段中的下拉列表中选择一个值，指示调查事故的状态。

事故摘要信息

“事故”页显示所有 威胁智能导向器事故的摘要信息。

表 *139:* 事故摘要信息

字段	说明
上次更新日期	自系统或用户上次更新事故以来的天数。要查看更新的日期和时间，请将光标悬停在该列中的相应值上。
事故 ID	事故的唯一标识符。此 ID 具有以下格式： `<type>-<date>-<number>` • `<type>` - 事故中涉及的指示器或可观察对象的类型。对于简单指示器，此值指示可观察对象类型：`IP`（IPv4 或 IPv6）、`URL` (URL)、`DOM`（域）或 `SHA` (SHA-256)。对于复杂指示器，此值为 `COM`。 • `<date>` - 创建事故的日期 (*yyyymmdd*)。 • `<number>` - 每日事故编号，即指定事故在每日事故序列中的发生位置的编号。</number> 请注意，此序列从 0 开始。例如，`DOM-20170828-10` 是当天创建的第 11 个事故。 在标识符旁边，系统会显示一个图标来指示事故是**部分实现**还是**完全实现**。有关详细信息，请参阅观察和事故生成，第 2425 页。
指示器名称	事故中涉及的指示器的名称。要查看有关指示器的其他信息，请点击此列中的值；请参阅查看和管理指示器，第 2440 页。
类型	事故中涉及的指示器的类型。 • 包含一个可观察对象的指示器显示数据类型（`URL`、`SHA-256` 等） • 包含两个或多个可观察对象的指示器显示为 `Complex` 。
采取的操作	系统就该事故所执行的操作。有关详细信息，请参阅事件详细信息，第 2428 页。
状态	您对事故的调查状态。有关详细信息，请参阅事件详细信息，第 2428 页。
删除（）	点击此图标将永久删除该事故。

事件详细信息

“事件详细信息”窗口显示了有关单个 威胁智能导向器 事件的相关消息。此窗口分为两个部分：

- 事故详细信息：基本信息，第 2429 页

• 事故详细信息：指示器和观察结果 ，第 2430 页

事故详细信息：基本信息

“事故详细信息”窗口的上半部分提供下述信息。

表 *140:* 基本事故信息字段

字段	说明
部分实现的 *IncidentID* 或完全实现的 *IncidentID*	一个图标，用于指示事故状态（已部分实现或已完全实现），以及事故的唯一标识符。 **注释** 在确定事故状态时，威胁智能导向器 会忽略不支持和无效的可观察对象以及不阻止列表中的可观察对象。
已打开	上次更新事故的日期和时间。
名称	您手动输入的自定义、可选事故名称。 提示：如果“说明”(Description) 字段（位于窗口底部）中有来自源的信息，则使用该字段中的信息来命名该事故。
说明	您手动输入的自定义、可选事故说明。 提示：如果“说明”(Description) 字段（位于窗口底部）中有来自源的信息，则使用该字段中的信息来说明该事故。
观察结果	事故中观察结果的数量。
置信度	您可以手动选择的可选评级，用于指示事故的相对重要性。
采取的操作	系统采取的操作：已监控、已阻止或已部分阻止。 已部分阻止表示事故同时包含已监控和已阻止观察结果。 **注释** **采取的操作**表示系统采取的操作，并不一定是在 威胁智能导向器 中选择的操作。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级 ，第 2433 页。
类别	您手动添加到事故中的自定义可选标记或关键字。
状态	表示事故分析当前所处阶段的值。在首次更改**状态**之前，所有事故的状态值都将为新。 此字段为选填字段。根据贵组织的需求，可以考虑使用如下所示的状态值： • 新 - 事故需要调查，但尚未开始调查。 • 打开 - 目标正对事故进行调查。 • 已关闭 - 已对事故进行了调查，并已采取操作。 • 已拒绝 - 已对事故进行了调查，并已确定没有采取任何操作。

字段	说明
删除（）	点击此图标将永久删除此事故。

事故详细信息：指示器和观察结果

“事故详细信息”窗口的下半部分提供指示器和观察结果信息的深入视图。此信息以**指示器**字段、指示器模式和**观察结果**字段的形式组织。

指示器部分

当第一次查看指示器详细信息时，该部分仅显示指示器名称。

点击指示器名称可在“指示器”页上查看指示器。

点击指示器名称旁边的向下箭头可查看更多指示器详细信息，无需离开事故。详细信息字段包括：

表 *141:* 指示器字段

字段	说明
说明	源提供的指示器说明。
来源	包含指示器的源。点击此链接可访问完整的源详细信息。
过期	根据源的 **TTL** 值，事故将过期的日期和时间。
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作 ，第 2447 页。
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据 ，第 2449 页。
下载 **STIX**	如果源类型为 `STIX`，请点击此按钮以下载 STIX 文件。

指示器模式

指示器模式是包含指示器的可观察对象和运算符的图形表示。运算符与指示器内的可观察对象链接。AND 关系通过 **AND** 运算符指示。OR 关系通过 **OR** 运算符或由多个可观察对象的紧密分组指示。

如果模式中的某个可观察对象已显示，则该可观察对象框为白色。如果某个可观察对象尚未显示，则该可观察对象框为灰色。

在指示器模式中：

- 点击**添加到不阻止列表 (Add to Do-Not-Block List)** 按钮 ，将可观察对象添加到不阻止列表。此图标在白色和灰色可观察对象框中均会显示。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表 ，第 2450 页。
- 如果将光标悬停在白色可观察对象框上，则系统将在**观察结果**部分中突出显示相关的观察结果。

- 如果点击白色可观察对象框，则系统将在**观察结果**部分中突出显示相关的观察结果，将该观察结果滚动到视图中（如果存在多个观察结果），然后扩展该观察结果的详细显示。
- 如果将光标悬停在指示器模式中的灰色可观察对象框上方或点击它，则**观察结果**部分中没有任何更改。因为可观测对象未显示，因此没有可显示的观察结果详细信息。

观察结果部分

默认情况下，**观察结果**部分显示摘要信息，其中包括：

- 触发观察结果的可观察对象的类型（例如 `Domain`）
- 包含可观察对象的数据
- 观察结果是第一个观察结果还是随后的观察结果，例如 `1st` 或 `3rd`）

注释 如果单个可观察对象已显示三次或多次，则威胁智能导向器显示第一个和最后一个观察结果详细信息。有关中间观察结果的详细信息不可用。

- 观察结果的日期和时间
- 为可观测对象配置的操作

如果将光标悬停在**观察结果**部分中的某个观察结果上，系统将在指示器模式中突出显示相关的可观察对象。

如果点击**观察结果**部分中的某个观察结果，系统将在指示器模式中突出显示相关的可观察对象，并将第一个相关的可观察对象滚动到视图中（如果存在多个可观察对象）。点击某个观察结果还会在**观察结果**部分中展开观察结果的详细信息。

观察结果详细信息包括以下字段：

表 *142:* 观察结果详细信息字段

字段	说明
源代码	触发观察结果的流量的源 IP 地址和端口。
目的	触发观察结果的流量的目标 IP 地址和端口。
其他信息	与触发观察结果的流量相关的 DNS 和身份验证信息。
活动	如果观察结果生成连接、安全智能、文件或恶意软件事件，将显示此可点击的链接。点击该链接可查看 Secure Firewall Management Center事件表中的事件；请参阅*Cisco Secure Firewall Management Center* 管理指南。

查看 威胁智能导向器 观察的事件

有关 威胁智能导向器 观察结果生成的 Secure Firewall Management Center事件的更多信息，请参阅 Secure Firewall Management Center事件中的 威胁智能导向器 观察对象 ， 第 2432 页。

为 威胁智能导向器 相关事件记录的系统操作可能会有所不同，具体取决于 威胁智能导向器 与其他 Secure Firewall Management Center 功能的交互。有关操作优先排序的详细信息，请参阅 威胁智能导向器-防火墙管理中心 操作优先级 ， 第 2433 页。

开始之前

- 配置功能，如如何设置威胁智能导向器 ， 第 2416 页中所述。
- 如配置策略以支持威胁智能导向器 ， 第 2417 页中所述，确认在访问控制策略中启用了 威胁智能导向器 所需的事件日志记录。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **事件**。

步骤 2 点击事故的**事故 ID** 值。

步骤 3 点击**指示器**部分中的观察结果以显示观察结果框。

步骤 4 通过点击该框左上角的箭头展开观察结果框。

步骤 5 点击观察结果信息中的**事件**链接。有关安全智能显示的详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南中的连接和安全智能事件一章。

Secure Firewall Management Center事件中的 威胁智能导向器 观察对象

如果完全配置了访问控制策略，威胁智能导向器 观察对象将生成以下 Secure Firewall Management Center事件：

表 *143:* 观察对象生成的 *Secure Firewall Management Center*事件

观察对象内容	连接事件表	安全智能事件表	文件事件表	恶意软件事件表
SHA-256	支持	否	支持	是，如果处置是恶意软件或自定义检测。
域名、URL 或 IPv4/IPv6	是 威胁智能导向器相关的连接事件由与 威胁智能导向器相关的**安全智能类别**值标识。	是 威胁智能导向器相关的安全智能事件由与 威胁智能导向器相关的**安全智能类别**值标识。	否	否

影响所执行操作的因素

系统在检测到匹配威胁智能导向器可观察对象的流量后，何时采取操作以及采取何种操作由许多因素决定。

- 在威胁智能导向器采取操作前，安全智能之类的功能会采取操作。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 2433 页。
- 通常情况下，为可观察对象配置的操作（可能与为其父指示器或源配置的操作不同）是将要采取的操作。
- 由于 STIX 源可能包含复杂指示器，所以源的“操作”设置只能设为“监控”。不过，STIX 源中包含的各个简单指示器或可观察对象可以设置为“阻止”。
- 指示器和可观察对象的“操作”设置可以继承，也可以单独进行配置以覆盖继承设置。请参阅威胁智能导向器 配置中的继承，第 2445 页 和 在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。
- 本来可以采取行动的流量可能在“不阻止”(Do Not Block) 列表中。有关详细信息，请参阅将威胁智能导向器 可观察对象添加到不阻止列表，第 2450 页。
- 为部分和完全实现的事件执行配置的操作。
- 可部分阻止基于复杂指示器的事件。如果指示器包括受监控和已阻止的观察结果，可能会出现这种情况。
- 暂停发布会影响系统采取的操作。请参阅关于暂停发布，第 2447 页 和 在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。
- 暂停 威胁智能导向器功能将阻止所有操作。恢复功能后，可采取操作的数据可能与之前不同。有关详细信息，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 2448 页。

威胁智能导向器-防火墙管理中心 操作优先级

如果 威胁智能导向器可观察对象操作与防火墙管理中心策略操作冲突，系统将优先执行以下操作：

- 安全智能不阻止
- TID 阻止
- 安全智能阻止
- TID 监控器
- 安全智能监控器

具体包括：

表 *144:* 威胁智能导向器 *URL* 可观察对象操作与安全智能操作

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
阻止	监控器	已阻止	阻止	由系统分析确定；请参阅 安全智能类别，第 1736 页	URL 阻止 (URL Block)
	阻止	已阻止	阻止	TID URL 阻止	URL 阻止 (URL Block)
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID URL 监控器	URL 监控
	阻止	已阻止	阻止	TID URL 阻止	URL 阻止 (URL Block)

表 *145:* 威胁智能导向器 *IPv4/IPv6* 可观察对象操作与安全智能操作

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
阻止	监控器	无 TID 事件	阻止	由系统分析确定；请参阅 安全智能类别，第 1736 页	IP 阻止
	阻止	已阻止	阻止	TID IPv4 阻止 TID IPv6 阻止	IP 阻止

设置：安全智能操作	设置：威胁智能导向器可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID IPv4 监控 TID IPv6 监控	IP 监控
	阻止	已阻止	阻止	TID IPv4 阻止 TID IPv6 阻止	IP 阻止

表 *146:* 威胁智能导向器域名可观察对象操作与 *DNS* 策略操作

设置：DNS 策略操作	设置：威胁智能导向器域名可观察对象操作	威胁智能导向器事故字段：已执行的操作	安全智能事件字段：		
			操作	安全智能类别	原因
不阻止	监控或阻止	无 TID 事件	安全智能事件		
丢弃、无法找到域 Sinkhole - 日志 Sinkhole - 阻止和记录	监控器	已阻止	阻止	由系统分析确定；请参阅 安全智能类别，第 1736 页	DNS 阻止
	阻止	已阻止	阻止	TID 域名阻止	DNS 阻止
监控器	监控器	受监控	由在安全智能和 TID 之后处理的访问控制规则确定。	TID 域名监控器	DNS 监控
	阻止	已阻止	阻止	TID 域名阻止	DNS 阻止

表 *147: TID SHA-256* 可观察对象操作与恶意软件云查找文件策略

文件处置	威胁智能导向器 SHA-256 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
清洁	监控或阻止	受监控	恶意软件云查找	不可用
恶意软件	监控或阻止	受监控	恶意软件云查找	不可用

文件处置	威胁智能导向器 **SHA-256** 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
Custom	监控或阻止	受监控	• 恶意软件云查找，如果 SHA-256 不在自定义检测列表中。 • 自定义检测，如果 SHA-256 在自定义检测列表中。	• 恶意软件云查找，如果 SHA-256 不在自定义检测列表中。 • 自定义检测，如果 SHA-256 在自定义检测列表中。
未知	监控或阻止	受监控	恶意软件云查找	不可用

注释 先执行 威胁智能导向器 匹配，再由系统发送文件进行动态分析。

表 ***148: TID SHA-256*** 可观察对象操作与阻止恶意软件文件策略

文件处置	威胁智能导向器 **SHA-256** 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
安全或未知	监控器	受监控	恶意软件云查找	不可用
	阻止	已阻止	• TID 阻止，如果 SHA-256 不在自定义检测列表中。 修改后的文件处置为自定义。 • 自定义检测阻止，如果 SHA-256 在自定义检测列表中。	TID 阻止 修改后的文件处置为自定义。

文件处置	威胁智能导向器 **SHA-256** 可观察对象操作	在 威胁智能导向器 事故中执行的操作	文件事件中的操作	恶意软件事件中的操作
恶意软件或自定义	监控器	已阻止	阻止恶意软件	阻止恶意软件
	阻止	已阻止	• TID 阻止，如果 SHA-256 不在自定义检测列表中。 修改后的文件处置为自定义。 • 自定义检测阻止，如果 SHA-256 在自定义检测列表中。	TID 阻止 修改后的文件处置为自定义。

查看和更改威胁智能导向器 配置

可以使用以下信息以查看并根据需要微调您的配置。

查看元素（托管设备）的 威胁智能导向器 状态

作为托管设备注册到 防火墙管理中心的所有设备都会在“元素”页面上自动显示。所有正确配置的元素（如配置策略以支持威胁智能导向器，第 2417 页中的规定）都将收到所有当前已发布的可观察对象，包括在添加元素之前的注入的可观察对象。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁情报导向器** > **元素**。

步骤 2 要查看元素是否已连接并已启用 威胁智能导向器，请将鼠标悬停在元素名称旁边的图标上。

注释
部署后，此页面上的信息最多可能需要 5 分钟才能更新，包括应用的访问控制策略以及是否启用 TID。

查看和管理源

"源”页面显示有关所有已配置源的摘要信息；请参阅源摘要信息，第 2438 页。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 2 查看您的源：

- 要过滤页面上显示的源，请点击 **过滤器**（）。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 2444 页。
- 要查看详细的注入状态，请将光标悬停在**状态**列中的文本上。有关详细信息，请参阅源状态详细信息，第 2439 页。

步骤 3 管理您的源：

- 要编辑**操作**设置，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第2447页。如果某个操作是固定的，则它是该源**类型**唯一支持的操作。
- 要编辑**发布 (Publish)** 设置，请点击 **滑块**（）。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。
- 要暂停或继续 威胁智能导向器 更新源代码，请点击**暂停更新**或**继续更新**。如果暂停更新，则更新将暂停，但现有指示器和可观察对象仍保留在 TID 中。
- 要删除源，请点击 **删除**（）。如果源仍在处理，”删除“(Delete) 将灰显。删除一个源将删除与该源关联的所有指示器。关联的可观察对象也可能被删除；如果它们与系统中剩余的指示器关联，这些可观察对象将会保留。

源摘要信息

“源”页面显示所有已配置源的摘要信息。下表提供了对摘要显示中的字段的简要说明。有关这些字段的详细信息，请参阅源的相关配置主题中的说明：请参阅采集数据源的选项，第 2418 页。

表 *149:* 源摘要信息

字段	说明
名称	源名称
类型	源的数据格式（STIX 或 平面文件）。
交付	威胁智能导向器 用于检索源的方法。
操作	系统配置为对匹配此源中所包含数据的流量执行的操作（阻止或监控）。 有关 威胁智能导向器 操作的详细信息，包括可用性、继承和重写继承，请参阅影响所执行操作的因素，第 2433 页。

字段	说明
发布	开或关指定 威胁智能导向器 是否将源中的数据发布到已注册的元素（为支持 威胁智能导向器 而配置的托管设备）。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
上次更新时间	威胁智能导向器 上次更新源的日期和时间。
状态	源的当前状态。 • **新的** - 新建源。 • **已计划** - 已计划初始下载或后续更新，但尚未进行。 • **正在下载** - 威胁智能导向器 正在执行初始下载或更新刷新。 • **正在分析** 或 **正在处理**-威胁智能导向器 正在获取源代码。 • **已完成**-威胁智能导向器 已完成源代码的获取。 • **已完成，但有错误**-威胁智能导向器 已完成对源的获取，但某些可观察对象不受支持或无效。 • **错误**-威胁智能导向器 遇到问题。如果源是指定了**更新频率**的 TAXII 或 URL 源，并且未暂停更新，则 威胁智能导向器 将在下次计划更新时重试。 请刷新此页面更新状态。
编辑 ()	点击此图标可编辑源的设置。
删除（）	点击此图标将永久删除源。

源状态详细信息

当您将光标悬停在“源摘要”页面中的**状态**值上时，威胁智能导向器 提供下面所述的其他详细信息。

数据	说明
状态消息	简要说明源的当前状态。
上次更新日期	指定 威胁智能导向器 上次更新源的日期和时间。
下一次更新	对于 TAXII 和 URL 源，此值指定威胁智能导向器下次将在何时更新源。

数据	说明
指示灯	指定指示器计数： • **已消耗 (Consumed)** - 在最新的源更新过程中处理的指示器 威胁智能导向器 数量。此数字表示更新中包含的所有指示器，无论它们是被获取还是丢弃。 • **已丢弃** - 在最新更新期间，系统未添加到 威胁智能导向器 的格式错误的指示器数量。 **注释** 对于 TAXII 源，威胁智能导向器 提供单独的**上次更新时间**和**总数**指示器计数，因为 TAXII 更新会增加增量数据，而不是替换现有的数据。对于来自其他源类型的指示器，威胁智能导向器 仅提供**上次更新时间**计数，因为来自这些源的更新将完全替换现有的数据集。 如果所有指示器的可观察对象都**无效**，则 威胁智能导向器 将丢弃该指示器。
可观察对象	指定可观察对象计数： • **已消耗 (Consumed)** - 在最新的源更新过程中处理的可观察对象 威胁智能导向器 数量。此数字表示更新中包含的所有可观察对象，无论它们是被获取还是丢弃。 • **不受支持** - 在最新更新期间，系统未添加到威胁智能导向器 的不受支持的可观察对象数量。 有关受支持的可观察对象类型的详细信息，请参阅源要求，第 2415 页中关于内容类型的信息。 • **无效** - 在最新更新期间，系统未添加到 威胁智能导向器 的无效可观察对象数量。 如果可观察对象未正确构造，则无效。例如，`10.10.10.10.123` 不是有效的 IPv4 地址。 **注释** 对于 TAXII 源，威胁智能导向器 提供单独的**上次更新时间**和**总数**可观察对象计数，因为 TAXII 更新会增加增量数据，而不是替换现有的数据。对于来自其他源类型的可观察性，威胁智能导向器 仅提供**上次更新时间**计数，因为来自这些源的更新将完全替换现有的数据集。

查看和管理指示器

指示器将从获取的源自动生成。有关此页面上的信息的详细信息，请参阅指示器摘要信息，第2441页。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 2 点击**指示器**。

步骤 3 查看您当前的指示器：

- 要过滤页面上显示的指示器，请点击**过滤器**（）。有关详细信息，请参阅过滤表视图中的威胁智能导向器 数据，第 2444 页。
- 要查看有关指示器（包括关联的可观察对象）的其他详细信息，请点击指示器名称。有关详细信息，请参阅指标详细信息，第 2442 页。
- 在**事件 (Incidents)** 列中，点击编号可查看与指示器关联的事故的信息，或将光标悬停在”事故“上以查看事故是完全实现还是部分实现。
- 要确定 威胁智能导向器 是否已完成从源获取指示器，请查看**状态**列。

步骤 4 管理您当前的指示器：

- 要编辑**操作**，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。如果某个操作是固定的，则它是该源**类型**唯一支持的操作。
- 要编辑**发布**设置，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。
- 要将一个指示器的一个或多个可观察对象列入不阻止名单，请点击指示器名称以访问“指示器详细信息”页面。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。

指示器摘要信息

“指示器”页面显示与配置的源关联的所有指示器的摘要信息。

表 *150:* 指示器摘要信息

字段	说明
类型	• 使某一可观察对象列出该可观察对象的数据类型（URL、SHA-256 等）的指示器 • 使两个或多个可观察对象都被列复杂的指示器。 将鼠标指针悬停在类型上，以查看特定的可观察对象。
名称	指示器名称。
来源	包含指示器的源（父源）。
突发事件	有关与指示器关联的任何事故的信息： • 指定事故是 **部分** 或 **完全** 实现的图标 • 与指示器关联的事故的数量

字段	说明
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑威胁智能导向器操作，第 2447 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
上次更新时间	威胁智能导向器上次更新指示器的日期和时间。
状态	指示器的当前状态。 • **待处理**-威胁智能导向器 正在获取指示器的可观察对象。 • **完成**-威胁智能导向器 已成功获取指示器的所有可观察对象。 • **已完成，但有错误**-威胁智能导向器 已完成获取指示器，但某些可观察对象不受支持或无效。

指标详细信息

“指示器详细信息”页面显示事件的指示器和可观察数据。

表 *151:* 指示器详细信息

字段	说明
名称	指示器名称。
说明	源提供的指示器说明。
来源	包含指示器的源。
过期	根据源的 **TTL** 值，指示器将过期的日期和时间。
操作	与指示器关联的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。

字段	说明
发布	指示器的发布设置。有关详细信息，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
指示器模式	构成指示器模式的可观察对象和运算符。运算符与指示器内的可观察对象链接。AND 关系通过 **AND** 运算符指示。OR 关系通过 **OR** 运算符或由多个可观察对象的紧密分组指示。 或者，点击 **添加到不阻止列表** 按钮，将可观察对象添加到不阻止列表。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。

查看和管理可观察对象

“可观察对象”页面显示所有成功注入的可观察对象；请参阅可观察对象摘要信息，第 2444 页。

开始之前

- 按照获取要用作源的 TAXII 源，第 2419 页、从 URL 获取源，第 2420 页或上传本地文件以用作源，第 2421 页中的说明配置一个或多个源。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **源**。

步骤 2 点击**可观察对象**。

步骤 3 查看您当前的可观察对象：

- 要过滤页面上显示的可观看对象，请点击 **过滤器**（）。有关详细信息，请参阅过滤表视图中的 威胁智能导向器 数据，第 2444 页。
- 如果**值**列中的信息被剪切掉，请将鼠标指针悬停在值上。
- 要查看包含可观察对象的指示器，请点击**指示器**列中的数字。“事故”页面将会打开，并采用可观察对象值作为过滤器。有关详细信息，请参阅查看和管理指示器，第 2440 页。

步骤 4 管理您当前的可观察对象：

- 要编辑**操作**，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。
- 要编辑可观察对象的**发布**设置，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。
- 要更改可观察对象的到期日期，请修改父源的**TTL**。有关详细信息，请参阅查看和管理源，第 2437 页。

- 要将可观察对象添加到“不阻止”列表，请点击**添加到不阻止列表**按钮。有关详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。

可观察对象摘要信息

“可观察对象”页面显示所有获取的可观察对象的摘要信息。

表 *152:* 可观察对象摘要信息

字段	说明
类型	可观察对象数据的类型：SHA-256、Domain、URL、IPv4 或 IPv6。
值	包含可观察对象的数据。
指示灯	包含可观察对象的父指示器的数量。
操作	为可观察对象配置的操作。有关详细信息，请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页。 指示器可以从父源继承**操作**设置，而可观察对象可以从父指示器继承**操作**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
发布	可观察对象的发布设置；请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。 指示器可以从父源继承**发布**设置，而可观察对象可以从父指示器继承**发布**设置。有关详细信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
更新时间	威胁智能导向器上次更新可观察对象的日期和时间。
过期	基于父指示器的 **TTL** 自动从威胁智能导向器清除可观察对象的日期。
添加到不阻止列表 (Add to Do-Not-Block List) 按钮	点击此按钮会将可观察对象添加到“不阻止”列表；请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。

过滤表视图中的 威胁智能导向器 数据

过程

步骤 1 选择以下其中一个 威胁智能导向器 表视图：

- **集成** > **+ 显示更多** > **威胁智能导向器** > **事件**

- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**
- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**指示器**
- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**可观察对象**

步骤 2 点击 **过滤器**（） 并选择过滤器属性。

步骤 3 为该过滤器属性选择或输入一个值。

过滤器区分大小写。

步骤 4 （可选）若要按多个属性进行过滤，请点击 **过滤器**（），然后重复执行步骤 2 和步骤 3。

步骤 5 要取消上次应用过滤器后所做的更改，请点击**取消**。

步骤 6 点击**应用**以使用应用的过滤器刷新表。

步骤 7 要单独删除某个过滤器属性，请点击该过滤器属性旁边的 **删除**（），然后点击**应用 (Apply)** 以刷新表。

威胁智能导向器 配置中的继承

当威胁智能导向器摄取源中的智能数据时，将创建指示器和可作为该源子对象的可观察对象。创建后，这些子对象将从父配置继承**操作**和**发布**设置。

指示器从父源继承这些设置。指示器只能有一个父源。

可观察对象从父指示器继承这些设置。可观察对象可以有多个父指示器。

有关详细信息，请参阅：

- 继承多个父级的 TID 设置，第 2445 页
- 关于覆盖继承的 TID 设置，第 2446 页

继承多个父级的 TID 设置

如果某个可观察对象有多个父指示器，则系统会比较从所有父级继承的设置，并将最安全的选项分配给该可观察对象。因此：

- **操作**：`Block` 比 `Monitor` 安全
- **发布**：`On` 比 `Off` 安全

例如，SourceA 可能会贡献 IndicatorA 和相关的 ObservableA：

设置	SourceA	IndicatorA	ObservableA
操作	阻止 (Block)	阻止 (Block)	阻止 (Block)
发布	关闭	关闭	关闭

如果 SourceB 以后贡献 IndicatorB，其还包括 ObservableA，则系统会修改 ObservableA，如下所示：

设置	SourceB	IndicatorB	ObservableA
操作	监控器	监控器	`Block`（从 IndicatorA 继承）
发布	打开	打开	`On`（从 IndicatorB 继承）

在此示例中，ObservableA 有两个父级：一个父级用于其**操作**设置，另一个父级用于其**发布**设置。如果手动编辑可观察对象的设置，然后恢复设置，则系统会将**操作**设置设为 IndicatorA 值，并将**发布**设置设为 IndicatorB 值。

关于覆盖继承的 TID 设置

要覆盖继承的设置，请在子级更改此设置；请参阅在源、指示器或可观察对象级别编辑 威胁智能导向器操作，第 2447 页和在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。覆盖继承的设置后，尽管父对象发生了更改，但子对象仍保留该设置。

例如，您可以先设置以下初始设置，而不设置任何覆盖：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	关闭	关闭	关闭

如果覆盖 IndicatorA 的设置，则设置如下：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	打开	打开	打开

在这种情况下，对 SourceA 的**发布**设置所做的任何更改都不再自动层叠到 IndicatorA。但是，从 IndicatorA 到 ObservableA1 和 ObservableA2 的继承仍在继续，因为可观察对象设置当前未设置为覆盖值。

如果以后覆盖 ObservableA1 的设置：

设置	SourceA	IndicatorA	ObservableA1	ObservableA2
发布	关闭	打开	关闭	打开

对 IndicatorA 的**发布**设置所做的任何更改都不再自动层叠到 ObservableA1。但是，这些更改将继续层叠到 ObservableA2，因为它未设置为覆盖值。

在可观察对象级别，您可以从覆盖设置恢复为继承的设置，系统会将层叠设置更改从父指示器自动恢复到该可观察对象。

在源、指示器或可观察对象级别编辑 威胁智能导向器操作

注意：

- 编辑父项的操作会为所有子项设置该操作。如果在源级别编辑该操作，则会为其所有指示器设置该操作。如果在指示器级别编辑该操作，则会为其所有可观察对象设置该操作。
- 编辑子项的操作会中断继承。如果在指示器级别编辑该操作，随后又在源级别编辑该操作，则在编辑单个指示器的操作之前，系统会保留该指示器的操作。如果在可观察对象级别编辑该操作，随后又在指示器级别编辑该，则在编辑单个可观察对象的操作之前，系统会保留该可观察对象的操作。在可观察对象级别，您可以自动恢复到父指示器的操作。有关继承的更多信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。

您可能还想要查看其他影响所执行操作的因素，第 2433 页。

过程

步骤 1 选择如下选项之一：

- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**

  注释
  威胁智能导向器不支持在源级别阻止 TAXII 源。如果 TAXII 源包含一个简单指示器，则可以在指示器或可观察对象级别进行阻止。

- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**指示器**

  注释
  威胁智能导向器不支持阻止复杂的指示器，而是在复杂指示器中阻止单个可观察对象。

- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**可观察对象**

步骤 2 使用 **操作 (Action)** 下拉列表选择 **监控**（）或 **阻止图标**（）。

步骤 3 （仅可观察对象）如果要从父指示器继续继承操作设置，请点击可观察对象的**操作 (Action)** 设置旁边的 **恢复 (Revert)**。

关于暂停发布

- 如果在功能级别暂停发布，系统将清除存储在您的元素上的所有 威胁智能导向器可观察对象。这意味着 威胁智能导向器 无法检测、监控或阻止威胁。您的系统上的其他安全功能不受影响。
- 如果在源、指示器或可观察对象级别暂停发布，系统将从您的元素中删除暂停的 威胁智能导向器 可观察对象，以防它们匹配流量。

- 对父级暂停发布会暂停所有子项。如果在源级别暂停发布，则会为其所有指示器暂停发布。如果在指示器级别暂停发布，则会为其所有可观察对象暂停发布。
- 为子项暂停发布会中断继承。如果在指示器级别暂停发布，随后在源级别发布，则该指示器的发布将保持暂停状态，直到更改指示器的单个设置。如果在可观察对象级别暂停发布，随后在指示器级别发布，则该可观察对象的发布将保持暂停状态，直到更改可观察对象的单个设置。在可观察对象级别，您可以自动恢复到父指示器的发布状态。有关继承的更多信息，请参阅威胁智能导向器 配置中的继承，第 2445 页。
- 对于上传源的发布只能在指示器级别暂停。
- 有关暂停发布可观察对象与将可观察对象添加到“不阻止”列表的比较，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。
- 如果已对个别可观察对象或指示器指定发布/暂停设置，则即便更新包含相同的可观察对象或指示器，源更新也不会更改。
- 在对象管理页面上可以禁用“发布”。请参阅修改可观察对象的发布频率，第 2449 页。
- “源”页上用于暂停更新的选项与向元素发布数据无关；它适用于更新来自源的 防火墙管理中心上的源信息。

暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据



注意 此设置将暂停向所有元素发布内容，清除元素中存储的所有 威胁智能导向器 可观察对象，并停止使用 威胁智能导向器 功能检查流量。

要在更精细的级别禁用可观察对象，请参阅在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据，第 2449 页。

管理中心上的数据（现有事件和配置的源、指示器和可观察对象，以及来源采集）不受此设置影响。

过程

步骤 1 选择**集成** > **+ 显示更多** > **威胁智能导向器** > **设置**。

步骤 2 点击**暂停**。

下一步做什么

当您准备好恢复同步元素上的 威胁智能导向器 数据并生成观察结果时，请在此页面手动**恢复**发布。管理中心上的现有可观察对象将同时发布到所有元素。

在源、指示器或可观察对象级别暂停或发布 威胁智能导向器 数据

如果在源级别启用发布，系统将自动发布初始源数据和任何后续更改，包括：

- 定期源刷新引起的更改
- 由系统操作引起的更改（例如，**TTL** 到期）
- 任何用户启动的更改（例如，指示器或可观察对象的**操作**设置的更改）

注释 要同时从设备（元素）中清除所有 威胁智能导向器 可观察对象，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 2448 页。

开始之前

在暂停发布之前，请了解关于暂停发布，第 2447 页中所述的后果。

过程

步骤 1 选择如下选项之一：

- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**
- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**指示器**
- **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**可观察对象**

步骤 2 找到 **发布 滑块**（ ） 并使用它切换发布到元素。

步骤 3 （仅可观察对象）如果要从父指示器继续继承发布设置，请点击可观察对象的**发布 (Publish)** 设置旁边的**恢复 (Revert)**。

下一步做什么

- 至少等待 10 分钟，以便元素接收更改。涉及大源的更改将需要更长时间。
- （可选）在可观察对象级别更改 TID 数据的发布频率；请参阅修改可观察对象的发布频率，第 2449 页。

修改可观察对象的发布频率

默认情况下，系统每隔 5 分钟便会将可观察对象发布到 TID 元素。使用此过程可将该间隔设置为其他值。

开始之前

- 允许在可观察对象级别启用 TID 数据发布；请参阅在源、指示器或可观察对象级别暂停或发布威胁智能导向器 数据，第 2449 页。

过程

步骤 1 选择**对象** > **安全智能** > **网络列表和源**。

步骤 2 点击 **Cisco-TID-Feed** 接口旁边的 **编辑** ( ) 。

步骤 3 从**更新频率**下拉列表中选择值：

- 选择**禁用**可停止将可观察对象数据发布到元素。
- 选择任何其他值可设置可观察对象发布的间隔。

步骤 4 点击**保存**。

关于将 威胁智能导向器 可观察对象添加到“不阻止”列表

如果希望免除对简单指示器中的某个可观察对象执行指定的 **操作**（让流量通过，而不进行监控或阻止），可以将此可观察对象加入“不阻止”列表。

在复杂指示器中，威胁智能导向器 在评估流量时会忽略“不阻止”列表中的可观察对象，但仍会对该指示器中的其他可观察对象进行评估。例如，如果指示器包括可观察对象 1 和可观察对象 2，二者通过 AND 运算符链接，并且您将可观察对象 1 加入“不阻止”列表，则 威胁智能导向器 在看到可观察对象 2 时将生成完全实现的事故。

相比之下，在同一个复杂的指示器中，如果禁用可观察对象 1 的发布，而不是将其加入“不阻止”列表，则 威胁智能导向器 在看到可观察对象 2 时将生成部分实现的事故。

注释 如果将可观察对象添加到“不阻止”列表，则其优先级始终优于 **操作** 设置，与该可观察对象中的此设置是继承值还是覆盖值无关。

源更新不会影响它所包含的可观察对象的“不阻止”列表设置。

将 威胁智能导向器 可观察对象添加到不阻止列表

有关使用不阻止列表的详细信息，请参阅关于将 威胁智能导向器 可观察对象添加到“不阻止”列表，第 2450 页。

提示 “添加至不阻止列表”(Add to Do Not Block List) 按钮 ( ) 可以显示在 Web 接口中的多个位置。您可以通过点击此按钮将可观察对象添加到任何这些位置的“不阻止”列表。

过程

步骤 1 选择 **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**可观察对象**。

步骤 2 导航到您希望允许的可观察对象。

步骤 3 点击该可观察对象的 （**添加到不阻止列表 (Add to Do-Not-Block List)**）。

下一步做什么

（可选）如果您需要从“不阻止”列表删除某可观察对象，再次点击该按钮即可。

查看 STIX 源文件

过程

步骤 1 选择 **集成** > **+ 显示更多** > **威胁智能导向器** > **源**，然后点击**指示器**。

步骤 2 点击指示器名称。

步骤 3 点击**下载 STIX**。

步骤 4 在文本编辑器中打开文件。

对威胁智能导向器进行故障排除

以下章节介绍常见 威胁智能导向器 问题可能的解决方案和缓解方案。

获取或上传平面文件源会生成错误

如果系统无法获取或上传平面文件源，请检查平面文件中的数据与**集成** > **+ 显示更多** > **威胁智能导向器** > **源**页面上的**类型**列是否匹配。

TAXII 或 URL 源更新会生成错误

如果 TAXII 或 URL 源更新生成源状态错误，请检查您的服务器证书是否已过期。如果证书已过期，请输入新的**服务器证书**或删除现有的**服务器证书**，以便威胁智能导向器可以检索新证书。有关详细信息，请参阅为 威胁智能导向器 源配置 TLS/SSL 设置，第 2423 页。

“阻止”操作不是可用于指示器或源，只有“监控”可以

您可以更改指示器或源中单个可观察对象的操作。

威胁智能导向器 表视图返回“无结果”

表视图包括**源**、**指示器**、**可观察对象**和**事故**页面。

如果在某个 威胁智能导向器 表视图中没有看到数据：

- 检查您表过滤器并考虑展开**上次更新**过滤器属性的时间窗口；请参阅过滤表视图中的 威胁智能导向器 数据，第 2444 页。
- 验证您是否正确配置了您的源；请参阅采集数据源的选项，第 2418 页。
- 验证是否已将访问控制策略和相关策略配置为支持 威胁智能导向器；请参阅配置策略以支持威胁智能导向器，第 2417 页。例如，如果您的SHA-256可观察对象没有生成观察结果，请验证您部署的访问控制策略是否包含一个或多个调用**恶意软件云查找**或**阻止恶意软件**文件策略的访问控制规则。
- 验证是否已将 威胁智能导向器 支持的访问控制策略和相关策略部署到您的元素；请参阅部署配置更改，第 180 页。
- 验证您没有在功能级别暂停 威胁智能导向器 数据发布；请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 2448 页。

系统正在经历速度变慢或性能下降

有关性能影响的详细信息，请参阅威胁情报导向器的性能影响，第 2413 页。

Secure Firewall Management Center表视图不显示 威胁智能导向器 数据

如果要将可观察对象发布到您的元素，但没有 威胁智能导向器数据显示在连接、安全智能、文件或恶意软件事件表中，请检查部署到您的元素的访问控制和文件策略。有关详细信息，请参阅配置策略以支持威胁智能导向器，第 2417 页。

威胁智能导向器 数据导致一个或多个元素不堪重负

如果 威胁智能导向器 数据导致您的一个或多个设备不堪重负，请考虑暂停 威胁智能导向器 发布和清除存储在您的元素上的数据。有关详细信息，请参阅暂停 威胁智能导向器 并从元素中清除 威胁智能导向器 数据，第 2448 页。

系统正在执行恶意软件云查找而不是 TID 块

这是由设计决定的。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 2433 页。

系统正在执行安全智能或 DNS 策略操作，而不是 TID 操作

这是由设计决定的。有关详细信息，请参阅威胁智能导向器-防火墙管理中心 操作优先级，第 2433 页。

TID 被禁用

- 向设备添加内存。威胁情报导向器只能在内存至少为 15 GB 的设备上使用。

- 为 Secure Firewall Management Center启用 REST API 访问。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的启用 *REST API* 访问 。

系统不会生成 威胁智能导向器 事故或执行您预期的 威胁智能导向器 操作

- 验证是否所有托管设备均已为 威胁智能导向器 正确启用和配置。请参阅查看元素（托管设备）的 威胁智能导向器 状态， 第 2437 页 和 配置策略以支持威胁智能导向器， 第 2417 页。
- 将更改发布到元素至少需要 5-10 分钟时间，如果发布的数据源较大，可能需要更长的时间。
- 检查可观察对象的操作设置。请参阅查看和管理可观察对象， 第 2443 页。
- 有关影响系统所执行的 威胁智能导向器 操作的其他因素列表，请参阅影响所执行操作的因素， 第 2433 页。
- 元素（托管设备）可能不具备您认为它们应有的威胁数据。请参阅关于暂停发布， 第 2447 页。

遇到一次特定威胁还会生成多个事故

如果单个指示器包括在多个源中，可能会出现这种情况：

有关详细信息，请参阅处理重复指示器， 第 2422 页。

的历史记录威胁智能导向器

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
处理多个 STIX 源中包含的指示器	7.1	任意	如果 STIX 源包含相同的指示器，则会为每个源创建一个指示器，而这可能会导致为同一指示器生成多个事件。以前，只有最后下载的源才会生效。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息

操作优先级的变化	6.5	任意	如果有多项 Firepower 功能可能适用于特定可观察对象，这些变化将适用。
			TID阻止/监控可观察对象操作的优先级现在高于安全智能的阻止/监控。
			重要事项
			系统仍会像以前一样有效地处理流量。之前被阻止的流量仍被阻止，并且受监控的流量仍受到监控。这只会将事件中报告的组件更改为负责操作。您可能还会看到生成了更多的 TID 事件。
			• 如果配置了阻止TID 可观察对象操作，即使流量也与设置为阻止的安全智能阻止操作匹配：
			  • 连接事件中的安全智能类别是 TID 阻止的变体。
			  • 系统会生成一个 TID 事件，其中包含被阻止的操作。
			• 如果您配置监控 TID 可观察对象操作，即使流量与安全智能监控规则匹配也是如此：
			  • 连接事件中的安全智能类别是TID 监控器的一种变体
			  • 系统会生成一个 TID 事件，其中包含被监控的操作。
			以前，在上述每种情况下，系统通过分析报告类别，但未生成 TID 事件。

Cisco Secure Firewall 威胁智能导向器	6.2.2	任意	引入的功能：利用该功能，您可以使用来自外部源的威胁智能来识别和处理威胁。 新屏幕： 包含多个选项卡的新顶级**智能**菜单。 支持的平台： Secure Firewall Management Center



第 64 章

访问控制的高级设置

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。

- 高级设置的要求与前提条件，第 2455 页
- 为访问控制策略配置高级设置，第 2456 页
- 访问控制策略的高级设置历史记录，第 2471 页

高级设置的要求与前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员
- 您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。包含“修改访问控制策略”权限的现有预定义用户角色支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。精细化权限包括：
  - **策略** > **安全策略** > **访问控制** 并选择**访问控制策略** > **修改访问控制策略** > **修改威胁配置**允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。如果用户只有此选项，则不能修改策略或规则的其他部分。
  - **修改剩余访问控制策略配置** 控制编辑策略所有其他方面的能力。

为访问控制策略配置高级设置

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。默认设置适用于大多数的部署。请注意，规则更新可能会修改访问控制策略中的许多高级预处理和性能选项，如*Cisco Secure Firewall Management Center* 管理指南 中的更新入侵规则所述。

注意 有关重启 Snort 进程的高级设置修改列表，请参阅部署或激活时重启 Snort 进程的配置，第 176 页，以暂时中断流量检查。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

开始之前

从父策略继承设置：

- 如果访问控制策略具有基本策略，则可以选择从基本策略继承设置。对于要使用父策略设置的每个设置组，选择**从（基本策略）继承**。如果您可以为该策略配置独特设置，则必须取消选择“从基本策略继承”才能进行编辑。
- 如果显示**视图**()，则表明设置继承自祖先策略，或者您没有修改设置的权限。在这种情况下，已配置继承，因此这些设置处于锁定状态。设置为只读。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 创建或编辑访问控制策略。

步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 对于每个设置组，点击**编辑** ()并根据需要配置相关设置。

对于每个功能组，系统会打开一个单独的对话框，可在其中进行更改。点击**确定**以保存所有更改。

- **常规设置** - 这些设置广泛适用于该策略，包括 URL 过滤选项。有关详细信息，请参阅常规设置，第 2458 页。
- **身份策略设置** - 选择用于实施用户身份发现的策略。只有实施身份策略，才能获取连接事件中的用户或用户组信息，或者才能基于用户或组编写访问控制规则。有关详细信息，请参阅关于身份策略，第 2211 页。
- **解密策略设置** - 选择解密连接时要使用的策略。您必须解密流量才能对加密连接应用检测。
- **TLS 服务器身份识别** - 是否允许防火墙提取证书详细信息（例如通用名称 (CN)、组织或使用者备用名称 (SAN)），即使 TLS 1.3 加密通常会隐藏这些信息。这可以提高策略准确性，而无需解密规则；原始客户端连接保持加密状态。有关详细信息，请参阅TLS 服务器身份发现，第 2459 页。

- **预过滤策略设置** - 选择用于静态分流大流、实施早期连接阻断或重新划分纯文本隧道流量区域的策略。
- **网络分析和入侵策略** - 高级网络分析和入侵策略设置允许您：
  - 指定用于检查数据包的入侵策略和相关变量集，在系统确定如何准确检查该流量之前，这些数据包必须通过。
  - 更改访问控制策略的默认网络分析策略，该默认策略监管许多预处理选项。
  - 使用自定义网络分析规则和网络分析策略根据特定安全区域、网络和 VLAN 定制预处理选项。
- **威胁防御服务策略** - 可以使用该服务策略将服务应用到特定流量类别。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。在访问控制规则之后应用服务策略规则。有关详细信息，请参阅服务策略，第 2473 页。
- **文件和恶意软件设置** - 调整文件和恶意软件检测性能和存储，第 2318 页提供有关文件控制和恶意软件防护的性能选项信息。
- **威胁检测** - 配置端口扫描检测器，以检测和阻止所有类型流量中的端口扫描活动，保护网络免受潜在攻击。可以在允许和拒绝的流量中高效检测 Portscan 流量。有关详细信息，请参阅威胁检测，第 2491 页。
- **大象流设置** - 大象流是大型、长时间且高速的流量，可能会给 Snort 核心带来压力。有两种操作可应用于大象流，以减少系统压力、CPU 占用、丢包等。这些操作包括：
  - 绕过任何或所有应用-此操作绕过来自 Snort 检测的流。
  - Throttle-此操作对象流应用动态速率限制策略（降低 10%）。

  有关详细信息，请参阅配置大象流检测，第 2502 页。
- **智能应用绕行设置** —（请使用**大象流设置**，而非此选项。）智能应用绕行 (IAB) 是一种专业级配置，指定如果流量超出检查性能和流量阈值的组合，则应用绕行或测试是否要绕行。

  IAB 设置适用于 Snort2 设备或 7.2.0 版本之前的 Snort3 设备。有关详细信息，请参阅智能应用绕行，第 2461 页。
- **传输层/网络层预处理器设置** - 高级传输层和网络层预处理器设置全局应用于所有部署了访问控制策略的网络、区域和VLAN。有关详细信息，请参阅传输/网络层预处理器设置，第 2466 页。
- **检测增强设置** - 检测增强设置确定自适应配置文件是否用于访问控制策略中的应用检测和入侵规则。通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。有关详细信息，请参阅检测增强设置，第 2467 页。
- **性能设置** — 关于系统分析流量以检测入侵尝试时如何提高系统性能的信息。这些设置非常高级，大多数用户应保持默认设置。请参阅性能设置，第 2468 页。
- **基于延迟的性能设置**—基于延迟的性能的特定设置。这些设置非常高级，大多数用户应保持默认设置。请参阅基于延迟的性能设置，第 2470 页。

- **影子流量** - 影子流量控制面板可增强源自未经批准的隐私技术的流量的可视性。此类流量专门用于规避高级防火墙的传统网络监控和分析。连接事件和统一事件中还添加了影子流量类型属性。如果您不需要查看可能包含未经批准的内容的流量，则可以禁用此选项。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的影子流量构件
- **高级日志记录** - 启用此功能，以便使用应用数据丰富连接日志，并将生成的日志转发到系统日志目标。应用日志记录利用现有的深度数据包检查功能提取应用数据，使您能够加强网络监控并更深入地了解网络流量。此功能适用于 Snort 3 Firewall Threat Defense 设备。

  有关应用日志记录的详细信息，请参阅 。*Cisco Secure Firewall Management Center* 管理指南中的应用程序感知事件日志

  注释
  如果在访问控制规则中没有配置过滤器的情况下使用应用程序日志记录，则可能会导致网络中的性能下降。使用访问控制规则过滤特定流量类型，以减少记录的流量。

步骤 5 点击**保存** 以保存对访问控制策略的更改。

- 要返回规则列表，请点击数据包流程中的**访问控制**。
- 您必须部署配置，才能将更改应用到受管设备。

常规设置

以下是可为访问控制策略配置的常规高级设置

- **连接事件中存储的最大 URL 字符数** - 设置用户在连接结束事件中请求的每个 URL 的最大字符长度。禁用或限制存储的URL字符数可能会提升系统性能。默认值为1024。范围为0到4096。

  将长度设置为 0 可禁用 URL 日志记录。存储零字符（禁用 URL 日志记录）不会影响 URL 过滤。尽管系统不会记录流量，但会根据请求的 URL 过滤流量。

- **允许交互式阻止绕过限制（秒）** - 设置用户绕过URL过滤限制后允许浏览的时间。超时到期后，用户必须再次绕过阻止。默认值为 600 秒（10 分钟）。范围为 0 到 31536000（8760 小时）。

  将此值设置为 0 表示交互式阻止响应显示一次，并且用户绕行永远不会过期。

- **重试URL缓存未命中查询** - 此设置确定系统需要在云中查找URL的类别和信誉时执行的操作。

  系统第一次遇到没有本地存储的类别和信誉的 URL 时，会在云中查找该 URL 并将结果添加到本地数据存储中，以便在将来更快地处理该 URL。

  此设置默认启用。系统在云中检查URL的信誉和类别时会暂时延迟流量，并根据云判定结果处理流量。

  如果禁用此设置，当系统遇到不在其本地缓存中的URL时，会根据为未分类和无信誉流量配置的规则立即放行并处理该流量。

  在被动部署中，由于系统无法保留数据包，因此不会重试查询。

- **启用威胁情报导向器** - 是否使用威胁情报导向器。禁用此选项以停止将 TID 数据发布到配置的设备。默认设置为启用。有关详细信息，请参阅如何设置威胁智能导向器，第 2416 页。
- **启用 DNS 流量信誉实施** - 当浏览器查找域名以获取 IP 地址时，是否让系统在 URL 事务初期评估域类别和信誉。启用此选项可提高URL过滤的性能和效力。默认设置为启用。有关详细信息和其他说明，请参阅DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别，第 1798 页和子主题。
- **策略应用期间检查流量** - 部署配置更改时是否检查流量（除非特定配置要求重新启动 Snort 进程）。默认设置为启用。

  启用此选项后，资源需求可能会导致丢弃少量数据包而不进行检查。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重新启动场景，第 172 页。

TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

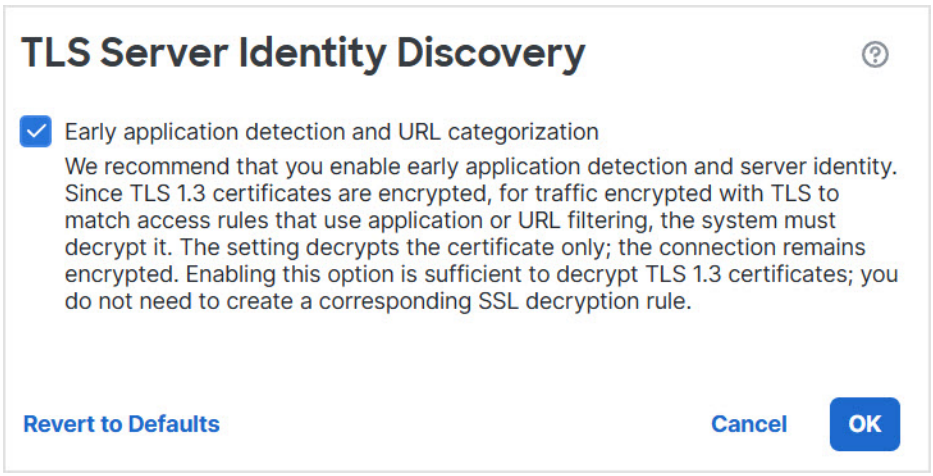
在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。某些功能不受支持，例如 STARTTLS 流量、HTTP CONNECT 方法，以及在已有其他设备正在解密流量的网络中。

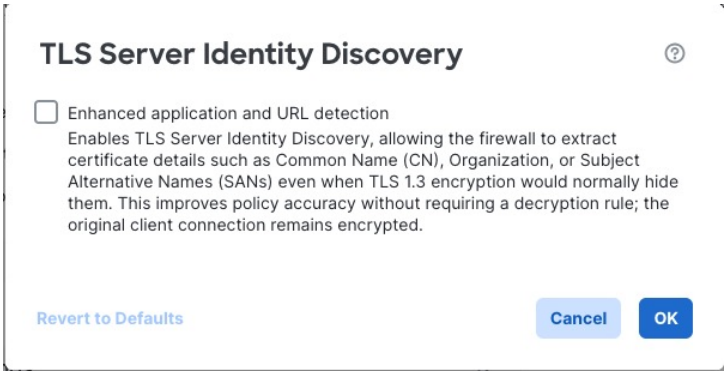
如果启用此选项，我们建议您同时启用解密策略的高级 TLS 自适应服务器身份探测选项。总之，这些选项可更有效地解密 TLS 1.3 流量。有关详细信息，请参阅TLS 1.3 解密最佳实践，第 1904 页。

当新连接开始且受 TLS 服务器身份发现影响时，Firewall Threat Defense 会保留原始 ClientHello 数据包，以确定其连接的服务器的身份，然后再继续。Firewall Threat Defense 设备会从 Firewall Threat Defense 向服务器发送专用连接。服务器的响应包括服务器证书，专用连接会被终止，并根据访问控制策略的要求评估原始连接。

TLS 服务器身份发现将证书的通用名称 (CN) 优先于服务器名称指示 (SNI)。

要启用 TLS 服务器身份发现，请点击**高级**选项卡，点击该设置旁的**编辑** (✎)，然后选择**增强应用和 URL 检测**。





我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。解密策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

注释

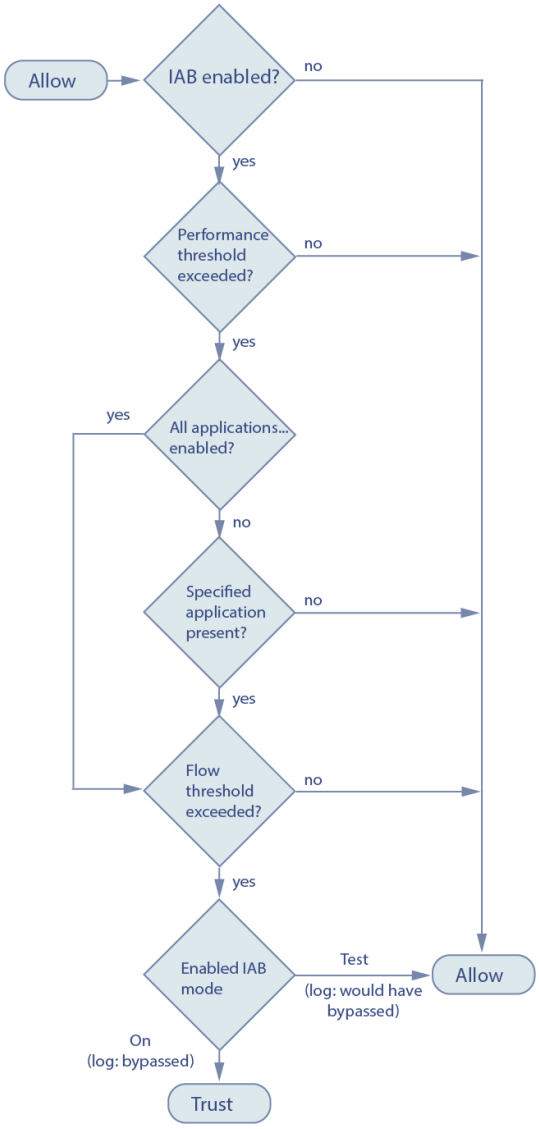
- TLS 服务器身份发现不能与以下任何一项配合使用：
  - STARTTLS 流量
  - HTTP CONNECT 方法
  - 已被网络上的其他设备解密的流量
- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由 Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。
- TLS 服务器身份发现也可在 TLS 1.2 会话上运行。

智能应用绕行

智能应用绕行 (IAB) 可识别您信任的应用，当超出性能和流量阈值时，允许其流经网络而无需进一步检测。例如，如果每次晚间的备份会显著影响系统的性能，您可以配置某些阈值，当超过这些阈值时则信任备份应用产生的流量。（可选）可以配置 IAB，使其在超出检查性能阈值时，无论应用类型如何，IAB 都信任超出任何流绕过阈值的所有流量。

在对流量进行深度检查之前，系统会对访问控制规则或访问控制策略的默认操作所允许的流量实施 IAB。您可以通过一种测试模式确定是否已超过阈值，如果已超过，则识别出在您实际启用了 IAB 的情况下会被绕过的应用数据流（称为绕行模式）。

下图展示 IAB 决策过程：



配置智能应用旁路

并非所有部署都需要 IAB，而那些需要 IAB 的部署也仅以有限的方式进行使用。除非您具备网络流量（特别是应用流量）和系统性能（包括可预测的性能问题的原因）方面的专业知识，否则不要启用 IAB。在绕行模式下运行 IAB 之前，请确保信任指定的流量不会使您处于风险中。

开始之前

IAB 设置适用于 Snort2 设备或 7.2.0 版本之前的 Snort3 设备。对于 Snort 3 设备，请改用大象流量检测。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的**更多** 下拉箭头中点击**高级设置**。然后，点击**智能应用绕行设置**旁边的 **编辑** (✎)。

步骤 2 为 IAB 设置启用**状态**。

关闭或**打开** IAB，或在**测试**模式下启用 IAB。

在测试模式下，连接事件和控制面板会告诉您在 IAB 开启时系统本会执行的操作，但流量不受影响。使用测试模式检查您的配置。

步骤 3 设置**性能采样间隔**。

性能采样间隔指定两次 IAB 性能采样扫描间隔的时间（秒），系统会在此期间收集系统性能指标以与 IAB 性能阈值进行比较。默认值为 5 秒。范围为 1 到 1000 秒。

步骤 4 选择**可绕行应用和过滤器**。

选项包括：

- ***X*应用/过滤器** — 点击链接，选择要绕过其流量的应用或应用过滤器。您可以按常规属性、特定应用或两者进行选择。例如，可以将可绕行的流量限制为仅允许流向风险极低的应用。
- **包括未识别应用在内的所有应用** — 不要限制旁路。超过检查性能阈值时，不管应用类型为何，IAB 都信任超过任何流绕行阈值的所有流量。这是默认值。

步骤 5 配置性能和流阈值。

您必须至少配置一个**检测性能阈值**和一个**流量旁路阈值**。但是，所有设置都有默认值，如果默认值适合您的网络，则无需更改设置。

当超过某一性能阈值时，系统会检查流阈值，并且如果超过某一阈值，则信任指定流量。如果启用其中一项以上，则只能超过其中一项。

a) 点击**检查性能阈值**下的**配置**并配置选项。

检查性能阈值提供入侵检查性能限值，如果超过该限值，则会触发流阈值检查。检查性能阈值设置为 0 时将被忽略。

您可以配置一个或多个以下阈值：

- **丢弃百分比** — 因昂贵入侵规则、文件策略、解压等引起的性能过载导致的数据包丢弃时，丢弃的平均数据包数占总数据包数的百分比。这并不是指入侵规则等正常配置丢弃的数据包数。

  请注意，当丢弃指定百分比的数据包时，指定大于 1 的整数会激活 IAB。指定 1 时，任何从 0 到 1 的百分比都会激活 IAB。这允许少量数据包激活 IAB。

  默认值为 5%。范围为 0 到 100。

- **处理器利用率百分比** — 使用的处理器资源的平均百分比。默认值为 95。范围为 0 到 100。
- — 平均数据包延迟（微秒）。默认值为 1000。范围为 0 到 1000000。
- **流速率** — 系统处理流的速率，以每秒的流数进行测量。请注意，此选项可配置 IAB 以测量流速率，而不是流计数。默认值为 0。范围为 0 到 1000000。

b) 点击**流绕行阈值**下的**配置**并配置选项。

流绕行阈值提供流限值，如果超过该限值，则会触发 IAB 信任绕行模式下的可绕行应用流量，或允许应用流量在测试模式下接受进一步检查。系统会忽略设置为 0 的流绕行阈值。

您可以配置一项或多项以下流绕行阈值：

- **单位流字节数** — 一个流可以包含的最大千字节数。默认值为 500000。范围为 0 至 2147483647。
- **单位流数据包数**—一个流可以包含的最大数据包数。默认值为 0。范围为 0 至 2147483647。
- **流持续时间** — 一个流保持开放的最大秒数。默认值为 0。范围为 0 至 2147483647。
- **流速**— 最高传输速率（千字节/秒）。默认值为 250000。范围为 0 至 2147483647。

步骤 6 点击**确定 (OK)** 保存 IAB 设置。

步骤 7 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

IAB 日志记录和分析

无论是否启用连接日志记录，IAB 都会强制连接结束事件记录已绕过的流和应已绕过的流。连接事件指示在绕行模式下绕过的流或在测试模式下应已绕过的流。基于连接事件的自定义控制面板构件和报告可以显示已绕过和应已绕过的流的长期统计信息。

IAB 连接事件

操作

当**原因 (Reason)** 包括 `Intelligent App Bypass` 时：

- **允许** — 指示已应用的 IAB 配置处于测试模式，并且**应用协议**指定的应用的流量仍可供检查。
- **信任** — 指示已应用的 IAB 配置处于绕行模式，并且**应用协议**指定的应用的流量受信任，可流经网络而不进行进一步检查。

原因

`Intelligent App Bypass` 指示 IAB 在绕行或测试模式下触发了事件。

应用协议

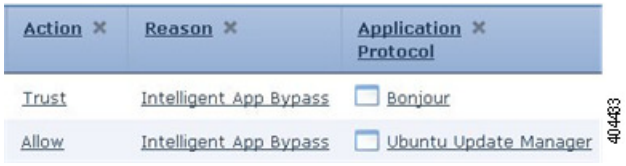
此字段显示触发了事件的应用协议。

示例 1

在以下截断的图形中，某些字段已省略。该图形显示根据两个单独访问控制策略中的不同 IAB 设置产生的两个连接事件的**操作 (Action)**、**原因 (Reason)** 和**应用协议 (Application Protocol)** 字段。

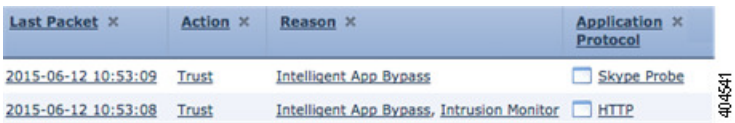
对于第一个事件，`Trust` 操作指示 IAB 在绕行模式下已启用，并且 Bonjour 协议流量受信任可通过而不进行进一步检查。

对于第二个事件，`Allow` 操作指示 IAB 在测试模式下已启用，因此 Ubuntu 更新管理器流量会接受进一步检查，但如果 IAB 在绕行模式下已启用，则应已绕过该流量。



示例 2

在以下截断的图形中，某些字段已省略。第二个事件中的流同时按照入侵规则（**原因 [Reason]**：`Intrusion Monitor`）进行绕过（**操作 [Action]**：`Trust`；**原因 [Reason]**：`Intelligent App Bypass`）和检查。`Intrusion Monitor` 原因指示检测到设置为**生成事件 (Generate Events)** 的入侵规则，但在连接过程中未阻止漏洞。在示例中，此情况发生在检测到应用之前。在检测到应用后，IAB 将应用识别为可绕过且受信任的流。



IAB 自定义控制面板构件

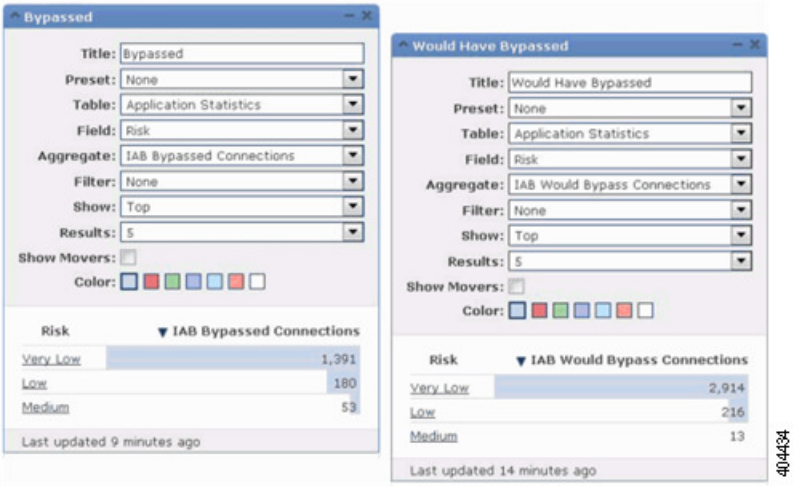
可以创建自定义分析控制面板构件以根据连接事件显示长期 IAB 统计信息。创建构件时，请指定以下信息：

- 预设：无
- 表：应用统计信息
- 字段 **(Field)**：any
- 汇聚 **(Aggregate)**：以下任一：
  - IAB Bypassed Connections
  - IAB Would Bypass Connections
- 过滤器 **(Filter)**：any

控制面板示例

在以下自定义分析控制面板构件示例中：

- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。.



IAB 自定义报告

可以创建自定义报告以根据连接事件显示长期 IAB 统计信息。创建报告时，请指定以下信息：

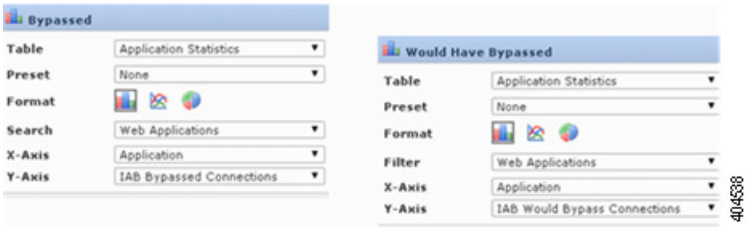
- 表：应用统计信息
- 预设：无
- 过滤器 **(Filter)**：any
- X 轴 **(X-Axis)**：any

- **Y 轴 (Y-Axis)**：以下任一：
  - IAB Bypassed Connections
  - IAB Would Bypass Connections

报告示例

下图中显示两个缩写的报告示例：

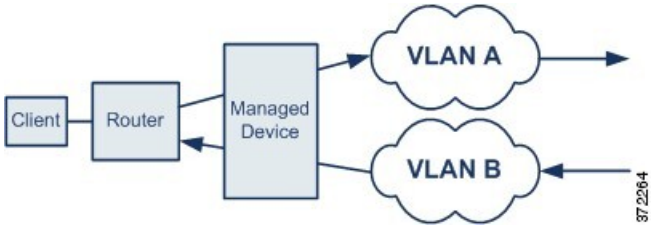
- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。



传输/网络层预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。

- **跟踪连接时忽略 VLAN 报头** -识别流量时忽略还是包含 VLAN 报头。同一连接中行进方向不同的流量中的 VLAN 标记不同，可能影响流量重组和规则处理。例如，对于同一连接，流量可以通过 VLAN A 传输，而通过 VLAN B 接收。如果设备可能为同一连接识别到不同的 VLAN，请选择此选项。该选项默认为关闭。



- **最大活动响应数** - 对于触发配置为提供活动响应的预处理器/入侵丢弃规则的 TCP 连接，是指每个 TCP 连接的最大活动响应数。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数 (Minimum Response Seconds)**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 将禁用由主动响应规则触发的额外主动响应。默认值为无限制。范围为 0 到 25。

注释 您必须专门配置丢弃规则，以提供主动响应。对于TCP连接，主动响应是RESET 数据包。对于 UDP 连接，系统会向连接源发送 ICMP 不可达数据包。

- **最小响应秒数** - 指定在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应之前等待的秒数，直至出现**最大活动响应数**。默认值为无限制。范围为 1 到 300。
- **会话终止日志记录阈值** - 请勿修改此选项，除非支持人员指示执行此操作。

  支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。此选项指定一个字节数，当会话终止并超过该指定数字时，将会记录消息。上限为 1GB。

检测增强设置

检测增强设置确定自适应配置文件是否用于访问控制策略中的应用检测和入侵规则。通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

注释 要在 Snort 3 中启用自适应配置文件，必须同时选择**启用**和**启用配置文件更新**选项。

- **启用** - 您必须启用自适应分析功能（其默认状态），以便访问控制规则执行应用程序和文件控制（包括恶意软件防护 (AMP)），并使入侵规则能够使用服务元数据。
- **启用配置文件更新** - 配置文件更新（例如可在网络分析策略中配置的基于目标的配置文件）有助于通过与目标主机上的操作系统相同的方式对IP数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。配置文件更新还会将入侵规则中的元数据与主机信息进行比对，以确定该规则是否应适用于特定主机。有关详细信息，请参阅：
  - 自适应配置文件更新，第 2468 页
  - 自适应配置文件更新和建议的规则，第 2468 页
- **自适应配置文件-属性更新间隔** - 启用配置文件更新后，您可以控制从管理中心向受管设备同步网络地图数据的频率（以分钟为单位）。系统使用该数据确定处理流量时应使用哪些配置文件。增大此选项的值可提升大型网络的性能。
- **自适应配置文件-网络** - 或者，启用配置文件更新后，您可以通过将限制在逗号分隔的IP地址、地址块和网络变量列表中来提高性能。如果使用网络变量，则系统会为您的访问控制策略使用与默认入侵策略相关联的变量集中的变量值。例如，可以输入：192.168.1.101, 192.168.4.0/24, $HOME_NET。支持 IPv4 和 IPv6。

  默认值 (0.0.0.0/0) 将自适应配置文件更新应用于所有网络。

自适应配置文件更新

通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

配置文件更新（就像可在网络分析策略中手动配置的基于目标的配置文件一样）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件应用您选择的默认操作系统配置文件，或绑定到特定主机的配置文件。但是，配置文件更新会根据目标主机的主机配置文件中的操作系统切换到相应的操作系统配置文件。

假设您为 10.6.0.0/16 子网配置配置文件更新，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置设置的防火墙管理中心中有一个包括 10.6.0.0/16 子网的网络映射。

- 当系统检测到来自主机 A（不在 10.6.0.0/16 子网中）的流量时，它使用基于 Linux 目标的策略重组 IP 分片。
- 当系统检测到来自主机 B（在 10.6.0.0/16 子网中）的流量时，它从网络映射检索主机 B 的操作系统数据。系统使用基于该操作系统的配置文件对传送到主机 B 的流量进行分片重组。

自适应配置文件更新和建议的规则

自适应配置文件功能是访问控制策略中的高级设置，它全局应用于由该访问控制策略调用的所有入侵策略。思科 建议的规则功能适用于您在其中配置该功能的各个入侵策略。

与建议的入侵规则一样，配置文件更新将规则中的元数据与主机信息进行比较，确定是否应为特定主机应用该规则。然而，建议的入侵规则会基于该信息提供规则启用或禁用的建议，而配置文件更新则利用这些信息将特定规则应用于特定流量。

建议的入侵规则需要您手动执行规则状态的建议更改。另一方面，配置文件更新不会修改入侵策略。基于配置文件更新的规则处理以逐包方式进行。

此外，建议的入侵规则可启用已禁用的规则。相比之下，配置文件更新仅影响入侵策略中已启用规则的应用，且配置文件更新从不更改规则状态。

您可以将配置文件更新与建议的入侵规则结合使用。部署入侵策略时，配置文件更新会使用规则的当前状态来确定是否将其列为应用候选规则，而您接受或拒绝建议的选择会反映在该规则状态中。您可以同时使用这两个功能来确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

性能设置

以下设置用于在系统分析流量入侵企图时优化性能。各组设置均有独立选项卡。

这些设置适用于 Snort，仅当您在规则中或作为默认动作应用入侵策略时才相关。仅当您是 Snort 入侵规则专家，或在思科技术支持指导下才更改这些设置。

模式匹配限制

- **每个数据包要分析的最大模式状态数** — 要排队的最大事件数。默认值为 5。
- **禁用对未来将进行重组的流量的内容检查** — 是否在重组前检测 TCP 负载。它包括数据流重组前后的数据包检测。这一过程需要更多的处理开销，并且可能会降低性能。如果未选中该选项，则在重组后检测 TCP 负载。默认为关闭。

性能统计数据

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

- **采样时间（秒）**— 进行性能采样的时间范围。默认值为 300 秒。

  为采样时间配置非常低的值（例如 1 秒）可能会对设备造成巨大影响；设备上记录的性能统计信息可能会导致磁盘空间问题并影响设备的运行。因此，建议您不要配置非常低的值。

- **最小数据包数** — 将多少个数据包视为有效性能统计信息的最小值。默认值为 0。
- **故障排除选项：**
  - **记录会话/协议分布** — 思科技术支持可能会在故障排除电话中要求您启用此选项，以配置系统仅在 Snort 进程关闭或重启时计算性能统计信息。
  - **摘要** — 仅当思科技术支持指示时才启用此选项。

正则表达式限制

默认的 Perl 兼容正则表达式 (PCRE) 限制确保了最低水平的性能。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

- **匹配限制状态** — 匹配正则表达式的限制。您可以选择**默认值**（即 3500）、**无限制**或**自定义**。如果您选择自定义，请在**匹配限制**中指定尝试匹配 PCRE 正则表达式中定义的模式的次数。指定 0 以完全禁用 PCRE 匹配评估。
- **匹配递归限制状态** — 匹配正则表达式递归的限制。您可以选择**默认值**（即 3500）、**无限制**或**自定义**。如果您选择自定义，请在**匹配递归限制**中指定评估数据包负载中的 PCRE 正则表达式时的递归次数。指定 0 以完全禁用 PCRE 递归。



注释 要使自定义匹配递归限制有意义，它必须小于匹配限制。

入侵事件日志记录限制

当入侵规则引擎根据规则评估流量时，它会将针对给定数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。配置入侵事件日志记录限制时，可指定队列中可放置的事件数量及要记录的事件数量，并可选择确定队列中事件顺序的条件。

- **每个数据包存储的最大事件数** — 可以为给定数据包或数据包流存储的最大事件数。默认值为 8。
- **每个数据包记录的最大事件数**—为给定数据包或数据包流记录的事件数。这不能超过**每个数据包存储的最大事件数量 (Maximum Events Stored Per Packet)** 的值。默认值为 5。
- **事件日志记录优先级依据**—用于确定事件队列中事件排序的值。通过用户界面报告排序最靠前的事件。您可以选择：
  - **内容长度**（默认），按最长识别内容匹配对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。
  - **优先级**，按事件优先级对队列中的事件进行排序。

基于延迟的性能设置

每个访问控制策略都具有基于延迟的设置，这些设置使用阈值来管理数据包和规则处理性能。

这些设置适用于 Snort，仅当您在规则中或作为默认动作应用入侵策略时才相关。默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。仅当您是 Snort 入侵规则专家，或在思科技术支持指导下才更改这些设置。

应用的延迟设置取决于与访问控制策略关联的网络分析策略 (NAP) 的安全级别。通常，这是指默认 NAP 策略。但是，如果已配置自定义网络分析规则，并且其中任意一个规则指定的 NAP 策略安全级别都高于默认 NAP 策略，则延迟设置取决于自定义规则中安全级别最高的 NAP 策略。如果默认 NAP 策略或任何自定义规则调用自定义 NAP 策略，则评估中使用的安全级别是每个自定义 NAP 策略所基于的系统提供的基本策略。

不论有效阈值和/或网络分析配置直接在策略中继承还是配置，上述情况均成立。

使用以下设置来调整系统的基于延迟的性能。

- **应用设置来源** — 是否从**已安装规则更新**（默认）或您的**自定义**设置中应用基于延迟的性能设置。
- **数据包处理**—数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。默认情况下，数据包处理的基于延迟的性能设置处于禁用状态。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。选择**已启用**以开启它。如果您选择了**自定义**，还需输入检查数据包应停止的**阈值**时间（微秒）。默认值为 256。
- **规则处理**—规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。仅当您选择**自定义**时才可以配置这些选项。
  - **启用**—如果您选择自定义，此选项会自动选中。如果您不想使用此功能，请取消选择该选项。此选项卡上的所有其他设置都需要启用该功能。
  - **阈值（微秒）**— 指定规则检查数据包时不应超过的时间（微秒）。默认值为 512。

- **暂停规则前的连续阈值违规次数**—指定规则在被暂停前检查数据包所用时间可以超过阈值时间的连续次数。默认值为 3。
- **暂停时间** — 暂停的规则应保持暂停多长时间。默认值为 10。

访问控制策略的高级设置历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
影子流量监控	10.0.0	10.0.0	监控源自未经批准的隐私技术的流量（称为影子流量）。 新增/修改的屏幕： • **策略** > **访问控制** > **编辑策略** > **更多** > **高级设置** > **影子流量** • **洞察与报告** > **控制面板** > **影子流量**
改进了端口扫描检测。	7.2	7.2 运行 Snort 3	通过改进的端口扫描检测器，您可以轻松地配置系统以检测或防止端口扫描。您可以细化要保护的网络，设置灵敏度等。对于运行 Snort 2 的设备以及运行版本 7.1 及更早版本的设备，请继续使用网络分析策略进行端口扫描检测。 新增/修改的屏幕：我们向访问控制策略的高级选项卡添加了 **威胁检测** 。 新增/修改的命令： **clear threat-detection portscan**、 **show threat-detection portscan**。
在 Snort 3 设备上绕过检查或限制大流量。	7.2.0	使用 Snort 3 的 7.2.0	您现在可以检测并选择性地绕过检查或限制大流量。默认情况下，访问控制策略设置为在系统发现大于 1 GB/10 秒的未加密连接时生成事件；速率限制可配置。 对于 Firepower 2100 系列，您可以检测象流，但不能绕过检查或限制。对于运行 Snort 2 的设备以及运行 7.1 及更低版本的设备，请继续使用智能应用绕行 (IAB)。 新增/修改的屏幕：我们在访问控制策略的“高级”选项卡中添加了 **象流设置** 。 有关更多信息，请参阅 象流检测。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DNS 过滤	7.0.0 6.7.0（实验性）	任意	如果启用并配置了 URL 过滤，则默认情况下会为每个新的访问控制策略启用一个新的选项，以用于增强类别和信誉过滤效率。 有关信息，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别，第 1798 页 和子主题。 访问控制策略的“高级”(Advanced) 选项卡在“常规设置”(General Settings) 下有一个新选项：**对 DNS 流量启用信誉实施 (Enable reputation enforcement on DNS traffic)**。
TLS 服务器身份发现	6.7.0	任意	在客户端连接到支持 TLS 1.3 的服务器时，启用访问控制策略以评估 URL 和应用条件。通过 TLS 服务器身份发现，无需解密流量即可对这些条件进行评估。 启用此功能可能会影响设备性能，但具体取决于型号。 访问控制策略的“高级”(Advanced) 选项卡页面具有新选项： • 警告会显示在“高级”(Advanced) 选项卡上；向右移动滑块可启用 TLS 服务器身份发现。 • “高级”(Advanced) 选项卡页面上的新选项：**TLS 服务器身份发现 (TLS Server Identity Discovery)**。
威胁防御服务策略。	6.3	任意	现在您可以将威胁防御服务策略配置为访问控制策略高级选项的一部分。您可以使用威胁防御服务策略将服务应用于特定流量类。支持的功能包括 TCP 状态绕行、随机生成 TCP 序列号、递减数据包的生存时间 (TTL) 值、失效连接检测、设置每个流量类和每个客户端的最大连接数和初期连接数限制以及初期、半闭和空闲连接的超时时间。 新屏幕： **策略 > 访问控制 > 访问控制**、 **高级** 选项卡， **威胁防御服务策略**。 支持的平台： Cisco Secure Firewall Threat Defense



第 65 章

服务策略

您可以使用威胁防御服务策略将服务应用于特定流量类。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

- 关于威胁防御服务策略， 第 2473 页
- 服务策略的要求和先决条件， 第 2475 页
- 服务策略准则和限制， 第 2475 页
- 配置威胁防御服务策略， 第 2476 页
- 监控服务策略， 第 2484 页
- 服务策略规则示例， 第 2484 页
- 威胁防御服务策略的历史记录， 第 2489 页

关于威胁防御服务策略

您可以使用威胁防御服务策略将服务应用到特定流量类别。使用服务策略，您不仅仅可以将相同的服务应用于进入设备或给定接口的所有连接。

流量类是接口和扩展访问控制列表(ACL)的组合。ACL“允许”规则确定哪些连接是该类的一部分。ACL 中的任何"被拒绝"流量只是没有应用于其上的服务： 这些连接实际上没有被丢弃。您可以使用 IP 地址和 TCP/UCP 端口根据需要精确识别匹配的连接。

有两种类型的流量类：

- 基于接口的规则 - 如果在服务策略规则中指定安全区域或接口组，则此规则适用于通过作为接口对象一部分的任何接口的 ACL“允许”流量。

  对于指定功能，适用于入口接口的基于接口的规则始终优先于全局规则：如果基于入口接口的规则应用于连接，则忽略任何匹配的全局规则。如果没有适用的入口接口或全局规则，则应用出口接口上的接口服务规则。

- 全局规则 - 这些规则适用于所有接口。如果基于接口的规则不适用于连接，则系统将检查全局规则并将其应用于 ACL“允许”的任何连接。如果没有适用的规则，则连接将继续，而不应用任何服务。

对于指定功能，给定连接只能匹配一个基于接口的流量类或全局流量类。指定接口对象/流量组合最多包含一条规则。

服务策略规则在访问控制规则之后应用。这些服务仅针对您允许的连接进行配置。

服务策略如何关联 FlexConfig 和其他功能

由于连接相关服务策略功能被视为与其他服务规则实施功能独立的功能组，因此应该不会遇到流量类重叠的问题。但是，进行以下配置请注意：

- 使用服务策略 CLI 实施 QoS 策略规则。这些规则在基于连接的服务策略规则之前应用。但是，QoS 和连接设置都可以应用于相同或重叠的流量类。
- 您可以使用 FlexConfig 策略来实施自定义应用检测和 NetFlow。使用 **show running-config** 命令检查已配置服务规则的 CLI，包括 **policy-map**、**class-map** 和 **service-policy** 命令。Netflow 和应用检测与 QoS 和连接设置兼容，但是您需要在实施 FlexConfig 之前了解现有配置。在应用检测和 Netflow 之前应用连接设置。



注释 从 Threat Defense 服务策略创建的流量类被命名为 **class_map_***ACLname*，其中 *ACLname* 是服务策略规则中使用的扩展 ACL 对象的名称。

什么是连接设置？

连接设置包含与管理流量连接相关的各种功能，例如通过 Firewall 威胁防御 的 TCP 流量。某些功能以组件命名，可以配置这些组件，以提供特定服务。

连接设置包括以下内容：

- **Global timeouts for various protocols** - 所有全局超时均具有默认值，因此，只有在遇到过早失去连接的情况下，才需要更改超时值。配置 Threat Defense 策略中的全局超时。依次选择**设备** > **平台设置**。
- **Connection timeouts per traffic class** - 可以使用服务策略覆盖特定流量类型的全局超时。所有流量类超时均具有默认值，因此，无需设置这些超时。
- **Connection limits and TCP Intercept** - 默认情况下，对于可以通过（或到达）Firewall 威胁防御的连接数量没有限制。可以使用服务策略规则来设置对特定流量类的限制，以保护服务器免受拒绝服务 (DoS) 攻击。具体而言，可以设置对初期连接（未完成 TCP 握手的连接）的限制，防止 SYN 泛洪攻击。当超过初期限制时，TCP 拦截组件会参与代理连接并确保攻击受到限制。
- **死连接检测 (DCD)** - 如果具有有效但经常空闲的持久连接，以至于这些连接因为超出空闲超时设置而关闭，就可以启用失效连接检测，以识别空闲但有效的连接并且（通过重置其空闲计时器）使之保持活动状态。每当超出空闲时间，DCD便会探测连接的两侧，了解两侧是否均同意连接是有效的。**show service-policy** 命令输出中包含计数器，以显示来自 DCD 的活动量。您可以使用 **show conn detail** 命令获取有关发起方和响应方的信息，以及各自发送探测的频率。

- **TCP 序列随机化** - 每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。默认情况下，Firewall 威胁防御 随机化入站和出站方向的 TCP SYN 的 ISN。随机化可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。但是，TCP 序列随机化有效地破坏了 TCP SACK（选择性确认），因为客户端看到的序列号与服务器看到的序列号不同。可以根据需要按流量类禁用随机化。
- **TCP 标准化** - TCP 规范器可防止异常数据包。可以按流量类配置处理某些数据包异常类型的方式。您可以使用 FlexConfig 策略配置 TCP 规范化。
- **TCP 状态旁路** - 如果在网络中使用非对称路由，可以绕过 TCP 状态检查。

服务策略的要求和先决条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

服务策略准则和限制

- 服务策略仅适用于路由或交换机接口，无论是处于路由模式还是透明模式。这些策略不适用于内联集或被动接口。
- 对于指定接口或全局策略，最多可以有25个流量类。具体而言，这意味着对于指定安全区域或接口组，全局策略的服务策略规则不能超过25条。但是，对于接口而言，由于同一接口可以同时出现在安全区域和接口组中，因此请注意，实际限制基于接口，而不是基于区域/组。因此，根据所在区域/组的成员资格，您可能无法为每个区域/组设置 25 条规则。
- 对于指定接口对象/流量组合，最多只能包含一条规则。
- 当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。如果希望所有连接立即使用新策略，则需要断开当前连接，以便使用新策略重新连接。在 SSH 或控制台 CLI 会话中，输入 **clear conn** 或 **clear local-host** 命令。

- QoS 规则和服务策略规则（在访问控制策略中）将转换为防火墙上的命令。这包括创建策略映射。每个接口只能有一个策略映射。系统会自动将 QoS 和服务策略配置合并到每个接口的单个策略映射中。

  但是，您也可以使用 FlexConfig 手动创建策略映射。对于低端防火墙（例如 Cisco Secure Firewall 3100），您可以在配置中创建多达 64 个策略映射。对于功能更强大的防火墙（例如 Firepower 4100），您最多可以创建 128 个策略映射。请注意不要超过此限制，否则部署将失败。您可以从 CLI 查看设备配置，也可以使用部署脚本查看如何将规则转换为命令。

配置威胁防御服务策略

您可以使用威胁防御服务策略将服务应用到特定流量类别。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

过程

步骤 1 选择 **策略** > **安全策略** > **访问控制**，点击要编辑其威胁防御服务策略的访问控制策略的 **编辑** (✎)。

步骤 2 从数据包流末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

步骤 3 点击**威胁防御服务策略 (Threat Defense Service Policy)** 组中的 **编辑** (✎)。

系统将打开一个对话框，显示现有策略。该策略由有序的规则列表组成，这些规则分为全局规则（适用于所有接口）和基于接口的规则。表格中显示了接口对象和扩展访问控制列表名称（其组合定义规则的流量类）以及所应用的服务。

步骤 4 执行以下任一操作：

- 点击**添加规则**以创建新规则。请参阅配置服务策略规则，第 2476 页。
- 点击**编辑** (✎)以编辑现有规则。请参阅配置服务策略规则，第 2476 页。
- 点击 **删除** (🗑) 以删除规则。
- 点击规则并将其拖动到新位置，以移动规则。您无法在接口和全局列表之间拖动规则，而是必须编辑规则以更改接口/全局设置。列表中与连接匹配的第一条规则将应用于连接。

步骤 5 完成策略编辑后，点击**确定** 。

步骤 6 在**高级**选项卡窗口中点击**保存**。在您点击保存之前，更改不会被保存。

配置服务策略规则

配置服务策略规则，以将服务应用于特定流量类。

开始之前

转到**对象** > **访问列表** > **扩展**并创建扩展访问列表，定义规则适用的流量。此规则适用于与扩展访问列表中的“允许”规则匹配的任何连接。准确定义ACL规则，以便您的服务策略规则仅适用于需要该服务的流量。

如果要创建基于接口的规则，则还必须在已分配的设备上配置接口，并将其添加到安全区域或接口组。

过程

步骤 1 如果尚未在“威胁防御服务策略”对话框中，请选择 **策略** > **安全策略** > **访问控制**，编辑访问控制策略，从数据包流行末尾的**更多**下拉箭头中选择**高级设置**，然后编辑**威胁防御服务策略**。

步骤 2 执行以下任一操作：

- 点击**添加规则**以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

系统将打开服务策略规则向导，逐步指导您完成配置规则的流程。

步骤 3 在**接口对象**步骤中，选择用于定义将使用此策略的接口的选项。

- **全局应用** - 选择此选项以创建适用于所有接口的全局规则。
- **选择接口对象** - 选择此选项以创建基于接口的规则。然后，选择包含所需接口的安全区域或接口对象，并点击**添加**以将其移到所选列表。系统将在所选对象中包含的每个接口上配置此服务策略规则；而不是在区域/组本身配置此规则。

满足接口条件后，点击**下一步**。

步骤 4 在**流量传输 (Traffic Flow)** 步骤中，选择用于定义规则适用的连接的扩展 ACL 对象，然后点击**下一步 (Next)**。

步骤 5 在**连接设置**步骤中，配置要应用于此流量类的服务。

- **启用 TCP 状态绕行**（仅适用于 TCP 连接）- 实施 TCP 状态绕行。任何检测引擎都不会检查受 TCP 状态绕行影响的连接，它们会绕过所有 TCP 状态检查和 TCP 规范化。有关详细信息，请参阅绕过非对称路由的 TCP 状态检查（TCP 状态绕行），第 2479 页。

  注释
  在进行故障排除或无法解析非对称路由时使用 TCP 状态绕行。此功能将禁用多项安全功能，如果您没有使用狭义定义的流量类正确实施该功能，则可能会导致大量连接。

- **随机生成 TCP 序列号**（仅适用于 TCP 连接）- 启用还是禁用 TCP 序列号随机化。默认情况下启用随机化。有关详细信息，请参阅禁用 TCP 序列随机化，第 2483 页。
- **启用递减 TTL**（仅适用于 TCP 连接）- 减少与类匹配的数据包的生存时间 (TTL)。如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包

含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。

注释
如果希望 Firewall Threat Defense设备显示在跟踪路由中，必须配置递减 TTL 选项并在平台设置策略中设置 ICMP 不可达速率限制。请参阅使 Firewall Threat Defense 设备显示在跟踪路由上，第 2487 页。

- **连接** - 整个类允许的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 整个类允许的最大同步 TCP 或 UDP 连接数，该值介于 0 到 2000000 之间。对于 TCP，这仅适用于已建立的连接。默认值为 0，允许无限制连接。由于限制适用于一个类，一台攻击主机可占用所有连接而且使其余所有主机无法与该类匹配。设置每个客户端的限制，以缓解这一问题。
  - **最大初期连接数**（仅适用于 TCP 连接）- 允许的最大同步初期 TCP 连接数（未完成 TCP 握手的连接数），该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。通过设置非零限制启用 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。另外，请设置每客户端选项，以防止SYN泛洪。有关详细信息，请参阅保护服务器免受 SYN 洪水 DoS 攻击（TCP 拦截），第 2485 页。
- **每个客户端连接数** - 指定客户端（源 IP 地址）的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 每个客户端允许的最大同步连接数，该值介于 0 到 2000000 之间。对于 TCP 连接，这包括现有、半开和半闭连接。默认值为 0，允许无限制连接。此选项限制与类匹配的每台主机所允许的最大同步连接数。
  - **最大初期连接数**（仅适用于 TCP 连接）- 每个客户端允许的最大同步初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。有关详细信息，请参阅保护服务器免受 SYN 洪水 DoS 攻击（TCP 拦截），第 2485 页。
- **连接同步 Cookie MSS (Connections Syn Cookie MSS)** - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当您为连接和/或每个客户端配置了**最多初期连接次数 (Maximum Embryonic)** 时，此设置才有意义。
- **连接超时** - 要应用于流量类的超时设置。这些超时设置会覆盖平台设置策略中定义的全局超时设置。您可以配置以下内容：
  - **初期连接数**（仅适用于 TCP 连接）- TCP 初期（半开）连接关闭之前的超时时间，该值介于 0:0:5 到 1193:00:00 之间。默认值为 0:0:30。
  - **半闭**（仅适用于 TCP 连接）- 半闭连接关闭之前经过的空闲超时时间，该值介于 0:0:30 到 1193:0:0 之间。默认值为 0:10:0。半闭连接不受失效连接检测 (DCD) 影响。此外，如果取消半闭连接，系统将不发送重置消息。
  - **空闲**（仅适用于 TCP、UDP、ICMP、IP 连接）- 任何协议的已建立连接关闭之前经过的空闲超时时间，该值介于 0:0:1 到 1193:0:0 之间。除非您选择“TCP 状态绕行”选项（其中默认值为 0:2:0），否则默认值为 1:0:0。

- **超时后重置连接**（仅适用于 TCP 连接）- 是否在空闲连接删除后将 TCP RST 数据包发送到两个终端系统。

- **检测失效连接**（仅限 TCP 连接）- 是否启用失效连接检测 (DCD)。在空闲连接失效前，系统会探测终端主机以确定连接是否有效。如果两台主机均响应，系统会保留连接，否则会释放连接。在透明防火墙模式下运行，必须为终端配置静态路由。您无法在也已分流的连接上配置DCD，因此请勿在预过滤器策略中的快速路径连接上配置 DCD。在 Firewall Threat Defense CLI 中使用 **show conn detail** 命令跟踪发起方和响应方发送的 DCD 探测数量。

  配置以下选项：

  - **检测超时** - 每个 DCD 探测器无响应之后发送另一个探测器之前的等待时间（采用 hh:mm:ss 格式），该值介于 0:0:1 到 24:0:0 之间。默认值为 0:0:15。

    对于在集群或高可用性配置中运行的系统，我们建议您不要将间隔设置为小于一分钟(0:1:0)。如果需要在系统之间移动连接，则所需的更改需要花费超过30秒，并且连接可能会在完成更改之前被删除。

  - **检测重试次数** - DCD 在宣称连接为失效连接之前可连续失败重试的次数，该值介于 1 到 255 之间。默认值为 5。

步骤 6 点击**完成**以保存所做的更改。

此规则将添加到相应列表的底部，即接口或全局。全局规则以自上而下的顺序匹配。接口列表中的规则按自上而下的顺序匹配每个接口对象。请将狭义定义的流量类的规则置于更广泛的规则之上，以确保应用正确的服务。您可以通过拖放操作在每个列表中移动规则。您无法在列表之间移动规则。

绕过非对称路由的 TCP 状态检查（TCP 状态绕行）

如果网络中有非对称路由环境，其中给定连接的出站和入站流量可通过两个不同的Firewall威胁防御设备，则需要在受影响的流量上实施 TCP 状态绕行。

但是，TCP 状态绕行会削弱网络安全性，因此应在非常具体的有限流量类上应用绕行。

以下主题详细介绍该问题和解决方案。

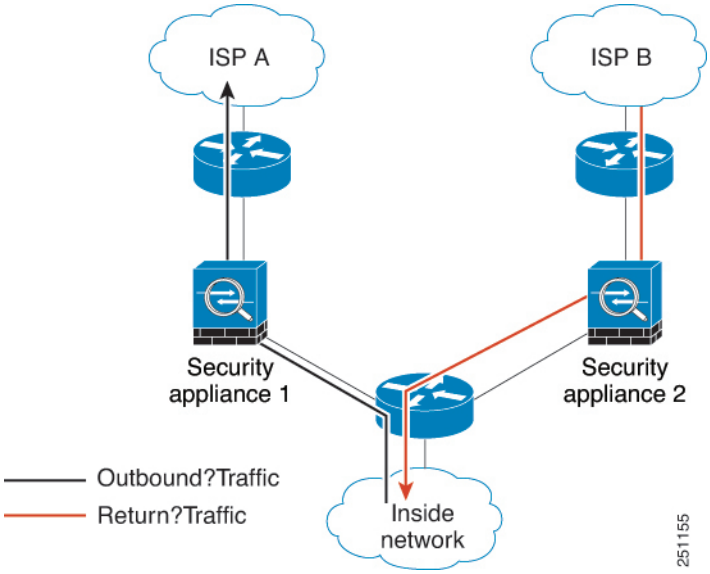
非对称路由问题

默认情况下，所有经过 Firewall 威胁防御 的流量都会使用自适应安全算法检查，并根据安全策略允许通过或予以丢弃。Firewall 威胁防御 通过检查每个数据包的状态（新连接还是现有连接）并将其分配到会话管理路径（新连接SYN数据包）、快速路径（现有连接）或控制平面路径（高级检测），最大程度地提高防火墙性能。

匹配快速路径中现有连接的 TCP 数据包，不重新检查安全策略的每个方面即可通过 Firewall 威胁防御。此功能可最大程度地提高性能。但是，使用SYN数据包在快速路径中建立会话的方法，以及在快速路径中进行的检查（例如TCP序列号），可能会阻碍非对称路由解决方案：出站和入站连接流必须通过同一 Firewall 威胁防御 。

例如，有一个新连接传入安全设备 1。SYN 数据包通过会话管理路径，而且连接的条目添加到快速路径表中。如果此连接的后续数据包通过安全设备 1，则这些数据包与快速路径中的该条目匹配，可以通过。但是，如果后续数据包传入安全设备 2，其中没有经过会话管理路径的 SYN 数据包，则快速路径中没有该连接的条目，数据包将被丢弃。下图显示一个不对称路由示例，其中，出站流量通过一个与入站流量不同的 Firewall 威胁防御：

图 *453:* 非对称路由



如果在上游路由器中配置了不对称路由，且流量在两个 Firewall 威胁防御 之间交替，则可以为特定流量配置 TCP 状态绕行。TCP 状态绕行将改变会话在快速路径中建立的方式，并且禁用快速路径检查。此功能按处理 UDP 连接的大致方式来处理 TCP 流量：当匹配指定网络的非 SYN 数据包进入 Firewall 威胁防御 时，其中没有快速路径条目，该数据包将通过会话管理路径在快速路径中建立该连接。流量到达快速路径后，将绕过快速路径检查。

有关 TCP 状态绕行的准则和限制

TCP 状态绕行不支持的功能

使用 TCP 状态绕行时不支持以下功能：

- 应用检测 - 检测要求入站和出站流量通过同一 Firewall 威胁防御，因此不会对 TCP 状态绕行流量应用检测。
- Snort 检测 - 检测要求入站和出站流量通过同一设备。但是，对于 TCP 状态绕行流量，不会自动绕过 Snort 检测。还必须针对您配置 TCP 状态绕行的相同流量类配置预过滤器快速路径规则。否则，数据包可能会被意外丢弃，因为 TCP 规范器也未启用。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - Firewall 威胁防御 不跟踪连接的状态，因此不会应用这些功能。
- TCP 标准化 - 禁用 TCP 规范器。

- 在内联或内联分流接口上使用 TCP 状态绕行时，无法使用 TLS 服务器身份发现。

TCP 状态绕行 NAT 准则

由于转换会话是为每个设备单独建立，请务必在两个设备上均为 TCP 状态绕行流量配置静态 NAT。如果使用动态 NAT，则在设备 1 上为会话选择的地址将与在设备 2 上为会话选择的地址不同。

配置 TCP 状态绕行

要在非对称路由环境中绕过 TCP 状态检查，请仔细定义仅适用于受影响主机或网络的流量类，然后通过服务策略在该流量类上启用 TCP 状态绕行。您还必须为相同的流量配置相应的预过滤器快速路径策略，以确保此流量也绕过检查。

由于绕行会降低网络安全性，请尽可能限制网络应用。

过程

步骤 1 创建定义流量类的扩展 ACL。

例如，要为从 10.1.1.1 到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象** > **访问列表** > **扩展**。
b) 点击**添加扩展访问列表**。
c) 为对象输入一个**名称**，例如 bypass。
d) 点击**添加**以添加规则。
e) 保持**允许**操作。
f) 在**源**列表下方输入 10.1.1.1 并点击**添加 (Add)**，然后在**目标**列表下方输入 10.2.2.2 并点击**添加 (Add)**。
g) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
h) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
i) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置 TCP 状态绕行服务策略规则。

例如，要为此流量类全局配置 TCP 状态绕行，请执行以下操作：

a) 选择**策略** > **安全策略** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用**，然后点击**下一步**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 选择**启用 TCP 状态绕行**。
g) （可选。）调整绕行连接的**空闲**超时。默认值为 2 分钟。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。

i) 点击**确定** 以保存对服务策略所做的更改。

j) 点击**高级 (Advanced)** 中的**保存**，以保存对访问控制策略所做的更改。

步骤 3 配置流量类的预过滤器快速路径规则。

不能在预过滤器规则中使用ACL对象，因此您需要直接在预过滤器规则中重新创建流量类，或者通过首先创建定义类的网络对象来创建流量类。

以下程序假定您已经在访问控制策略中附加了预过滤器策略。如果尚未创建预过滤器策略，请转至**策略 (Policies)** > **预过滤器 (Prefilter)**，然后首先创建策略。然后，您可以按照此程序将其附加到访问控制策略并创建规则。

在我们的示例中，此程序为 10.1.1.1 到 10.2.2.2 的 TCP 流量创建快速路径规则。

a) 选择**策略** > **安全策略** > **访问控制**，然后编辑具有 TCP 绕行服务策略规则的策略。

b) 点击**预过滤器策略**链接，该策略位于策略说明的左下方。

c) 在“预过滤器策略”对话框中，选择要分配给设备的策略（如果尚未选择正确的策略）。不要点击“确定”。

由于您无法将规则添加到默认预过滤器策略，因此必须选择自定义策略。

d) 在“预过滤器策略”对话框中，点击**编辑**(✎)。此操作将打开一个新的浏览器窗口，您可以在其中编辑策略。

e) 点击**添加预过滤器规则**并配置包含以下属性的规则。

- **名称** - 您觉得有意义的任何名称均可，例如 TCPBypass。
- **操作** - 选择**快速路径**。
- **接口对象 (Interface Objects)** - 如果已将 TCP 状态绕行配置为全局规则，则为源和目标接口保留默认值“any”。如果已创建基于接口的规则，则在**源接口对象**列表中选择用于规则的相同接口对象，并将“any”作为目标接口。
- **网络 (Networks)** - 将 10.1.1.1 添加到**源网络 (Source Networks)** 列表中，并将 10.2.2.2 添加到**目标网络 (Destination Networks)** 列表中。您可以使用网络对象或手动添加地址。
- **端口 (Ports)** - 在**选定源端口 (Selected Source Ports)** 下, 选择 TCP(6)，**不要输入端口**，然后点击**添加 (Add)**。这会将规则应用于所有（且仅限）TCP 流量（不考虑 TCP 端口号）。

f) 点击**添加**以将规则添加到预过滤器策略中。

g) 点击**保存**以保存对预过滤器策略所做的更改。

现在您可以关闭预过滤器编辑窗口并返回访问控制策略编辑窗口。

h) 在访问控制策略编辑窗口中，“预过滤器策略”对话框仍处于打开状态。点击**确定** 以保存对预过滤器策略分配所做的更改。

i) 如果您做出了更改，则点击访问控制策略上的**保存**以保存已更改的预过滤器策略分配。

现在您可以将更改部署到受影响的设备。

禁用 TCP 序列随机化

每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。Firewall Threat Defense设备会为通过入站和出站两个方向的 TCP SYN 随机生成 ISN。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。但是，TCP 序列随机化有效地破坏了 TCP SACK（选择性确认），因为客户端看到的序列号与服务器看到的序列号不同。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。以下是您可能希望禁用随机化的一些情况：

- 如果另一个在线防火墙也随机化初始序列号，则即使此操作不影响流量，两个防火墙也无需执行此操作。
- 如果通过此设备使用 eBGP 多跳，并且 eBGP 对等设备在使用 MD5。随机化会中断 MD5 校验和。
- 如果使用要求设备不为连接随机生成序列号的 WAAS 设备。
- 如果为 ISA 3000 启用硬件旁路，当 ISA 3000 不再是数据路径时的一部分时，TCP 连接将被丢弃。

过程

步骤 1 创建定义流量类的扩展 ACL。

例如，要从任何主机到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象** > **访问列表** > **扩展**。
b) 点击**添加扩展访问列表**。
c) 为对象输入一个**名称**，例如 preserve-sq-no。
d) 点击**添加**以添加规则。
e) 保持**允许**操作。
f) 将**源 (Source)** 列表留空，在**目标 (Destination)** 列表下方输入 10.2.2.2，然后点击**添加 (Add)**。
g) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
h) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
i) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置将禁用 TCP 序列号随机化的服务策略规则。

例如，要为此流量类全局禁用随机化，请执行以下操作：

a) 选择**策略** > **安全策略** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则 (Add Rule)**。

d) 选择**全局应用**，然后点击**下一步**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 取消选择**随机生成 TCP 序列号**。
g) （可选。）根据需要调整其他连接选项。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
i) 点击**确定** 以保存对服务策略所做的更改。
j) 点击**高级 (Advanced)** 中的**保存**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

监控服务策略

您可以使用设备 CLI 监控服务策略相关信息。以下是一些有用的命令。

- **show conn** [**detail**]

  显示连接信息。详细信息使用标志来表示特殊连接特性。例如，“b”标志表示会对流量应用 TCP 状态绕行。

  使用 **detail** 关键字时，您可以查看有关失效连接检测 (DCD) 探测的信息，这会显示发起方和响应方探测连接的频率。例如，对于启用 DCD 的连接，其连接详细信息如下所示：

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  显示服务策略统计信息，包括失效连接检测 (DCD) 统计信息。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  查看遭受攻击的前 10 名受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史采样数据。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。

服务策略规则示例

以下主题提供服务策略规则示例。

保护服务器免受 SYN 洪水 DoS 攻击（TCP 拦截）

当攻击者将一系列 SYN 数据包发送到主机时，即表示发生 SYN 泛洪拒绝服务 (DoS) 攻击。这些数据包通常来自虚假 IP 地址。SYN 数据包的持续泛洪将使服务器 SYN 队列始终处于充满状态，而无法处理来自合法用户的连接请求。

可以限制初期连接的数量，这样有助于防止SYN泛洪攻击。半开连接是源与目标之间尚未完成必要握手的连接请求。

当超过连接的初期连接阈值时， Firewall Threat Defense 将充当服务器代理，使用 SYN cookie 方法向客户端 SYN 请求生成 SYN-ACK 响应，使该连接不加入到目标主机的 SYN 队列中。SYN Cookie 是在SYN-ACK 中返回的初始序列号，它由MSS、时间戳和其他项目的数学散列构成，用于创建密钥。如果在有效的时间窗口内 Firewall Threat Defense 收到来自客户端的具有正确序列号的 ACK，可以对实际客户端的真实性进行身份验证，并且允许连接到服务器。执行代理的组件称为 TCP 拦截。

设置连接限制可以保护服务器免受 SYN 泛洪攻击。或者，您可以选择启用 TCP 拦截统计信息并监控策略的结果。以下程序介绍端到端流程。

开始之前

- 请确保设置的初期连接限制低于要保护的服务器上的 TCP SYN 积压工作队列。否则，在 SYN 攻击期间，有效客户端将无法访问服务器。为了确定初期限制的合理值，请仔细分析服务器容量、网络和服务器使用情况。
- 根据 Cisco Secure Firewall Threat Defense型号中 CPU 内核数量，由于每个内核管理连接的方式不同，最大并发和正在建立的连接可能超出配置的数量。在最糟糕的情况下，此设备最多允许 n-1 个额外连接和初期连接，其中 n 是内核数量。例如，如果设备型号有 4 个核心，而配置了 6 个并发连接和 4 个初期连接，那么每个类型可能有 3 个额外连接。要确定型号的内核数量，请在设备 CLI 中输入 **show cpu core** 命令。

过程

步骤 1 创建定义流量类的扩展 ACL，该列表是要保护的服务器列表。

例如，要定义流量类以使用 IP 地址 10.1.1.5 和 10.1.1.6 保护 Web 服务器，请执行以下操作：

a) 选择**对象** > **访问列表** > **扩展**。
b) 点击**添加扩展访问列表**。
c) 为对象输入一个**名称**，例如，protected-servers。
d) 点击**添加**以添加规则。
e) 保持**允许**操作。
f) 将**源 (Source)** 列表留空，在**目标 (Destination)** 列表下方输入 10.1.1.5，然后点击**添加 (Add)**。
g) 此外，在**目标 (Destination)** 列表下方输入 10.1.1.6，然后点击**添加 (Add)**。
h) 点击**端口 (Port)**，从可用端口列表中选择 **FMC_CONNECTION**，然后点击**添加到目标 (Add to Destination)**。如果您的服务器还支持 HTTPS 连接，还需添加此端口。
i) 点击 **添加** 以将规则添加至 ACL。

j) 点击**保存**保存 ACL 对象。

步骤 2 配置用于设置初期连接限制的服务策略规则。

例如，要将总并发初期连接限制设置为 1000 个并将每客户端的连接限制设置为 50 个，请执行以下操作：

a) 选择**策略** > **安全策略** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用**，然后点击**下一步**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 为**连接** > **最大初期连接数**输入 1000。
g) 为**每个客户端的连接数** > **最大初期连接数**输入 50。
h) （可选。）根据需要调整其他连接选项。
i) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
j) 点击**确定** 以保存对服务策略所做的更改。
k) 点击**高级 (Advanced)** 中的**保存**，以保存对访问控制策略所做的更改。

步骤 3 （可选。）配置 TCP 拦截统计信息的速率。

TCP 拦截使用以下选项来确定收集统计信息的速率。所有选项都具有默认值，因此如果这些速率符合您的需求，您可以跳过此步骤。

- 速率间隔 - 历史监控窗口的大小，该值介于 1 到 1440 分钟之间。默认值为 30 分钟。在此间隔期间，系统会进行 30 次攻击数量采样。
- 突发速率 - 系统日志消息生成的阈值，该值介于 25 到 2147483647 之间。默认值为每秒 400 条消息。超出突发速率时，设备将生成系统日志消息 733104。
- 平均速率 - 系统日志消息生成的平均速率阈值，该值介于 25 到 2147483647 之间。默认值为每秒 200 条消息。超出平均速率时，设备将生成系统日志消息 733105。

如果要调整这些选项，请执行以下操作：

a) 选择**对象** > **FlexConfig** > **文本对象**。
b) 点击 **threat_defense_statistics** 系统定义对象的 **编辑** (✎)。
c) 虽然您可以直接更改值，但建议的方法是打开**覆盖**部分，然后点击**添加**以创建设备覆盖。
d) 选择要为其分配服务策略的设备（通过访问控制策略分配），然后点击**添加**以将其移动到所选列表中。
e) 点击**覆盖 (Override)**。
f) 此对象必须有 3 个条目，因此请根据需要点击**计数 (Count)**，直至获得 3 个条目。
g) 按照 1-3 的顺序输入所需的值作为速率间隔、突发速率和平均速率。请参阅对象说明以验证您是否按正确的顺序输入值。
h) 在“对象覆盖”对话框中点击**添加 (Add)**。
i) 在“编辑文本对象”对话框中点击**保存**。

步骤 4 启用 TCP 拦截统计信息。

您必须配置 FlexConfig 策略以启用 TCP 拦截统计信息。

a) 选择**设备** > **+ 显示更多** > **FlexConfig**。
b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新策略并将其分配给受影响的设备。
c) 选择**可用 FlexConfig** 列表中的 **Threat_Detection_Configure** 对象，然后点击 **>>**。此对象将添加到**所选附加 Flexconfig** 列表中。
d) 点击**保存**。
e) （可选。）您可以通过点击**预览配置**并选择其中一个设备来验证是否具有正确的设置。

系统会生成将在下次部署期间写入设备的 CLI 命令。这些命令将包括服务策略所需的命令以及威胁检测统计信息所需的命令。滚动到预览的底部以查看附加的CLI。如果使用默认值，TCP拦截统计信息命令应如下所示（为清晰起见已添加换行符）：

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

步骤 5 现在您可以将更改部署到受影响的设备。

步骤 6 使用以下命令从设备 CLI 监控 TCP 拦截统计信息：

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 查看遭受攻击的前 10 台受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史采样数据。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。

  注释
  您可以使用 **shun** 命令阻止攻击主机 IP 地址。要删除阻止列表，请使用 **no shun** 命令。

- **clear threat-detection statistics tcp-intercept**- 清除 TCP 拦截统计信息。

示例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

使 Firewall Threat Defense 设备显示在跟踪路由上

默认情况下，Firewall Threat Defense不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，必须配置服务策略规则并调整 ICMP 平台设置策略。

注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

步骤 1 创建扩展 ACL，以定义要为其启用跟踪路由报告的流量类。

例如，要为所有地址（但不包括 OSPF 流量）定义流量类，请执行以下操作：

a) 选择**对象** > **访问列表** > **扩展**。
b) 点击**添加扩展访问列表**。
c) 为对象输入一个**名称**，例如，traceroute-enabled。
d) 点击**添加**以添加规则，从而排除 OSPF。
e) 将操作更改为**阻止 (Block)**，点击**端口 (Port)** 选项卡，选择 **OSPFIGP (89)** 作为**目标端口 (Destination Ports)** 列表下方的协议，然后点击**添加 (Add)** 将此协议添加到所选列表。
f) 在“扩展访问列表条目”对话框中点击**添加**，以将 OSPF 规则添加到 ACL。
g) 点击**添加**以添加规则，从而包含所有其他连接。
h) 保持**允许**操作，并将“源”和“目标”列表留空。
i) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。

确保 OSPF 拒绝规则优先于“允许所有”规则。如有必要，拖放以移动规则。

j) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

步骤 2 配置用于递减生存时间值的服务策略规则。

例如，要全局递减生存时间，请执行以下操作：

a) 选择**策略** > **安全策略** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则 (Add Rule)**。
d) 选择**全局应用**，然后点击**下一步**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 选择**启用递减 TTL**。
g) （可选。）根据需要调整其他连接选项。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
i) 点击**确定** 以保存对服务策略所做的更改。
j) 点击**高级 (Advanced)** 中的**保存**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

步骤 3 增加 ICMP 不可达消息的速度限制。

a) 选择**设备** > **平台设置**。
b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新的威胁防御平台设置策略并将其分配给受影响的设备。
c) 从目录中选择 **ICMP**。
d) 增加**速率限制**，例如，增加至 50。您可能还希望将 **突发大小** 增加到 10，以确保在速率限制内生成足够的响应。

   您可以将 ICMP 规则表留空，它与此任务无关。

e) 点击**保存**。

步骤 4 现在您可以将更改部署到受影响的设备。

威胁防御服务策略的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	说明
威胁防御服务策略。	6.3	任意	您现在可以将威胁防御服务策略配置为访问控制策略高级选项的一部分。您可以使用威胁防御服务策略将服务应用到特定流量类别。支持的功能包括 TCP 状态绕过、随机化 TCP 序列号、递减数据包上的生存时间 (TTL) 值、死连接检测、为每个流量类别和每个客户端设置最大连接数和半开连接数限制，以及为半开、半关闭和空闲连接设置超时。 新屏幕： **策略** > **访问控制** > **访问控制**、 **高级** 选项卡， **威胁防御服务策略**。 支持的平台： Cisco Secure Firewall Threat Defense
死连接检测 (DCD) 的发起方和响应方信息，以及集群中的 DCD 支持。	6.5	任意	如果启用死连接检测 (DCD)，您可以使用 **show conn detail** 命令获取有关发起方和响应方的信息。死连接检测允许您维持不活动的连接，**show conn** 输出会告诉您端点被探测的频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出） 支持的平台： Cisco Secure Firewall Threat Defense
配置初期连接的最大分段大小 (MSS)。	7.1	任意	您可以配置服务策略，以在达到初期连接限制时为初期连接的SYN-Cookie设置服务器最大分段大小 (MSS)。这对于还设置初期连接最大值的服务策略非常重要。 新增或更改的屏幕：添加/编辑服务策略向导中的**连接设置**。



第 66 章

威胁检测

威胁检测的端口扫描检测器是一种机制，旨在帮助您检测和阻止所有类型流量中的端口扫描活动，以保护网络免受潜在攻击。可以在允许和拒绝的流量中高效检测 Portscan 流量。

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者确定主机支持的网络协议或服务类型，并将特制数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

- 端口扫描检测和预防， 第 2491 页
- 威胁检测的要求和先决条件， 第 2493 页
- 威胁检测准则和限制， 第 2494 页
- 端口扫描防护最佳实践， 第 2494 页
- 配置端口扫描检测和预防， 第 2495 页
- 监控威胁检测， 第 2497 页
- 威胁检测的历史记录， 第 2499 页

端口扫描检测和预防

使用威胁检测识别端口扫描活动。您可以使用系统检测端口扫描，并在发现端口扫描时发出事件。或者，您可以将系统配置为通过自动阻止扫描程序来阻止端口扫描。在阻止端口扫描时，系统会向您发送事件，并在您设置的持续时间段内阻止攻击者。

端口扫描检测的预定义敏感度级别

配置检测设置时，您可以选择以下预定义的灵敏度级别。除“自定义”外，每个级别都为每个协议的端口 (TCP/UDP)、协议 (IP) 或主机 (TCP/UDP/IP/ICMP) 数预设了必须在设定的时间间隔内扫描的值（以秒为单位）。此外，还会启用所有类型的扫描/清扫。

注释 在对端口/协议进行计数时，如果当前数据包中的端口/协议与前一个数据包不同，威胁检测就会让数字递增。例如，如果您有一个应用会随机打开10个端口的连接，那么扫描的端口总数可能会迅速增加，以至于您的端口数会在时间间隔内被超过。系统不会仅对唯一端口进行计数。

超过间隔内的数字可能表示扫描攻击。仅当超出移动时间间隔窗口的端口/协议/主机号时，才会生成端口扫描事件。

- 低- 此级别使用端口扫描检测的最短时间窗口，并为端口/协议/主机加上高计数。因此，您应该只看到最积极的扫描程序的端口扫描事件。选择此级别的灵敏度可抑制误报，但请记住，这样可能会遗漏某些类型的端口扫描（慢速扫描、过滤扫描）。有关低灵敏度检测工作原理的更多详细信息，请参阅 在低敏感度级别检测，第 2493 页。
  - 间隔 (TCP/UDP/IP/ICMP) - 60 秒。
  - **TCP/UDP portscan** 端口数-120。
  - **TCP/UDP** 端口清扫 主机数量-180。
  - **IP** 协议扫描协议数量-30。
  - **IP** 协议扫描主机数-25。
  - **ICMP** 主机扫描主机数-50。
- 中- 此级别对间隔和端口/协议/主机计数使用中等值。但是，非常活跃的主机（例如网络地址转换器和代理）可能会生成误报。将此类主机添加到忽略扫描程序列表。这是默认的敏感度级别，也是一个很好的起点。
  - 间隔 (TCP/UDP/IP/ICMP) - 90 秒。
  - **TCP/UDP portscan** 端口数-90。
  - **TCP/UDP** 端口清扫 主机数量-150。
  - **IP** 协议扫描协议数量-15。
  - **IP** 协议扫描主机数-20。
  - **ICMP** 主机扫描主机数-30。
- 高- 此级别为端口扫描检测使用更长的时间窗口，并为端口/协议/主机提供较低的计数。使用此级别，即使是最不严格的端口扫描/清扫，您也最有可能看到事件，因此您更有可能注意到所有攻击者。另一方面，此级别可能会导致发出大多数端口扫描事件，并可能导致最高数量的误报。
  - 间隔 (TCP/UDP/IP/ICMP) - 600 秒（10 分钟）。
  - **TCP/UDP portscan** 端口数-60。
  - **TCP/UDP** 端口清扫主机数量-100。
  - **IP** 协议扫描协议数量-10。

- **IP 协议扫描主机数**-10。
- **ICMP 主机扫描主机数**-20。

- **自定义**- 如果要配置与某个预定义灵敏度级别不同的任何设置，或者要禁用特定类型的扫描/清扫，级别会自动切换到“自定义”。如果要调整选项，请先选择与所需选项最匹配的级别，然后根据需要编辑值。

在低敏感度级别检测

如果选择低灵敏度级别，系统则跟踪 TCP、UDP 和 ICMP 初始数据包的否定响应。仅当不成功的连接数超过拒绝阈值（低灵敏度时为 10%）且端口/IP 协议计数超过配置的阈值时，才会触发警报。这可以减少误报。

拒绝阈值仅适用于低灵敏度（或同等的自定义设置）；不适用于其他灵敏度级别或同等的自定义设置。

如果同时存在允许和阻止的流量，则根据允许和阻止的流量之间的差异计算拒绝端口或主机的数量。在仅阻止流量的情况下，不考虑拒绝阈值。

这些条件不适用于内联集中配置的接口上的 UDP/ICMP 连接。

例如，在低灵敏度模式下，端口计数阈值为 120。因此，拒绝计数阈值为 120 的 10%，即 12。以下是在此配置下系统如何发出端口扫描事件的示例：

- 攻击者发起与目标的 131 个端口的连接，目标肯定确认所有发起。端口计数 = 131，大于阈值，但由于没有否定确认，因此不会触发端口扫描警报。
- 攻击者发起与目标的 131 个端口的连接，目标肯定确认 121 次发起，否定确认 10 次。端口计数 = 131，大于阈值，但拒绝端口计数 = 10，小于拒绝阈值。因此，不会触发端口扫描警报。
- 攻击者发起与目标的 134 个端口的连接，目标肯定确认 121 次发起，否定确认 13 次。端口计数 = 134，大于阈值，拒绝端口计数 = 13 也高于拒绝阈值。因此，会触发端口扫描警报。

威胁检测的要求和先决条件

型号支持

Firewall Threat Defense 运行版本 7.2+ 和 Snort 3。

支持的域

任意

用户角色

管理员

访问管理员

网络管理员

威胁检测准则和限制

- 威胁检测需要 Snort 3。对于运行 Snort 3 的设备，NAP 端口扫描配置始终被忽略；您必须使用威胁检测来配置端口扫描。对于 Snort 2，只能通过 NAP 策略配置端口扫描。如果有运行 Snort 2 的设备分配给访问控制策略，威胁检测设置将不会部署到这些不受支持的设备。
- 威胁检测仅适用于通过设备的流量。它不适用于定向到设备的流量。
- 在高可用性设置中，端口扫描统计信息不会同步到备用设备。但是，被阻止的主机将同步并继续被阻止，直到持续时间到期，以防发生故障切换。
- （运行 威胁防御 版本 7.2-7.7 的设备）。对于集群中的节点，检测和防御在单个集群节点上进行。也就是说，如果节点 B 检测到并阻止来自主机的流量，节点 A 不会注意到该操作，因为端口扫描统计信息不会在集群节点之间同步。
- （运行 威胁防御 版本 10.0+ 的设备）。对于集群中的节点，检测和预防在集群级别进行。当跨节点或在单个节点中发生端口扫描时，可以检测到端口扫描。被隔离的主机在集群中的所有设备上被隔离。隔离在所有节点上同时释放。统计信息在集群级别可用。
- 对于内联集，或配置为等价多路径 (ECMP) 流量区域的接口，检测和防护均在区域级别进行。跨区域的所有接口累积主机的端口扫描统计信息。同样，当主机超过配置的阈值时，会在相应区域的所有接口上被阻止。
- 尽管威胁检测功能生成的端口扫描事件与 Snort 为端口扫描发出的事件相同，但无需启用端口扫描入侵规则即可获取这些事件。无论您的入侵策略实施如何，威胁检测都能正常工作。

端口扫描防护最佳实践

端口扫描预防模式可能会导致流量意外中断。在防护模式下，主机被阻止在配置的持续时间内对所有协议上的网络进行进一步扫描。请仔细查看检测和防御参数，确保合法流量未被阻止。

在防护模式下配置端口扫描前，我们强烈建议：

1. 先在检测模式下使用端口扫描。
2. 观察生成的端口扫描事件。
3. 调整灵敏度级别、受监控网络、忽略扫描器列表和忽略目标列表。如果预定义的敏感度级别不适用于您的情况，请根据需要配置自定义设置。
4. 重复此过程，直到消除误报，并且事件速率可以准确反映网络中的端口扫描。确保您熟悉如何阻止已识别的其余扫描程序。

配置端口扫描检测和预防

端口扫描是一种通常被攻击者用作攻击前奏的网络侦察形式。在端口扫描中，攻击者确定主机支持的网络协议或服务类型，并将特制数据包发送到目标主机。通过检查主机响应时所用的数据包，攻击者通常可以直接或通过推理确定主机上的哪些端口是开放的，以及哪种应用协议正在这些端口上运行。

您可以启用威胁检测以监视端口扫描活动，也可以选择在一段时间内自动阻止扫描程序。

开始之前

端口扫描配置不支持 FQDN、通配符掩码、any、any-ipv4 和 any-ipv6 网络对象。这些对象不会显示在**监控 (Monitor)**、**忽略扫描程序 (Ignore Scanner)**、**忽略目标 (Ignore Target)** 和**排除 (Exclude)** 字段下。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的**更多** 下拉箭头中点击**高级设置**。然后，点击**威胁检测**旁边的 **编辑** (✎) 。

步骤 2 在 **威胁检测** 窗口中，选择 **端口扫描模式：**

- **禁用** - 关闭威胁检测。该模式为默认模式。您可以点击 **恢复到默认** 以恢复到此未配置状态。
- **检测**-执行端口扫描检测，但仅在出现问题时发出警报。请勿对潜在的攻击者执行操作。我们建议您最初使用此模式，直到微调威胁检测设置以避免过多的误报。
- **防御**- 执行端口扫描检测并主动阻止已识别的扫描程序，即正在执行端口扫描的主机。

步骤 3 配置 **流量选择** 选项。

流量选择选项确定要监控的网络、监控的连接类型，以及是否应从受监控网络排除任何扫描程序或目标主机。默认情况下，系统会监控所有网络上允许的连接。

- **流量检测**- 选择将监控端口扫描活动的连接类型： **允许**、 **拒绝**或 **所有** 流量。默认为**允许**。
- **监控**- 选择定义要监控端口扫描或清扫活动的网络的网络对象。默认值为任何网络、IPv4 或 IPv6。使用此选项可限制对不受信任网络的扫描。
- **忽略扫描程序**-从受监控网络的范围内选择定义应忽略的主机或网络的网络对象。例如，如果您设置了自己的扫描仪来测试网络，则可以豁免扫描仪的地址，以避免不必要的地址报告。请勿包含受监控网络外部的地址，因为这些地址已被忽略。
- **忽略目标**-选择定义应作为目标忽略的主机或网络（即端口扫描或清扫的受害者）的网络对象。

步骤 4 点击 **配置** 选项卡，然后选择扫描灵敏度级别。

预定义的敏感度级别**低**、**中**和**高**将端口扫描选项设置为越来越严格的值。例如，如果选择“低”，预计会看到更少的端口扫描事件，并且比选择“中”或“高”时更容易漏掉攻击者。另一方面，如果选择“高”，您可能会看到更多事件，也可能会出现更多误报。默认级为“中”。有关级别的信息，请参阅端口扫描检测的预定义敏感度级别，第 2491 页。

选择级别时，您可以在协议部分中看到相关值：**TCP**、**UDP**、**IP**和 **ICMP**。如果更改任何预设值或禁用某种类型的扫描，灵敏度模式会自动更改为“**自定义**”。

在每个协议部分中，选项包括：

- **间隔**- 超出为端口扫描或端口清扫配置的值的时间范围（以秒为单位）。例如，如果选择 90 秒和 60 作为 TCP 端口扫描端口数，则扫描程序需要在 90 秒内尝试主机上的 60 个端口，才会被视为端口扫描。仅当超过指定间隔内的端口、协议或主机数（对于端口清扫）时，系统才会生成事件。

  您可以指定 30-600 秒之间的范围。时间段越长，主机被识别为扫描程序的可能性就越大。

- **端口扫描** (TCP/UDP) - 选择是否监控单个主机的端口扫描，并指定在间隔内必须扫描的端口数，才能计为端口扫描攻击。允许的范围为 1-256。

- **端口清扫** (TCP/UDP) - 选择是否针对多个主机监控端口清扫，并指定在间隔内必须为给定端口扫描多少主机才能计为端口清扫攻击。允许的范围为 1-256。

- **协议扫描** (IP) - 选择是否监控单个主机的协议扫描，并指定在间隔内必须扫描的协议数，才能计为协议扫描攻击。允许的范围为 1-255。

- **协议扫描** (IP) - 选择是否监控多个主机的协议扫描，并指定在间隔内必须为给定协议扫描多少主机才能计为协议扫描攻击。允许的范围为 1-256。

- **主机清扫** (ICMP) - 选择是否针对多个主机监控 ICMP 主机清扫，并指定在间隔内必须扫描的主机数，才能将其计为主机清扫攻击。允许的范围为 1-256。

步骤 5 如果选择了防护模式，请点击 **防护** 选项卡并配置选项。

在预防模式下，会在配置的持续时间内自动阻止主机进一步扫描基于所有协议的网络。请仔细查看检测和防御参数，确保合法流量未被阻止。

- **排除**- 从受监控网络的范围内选择定义应从自动阻止中排除的主机或网络的网络对象。即使这些主机违反了您的扫描检测参数，系统也不会阻止它们。

- **持续时间**- 应阻止自动阻止的扫描程序主机通过设备发送任何类型的流量的时长（以秒为单位）。持续时间结束后，主机会自动清除，并且可以再次通过设备发送流量。允许的范围为 600-2592000 秒。默认值为 3600 秒（1 小时）。

  如果需要手动取消阻止主机，请通过 SSH 连接到阻止主机的防火墙，并使用 **clear threat-detection portscan attacker** 命令。

步骤 6 点击**确定**以保存威胁检测设置。

步骤 7 点击**保存** 保存访问控制策略。

下一步做什么

部署配置更改；请参阅 部署配置更改，第 180 页。

监控威胁检测

以下主题介绍如何监控端口扫描活动

查看端口扫描警报

端口扫描活动会通过现有端口扫描特定入侵事件来发出警报。会生成生成器 ID (GID) 为 122 且 Snort ID 为 1 至 27 的入侵事件。对于这些事件，在事件消息中会附加 *(port_scan)* 字符串。事件包括数据包信息以及包含触发警报的统计信息的数据包数据。

要查看端口扫描事件，请转至**事件和日志** > **+ 显示更多** > **入侵** > **事件**。

无论入侵策略或 NAP 配置如何，Portscan 都会发出这些事件。仅当扫描程序的数量超过为关联协议配置的时间间隔内为各种类型的扫描或清扫而配置的端口/协议/主机数时，才会发出事件。一旦达到阈值，来自一个主机的端口扫描就会在每个设置的间隔内生成一个事件。如果同一主机在同一间隔内启动新的端口扫描，则不报告任何事件。

下表显示了可能的事件。

表 *153:* 端口扫描事件

端口扫描类型	入侵事件
TCP 常规、欺骗、分布式扫描	122:1 (port_scan) TCP 端口扫描
TCP 端口清扫	122:3 (port_scan) TCP 端口清扫
TCP 分布式扫描	122:4 (port_scan) TCP 分布式端口扫描
IP 常规、欺骗、分布式协议扫描	122:9 (port_scan) IP 协议扫描
IP 协议清扫	122:11 (port_scan) IP 协议扫描
IP 分布式扫描	122:12 (port_scan) IP 分布式协议扫描
UDP 常规、欺骗、分布式扫描	122:17 (port_scan) UDP 端口扫描
UDP 端口清扫	122:19（port_scan）UDP 端口清扫
UDP 分布式扫描	122:20 (port_scan) UDP 分布式端口扫描
ICMP 扫描	122:25 (port_scan) ICMP 扫描
端口扫描阻止	122:100 (port_scan) 主机因端口扫描活动被阻止

在防火墙上监控端口扫描

要监控端口扫描，请登录设备 CLI 并使用以下命令。

- **show threat-detection portscan** [**attacker** | **target** | **shun**]

  显示扫描仪的 IP 地址、已避开（阻止）的扫描仪以及已成为扫描或清扫目标的主机。

- **show threat-detection portscan statistics** [**host** [*ipv4_address* | *ipv6_address*]] [**protocol** {**tcp** | **udp** | **ip** | **icmp**}]

  显示与端口扫描系统相关的统计信息。您可以指定主机、协议或主机和协议，以将输出过滤为所需的信息。

- **clear threat-detection portscan** [**attacker** | **target** | **shun**] [*ipv4_address mask* | *ipv6_address/prefix*]

  手动取消阻止扫描程序（攻击者）或识别的目标。输入不带参数的命令，以清除所有攻击者、目标或避开的主机。

- **clear threat-detection portscan statistics** [**host** [*ipv4_address* | *ipv6_address*]] [**protocol** {**tcp** | **udp** | **ip** | **icmp**}]

  清除与端口扫描相关的统计信息，以便您可以更清楚地查看通过此设备扫描的当前状态。输入不带参数的 命令以清除所有统计信息。或者，指定主机、协议或主机和协议，以将重置限制为指定项目。

取消阻止主机

如果在防御模式下配置威胁检测，并且系统阻止了您知道不是攻击者的主机，则可以在持续时间到期后自动取消阻止主机之前手动取消阻止该主机。

要手动取消阻止主机，请登录到主机被阻止的设备 CLI，然后输入 **clear threat-detection portscan attacks** 命令。例如：

```
> clear threat-detection portscan attacker 10.2.0.100 255.255.255.255
1 tracker object deleted and 1 shun entry removed
```

考虑将主机 IP 添加到防护配置中的“排除”列表。

威胁检测的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	说明
威胁检测对集群的支持。	10.0	10.0	现在可以在集群级别配置威胁检测。对于集群中的节点，检测和预防在集群级别进行。当跨节点或在单个节点中发生端口扫描时，可以检测到端口扫描。被隔离的主机在集群中的所有设备上被隔离。隔离在所有节点上同时释放。统计信息在集群级别可用。 威胁检测的配置方式没有变化。
改进了低灵敏度检测。	7.4	7.4	在低灵敏度级别运行时，识别端口扫描和清扫的方法已得到改进。更改是自动的；没有新的配置设置。
改进了端口扫描检测。	7.2	7.2 运行 Snort 3	通过改进的端口扫描检测器，您可以轻松地配置系统以检测或防止端口扫描。您可以细化要保护的网络，设置灵敏度等。对于运行 Snort 2 的设备以及运行版本 7.1 及更早版本的设备，请继续使用网络分析策略进行端口扫描检测。 新增/修改的屏幕：我们向访问控制策略的高级选项卡添加了 **威胁检测**。 新增/修改的命令：**clear threat-detection portscan**、**show threat-detection portscan**。



第 67 章

大象流检测

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的连续流通过网络链路测量。默认情况下，大象流是速率大于每 10 秒 1GB 的流。它们可能会在 Snort 核心中造成性能威胁。大象流并不多，但它们可以在一段时间内占总带宽的不成比例。它们可能导致问题，例如CPU 占用、丢包等。

从 防火墙管理中心 7.2.0 开始（仅限 Snort 3 设备），您可以使用象流检测功能对象流进行监测和补救，这有助于减少系统压力并解决上述问题。

- 关于大象流检测和补救， 第 2501 页
- 从智能应用绕行升级大象流， 第 2501 页
- 配置大象流检测， 第 2502 页
- 大象流检测示例， 第 2505 页

关于大象流检测和补救

您可以使用大象流检测功能来检测和补救大象流。可应用以下补救操作：

- **绕过大象流 (Bypass elephant flow)** - 您可以配置大象流以绕过 Snort 检测。如已配置，则 Snort 不会收到来自该流的任何数据包。
- **限制大象流 (Throttle elephant flow)** – 您可以对流应用速率限制并继续检查流。流速会以动态方式进行计算，流速会降低 10%。Snort 会将判定（流量减少 10% 的 QoS 流）发送到防火墙引擎。如果选择绕过所有应用，包括未识别的应用，您将无法为任何流配置限制操作（速率限制）。



注释 要使大象流检测正常工作，Snort 3 必须是检测引擎。

从智能应用绕行升级大象流

从 7.2.0 版开始，在 Snort 3 设备中已弃用智能应用绕行 (IAB)。

对于运行 7.2.0 或更高版本的设备，您必须在 AC 策略（高级设置选项卡）的**大象流设置 (Elephant Flow Settings)** 部分下配置象流设置。

在升级到 7.2.0（或更高版本）后，如果您使用的是 Snort 3 设备，则将从**大象流设置**部分而不是从**智能应用绕行设置**部分中挑选和部署大象流配置设置，这样，如果您没有迁移到大象流配置设置，那么您的设备在下次部署时将失去大象流配置。

下表显示了可应用于运行 Snort 3 或 Snort 2 引擎的版本 7.2.0 或更高版本以及版本 7.1.0 或更早版本的 IAB 或大象流配置。

防火墙管理中心	Firewall Threat Defense	大象流或 IAB 配置
防火墙管理中心 7.0 或 7.1	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备	来自 IAB 的配置将适用。
防火墙管理中心 7.2.0	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备（7.1.0 及更早版本）	来自 IAB 的配置将适用。
	Snort 3 设备（7.2.0 及更高版本）	大象流中的配置将适用。

配置大象流检测

您可以配置大象流以便对大象流执行操作，这有助于解决系统强制、高 CPU 使用率、丢包等问题。

注意 大象流检测不适用于不通过 Snort 处理的预过滤流、受信任流或快速转发流。由于大象流由 Snort 检测，因此大象流检测不适用于加密流量。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中点击 **高级设置** 。然后，点击 **大象流设置**旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

图 *454:* 配置大象流检测

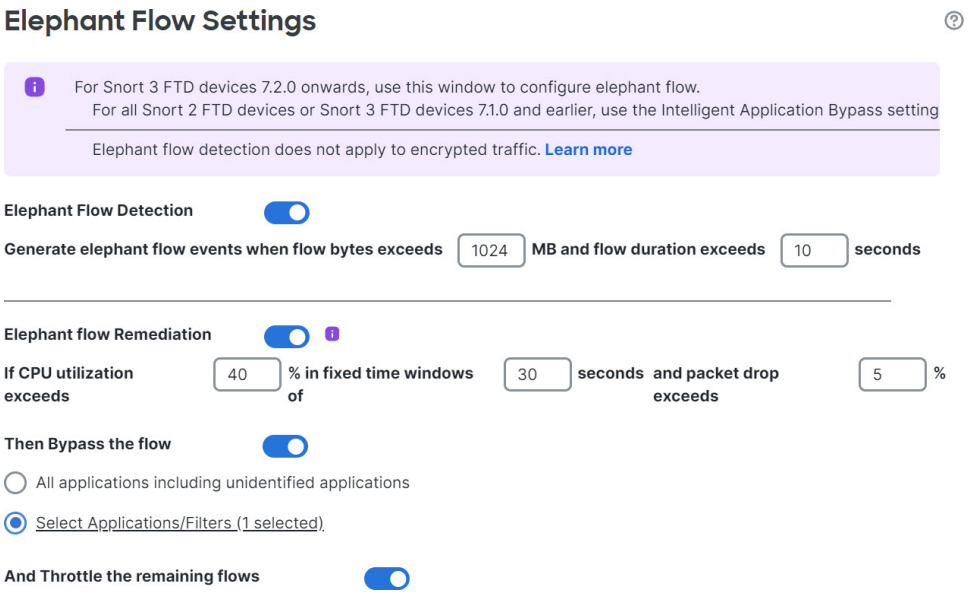


图 *455:* 配置大象流检测

步骤 2 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。您可以配置流字节和流持续时间的值。当它们超过配置的值时，就会生成大象流事件。

步骤 3 要补救大象流，请启用 **大象流补救** 切换按钮。

步骤 4 要设置大象流补救标准，请配置 CPU 利用率 %、固定时间窗口的持续时间和丢包百分比的值。

CPU利用率是根据流延迟计算的每个大象流。如果CPU使用率超出配置的阈值，并且也匹配其他配置（例如固定时间窗口和丢包），则会应用大象流补救操作。同样，丢包计算基于每个CPU丢弃的数据包。当丢包百分比超过特定CPU上的配置值后，系统将应用补救操作。例如，假设配置设置为默认值，即 CPU 使用率为 40%，固定时间窗口为 30 秒，丢包率为 5%。在特定 CPU 上，如果检测到的丢包数超过 5%，并且每个数据流的 CPU 使用率在 30 秒的固定时间范围内超过 40%，则会绕过或限制这些数据流。

步骤 5 当大象流补救符合配置的条件时，您可以对其执行以下操作：

1. **绕过流 (Bypass the flow)** - 启用此按钮可绕过所选应用或过滤器的 Snort 检查。选项包括：
   - **包括未识别应用在内的所有应用 (All applications including unidentified applications)** - 选择此选项可绕过所有应用流量。如果配置此选项，则无法为任何流配置限制操作（速率限制）。
   - **选择应用/过滤器** - 选择此选项可选择要绕过其流量的应用或过滤器；请参阅《Cisco Secure Firewall Management Center 设备配置指南》的**访问控制规则**一章中的**配置应用条件和过滤器**主题。
2. **限制流 (Throttle the flow)** - 启用此按钮可对流应用速率限制并继续检查流。请注意，您可以选择应用或过滤器来绕过 Snort 检查，同时限制剩余流量。

注释

当系统摆脱压力时，即 Snort 数据包丢弃的百分比小于配置的阈值时，会自动从已限制的大象流中删除限制。因此，速率限制也会被删除。

您还可以使用以下威胁防御命令从已限制的流量中手动删除限制：

- **clear efd-throttle <5-tuple/all> bypass** - 此命令从已限制的大象流中删除限制并绕过 Snort 检查。
- **clear efd-throttle <5-tuple/all>** - 此命令从已限制的大象流中删除限制，Snort 检测将继续。使用此命令后，系统将跳过大象流补救。

有关这些命令的详细信息，请参阅《Cisco Secure Firewall Threat Defense 命令参考》。

步骤 6 在 **补救豁免规则** 部分，点击 **添加规则** 为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。

步骤 7 在 **添加规则** 窗口中，使用 **网络** 选项卡添加网络详细信息，即源网络和目的网络。使用 **端口** 选项卡添加源端口和目的端口。

如果检测到象流并且它与定义的规则相匹配，则会在 **连接事件**的 **原因** 列标题中生成一个事件，其原因为 **象流豁免** 。

步骤 8 在 **补救豁免规则** 部分，可以查看免于执行补救操作的流。

步骤 9 点击**确定** 以保存大象流设置。

步骤 10 点击**保存**保存策略。

下一步做什么

部署配置更改；请参阅 部署配置更改，第 180 页。

配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。出现大象流连接的三个原因是：

- 大象流
- 受限制的大象流
- 受信任的大象流



注意 仅启用大象流检测不会导致为大象流生成连接事件。如果由于其他原因已记录连接事件，并且流也是大象流，则 **原因** 字段包含此信息。但是，要确保记录所有大象流，必须在适用的访问控制规则中启用连接日志记录。

有关详细信息，请参阅 Cisco Secure Firewall 大象流检测 。

大象流检测示例

关于大象流

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的相对长运行的网络连接通过网络链路测量。默认情况下，大象流是速率大于每 10 秒 1GB 的流。它们可能会在 Snort 核心中造成性能威胁或问题。大象流很重要，因为它们可能会消耗过多的CPU资源，并影响检测资源的其他竞争流，并导致延迟增加或丢包等问题。

关于大象流检测和补救的优势

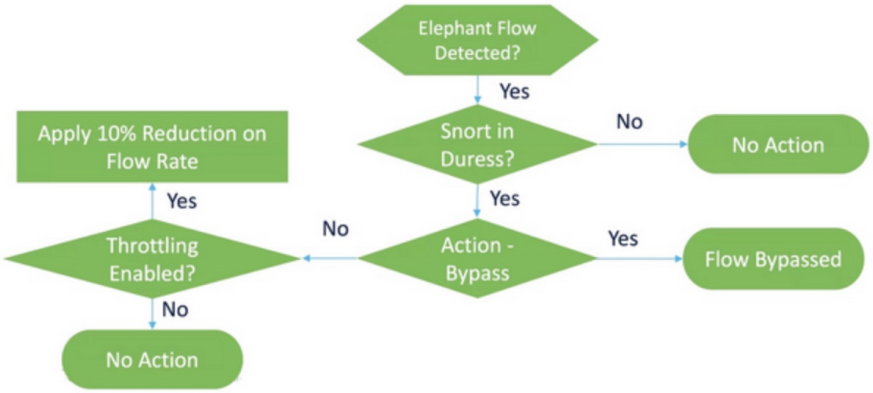
- 大象流配置允许自定义和绕过甚至限制大象流的选项。
- 您可以选择绕过或限制基于所选应用的流量，以提供可疑流量的Snort检查，同时绕过更受信任的流量。
- 大象流补救有助于根据您的特定要求确定优先级并为内部应用释放更多带宽。

大象流工作流程

当根据配置的参数检测到大量流时，您可以选择绕过或限制该流。当流量被绕过时，允许流量通过而不进行 Snort 检查。限制表示流量吞吐量降低。以 10% 的增量降低流量，直到 CPU 使用率降至配置的阈值以下。在识别大流并满足额外的CPU和时间窗口参数后，会发生绕行或限制。在识别大流之前，入侵策略会处理流，假设您已在“允许”规则中配置此流。这意味着不允许大量流在完全未经检查的情况下通过系统，因为大多数攻击都是在连接中很早就被检测到的。

要了解如何处理流，请参阅以下流程图。

图 *456:* 大象流工作流程



除非系统检测到Snort强制条件（性能问题），否则不会执行任何操作。系统不会仅仅因为流量大而限制或绕过流量。此外，限制和旁路的操作是相互排斥的。这意味着您可以绕过或限制流，但不能同时绕过或限制流。

如果您不想绕过导致威胁的所有大流，可以将绕过选项限制为仅适用于特定应用。您可以优先考虑您信任的应用的连接，而不会限制性能。您可以配置必须绕过的应用，但剩余流量（导致威胁）将受到限制。这可确保其他不受信任的应用流仍会收到完整的 Snort 检测，尽管其带宽已减少。

示例业务情景

在数据中心中，会发生多项活动，例如集群之间的数据复制、虚拟机集成和数据库备份。组织中的用户可能正在OTT上观看或下载视频。此类活动的带宽利用率可能会导致大量流量，降低网络速度并影响重要任务的性能。作为网络管理员（根据您的特定要求），您希望了解导致带宽问题的大型数据流并进行补救。

例如，让我们看看如何配置大流参数来绕过WebEx流量（您的组织用于实时视频会议）并限制其余应用或连接，包括视频、电影等。

前提条件

- 确保您运行的是管理中心 7.2.0 或更高版本，并且托管威胁防御也是 7.2.0 或更高版本。
- 仅启用大象流检测不会生成其他连接事件。大象流检测将大象流表示法添加到已记录到管理中心的匹配连接。**要记录这些事件，必须在访问控制策略中启用连接日志记录**。您可以对特定规则执行此操作，也可以添加记录所有连接（包括大流）的监控规则。

配置大象流参数

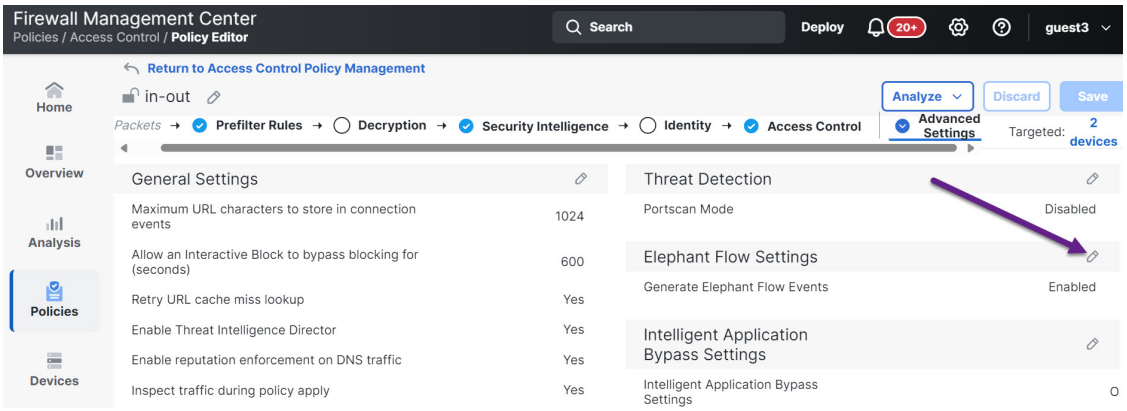
过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎)。

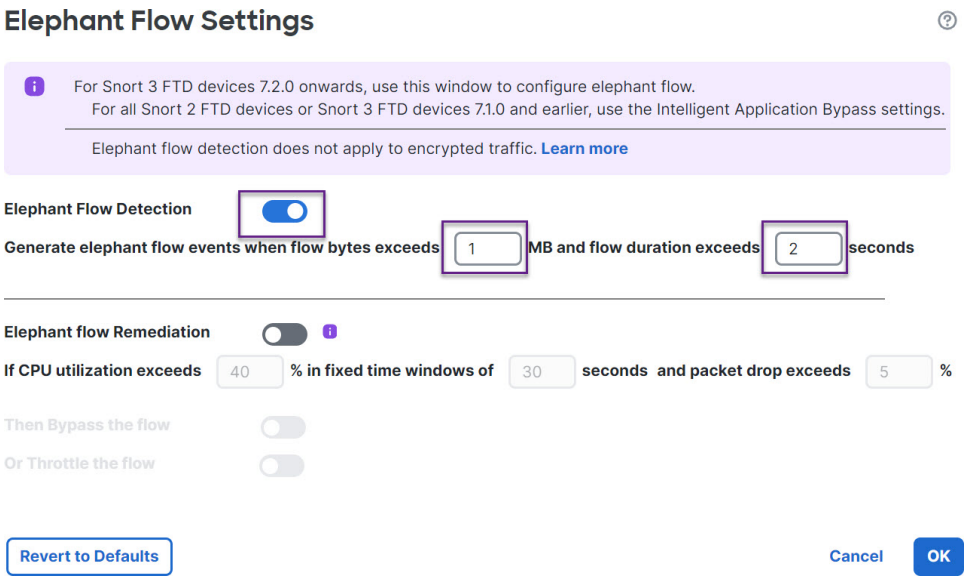
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** (✎)。



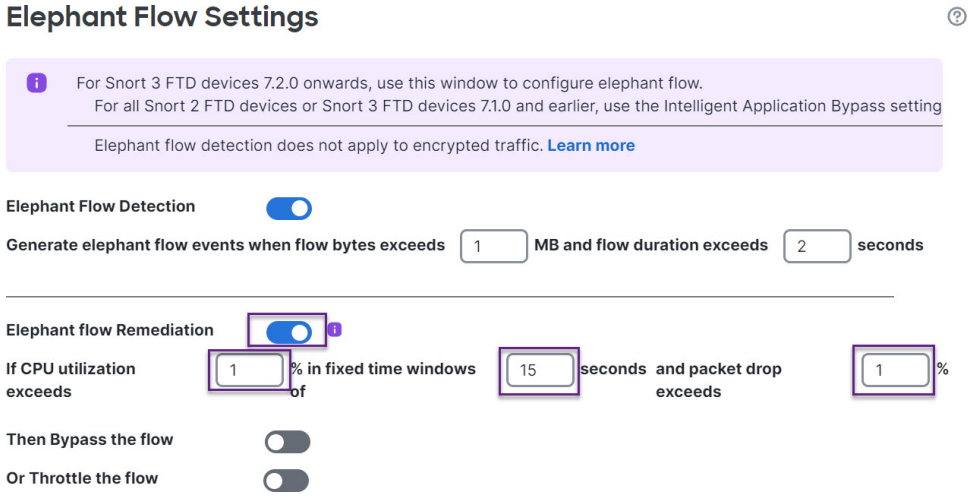
步骤 5 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。默认设置仅启用检测，不配置默认操作。检测设置允许您调整流字节和持续时间，以便可以识别系统中的大象流。

作为测试设置，配置流字节和持续时间参数，如下图所示。

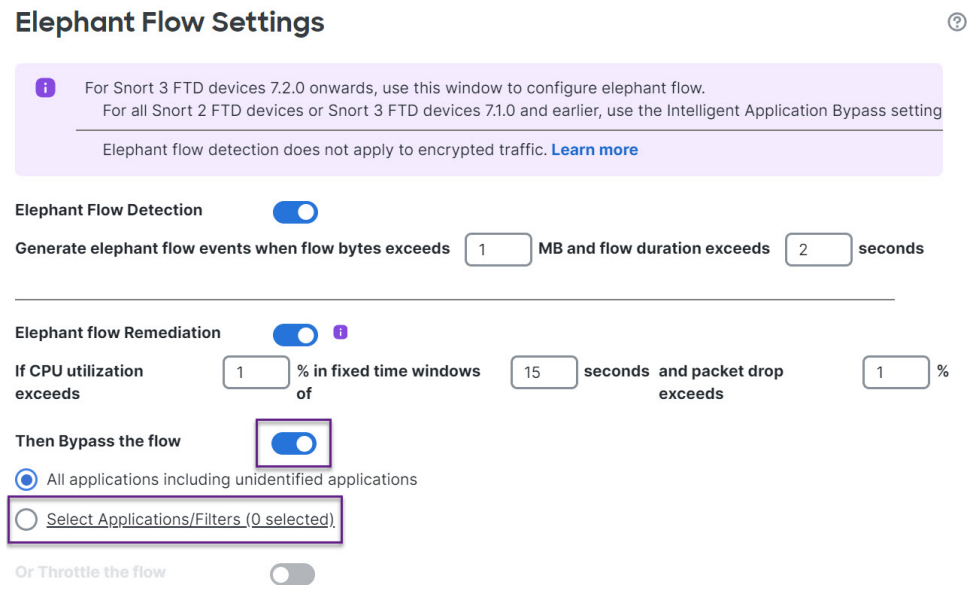


步骤 6 启用**大象流补救**切换按钮。当检测到大象流时，您可以选择绕过或限制该流。绕过流意味着允许流量通过而无需 Snort 检查。限制表示流量吞吐量降低。此速率降低以 10% 为增量，直到 CPU 使用率降至低于配置的阈值。

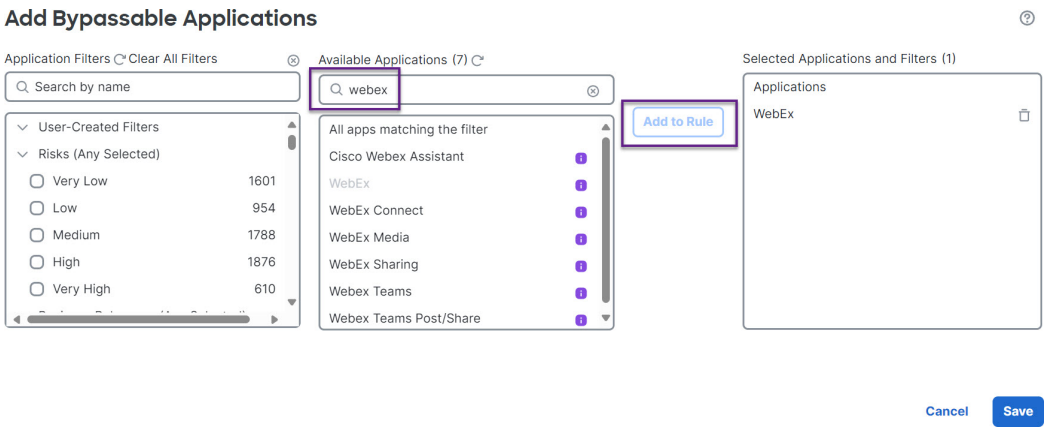
作为测试设置，配置大象流补救参数，如下图所示。



步骤 7 启用 **绕过流** 切换按钮，然后点击 **选择应用/过滤器** 单选按钮。



步骤 8 在 **应用过滤器** 下，搜索并选择 **WebEx** 应用，将其添加到规则中，然后点击 **保存**。这意味着 WebEx 连接是受信任的和优先的，如果这些 WebEx 连接被检测为大象流，则将根据配置的参数跳过 Snort 检查。



步骤 9 启用 **限制** 切换按钮以限制剩余流量（导致强制）。这可确保所有其他流量以 10% 的增量减慢，直到满足 Snort 强制条件。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改。

查看大象流的事件

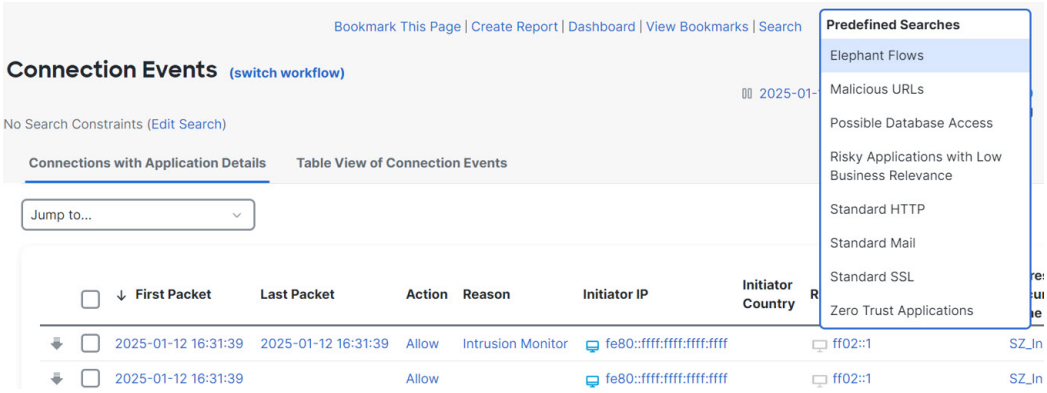
配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。大象流连接的三种类型为：

- 大象流
- 受限制的大象流
- 受信任的大象流

过程

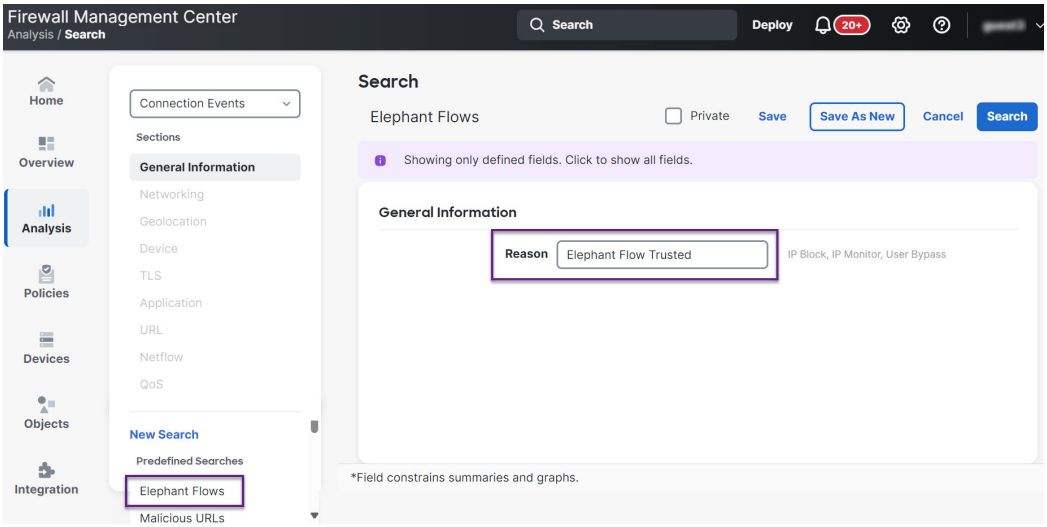
步骤 1 选择**事件和日志** > **+ 显示更多** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 在 **连接事件** 页面中，从 **预定义搜索** 下拉列表中选择 **大象流** 以显示象形流事件。

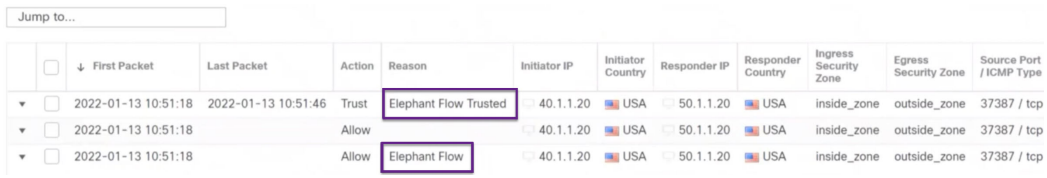


提示

要查看 **受信任的大象流** 或 **受限制的大象流** 事件类型，请点击页面左上角的 **编辑搜索** 链接，然后在 **原因** 字段中，选择左侧面板中的 **大象流** 。根据要搜索的内容，输入 **受信任的大象流** 或 **受限制的大象流**。



步骤 3 查看在流中检测到的大象流，并且 **原因** 字段显示 **大象流**。在流结束时，它被绕过，并且 **原因** 字段显示 **受信任的大象流**。



配置大象流补救豁免

您可以为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。如果检测到大型流，并且该流与为必须豁免补救操作的流定义的规则匹配。

开始之前

您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**。

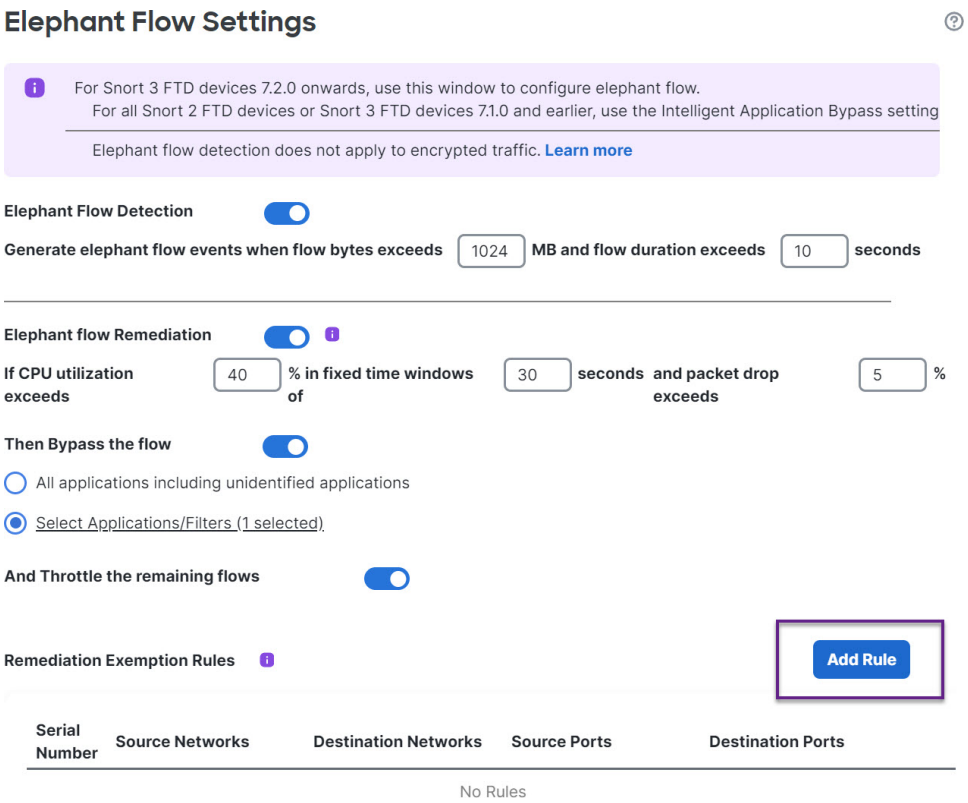
步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

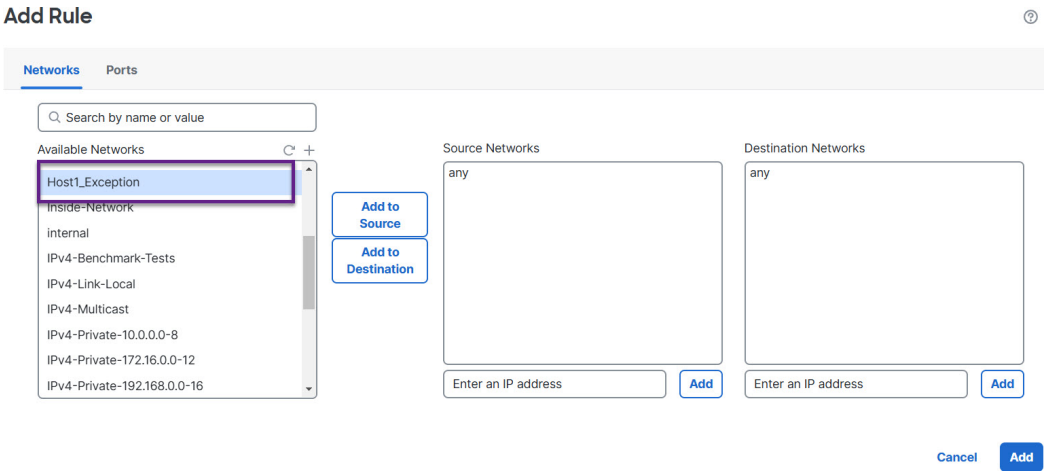
步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** (✎)。

步骤 5 确保您已配置大象流检测和补救参数。请参阅配置大象流参数，第 2506 页。

步骤 6 点击 **补救豁免规则**旁边的 **添加规则** 按钮。



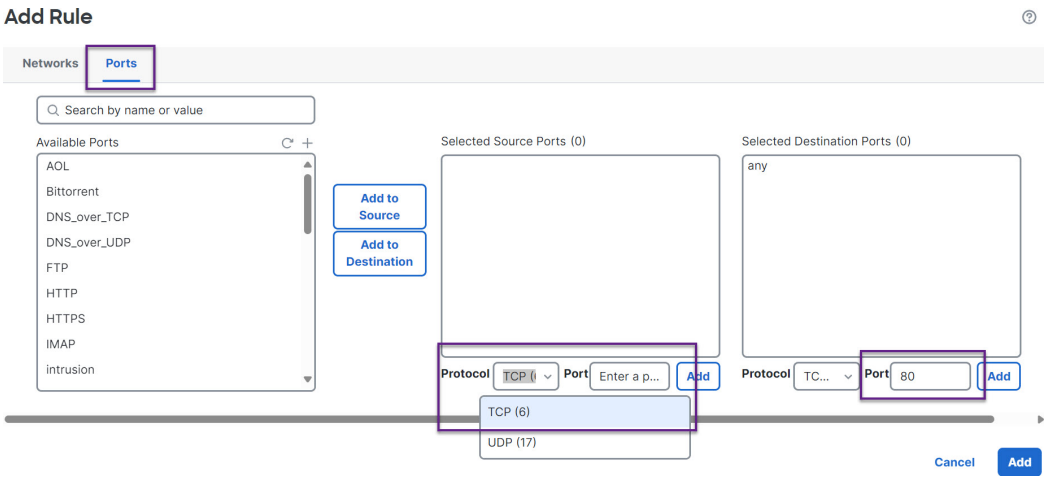
步骤 7 从 **可用网络**列表中，选择要免于执行大象流补救的已配置主机。在本示例中，我们创建了一个名为“Host1_Exception”的主机。



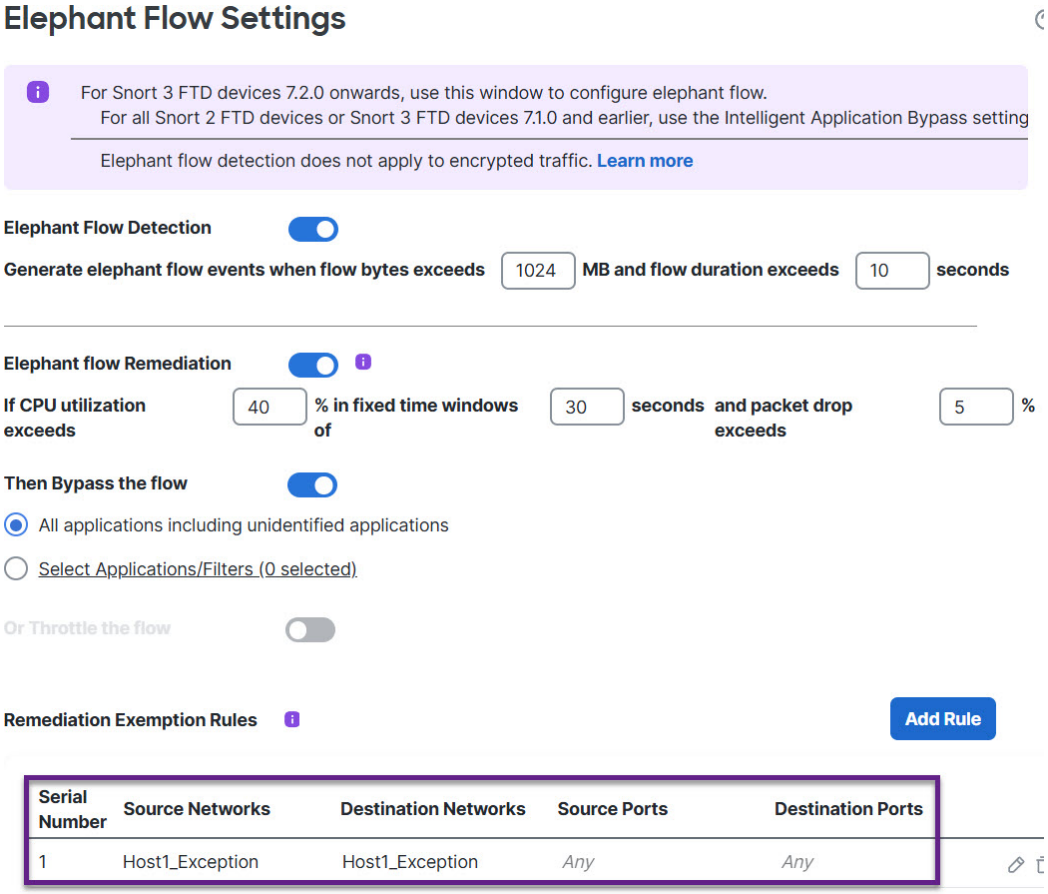
步骤 8 点击 **添加到源** 或 **添加到目标** （根据需要），将此主机添加到源或目标。

步骤 9 点击**端口**选项卡。

步骤 10 对于源端口，选择 **协议** 作为 TCP 并输入 **80** 作为目的端口，然后点击 **添加**。



步骤 11 点击**确定 (OK)**。



步骤 12 点击保存 **(Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改。

查看大象流补救豁免事件

过程

步骤 1 选择事件和日志 > + 显示更多 > 连接 > 事件。您还可以在 统一事件 查看器中查看事件。

步骤 2 查看免于补救的大象流。 理由 字段显示 免于补救的大象流。


Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol
▾	2022-12-19 11:23:58	2022-12-19 11:24:30	Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	2022-12-19 11:23:58		Allow		172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	2022-12-19 11:23:58		Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.6		inside-zone56	outside-zone56	37780 / tcp	443 (https) / tcp	HTTP
▾	2022-12-19 11:23:44	2022-12-19 11:23:50	Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.5		inside-zone56	outside-zone56	50056 / tcp	80 (http) / tcp	HTTP
▾	2022-12-19 11:23:44		Allow	Elephant Flow Exempted	172.16.77.1		172.16.4.5		inside-zone56	outside-zone56	50056 / tcp	80 (http) / tcp	HTTP

其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 大象流检测”一章或以下链接中的内容：

- 大象流检测



第 XII 部分

网络发现

- 网络发现概述， 第 2517 页
- 主机身份源， 第 2527 页
- 应用检测， 第 2563 页
- 网络发现策略， 第 2583 页



第 68 章

网络发现概述

以下主题讨论网络发现：

- 主机、应用和用户数据的检测，第 2517 页
- 主机和应用检测基础知识，第 2518 页

主机、应用和用户数据的检测

主机、应用和用户数据的检测是一种网络监控功能

- 根据网络发现策略设置，使用主机身份源和应用检测器收集主机和应用数据；
- 根据网络发现和身份策略配置，通过用户身份源收集用户数据，以及
- 支持全面的网络资产映射、调查分析、行为分析、访问控制和漏洞缓解。

主机、应用和用户数据收集

系统使用 网络发现和 身份 策略收集网络上流量的主机、应用和用户数据。系统分析发现和身份数据，以创建详细的网络资产映射、执行调查分析、行为剖析和访问控制，并对组织的潜在漏洞和危险做出响应。

系统会收集各种类型的数据，以增强网络安全和性能分析：

- 主机和应用数据：由主机身份源和应用检测器根据网络发现策略中的设置进行收集。托管设备会观察指定网段上的流量。

  有关主机和应用数据的基础知识的详细信息，请参阅主机和应用检测基础知识，第 2518 页

- 用户数据：由用户身份源根据网络发现和身份策略中的设置进行收集。使用这些数据获取用户感知和用户控制。

  有关用户身份的更多信息，请参阅关于用户身份，第 1975 页。

通过日志记录发现和身份数据，您可以利用系统中的许多功能，包括：

- 查看网络映射，网络映射是对网络资产和拓扑的详细表示，可通过对主机和网络设备、主机属性、应用协议或漏洞进行分组来查看。

- 使用访问控制规则，结合应用条件、领域条件、用户条件、用户组条件和 ISE 属性条件，执行应用和用户控制。
- 查看受检测主机的完整配置文件。
- 通过控制面板监控网络资产和用户活动。
- 查看关于发现事件和用户活动的详细信息。

  记录和使用 NetFlow 连接（如果适用）。
- 将主机、服务器和客户端与易受漏洞攻击的主机、服务器和客户端关联，以识别和减少漏洞。

  评估入侵事件对您的网络的影响，并优化入侵规则状态，以便它们为您的网络资产提供最大的保护。
- 在系统生成具有特定影响标志的入侵事件或特定类型的发现事件时，通过邮件、SNMP 陷阱或系统日志接收警报。
- 监控组织是否遵守允许的 allow 操作系统、客户端、应用协议和协议的列表
- 在系统生成发现事件或检测用户活动时，创建具有会触发和生成关联事件的规则的关联策略。

主机和应用检测基础知识

网络发现策略是一项实现多种功能的功能。您可以执行以下操作：

- 启用设备标识，
- 监控网络设备和服务，以及
- 配置检测设置，以跟踪性能。

有关主机和应用检测的详细信息，请参阅概述：主机数据收集，第 2527 页和概述：应用检测，第 2563 页。

操作系统和主机数据被动检测

被动检测是一种网络映射方法，

- 分析网络流量和任何导出的 NetFlow 数据以填充网络映射
- 提供有关您的网络资产（如操作系统和正在运行的应用）的情景信息，以及
- 作为系统的默认检测方法。

操作系统确定过程

如果来自受监控主机的流量不提供主机操作系统的确凿证据，则网络映射将显示最有可能的操作系统。例如，由于在 NAT 设备“后面”的主机，NAT 设备可能看起来正在运行多个操作系统。为了

做出最可能的决定，系统使用其为每个检测到的操作系统分配的置信值，以及检测到的操作系统之间的确认数据量。



注释 系统在确定时不考虑报告的“unknown”应用和操作系统。

如果被动检测不准确地识别您的网络资产，请考虑更换托管设备。您还可以使用自定义操作系统指纹和自定义应用检测器来增强系统的被动检测功能。或者，您可以使用主用检测，它不基于流量分析，而是允许您使用扫描结果或其他信息源直接更新网络映射。

操作系统和主机数据主动检测

主动检测是一种网络发现功能，

- 将主动源收集的主机信息添加到网络映射，
- 使用 Nmap Scanner 等工具发现主机上的操作系统和应用，以及
- 允许将主机输入数据主动添加到网络映射中。

主机输入数据分类为：

- 用户输入数据 — 通过系统用户界面添加的数据，允许修改主机的操作系统或应用身份。
- 托管导入输入数据 - 使用命令行实用程序导入的数据。

身份保留和优先级行为

系统将为每个主动源保留一个身份。例如，当您运行 Nmap 扫描实例时，先前的结果会用新的扫描数据进行更新。但是，如果用通过命令行导入的客户端数据替换扫描结果，系统将保留两者的身份信息。然后，系统会使用网络发现策略中设置的优先级来确定用作当前身份的主动身份。

用户输入无论来源如何，都会取代其他身份。例如，如果用户 A 通过主机配置文件设置操作系统，然后用户 B 通过主机配置文件更改该定义，则保留用户 B 设置的定义。用户输入会覆盖所有其他的主动源，并会用作当前身份（如果其存在）。

应用和操作系统的当前身份

当前身份是应用或操作系统的身份确定，

- 表示系统认为最有可能正确的身份，
- 用于漏洞分配和影响评估，以及
- 当同一主机存在多个身份时，由源优先级确定。

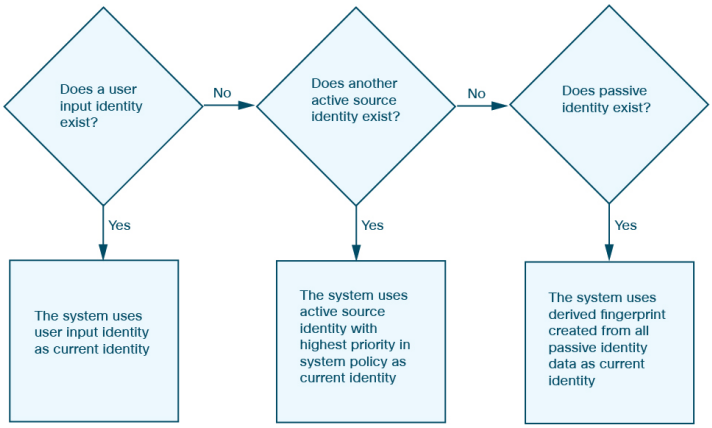
当前身份用户

系统会将操作系统或应用的当前身份用于这些用途：

- 分配漏洞至主机
- 评估影响
- 评估与操作系统标识、主机配置文件资格和合规性 allow 列表相关的关联规则
- 在工作流程的“主机”和“服务器”表格视图中进行显示
- 在主机配置文件中进行显示
- 在“发现统计信息”页面上计算操作系统和应用统计信息

系统会使用源优先级来确定哪个主动身份应该用作应用或操作系统的当前身份。

图 *457:* 当前身份确定过程



对于主机上的操作系统或特定应用，数据库可能保留来自多个源的信息。

如果数据的源拥有最高的源优先级，系统会将操作系统或应用身份视作当前身份。可能的源的优先级顺序如下：

1. 用户
2. 扫描程序和应用（在网络发现策略中设置）
3. 受管设备
4. NetFlow 记录

如果新的、优先级更高的应用标识比当前标识的细节更少，则不会覆盖当前应用标识。

此外，如果出现身份冲突，冲突的解决取决于网络发现策略中的设置或者手动解决。

分配操作系统作为当前身份

例如，如果用户在一台主机上将操作系统设置为 Windows 2003 Server，则 Windows 2003 Server 成为当前身份，并且该主机上针对 Windows 2003 Server 漏洞的攻击将具有更高的影响。主机配置文件中针对该主机列出的漏洞包括 Windows 2003 Server 漏洞。

当前用户身份

当前用户身份由系统确定：

- 当多个用户登录到同一主机时，将最后的授权用户登录识别为当前用户
- 假定一次只能有一个用户登录到任何给定主机
- 记录用户在特定主机上的首次登录，但忽略同一用户的后续登录，并且
- 当多个用户通过远程会话登录时，向 防火墙管理中心 报告服务器检测到的最后一个用户。

用户登录跟踪行为

系统使用特定规则确定当前用户身份：

- 当系统检测到不同用户多次登录同一主机时，系统将假设某一时刻只有一个用户登录到了某给定主机，并且一个主机的当前用户是最后授权的用户登录。如果只有非授权用户登录用户登录主机，则最后的非授权用户登录用户将被视为当前用户。如果有多个用户通过远程会话登录，则服务器报告的最后用户是报告给 防火墙管理中心的用户。
- 当系统检测到同一用户多次登录到同一主机时，系统会记录用户在特定主机的首次登录并忽略后续的登录。如果单个用户是唯一登录到特定主机的人员，则系统唯一记录的登录为原始登录。
- 但是，如果另一用户登录到该主机，则系统会记录新的登录。如果原始用户再次登录，系统会记录其新的登录。

应用和操作系统的身份冲突

身份冲突是一种系统条件

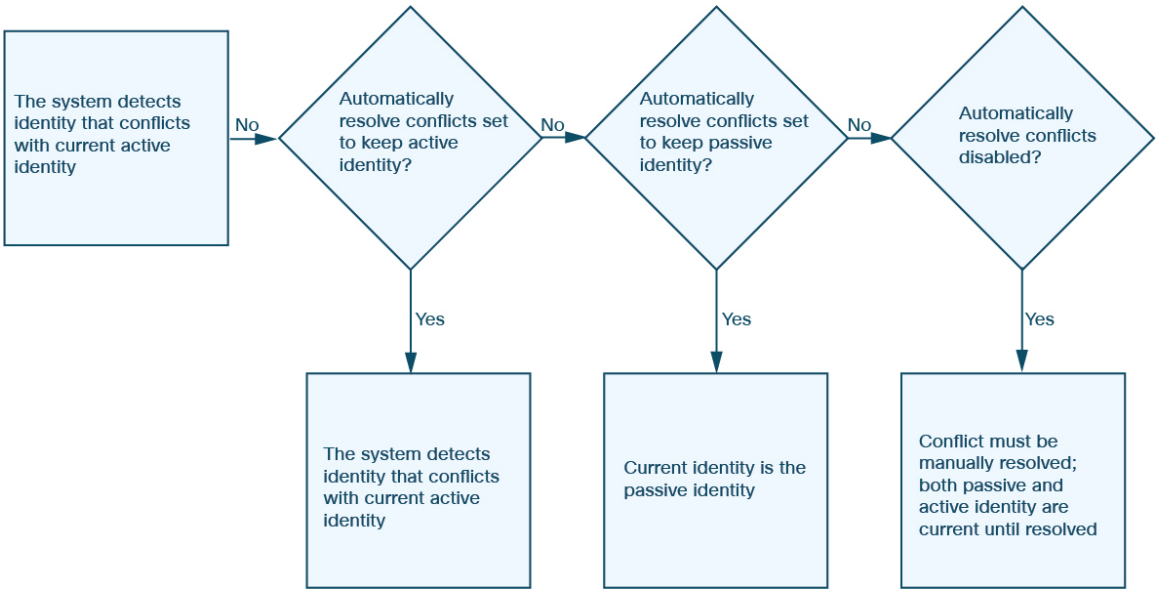
- 当系统报告新的被动身份与当前主动身份和先前报告的被动身份冲突时发生。
- 导致两个冲突的身份都被列为当前身份并用于影响评估，直到冲突得以解决，以及
- 通过选择始终使用被动身份或始终使用主动身份即可自动解决。

身份冲突行为和解决方法

如果主机的操作系统或主机上的某个应用存在身份冲突，系统会将两个冲突的身份均列为当前身份，并将二者用于影响评估，直到冲突解决。

有管理员权限的用户可自动解决身份冲突，只需选择始终使用被动身份或始终使用主动身份。除非禁用身份冲突的自动解决，否则身份冲突始终会自动解决。

有管理员权限的用户还可配置系统，从而在身份冲突发生时生成事件。然后，该用户可设置带有相关性规则的相关策略，规则将Nmap扫描用作相关性响应。如果事件发生，Nmap会扫描主机以获取经过更新的主机操作系统和应用数据。



操作系统身份冲突场景

如将操作系统先前的被动身份报告为 Windows 2000，则主动身份 Windows XP 成为当前身份。接下来，系统检测到新的被动身份 Ubuntu Linux 8.04.1。身份 Windows XP 和 Ubuntu Linux 发生冲突。

NetFlow 数据

NetFlow 数据是网络流统计信息的集合，可以

- 通过 Cisco IOS 应用提供流经路由器的数据包统计信息
- 在思科网络设备可用，也可嵌入 Juniper、FreeBSD 和 OpenBSD 设备中，并且
- 在网络设备上启用 NetFlow 时，将流记录存储在设备上称为 NetFlow 缓存的数据库中。

NetFlow 数据处理与使用

数据流（在系统中称为连接）是数据包序列，代表使用特定端口、协议和应用协议的源主机和目标主机之间的会话。可以将网络设备配置为导出此 NetFlow 数据。在本文档中，通过此方式配置的网络设备称为 *NetFlow* 导出器。

托管设备可以配置为从 NetFlow 导出器收集记录，根据这些记录中的数据生成单向连接结束事件，最后将这些事件发送到 防火墙管理中心以记录在连接事件数据库中。您还可以配置网络发现策略，以根据 NetFlow 连接中的信息将主机和应用协议信息添加到数据库。

可以使用这些发现和连接数据补充托管设备直接收集到的数据。这在让 NetFlow 导出器监控托管设备无法监控的网络时尤为有用。

使用 NetFlow 数据的要求（原则）

要求：NetFlow 设备配置

在配置系统分析 NetFlow 数据前，**必须**在计划使用的路由器或其他支持 NetFlow 的网络设备上启用 NetFlow 功能。将设备配置为向托管设备传感接口所连接的网络广播 NetFlow 数据。

要求：NetFlow 版本与字段规范

系统可解析 NetFlow 版本 5 和版本 9 记录。若需导出数据，NetFlow 导出器**必须**使用上述版本之一。确保导出的 NetFlow 模板和记录包含特定字段，例如 IN_BYTES、IN_PKTS、PROTOCOL 等。如果 NetFlow 导出器使用的是可以自定义的版本 9，则**必须**确保已导出的模板和记录按任意顺序包含以下字段：

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

要求：托管设备部署

您的部署必须包含至少一台可监控 NetFlow 导出器的托管设备。将托管设备上的至少一个传感接口连接到网络，以收集导出的 NetFlow 数据。因传感接口缺乏 IP 地址，系统不支持直接收集。

注意：采样 NetFlow 注意事项

请注意，在某些网络设备上可用的采样 NetFlow 功能只会收集有关经过设备的数据包子集的 NetFlow 统计信息。启用此功能虽可提升 CPU 利用率，但可能影响系统分析所用的 NetFlow 数据准确性。

NetFlow 与受管设备数据之间的差异

NetFlow 与受管设备数据的差异属于分析性差异，

- 源于将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据，而不是直接分析流量，

- 影响检测到的连接、操作系统信息和应用数据的统计信息，以及
- 影响连接发起方和响应方的识别。

数据收集和分析方面的主要差异

NetFlow 数据代表的流量不会被直接分析 。相反，系统会将导出的 NetFlow 记录转换为连接日志以及主机和应用协议数据。

因此，转换后的 NetFlow 数据与托管设备直接收集到的发现数据和连接数据之间存在一些差异。在执行需要以下信息的分析时，应记住这些差异：

- 已检测的连接数量的统计信息
- 操作系统信息以及其他主机相关信息（包括漏洞）
- 应用数据，包括客户端信息、Web 应用信息，以及供应商和版本服务器信息
- 知道连接中哪个主机是发起方，哪个主机是响应方

网络发现策略与访问控制策略：

可以使用网络发现策略中的规则来配置 NetFlow 数据收集（包括连接日志记录）。可以将这种数据收集与托管设备（根据访问控制规则进行配置）检测到的连接的连接日志记录进行比较。

连接事件的类型：

- 由于 NetFlow 数据收集与网络而不是访问控制规则相关联，因此您不能非常精细地控制系统记录的 NetFlow 连接。
- NetFlow 数据无法生成安全智能事件。
- 基于 NetFlow 的连接事件只能存储在连接事件数据库中；无法将这些事件发送到系统日志或 SNMP 陷阱服务器。

每个受监控会话生成的连接事件数量：

对于托管设备直接检测到的连接，可将访问控制规则配置为在连接开始和/或结束时记录双向连接事件。

相反，由于导出的 NetFlow 记录包含单向连接数据，因此系统会为其处理的每个 NetFlow 记录生成至少两个连接事件。这也意味着，对于基于NetFlow数据的每次连接，摘要的连接数会每次递增2，从而提供网络上实际发生的快速增长的连接数量。

由于 NetFlow 导出器会定期输出记录（即使连接仍在进行中），长时间运行的会话可能导致多个导出记录，每个记录都会生成一个连接事件。例如，如果 NetFlow 导出器每 5 分钟导出一次，且特定连接持续 12 分钟，那么系统将会为该会话生成 6 个连接事件：

- 前 5 分钟生成一对事件
- 第二个 5 分钟生成一对事件
- 连接终止时生成最后一对事件

主机和操作系统数据：

从 NetFlow 数据添加到网络映射的主机不具有操作系统、NetBIOS 或主机类型（主机与网络设备）信息。但是，您可以使用主机输入功能手动设置主机的操作系统身份。

应用数据：

对于托管设备直接检测到的连接，系统可以通过检查连接中的数据包来识别应用协议、客户端和Web应用。

系统处理 NetFlow 记录时，会使用 `/etc/sf/services` 中的端口关联来推断应用协议身份。不过，这些应用协议不包含供应商或供应商信息，而且连接日志不包含关于会话中使用的客户端或 Web 应用的信息。但是，可以使用主机输入功能手动提供这些信息。

请注意，简单端口关联意味着在非标准端口上运行的应用协议可能不会被识别或被错误识别。此外，如果不存在关联，系统会在连接日志中将应用协议标记为 `unknown`。

漏洞映射：

系统无法将漏洞映射到 NetFlow 导出器监控的主机，除非使用主机输入功能手动设置主机操作系统的身份或应用协议身份。请注意，由于 NetFlow 连接中没有客户端信息，因此您无法将客户端漏洞与根据 NetFlow 数据创建的主机相关联。

连接中的发起方和响应方信息：

对于托管设备直接检测到的连接，系统可确定哪个主机是发起方（即“源”），哪个主机是响应方（即“目标”）。但是，NetFlow 数据不包含发起方或响应方信息。

当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

- 如果使用的两个端口都是或都不是公认端口，系统会将端口号较小的那个主机视为响应方。
- 如果只有一个主机在使用公认端口，系统会将该主机视为响应方。

为此，知名端口是指编号从 1 到 1023 的任何端口，或系统视为服务器端口的任何端口（无论其编号如何）。

NetFlow 字节计数

基于单向 NetFlow 记录的连接事件只包含一个字节计数（系统分配到**发起方字节数 [Initiator Bytes]** 或**响应方字节数 [Responder Bytes]**），具体取决于基于端口的算法。系统将另一个字段设置为 0。请注意，如果查看 NetFlow 记录的连接摘要（汇聚的连接数据），则这两个字段都可能会填充。

仅 NetFlow 连接事件字段

从 NetFlow 记录生成的连接事件中只存在少量字段；请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的连接时间字段中可用信息。



第 69 章

主机身份源

这些主题提供有关主机身份源的信息：

- 概述：主机数据收集，第 2527 页
- 主机身份源的要求和前提条件，第 2528 页
- 确定系统可以检测的主机操作系统，第 2528 页
- 识别主机操作系统，第 2528 页
- 自定义指纹，第 2529 页
- 主机输入数据，第 2536 页
- Nmap 扫描，第 2544 页
- 主机身份源的历史记录，第 2562 页

概述：主机数据收集

由于Firepower系统被动监控流经网络的流量，因此，它会根据既定的定义（称为指纹）比较特定数据包报头值以及来自网络流量的其他唯一数据，以确定关于网络上主机的信息，包括：

- 主机（包括网桥、路由器、负载均衡器和 NAT 设备等网络设备）数量和类型
- 基本网络拓扑数据，包括从网络上的发现点到主机的跳数
- 主机上运行的操作系统
- 主机上的应用以及与这些应用关联的用户

如果系统无法识别主机的操作系统，则您可以创建自定义客户端或服务器指纹。系统将使用这些指纹来识别新主机。您可以将指纹映射到漏洞数据库 (VDB) 中的系统，以便在使用自定义指纹识别主机时显示适当的漏洞信息。

注释 除从受监控网络流量中收集主机数据以外，系统还可以从导出的 NetFlow 记录收集主机数据，并且您可以使用 Nmap 扫描和主机输入功能主动添加主机数据。

主机身份源的要求和前提条件

型号支持

任意。

支持的域

任意，但自定义指纹除外，它仅限 枝叶。

用户角色

- 管理员
- 发现管理员，但第三方数据和自定义映射除外。

确定系统可以检测的主机操作系统

要了解系统可以进行指纹识别的确切操作系统，请查看在创建自定义操作系统指纹过程中显示的可用指纹的列表。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击**创建自定义指纹 (Create Custom Fingerprint)**。

步骤 4 查看**操作系统漏洞映射**部分的下拉列表中的选项列表。这些选项是系统可以进行指纹识别的操作系统。

下一步做什么

根据需要，请参阅识别主机操作系统 ， 第 2528 页。

识别主机操作系统

如果系统无法正确识别主机的操作系统（例如，操作系统在“主机配置文件”中显示为“未知”，或者识别的操作系统不正确），则请尝试下面的策略。

过程

尝试以下策略之一：

- 检查“网络发现身份冲突设置”。
- 创建主机的自定义指纹。
- 对主机运行 Nmap 扫描。
- 使用主机输入功能将数据导入到网络映射中。
- 手动输入操作系统信息。

自定义指纹

系统包含系统用于识别其检测的每个主机上的操作系统的操作系统指纹。然而，有时系统会因为不存在与操作系统匹配的指纹而无法识别主机操作系统，或者错误地识别主机操作系统。要纠正此问题，可创建自定义指纹，指纹提供未知或识别错误的操作系统所独有的操作系统特征模式，以便提供用于标识的操作系统名称。

如果系统无法匹配主机操作系统，则无法识别主机漏洞，因为系统通过其操作系统指纹为每个主机派生漏洞列表。例如，如果系统检测到运行Microsoft Windows的主机，则表明系统存储了Microsoft Windows 漏洞列表，其根据检测到的 Windows 操作系统将该列表添加至该主机的主机配置文件。

例如，如果网络上有多个运行新试用版Microsoft Windows的设备，则系统无法确定操作系统，或无法将漏洞映射到主机。然而，知道系统拥有Microsoft Windows的漏洞列表，您可能想要为某个主机创建自定义指纹，以帮助识别运行相同操作系统的其他主机。可将Microsoft Windows漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

创建自定义指纹时，防火墙管理中心将为运行相同操作系统的任何主机列出与该指纹关联的漏洞集。如果创建的自定义指纹没有任何漏洞映射，则系统将使用该指纹来分配在其中提供的自定义操作系统信息。当系统看到之前检测的主机发出的新流量时，系统用新指纹信息更新主机。首次检测到使用该操作系统的任何新主机时，系统还会使用新的指纹来识别这些主机。

在创建自定义指纹前，应确定主机未被正确识别的原因，从而确定自定义指纹是否为可行的解决方案。

可使用系统创建两种类型的指纹：

- 客户端指纹，这种指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。
- 服务器指纹，这种指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。

注释 如果客户端和服务器指纹均与相同的主机匹配，将会使用客户端指纹。

创建指纹后，必须先将其激活，然后系统才可以将其与主机关联。

相关主题

为客户端创建自定义指纹，第 2532 页
为服务器创建自定义指纹，第 2534 页

管理指纹

指纹创建和激活后，可编辑指纹以便做出更改或添加漏洞映射。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。如果系统正在等待数据以便创建指纹，将会每 10 秒自动刷新页面，直到指纹已创建。

步骤 3 管理自定义指纹：

- 激活/停用 - 激活或停用指纹，如激活和停用指纹，第 2530 页中所述。
- 创建 - 创建指纹，如为客户端创建自定义指纹，第 2532 页和为服务器创建自定义指纹，第 2534 页中所述。
- 编辑 - 编辑指纹，如编辑活动指纹，第 2531 页和编辑非活动指纹，第 2531 页中所述。
- 删除 - 点击要删除的指纹旁边的 **删除** ()，并点击**确定 (OK)** 以进行确认。只能删除已停用的指纹。

激活和停用指纹

必须先激活自定义指纹，然后系统才能将其用于识别主机。新指纹激活后，系统会将其用于重新识别先前发现的主机并发现新的主机。

如果想要停止使用指纹，可将其停用。停用指纹后，该指纹就不再可用，但仍可保留其在系统中。停用指纹后，对于使用该指纹的主机，操作系统被标记为未知。如果再次检测到这些主机，并且这些主机与不同的活动指纹匹配，则该活动指纹将对其进行识别。

删除指纹会将其从系统中完全删除。停用指纹后，即可将其删除。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击要激活或停用的指纹旁边的滑块。

注释
激活选项仅当创建的指纹有效时才可用。如果滑块不可用，请尝试重新创建指纹。

编辑活动指纹

如果指纹处于活动状态，可修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

可以修改指纹名称、描述、自定义操作系统显示，并向其映射额外的漏洞。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统**

步骤 3 点击想要编辑的指纹旁的 **编辑** ()。

步骤 4 必要时修改指纹名称、描述和自定义操作系统显示。

步骤 5 如果要删除漏洞映射，请点击页面的**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 部分中映射旁边的**删除 (Delete)**。

步骤 6 如果要为漏洞映射添加额外的操作系统，请选择**产品 (Product)**，且在适用的情况下，选择**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)**，然后点击**添加操作系统定义 (Add OS Definition)**。

漏洞映射会添加到**预定义操作系统产品映射 (Pre-Defined OS Product Maps)** 列表。

步骤 7 点击**保存**。

编辑非活动指纹

如果指纹处于非活动状态，可修改指纹的所有元素，并将其重新提交至 Secure Firewall Management Center。这包括创建指纹时指定的所有属性，如指纹类型、目标 IP 地址与端口、漏洞映射等。编辑非活动指纹并将其提交时，会将它重新提交至系统，如果指纹是客户端指纹，必须先将流量重新发送至设备，然后才可以将其激活。请注意，对于非活动指纹，仅可选择单一漏洞映射。激活指纹后，可将额外的操作系统和版本映射至其漏洞列表。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击想要编辑的指纹旁的 **编辑** (✎)。

步骤 4 请在必要时更改指纹：

- 如果要修改客户端指纹，请参阅为客户端创建自定义指纹，第 2532 页。
- 如果要修改服务器指纹，请参阅为服务器创建自定义指纹，第 2534 页。

步骤 5 点击**保存**。

下一步做什么

- 如已修改客户端指纹，切记将流量从主机发送至收集指纹的设备。

为客户端创建自定义指纹

客户端指纹根据 SYN 数据包识别操作系统，主机连接网络上的另一主机上运行的 TCP 应用时，会发送这种数据包。

如果 防火墙管理中心不与受监控的主机直接联系，指定客户端指纹属性时，可以指定防火墙管理中心管理的离想要为其设置指纹的主机最近的设备。

开始指纹设置流程之前，获取想要为其设置指纹的主机的以下相关信息：

- 主机与防火墙管理中心或用于获取指纹的设备之间的网络跳数。（思科强烈建议将防火墙管理中心或设备直接连接到与主机所连接到的同一子网）。
- 连接至主机所在网络的（防火墙管理中心或设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 访问主机以便生成客户端流量。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击**创建自定义指纹 (Create Custom Fingerprint)**。

步骤 4 从**设备**下拉列表中，选择要用于收集指纹的 防火墙管理中心或设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**客户端 (Client)**。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意
此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注释
可以使用管理接口或任何其他配置为设备上的感应接口的可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 如果要在设置指纹的主机的主机配置文件中显示自定义信息（或者如果要设置指纹的主机不在**操作系统漏洞映射**部分中），请选择**使用自定义操作系统显示**，并对于以下各项提供要显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。
- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 12 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定**供应商 (Vendor)** 和**产品 (Product)** 值。

要为所有版本的操作系统映射漏洞，请仅指定**供应商**和**产品**值。

注释
并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为主要版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商**列表中选择 **PalmSource, Inc.**，从**产品**列表中选择 **Palm 操作系统**，并让所有其他列表保持其默认设置。

步骤 13 点击**创建 (Create)**。

状态会短暂显示 `New`，然后切换至 `Pending`，此状态会保持不变，直到发现匹配指纹的流量。发现流量后，状态会切换至就绪 `(Ready)`。

“自定义指纹”(Custom Fingerprint) 状态页面每隔 10 秒进行刷新，直到其收到来自所述主机的数据。

步骤 14 将指定的 IP 地址用作目标 IP 地址，访问您尝试为其设置指纹的主机，并发起至设备的 TCP 连接。

要创建准确的指纹，收集指纹的设备**必须**发现流量。如果通过交换机进行连接，系统可能不会发现流向系统而不是设备的流量。

示例：

从想要为其设置指纹的主机访问 防火墙管理中心的 Web 界面，或者从主机使用 SSH 登录至 防火墙管理中心。如果使用的是 SSH，请使用以下命令，其中，localIPv6address 是在步骤 7 中指定的当前已分配到主机的 IPv6 地址，DCmanagementIPv6address 是 防火墙管理中心 的管理 IPv6 地址。然后，Custom Fingerprint 页面重新加载，其状态为“就绪”。

```
ssh -b localIPv6address DCmanagementIPv6address
```

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 2530 页中所述。

为服务器创建自定义指纹

服务器指纹根据 SYN-ACK 数据包识别操作系统，主机使用这种数据包来响应通向运行的 TCP 应用的传入连接。在开始之前，应获取关于想要为其设置指纹的主机的以下信息：

- 主机与用于获取指纹的设备之间的网络跳数。思科强烈建议将设备上不使用的接口直接连接到主机所连接到的相同子网。
- 连接至主机所在网络的（设备上的）网络接口。
- 主机的实际操作系统供应商、产品和版本。
- 未在使用的 IP 地址，并在主机所在网络上得到授权。

提示 如果 防火墙管理中心不与受监控的主机直接联系，指定服务器指纹属性时，可以指定离想要为其设置指纹的主机最近的托管设备。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**自定义操作系统 (Custom Operating Systems)**。

步骤 3 点击**创建自定义指纹 (Create Custom Fingerprint)**。

步骤 4 从**设备**列表中，选择要用于收集指纹的 防火墙管理中心或托管设备。

步骤 5 输入**指纹名称 (Fingerprint Name)**。

步骤 6 输入**指纹说明 (Fingerprint Description)**。

步骤 7 从**指纹类型 (Fingerprint Type)** 列表中，选择**服务器 (Server)** 以显示服务器指纹选项。

步骤 8 在**目标 IP 地址 (Target IP Address)** 字段中，输入要为其设置指纹的主机的 IP 地址。

请注意，指纹仅会基于流向和来自您指定的主机IP地址的流量，而不是主机的任何其他IP地址（如果其拥有）。

注意
只可以使用运行 5.2 及更高版本的设备捕获 IPv6 指纹。

步骤 9 在**目标距离 (Target Distance)** 字段中，输入主机与之前选择用于收集指纹的设备之间的网络跳数。

注意
此跳数必须是至主机的实际物理网络跳数，与系统检测到的跳数不一定相同。

步骤 10 从**接口 (Interface)** 列表中，选择连接到主机所在网段的网络接口。

注意
由于多个原因，思科建议**不要**将托管设备上的传感接口用于设置指纹。首先，如果传感接口位于 SPAN 端口之上，指纹技术将不起作用。另外，如果使用设备上的传感接口，设备在其收集指纹所花的时间内会停止监控网络。不过，可使用管理接口或任何其他可用网络接口来执行指纹收集。如果不知道哪个接口是设备上的传感接口，请参阅用于设置指纹的特定型号的《安装指南》。

步骤 11 点击**获取活动端口 (Get Active Ports)**。

步骤 12 在**服务器端口**字段中，输入想要设备选择用于收集指纹以便向其发起联系的端口，或者从**获取活动端口**下拉列表选择端口。

可使用主机上已知开放的任何服务器端口（例如，80，如果主机正在运行网络服务器）。

步骤 13 在**源 IP 地址 (Source IP Address)** 字段中，输入应用于尝试与主机通信的 IP 地址。

应使用经授权可在网络上使用，但目前未在使用的源 IP 地址，例如，当前未在使用的 DHCP 池地址。创建指纹时，这可防止临时访问另一离线主机。

创建指纹时，应从网络发现策略的监控中排除该IP地址。否则，网络映射和发现事件视图中将会出现大量关于该 IP 地址代表的主机的不准确信息。

步骤 14 在**源子网掩码 (Source Subnet Mask)** 字段中，输入正在使用的 IP 地址的子网掩码。

步骤 15 如果 **Source Gateway** 字段显示，输入应用于建立至主机的路由的默认网关 IP 地址。

步骤 16 如果要在设置指纹的主机的主机配置文件中显示自定义信息，或者如果要使用的指纹名称在“操作系统定义”(OS Definition) 部分中不存在，则可以在“自定义操作系统显示”(Custom OS Display) 部分中选择**使用自定义操作系统显示 (Use Custom OS Display)**。

对于以下项提供想要在主机配置文件中显示的值：

- 在**供应商字符串 (Vendor String)** 字段中，输入操作系统的供应商名称。例如，Microsoft Windows 的供应商为 Microsoft。

- 在**产品字符串 (Product String)** 字段中，输入操作系统的产品名称。例如，Microsoft Windows 2000 的产品名称为 Windows。
- 在**版本字符串 (Version String)** 字段中，输入操作系统的版本号。例如，Microsoft Windows 2000 的版本号为 2000。

步骤 17 在“操作系统漏洞映射”(OS Vulnerability Mappings) 部分中，选择要用于漏洞映射的操作系统、产品和版本。

如果要使用指纹来识别匹配主机的漏洞，或者如果不分配自定义的操作系统显示信息，则必须在此部分指定供应商和产品名称。

要为所有版本的操作系统映射漏洞，请仅指定供应商和产品名称。

注释
并非**主要版本 (Major Version)**、**次要版本 (Minor Version)**、**修订版本 (Revision Version)**、**内部版本 (Build)**、**补丁 (Patch)** 和**扩展版本 (Extension)** 下拉列表中的所有选项均可应用至选择的操作系统。此外，如果列表中没有显示与想要设置指纹的操作系统匹配的定义，可将这些值留空。请注意，如果不在指纹中创建任何操作系统漏洞映射，则系统无法使用指纹来为指纹识别的主机分配漏洞列表。

示例：

如果想要自定义指纹将 Redhat Linux 9 的漏洞列表分配到匹配主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

示例：

要添加所有版本的 Palm 操作系统，请从 **供应商 (Vendor)** 列表中选择 **PalmSource, Inc.**，从**产品 (Product)** 列表中选择 **Palm 操作系统 (Palm OS)**，并让所有其他列表保持其默认设置。

步骤 18 点击**创建 (Create)**。
“自定义指纹”(Custom Fingerprint) 状态页面每 10 秒刷新一次并应以“就绪”状态重新加载。

注释
如果目标系统在设置指纹的过程中停止响应，状态将会显示`错误：无响应 (ERROR: No Response)` 消息。如果看到此消息，请再次提交指纹。等待 3 至 5 分钟（时长可能因目标系统而异），点击 **编辑** (✎) 访问“自定义指纹”(Custom Fingerprint) 页面，然后点击 **创建 (Create)**。

下一步做什么

- 激活指纹，如激活和停用指纹 ， 第 2530 页中所述。

主机输入数据

您可以通过从第三方导入网络映射数据来扩充网络映射。您还可使用主机输入功能，只需使用 Web 界面修改操作系统或应用身份，或删除应用协议、协议、主机属性或客户端。

系统可协调来自多个源的数据，以确定操作系统或应用的当前身份。

从网络映射中删除受影响的主机后，将会丢弃除第三方漏洞之外的所有数据。有关设置脚本或导入文件的详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

要将已导入数据纳入影响关联中，必须将数据映射至数据库中的操作系统和应用定义。

第三方数据使用要求

可以从网络上的第三方系统导入发现数据。但是，要启用将入侵和发现数据结合使用的功能（例如思科建议、自适应配置文件或影响评估），应将其中尽可能多的元素映射到对应的定义。考虑对使用第三方数据的以下要求：

- 如果拥有在您的网络资产上有特定数据的第三方系统，则可使用主机输入功能导入该数据。但是，由于第三方可能会以不同的方式命名产品，因此必须将第三方供应商、产品和版本映射到对应的思科产品定义。映射产品后，必须在 防火墙管理中心配置中为影响评估启用漏洞映射，以允许影响关联。对于无版本或无供应商的应用协议，需要在 防火墙管理中心配置中映射应用协议的漏洞。
- 如果导入来自第三方的修补程序信息，并想要将修补程序修补的所有漏洞标记为无效，则必须将第三方修补程序的名称映射至数据库中的定义。修补程序针对的所有漏洞随后会从添加该修补程序所在的主机中移除。
- 如果导入来自第三方的操作系统和应用协议漏洞，并想将其用于影响关联，则必须将第三方漏洞标识字符串映射至数据库中的漏洞。请注意，尽管许多客户端拥有相关的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。映射漏洞后，必须在 防火墙管理中心配置中为影响评估启用第三方漏洞映射。要使没有供应商或版本信息的应用协议映射到漏洞，管理用户还必须在 防火墙管理中心配置中映射应用的漏洞。
- 如果导入应用数据并要将该数据用于影响关联，则必须将每个应用协议的供应商字符串映射到对应的应用协议定义。

相关主题

映射第三方产品，第 2538 页
映射第三方产品修补程序，第 2539 页
映射第三方漏洞，第 2540 页
创建自定义产品映射，第 2541 页

第三方产品映射

如果通过用户输入功能将第三方数据添加至网络映射，则必须将第三方使用的供应商、产品和版本名称映射到思科产品定义。将产品映射到思科定义后，将根据这些定义分配漏洞。

类似地，如果正在导入第三方修补程序信息，如修补程序管理产品，则必须将修补程序的名称映射至适当供应商和产品以及数据库中的相应修补程序。

映射第三方产品

如果从第三方导入数据，则必须将思科产品映射到第三方名称，以分配漏洞并使用该数据执行影响关联。映射产品可以将思科漏洞信息与第三方产品名称关联，这样，系统就可使用该数据执行影响关联。

如果使用主机输入导入功能导入数据，还可以在导入过程中，使用 AddScanResult 函数将第三方产品映射至操作系统和应用漏洞。

例如，如果从将 Apache Tomcat 列为应用的第三方导入数据，并且知道它是该产品的第 6 版，则可以添加第三方映射，其中：

- **供应商名称 (Vendor Name)** 设置为 `Apache`。
- **产品名称 (Product Name)** 设置为 `Tomcat`。
- **Apache** 是从**供应商 (Vendor)** 下拉列表中选择。
- **Tomcat** 是从**产品 (Product)** 下拉列表中选择。
- **6** 是从**版本 (Version)** 下拉列表中选择。

该映射会使 Apache Tomcat 6 的任何漏洞分配到其应用列出了 Apache Tomcat 的主机。

请注意，对于无版本或无供应商的应用，必须在 Secure Firewall Management Center配置中为应用类型映射漏洞。尽管许多客户端具有关联的漏洞，而且客户端用于影响评估，但不能导入和映射第三方客户端漏洞。

提示 如已在另一 Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此防火墙管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加产品映射 (Add Product Map)**。

- 编辑 - 要编辑现有第三方产品映射集，请点击要修改的映射集旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 输入第三方产品使用的**供应商字符串 (Vendor String)**。

步骤 8 输入第三方产品使用的**产品字符串 (Product String)**。

步骤 9 输入第三方产品使用的**版本字符串 (Version String)**。

步骤 10 在“产品映射”部分中，从以下字段为漏洞映射选择要使用的操作系统、产品和版本：**供应商**、**产品**、**主要版本**、**次要版本**、**修订版本**、**内部版本**、**补丁**和**扩展版本** 。

示例：

如果要运行其名称包含第三方字符串的产品的主机使用 Red Hat Linux 9 的漏洞，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 11 点击**保存**。

映射第三方产品修补程序

如果将修补程序名称映射至数据库中一组特定的修补程序，则可从第三方修补程序管理应用中导入数据，并对一组主机应用该修补程序。修补程序名称导入至主机后，对于该主机，系统会将修补程序针对的所有漏洞标记为无效。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新的映射集，请点击**创建产品映射集 (Create Product Map Set)**。
- 编辑 - 要编辑现有映射集，请点击要修改的映射集旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 输入**映射集名称 (Mapping Set Name)**。

步骤 5 输入**说明**。

步骤 6 您有两种选择：

- 创建 - 要映射第三方产品，请点击**添加修补程序映射 (Add Fix Map)**。
- 编辑 - 要编辑现有第三方产品映射，请点击映射旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 7 在**第三方修补程序名称 (Third-Party Fix Name)** 字段中，输入要映射的修补程序的名称。

步骤 8 在**产品映射 (Product Mappings)** 部分中，从以下字段为修补程序映射选择要使用的操作系统、产品和版本：

- **供应商**

- 产品
- 主要版本
- 次要版本
- 修订版本
- 构建
- 修补
- 分机

示例：

如果想要映射将 Red Hat Linux 9 的修补程序分配到应用补丁的主机，请选择 **Redhat, Inc.** 作为供应商、**Redhat Linux** 作为产品以及 **9** 作为版本。

步骤 9 点击**保存**，以保存修补程序映射。

映射第三方漏洞

要将第三方的漏洞信息添加至VDB，必须将每个导入的漏洞的第三方标识字符串映射至任何现有的SVID、Bugtraq或SID。为漏洞创建映射之后，该映射适用于已导入网络映射中主机的所有漏洞，且可为这些漏洞执行影响关联。

必须为第三方漏洞启用影响关联，才能允许关联发生。对于无版本或无供应商的应用，还必须在Secure Firewall Management Center配置中为应用类型映射漏洞。

尽管许多客户端拥有关联的漏洞，而且客户端用于影响评估，但不能将第三方客户端漏洞用于影响评估。

提示 如已在另一 Secure Firewall Management Center上创建了第三方映射，则将其导出后可导入至此防火墙管理中心。然后，可根据自己的需求编辑已导入的映射。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击**用户第三方映射 (User Third-Party Mappings)**。

步骤 3 您有两种选择：

- 创建 - 要创建新漏洞集，请点击**创建漏洞映射集 (Create Vulnerability Map Set)**。
- 编辑 - 要编辑现有漏洞集，请点击漏洞集旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击 **Add Vulnerability Map**。

步骤 5 在**漏洞 ID (Vulnerability ID)** 字段中输入第三方漏洞标识。

步骤 6 输入**漏洞说明 (Vulnerability Description)**。

步骤 7 或者：

- 在 **Snort 漏洞 ID 映射**字段中输入 Snort ID。
- 在 **SVID 映射 (SVID Mappings)** 字段中输入旧版漏洞 ID。
- 在 **Bugtraq 漏洞 ID 映射 (Bugtraq Vulnerability ID Mappings)** 字段中输入 Bugtraq 标识号。

步骤 8 点击**添加 (Add)**。

相关主题

启用网络发现漏洞影响评估，第 2597 页

自定义产品映射

可以使用产品映射来确保由第三方输入的服务器与适当的思科定义相关联。定义并激活产品映射后，具有映射供应商字符串的受监控主机上的所有服务器或客户端都使用自定义产品映射。为此，您可能想要为网络中带有特定供应商字符串的服务器映射漏洞，而不是显式地为服务器设置供应商、产品和版本。

创建自定义产品映射

如果系统无法将服务器映射到VDB中的供应商和产品，您可以手动创建映射。激活自定义产品映射后，系统会将指定供应商和产品的漏洞映射到出现该供应商字符串的网络映射中的所有服务器。

注释 自定义产品映射将应用于所有出现应用协议的位置，无论应用数据的源为何（如Nmap、主机输入功能或系统自身）。然而，如果使用主机输入功能导入的数据的第三方漏洞映射与通过自定义产品映射设置的映射发行冲突，则输入出现时，第三方漏洞映射将覆盖自定义产品映射并使用第三方漏洞映射设置。

可创建产品映射列表，然后通过激活或停用每份列表而一次性启用或禁用多个映射。指定将要映射到的供应商后，系统将更新产品列表，以仅包含该供应商提供的产品。

创建自定义产品映射后，必须激活自定义产品映射列表。激活自定义产品映射列表后，系统将更新出现指定供应商字符串的所有服务器。对于通过主机输入功能导入的数据，漏洞将更新，除非已为此服务器显式设置产品映射。

例如，如果贵公司将您的 Apache Tomcat Web 服务器的横幅修改为 `Internal Web Server`，则可将供应商字符串 `Internal Web Server` 映射到供应商 **Apache** 和产品 **Tomcat**，然后激活包含该映射的列表，出现标有 `Internal Web Server` 的服务器的所有主机均拥有数据库中的 Apache Tomcat 漏洞。

提示 可使用此功能将漏洞映至至本地入侵规则，只需将规则的 SID 映射至另一漏洞。

过程

步骤 1 选择策略 > + 显示更多 > 高级 > 自定义应用检测器。
步骤 2 点击自定义产品映射 (Custom Product Mappings)
步骤 3 点击 Create Custom Product Mapping List。
步骤 4 输入自定义产品映射列表名称 (Custom Product Mapping List Name)。
步骤 5 点击添加供应商字符串 (Add Vendor String)。
步骤 6 在供应商字符串 (Vendor String) 字段中，输入供应商字符串，该字符串标识应映射到所选供应商和产品值的应用。
步骤 7 从供应商 (Vendor) 下拉列表，选择要映射的供应商。
步骤 8 从产品 (Product) 下拉列表，选择要映射的产品。
步骤 9 点击添加 (Add)，以将已映射的供应商字符串添加到列表。
步骤 10 或者，在必要时，重复第 4 至 8 步，将额外的供应商字符串映射添加至列表。
步骤 11 点击保存。

下一步做什么

- 激活自定义产品映射列表。有关详细信息，请参阅激活和停用自定义产品映射，第 2543 页。

编辑自定义产品映射列表

可修改现有自定义产品映射列表，只需添加或移除供应商字符串或更改列表名称。

过程

步骤 1 选择策略 > + 显示更多 > 高级 > 自定义应用检测器。
步骤 2 点击自定义产品映射 (Custom Product Mappings)。
步骤 3 点击要编辑的产品映射列表旁边的 编辑 ()。

如果显示视图 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 对列表进行更改，如创建自定义产品映射，第 2541 页中所述。
步骤 5 完成后，点击保存。

激活和停用自定义产品映射

可一次性启用或禁用整个自定义产品映射列表。激活自定义产品映射列表后，该列表上的每个映射均应用所有带有指定供应商字符串的应用，无论是通过托管设备检测到的，还是通过主机输入功能导入的。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击**自定义产品映射 (Custom Product Mappings)**。

步骤 3 点击要激活或停用的自定义产品映射列表旁边的滑块。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置主机输入客户端

主机输入功能允许您从另一台设备上运行的客户端程序更新 防火墙管理中心的网络映射。例如，您可以从网络映射添加或删除主机，或者更新主机操作系统和服务信息。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

只有先从“主机输入客户端”页面将客户端添加到 防火墙管理中心的对等数据库，然后才能运行远程客户端。还必须将 防火墙管理中心生成的身份验证证书复制至客户端。完成这些步骤之后，客户端可连接到 防火墙管理中心。

在多域部署中，可以在任何域中创建客户端。身份验证证书允许客户端为与客户端证书的域关联的任何分叶域提交网络映射更新。如果您为祖先域创建证书（或如果您的证书域在添加后代域之后成为祖先域），则使用该证书的任何客户端都必须指定每个事务的目标分叶域，如《*Firepower* 系统主机输入 *API* 指南》中所述。

“主机输入客户端”(Host Input Client) 仅显示与当前域关联的客户端，因此，如果您要下载或撤销证书，请切换至创建客户端时所在的域。

此连接使用 TLS 1.2。

过程

步骤 1 选择 **集成** > **+ 显示更多** > **主机输入客户端**

步骤 2 点击**创建客户端 (Create Client)**。

步骤 3 在**主机名 (Hostname)** 字段中，输入运行主机输入客户端的主机的主机名称或 IP 地址。

注释
如果尚未配置 DNS 解析，请使用 IP 地址。

步骤 4 如果要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。

步骤 5 点击**保存**。
主机输入服务将允许主机访问 防火墙管理中心上的 8307 端口，并会创建在客户端-服务器身份验证过程中使用的身份验证证书。

步骤 6 点击证书文件旁边的 **下载** （）。

步骤 7 将证书文件保存至客户端用于 SSL/TLS 身份验证的目录。

步骤 8 要撤消客户端的访问权限，请点击想要移除的主机旁边的 **删除** ()。

Nmap 扫描

Firepower 系统通过对网络上的流量进行被动分析构建网络映射。根据系统的情况，通过这种被动分析获取的信息有时可能并不完整。不过，您可以主动扫描主机，获取完整信息。例如，如果主机有一台服务器在开放端口上运行，但该服务器在系统监控网络期间未收发流量，则系统不会向网络映射添加有关该服务器的信息。但是，如使用主动扫描程序直接扫描主机，则可检测到服务器的存在。

Firepower 系统与用于网络探索和安全审核的开源主动扫描程序 Nmap™ 集成。

使用 Nmap 扫描主机时，系统会：

- 将之前未检测到的开放端口上的服务器添加至该主机配置文件中的服务器列表。主机配置文件在“扫描结果”(Scan Results) 部分列出在已过滤或关闭 TCP 端口或 UDP 端口上检测到的任何服务器。默认情况下，Nmap 扫描 1660 多个 TCP 端口。

  如果系统识别在 Nmap 扫描中已确定的服务器且有对应的服务器定义，系统会将 Nmap 用于该服务器的名称映射至对应的思科服务器定义。

- 然后，将扫描结果与超过1500个已知操作系统指纹进行对比，确定操作系统，并为每个操作系统评分。分配给主机的操作系统是得分最高的操作系统指纹。

  系统会将 Nmap 操作系统名称映射至思科操作系统定义。

- 为添加的服务器和操作系统将漏洞分配至主机。

注意：

- 只有网络映射中存在主机，Nmap 才能将其结果附加至主机配置文件。
- 如果从网络映射中删除主机，则将丢弃该主机的任何 Nmap 扫描结果。

提示 有些扫描选项（例如，端口扫描）会显著增加低带宽网络的负载。请将此类扫描安排在网络使用量较低的时段运行。

有关用于扫描的基础 Nmap 技术的详细信息，请参阅 http://insecure.org/ 上的 Nmap 文档。

Nmap 补救选项

可以创建 Nmap 补救以定义 Nmap 扫描设置。Nmap 补救可用作关联策略中的响应，按需运行，或预定在特定时间运行。

请注意，Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 扫描主机以获取操作系统和服务器数据，则可能要设置定期扫描，随时更新任何 Nmap 提供的操作系统和服务器数据。

下表说明可在 Nmap 补救中配置的选项。

表 *154: Nmap* 补救选项

选项	说明	对应的 Nmap 选项
扫描事件中的哪个地址？(Scan Which Address(es) From Event?)	将 Nmap 扫描用作对关联规则的响应时，选择以下其中一个选项以控制扫描事件中的哪个地址，源主机的地址和/或目标主机的地址： • **扫描源地址和目标地址 (Scan Source and Destination Addresses)**，扫描事件中源 IP 地址和目标 IP 地址代表的主机。 • **仅扫描源地址 (Scan Source Address Only)**，扫描事件的源 IP 地址代表的主机。 • **仅扫描目标地址 (Scan Destination Address Only)**，扫描事件的目标 IP 地址代表的主机。	不适用
扫描类型 (Scan Types)	选择 Nmap 如何扫描端口： • **TCP 同步 (TCP Syn)** 扫描可以快速连接到数千个端口，无需使用完整的 TCP 握手。此选项可用于在以下主机上以隐形模式快速扫描，可发起但不完成 TCP 连接：`admin` 帐户拥有原始数据包访问权限的主机，或未运行 IPv6 的主机。如果主机确认在 TCP Syn 扫描中发送的 Syn 数据包，Nmap 会重置连接。 • **TCP 连接 (TCP Connect)** 扫描使用 `connect()` 系统调用，打开穿过主机操作系统的连接。如果 防火墙管理中心或托管设备上的 `admin` 用户在主机上没有原始数据包权限，或正在扫描 IPv6 网络，则可使用“TCP 连接”扫描。换句话说，在无法使用“TCP 同步”(TCP Syn) 扫描的情况下使用此选项。 • **TCP ACK** 扫描发送 ACK 数据包，检查端口是否已被过滤。 • **TCP 窗口 (TCP Window)** 扫描的工作方式与 TCP ACK 扫描相同，但也可确定端口已打开还是关闭。 • **TCP Maimon** 扫描使用 FIN/ACK 探针识别 BSD 派生系统。	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
扫描 UDP 端口 (Scan for UDP ports)	启用此选项，可扫描 UDP 端口以及 TCP 端口。请注意，扫描 UDP 端口可能比较耗时，因此，如果想快速扫描，请避免使用此选项。	`-sU`

选项	说明	对应的 Nmap 选项
使用事件中的端口 (Use Port From Event)	如果计划将补救用作关联政策中的响应，请启用此选项，使补救仅扫描在触发关联响应的事件中指定的端口。 • 选择**打开 (On)** 以扫描关联事件中的端口，而不是在 Nmap 补救配置过程中指定的端口。如果扫描关联事件中的端口，请注意，补救将扫描在 Nmap 补救配置过程中指定的 IP 地址上的端口。这些端口也会添加至补救的动态扫描目标。 • 选择**关闭 (Off)**，仅扫描在 Nmap 补救配置过程中指定的端口。 您也可以控制 Nmap 是否收集关于操作系统和服务器信息的信息。启用**使用事件中的端口 (Use Port From Event)** 选项，可扫描与新服务器关联的端口。	不适用
从报告检测引擎扫描 (Scan from reporting detection engine)	启用此选项，可从报告主机的检测引擎所驻留的设备扫描主机。 • 要从运行报告检测引擎的设备扫描，请选择**打开 (On)**。 • 要从已在补救中配置的设备扫描，请选择**关闭 (Off)**。	不适用
快速端口扫描 (Fast Port Scan)	启用此选项，仅扫描 `nmap-services` 文件中所列的 TCP 端口，而忽略其他端口设置，该文件位于执行扫描设备上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中。请注意，不能同时使用此选项与**端口范围和扫描顺序 (Port Ranges and Scan Order)** 选项。 • 要仅扫描 `nmap-services` 文件中列出的端口，而忽略其他端口设置，请选择**打开 (On)**，该文件可在扫描设置上的 `/var/sf/nmap/share/nmap/nmap-services` 目录中找到。 • 要扫描所有 TCP 端口，请选择**关闭 (Off)**。	`-F`
端口范围和扫描顺序 (Port Ranges and Scan Order)	使用Nmap端口规范语法设置要扫描的特定端口及其扫描顺序。请注意，不能同时使用此选项与**快速端口扫描 (Fast Port Scan)** 选项。	`-p`
探测开放端口以获取供应商和版本信息(Probe open ports for vendor and version information)	启用此选项，可检测服务器供应商和版本信息。如果探测开放端口以获取服务器供应商和版本信息，Nmap将获取其用来识别服务器的服务器数据。然后，它会为该服务器替换思科服务器数据。 • 选择**On**，扫描主机上的开放端口以获取服务器信息，识别服务器厂商和版本。 • 选择**关闭 (Off)**，继续使用主机的思科服务器信息。	`-sV`

选项	说明	对应的 Nmap 选项
服务版本强度 (Service Version Intensity)	选择适用于服务器版本的 Nmap 探针强度。 • 要使用更多探针进行更精确、更长久的扫描，请选择一个较大的数字。 • 要使用更少探针进行不太精确、更加快速的扫描，请选择一个较小的数字。	`--version-intensity` <强度>
检测操作系统 (Detect Operating System)	启用此选项，可检测主机的操作系统信息。 如果配置主机的操作系统检测，Nmap将扫描主机，并使用扫描结果创建每个操作系统的评级，反映操作系统在主机上运行的可能性。 • 选择 **On**，扫描主机获取信息，识别操作系统。 • 选择**关闭 (Off)**，继续使用主机的思科操作系统信息。	`-o`
将所有主机视为在线 (Treat All Hosts As Online)	启用此选项，可跳过主机发现过程，在目标范围内的每台主机上运行端口扫描。请注意，启用此选项时，Nmap 会忽略**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 的设置。 • 要跳过主机发现过程，在目标范围中的每台主机上运行端口扫描，请选择**打开 (On)**。 • 要使用**主机发现方法 (Host Discovery Method)** 和**主机发现端口列表 (Host Discovery Port List)** 设置执行主机发现，并跳过任何不可用的主机上的端口扫描，请选择**关闭 (Off)**。	`-PN`

选项	说明	对应的 Nmap 选项
主机发现方法 (Host Discovery Method)	选择此选项，在**主机发现端口列表 (Host Discovery Port List)** 中列出的端口上，为目标范围中的所有主机执行主机发现，或者，如未列出端口，则在适用于主机发现方法的默认端口上执行。 然而，请注意，如也启用**将所有主机视为在线 (Treat All Hosts As Online)**，**主机发现方法 (Host Discovery Method)** 选项不起作用，也不执行主机发现。 选择 Nmap 进行测试以查看主机是否存在且可用时使用的方法： • 如果收到响应，**TCP SYN** 选项将发送设置了 SYN 标记的空 TCP 数据包，并认为主机可用。默认情况下，TCP SYN 扫描端口 80。请注意，TCP SYN 扫描不太可能被设有状态性防火墙规则的防火墙拦截。 • 如果收到响应，**TCP ACK** 选项将发送设置了 ACK 标志的空 TCP 数据包，并认为主机可用。默认情况下，TCP ACK 也扫描端口 80。请注意，TCP ACK 扫描不太可能被设有无状态防火墙规则的防火墙拦截。 • 如果端口不可达响应来自已关闭端口，**UDP** 选项将发送 UDP 数据包，并假设主机可用性。默认情况下，UDP 扫描端口 40125。	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
主机发现端口列表 (Host Discovery Port List)	指定在执行主机发现时要扫描的自定义端口列表，用逗号隔开。	主机发现方法端口列表
默认 NSE 脚本 (Default NSE Scripts)	启用此选项，可以运行默认 Nmap 脚本集，执行主机发现以及服务器、操作系统和漏洞检测。请登录 https://nmap.org/nsedoc/categories/default.html，查看默认脚本列表。 • 要运行默认 Nmap 脚本集，请选择**打开 (On)**。 • 要跳过默认 Nmap 脚本集，请选择**关闭 (Off)**。	`-sC`
计时模板 (Timing Template)	选择扫描过程的时间；选择的数字越大，扫描越快、越不全面。	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 扫描准则

尽管主动扫描可以获取宝贵信息，但过度使用 Nmap 等工具可能会使您的网络资源超载，甚至使重要的主机瘫痪。使用任何主动式扫描工具时，应遵循这些准则创建扫描策略，确保仅扫描需要扫描的主机和端口。

选择适当的扫描目标

配置 Nmap 时，可创建扫描目标以识别要扫描的主机。扫描目标包括一个 IP 地址、CIDR 块或八位字节 IP 地址范围、IP 地址范围或要扫描的 IP 地址或范围列表，以及一台或多台主机上的端口。

可通过以下方式指定目标：

- 对于 IPv6 主机：
  - 确切的 IP 地址（例如 `2001:DB8:1::178:ABCD`）
- 对于 IPv4 主机：
  - 精确的 IP 地址（例如，`192.168.1.101`）或 IP 地址列表（用逗号或空格隔开）
  - 使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机）
  - 使用八位字节范围寻址的 IP 地址范围（例如，`192.168.0-255.1-254` 扫描 192.168.x.x 范围内的所有地址，但以 .0 和 .255 结尾的地址除外）
  - 使用连字符的 IP 地址范围（例如，`192.168.1.1 - 192.168.1.5` 扫描在 192.168.1.1 和 192.168.1.5（含）之间的六台主机）
  - 地址或范围列表，用逗号或空格隔开（例如，`192.168.1.0/24`，`194.168.1.0/24` 扫描 192.168.1.1 和 192.168.1.254（含）之间的 254 台主机，以及 194.168.1.1 和 194.168.1.254（含）之间的 254 台主机）

Nmap扫描的理想扫描目标包括有系统无法识别的操作系统的主机、有无法识别的服务器的主机，或者最近在网络上检测到的主机。请记住，Nmap 结果不能添加到不存在于网络映射中主机的网络映射。

⚠

注意

- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。
- 如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。
- 请确保您有权限扫描您的目标。使用 Nmap 扫描不属于您或贵公司的主机可能违法。

选择适当端口进行扫描

可为已配置的每个扫描目标选择要扫描的端口。您可以指定各个端口号、端口范围或一系列端口号和端口范围，识别应当在每个目标上扫描的精确端口集。

默认情况下，Nmap 扫描 TCP 端口 1 至端口 1024。如果计划将补救用作关联政策中的响应，则可使补救仅扫描在触发关联响应的事件中指定的端口。如果按需运行补救或将补救作为预定任务加以运行，或者，如不使用来自事件的端口，则可使用其他端口选项确定哪些端口已扫描。可选择仅扫描在 `nmap-services` 文件中列出的 TCP 端口，忽略其他端口设置。除 TCP 端口外，还可扫描 UDP 端口。请注意，扫描UDP端口可能比较耗时，因此，如要快速扫描，请避免使用此选项。为选择要扫描的特定端口或端口范围，请使用 Nmap 端口规范语法识别端口。

设置主机发现选项

在开始主机的端口扫描之前，可决定是否执行主机发现，或者，可假设计划要扫描的所有主机均在线。如果选择不将所有主机视为在线，则可选择要使用的主机发现方法，如果需要，自定义在主机发现过程中扫描的端口列表。主机发现不能从已列出端口探测操作系统或服务器信息；它仅使用特殊端口上的响应确定主机是否活动且可用。如果执行主机发现且主机不可用，Nmap则不扫描该主机上的端口。

示例：使用 Nmap 解析未知操作系统

本示例介绍用于解析未知操作系统的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅 管理 Nmap 扫描，第 2552 页。

如果系统无法确定网络上主机的操作系统，则可使用Nmap主动扫描主机。Nmap使用其通过扫描获取的信息对可能的操作系统进行评级。然后，它使用评级最高的操作系统作为主机操作系统标识。

使用 Nmap 向新主机质询操作系统和服务器信息，会停用系统对已扫描主机的该数据进行的监控。如果使用 Nmap 发现系统标记为拥有未知操作系统的主机的主机操作系统和服务器操作系统，您也许能够识别相似的主机组。然后，可根据其中一个主机组创建自定义指纹，使系统能够根据 Nmap 扫描，将指纹与已知在主机上运行的操作系统相关联。尽可能创建自定义指纹，而不是通过第三方来源（例如，Nmap）输入静态数据，因为自定义指纹允许系统继续监控主机操作系统并按需更新。

在本例中，您将：

1. 配置扫描实例，如添加 Nmap 扫描实例，第 2553 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建在系统检测到具有未知操作系统的主机时触发的关联规则。该规则应在**发生发现事件**并且**主机的操作系统信息已更改**且符合以下条件时触发：**操作系统名称未知**。

4. 创建包含关联规则的关联策略。
5. 在关联策略中，将第 2 步中创建的 Nmap 补救作为响应添加至第 3 步中创建的规则。
6. 激活关联策略。
7. 清除网络映射上的主机，强制网络发现重新启动，重建网络映射。
8. 一两天后，搜索关联策略生成的事件。分析在主机上检测到的操作系统的Nmap结果，弄清网络上是否有系统无法识别的特殊主机配置。
9. 如果发现未知操作系统的Nmap结果相同的主机，请为其中一台主机创建自定义指纹，并用它识别未来的类似主机。

相关主题

创建 Nmap 补救，第 2556 页
Nmap 扫描结果，第 2559 页
为客户端创建自定义指纹，第 2532 页

示例：使用 Nmap 响应新主机

此示例介绍旨在对新主机作出响应的 Nmap 配置。有关 Nmap 配置的完整介绍，请参阅 管理 Nmap 扫描，第 2552 页。

当系统在子网中检测到可能被入侵的新主机时，您可能想扫描该主机，确保获取该主机漏洞的准确信息。

要完成此操作，可创建和激活关联策略，当子网中出现新主机时进行检测，并启动补救以对该主机执行 Nmap 扫描。

为此，将会执行以下操作：

1. 配置扫描实例，如添加 Nmap 扫描实例，第 2553 页中所述。
2. 使用以下设置创建 Nmap 补救：
   - 启用 **Use Port From Event**，可扫描与新服务器相关的端口。
   - 启用**检测操作系统 (Detect Operating System)**，可检测主机的操作系统信息。
   - 启用**探测开放端口以了解厂商和版本信息 (Probe open ports for vendor and version information)**，可检测服务器厂商和版本信息。
   - 启用**将所有主机视为在线 (Treat All Hosts as Online)**，因为已知该主机存在。
3. 创建当系统在特定子网上检测到新主机时触发的关联规则。此规则应在**发生发现事件**并**检测到新主机时**触发。
4. 创建包含关联规则的关联策略。
5. 在关联策略中，将在以前步骤中创建的 Nmap 补救作为响应添加至在第 3 步中创建的规则。
6. 激活关联策略。

7. 收到出现新主机的通知时，检查主机配置文件，以查看Nmap扫描结果并解决适用于该主机的任何漏洞。

激活策略后，可以定期检查补救状态视图（**事件和日志** > **+ 显示更多** > **关联** > **状态**）以查看补救启动时间。补救的动态扫描目标应当包括因服务器检测而扫描到的主机的 IP 地址。根据 Nmap 检测到的操作系统和服务器，查看这些主机的主机配置文件，弄清主机上是否存在需要解决的漏洞。

注意 如有大型或动态网络，新主机检测可能太频繁，而无法使用扫描进行响应。为防止资源超载，请避免使用 Nmap 扫描响应频繁发生的事件。另请注意，如果使用 Nmap 向新主机质询操作系统和服务器信息，则会停用思科对已扫描主机的该数据进行的监控。

相关主题

创建 Nmap 补救，第 2556 页

管理 Nmap 扫描

要使用 Nmap 扫描，至少必须配置一个 Nmap 扫描实例和一个 Nmap 补救。是否配置 Nmap 扫描目标可以选择。

过程

步骤 1 配置 Nmap 扫描：

- 如添加 Nmap 扫描实例，第 2553 页中所述，添加 Nmap 扫描实例。
- 如创建 Nmap 补救，第 2556 页中所述，创建 Nmap 补救。
- 或者，也可以如添加 Nmap 扫描目标，第 2554 页中所述，添加 Nmap 扫描目标。

步骤 2 运行 Nmap 扫描：

- 如运行按需 Nmap 扫描，第 2558 页中所述，运行按需 Nmap 扫描。
- 如*Cisco Secure Firewall Management Center* 管理指南的*Nmap* 扫描自动化中所述，配置自动 Nmap 扫描。
- 如*Cisco Secure Firewall Management Center* 管理指南的安排 *Nmap* 扫描中所述，安排自动 Nmap 扫描。

下一步做什么

- 通过查看相关任务，监控正在进行的 Nmap 扫描；请参阅*Cisco Secure Firewall Management Center* 管理指南中的查看任务消息。
- 或者，也可以优化扫描：
  - 如编辑 Nmap 扫描实例，第 2554 页中所述，编辑 Nmap 扫描实例。

- 如编辑 Nmap 扫描目标，第 2555 页中所述，编辑 Nmap 扫描目标。
- 如编辑 Nmap 补救，第 2558 页中所述，编辑 Nmap 补救。

添加 Nmap 扫描实例

可为要用于扫描网络漏洞的每个 Nmap 模块设置独立的扫描实例。可为 Secure Firewall Management Center上的本地 Nmap 模块以及要用于远程运行扫描的任何设备设置扫描实例。每次扫描的结果始终存储在 防火墙管理中心上，可在这里配置扫描，即使是从远程设备运行扫描。为防止意外或恶意扫描关键任务主机，可创建实例黑名单，指出不应通过实例扫描的主机。

不能添加名称与任何现有扫描实例相同的扫描实例。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > **+ 显示更多** > **关联** > **实例**。
- 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

步骤 2 添加补救：

- 如果通过上述第一种方法访问列表，请找到“添加新实例”(Add a New Instance) 部分，从下拉列表中选择“Nmap 补救”(Nmap Remediation) 模块，然后点击**添加 (Add)**。
- 如果通过上述第二种方法访问该列表，请点击**添加 Nmap 实例 (Add Nmap Instance)**。

步骤 3 输入**实例名称 (Instance Name)**。

步骤 4 输入**说明**。

步骤 5 或者，在**豁免的主机 (Exempted hosts)** 字段中，使用以下语法指定任何 绝不应使用此扫描实例扫描的主机或网络：

- 对于 IPv6 主机，精确的 IP 地址（例如，`2001:DB8::fedd:eeff`）
- 对于 IPv4 主机，精确的 IP 地址（例如，`192.168.1.101`）或使用 CIDR 表示法的 IP 地址块（例如，`192.168.1.0/24` 扫描 `192.168.1.1` 和 `192.168.1.254` [含] 之间的 254 台主机）
- 请注意，不能使用感叹号 (!) 否定地址值。

注释
如果明确将黑名单网络中的主机作为扫描目标，该扫描将不运行。

步骤 6 或者，要从远程设备而非防火墙管理中心运行扫描，请在**远程设备名称 (Remote Device Name)** 字段中指定设备的 IP 地址或名称，因为它会显示在 防火墙管理中心 Web 界面中的设备“信息”(Information) 页面中。

步骤 7 点击**创建 (Create)**。
系统创建完实例后，以编辑模式显示实例。

步骤 8 或者，将 Nmap 补救添加到实例。为此，请找到实例的“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**，然后创建补救，如创建 Nmap 补救，第 2556 页中所述。

步骤 9 点击**取消 (Cancel)**，返回实例列表。

注释
如果您通过**扫描程序 (Scanners)** 访问 Nmap 扫描实例列表，系统不会显示您添加的实例，除非您也将补救添加到该实例。要查看尚未添加补救的实例，请使用**实例 (Instances)** 菜单选项访问列表。

编辑 Nmap 扫描实例

当编辑扫描实例时，可以查看、添加和删除与实例关联的补救。不再想使用 Nmap 扫描实例中描述的 Nmap 模块时，请删除该 Nmap 扫描实例。请注意，如果删除扫描实例，也将删除使用该实例的任何补救。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > + **显示更多** > **关联** > **实例**。
- 选择**策略** > + **显示更多** > **关联** > **扫描器**。

步骤 2 在要编辑的实例旁，点击 **视图** ( )。

步骤 3 对扫描实例设置进行更改，如添加 Nmap 扫描实例，第 2553 页中所述。

步骤 4 点击**保存**。

步骤 5 点击 **Done**。

下一步做什么

- 或者，将新补救添加到扫描实例；请参阅 创建 Nmap 补救，第 2556 页
- 或者，编辑与实例关联的补救；请参阅编辑 Nmap 补救，第 2558 页。
- 或者，删除与实例关联的补救；请参阅运行按需 Nmap 扫描，第 2558 页。
- 或者，通过点击扫描目标旁边的 **删除** ( ) 来删除扫描实例。

添加 Nmap 扫描目标

配置 Nmap 模块时，可创建和保存扫描目标，识别想在执行按需或预定扫描时作为扫描目标的主机和端口，从而避免每次构建新扫描目标。扫描目标包括一个或一组要扫描的 IP 地址，以及一台或多台主机上的端口。对于 Nmap 目标，也可使用 Nmap 八位字节范围寻址或 IP 地址范围。有关 Nmap 八位组范围寻址的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

注意：

- 扫描包含大量主机的扫描目标可能需要延长的时间。作为一种解决方法，每次仅扫描几台主机。
- Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击 **Create Scan Target**。

步骤 4 在**名称 (Name)** 字段中，输入要用于此扫描目标的名称。

步骤 5 在 **IP 范围 (IP Range)** 文本框中，使用Nmap 扫描准则，第 2549 页中所述的语法指定要扫描的一个或多个主机。

注释
如果在扫描目标中的 IP 地址或范围列表中使用逗号，则保存目标时，逗号将转换为空格。

步骤 6 在**端口 (Ports)** 字段中，指定要扫描的端口。

可使用从 1 到 65535 的值输入以下任意项：

- 端口号
- 用逗号分隔的端口列表
- 用连接号分隔的端口号范围
- 多个用连接号分隔的端口号范围，用逗号分隔

步骤 7 点击**保存**。

编辑 Nmap 扫描目标

提示 如果不想使用补救扫描特定 IP 地址，但是该 IP 地址已添加至目标，则可能想编辑补救的动态扫描目标，因为主机参与了启动补救的关联策略违反事件。

如果不再想扫描已在扫描目标中列出的主机，请删除扫描目标。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

步骤 2 在工具栏上，点击 **Targets**。

步骤 3 点击要编辑的扫描目标旁边的 **编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 按需进行修改。有关详细信息，请参阅添加 Nmap 扫描目标，第 2554 页。

步骤 5 点击**保存**。

步骤 6 或者，通过点击扫描目标旁边的 **删除** () 来删除扫描目标。

创建 Nmap 补救

Nmap补救只可以通过将它添加到现有Nmap扫描实例来创建。补救定义了扫描的设置。它可用作关联策略中的响应、按需运行或在指定时间作为预定任务运行。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

有关 Nmap 功能的一般信息，请参阅 http://insecure.org 上的 Nmap 文档。

开始之前

- 如添加 Nmap 扫描实例，第 2553 页中所述，添加 Nmap 扫描实例。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **实例**。

步骤 2 点击要添加补救的实例旁边的 **视图** ()。

步骤 3 在“已配置补救”(Configured Remediations) 部分，点击**添加 (Add)**。

步骤 4 输入**补救名称 (Remediation Name)**。

步骤 5 输入**说明**。

步骤 6 如果计划使用此补救响应在发生入侵事件、连接事件或用户事件时触发的关联规则，请配置**扫描事件中的哪个地址？(Scan Which Address(es) From Event?)** 选项。

提示
如果计划使用此补救响应在发生发现事件或主机输入事件时触发的关联规则，默认情况下，补救将扫描事件涉及到的主机的 IP 地址；无需配置此选项。

注释
请**勿**为了响应在流量配置文件发生变化时触发的关联规则而分配 Nmap 补救。

步骤 7 配置**扫描类型 (Scan Type)** 选项。

步骤 8 或者，除了 TCP 端口，还要扫描 UDP 端口，请为**扫描 UDP 端口 (Scan for UDP ports)** 选项选择**开启 (On)**。

提示
UDP 端口扫描比 TCP 端口扫描需要更多的时间。要加速扫描，请禁用此选项。

步骤 9 如果计划使用此补救响应关联策略违反事件，请配置**使用事件中的端口 (Use Port From Event)** 选项。

步骤 10 如果计划使用此补救响应关联策略违反事件，并希望使用运行检测引擎来检测事件的设备运行扫描，请配置**从报告检测引擎扫描 (Scan from reporting detection engine)** 选项。

步骤 11 配置**快速端口扫描 (Fast Port Scan)** 选项。

步骤 12 在**端口范围和扫描顺序 (Port Ranges and Scan Order)** 字段中，输入要在默认情况下使用 Nmap 端口规范语法按自己想要的顺序扫描的端口。

使用以下格式：

- 指定从 1 到 65535 的值。
- 使用逗号或空格分隔端口。
- 使用连字符指明端口范围。
- 扫描 TCP 和 UDP 端口时，以 T 作为要扫描的 TCP 端口列表的开端，以 U 作为 UDP 端口列表的开端。

注释
启动补救以响应关联策略违反事件时，**使用事件中的端口 (Use Port From Event)** 选项将覆盖此设置，如第 8 步中所述。

示例：

要扫描 UDP 流量的端口 53 和 111，然后扫描 TCP 流量的端口 21-25，请输入 `U:53,111,T:21-25`。

步骤 13 要探测开放端口以了解服务器厂商和版本信息，请配置**探测开放端口以获取供应商和版本信息 (Probe open ports for vendor and version information)**。

步骤 14 如果选择探测开放端口，请从**服务版本强度 (Service Version Intensity)** 下拉列表中选择一个数字，设置使用的探针数量。

步骤 15 要扫描操作系统信息，请配置**检测操作系统 (Detect Operating System)** 设置。

步骤 16 要确定主机发现是否发生，是否仅针对可用端口运行端口扫描，请配置**将所有主机视为在线 (Treat All Hosts As Online)**。

步骤 17 要设置希望 Nmap 在测试主机可用性时使用的方法，请从**主机发现方法 (Host Discovery Method)** 下拉列表中选择一种方法。

步骤 18 如果要在主机发现过程中扫描自定义端口列表，请在**主机发现端口列表 (Host Discovery Port List)** 字段中输入适合所选主机发现方法的端口列表，用逗号隔开。

步骤 19 配置**默认 NSE 脚本 (Default NSE Scripts)** 选项，控制是否使用默认 Nmap 脚本集进行主机发现以及服务器、操作系统和漏洞发现。

提示
请参阅 http://nmap.org/nsedoc/categories/default.html，获取默认脚本列表。

步骤 20 要设置扫描过程的时间选择，请从**计时模板 (Timing Template)** 下拉列表中选择计时模板编号。

选择的编号越大，速度越快，扫描越不全面；而选择的编号越小，速度越慢，扫描越全面。

步骤 21 点击**创建 (Create)**。
系统创建完补救后，在编辑模式中显示它。

步骤 22 点击**完成 (Done)** 以返回相关实例。

步骤 23 点击**确定 (OK)** 以返回实例列表。

相关主题

Nmap 补救选项，第 2545 页

编辑 Nmap 补救

对 Nmap 补救所做的更改不会影响正在进行的扫描。新设置将在下一次扫描开始时生效。删除不再需要的 Nmap 补救。

过程

步骤 1 使用以下任一种方法访问 Nmap 扫描实例列表：

- 选择**策略** > + **显示更多** > **关联** > **实例**。
- 选择**策略** > + **显示更多** > **关联** > **扫描器**。

步骤 2 访问要编辑的补救：

- 如果通过上述第一种方法访问列表，请点击相关实例旁的 **视图** ()，然后在要在“已配置补救”部分中编辑的补救旁边再次点击该补救。
- 如果通过上述第二种方法访问列表，请点击要编辑的补救边的 **视图** ()。

步骤 3 根据需要进行修改，如创建 Nmap 补救，第 2556 页中所述。

步骤 4 如果要保存更改，请点击**保存**，或者如果要不保存而直接退出，请点击**完成**。

步骤 5 或者，通过点击补救旁边的 **删除** () 来删除补救。

运行按需 Nmap 扫描

可在需要时启动按需 Namp 扫描。可以通过输入要扫描的 IP 地址和端口或者通过选择现有扫描目标，指定按需扫描目标。

Nmap提供的服务器和操作系统数据将保持不变，直到您运行另一个Nmap扫描为止。如果计划使用 Nmap 来扫描主机，请定期安排扫描。如果从网络映射中删除主机，将丢弃任何 Nmap 扫描结果。

开始之前

- 或者，添加 Nmap 扫描目标；请参阅添加 Nmap 扫描目标，第 2554 页。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

步骤 2 在要用于执行扫描的 Nmap 补救旁，点击 **扫描**（ ）。

步骤 3 或者，要使用已保存的扫描目标进行扫描，请从**已保存的目标**下拉列表中选择目标，然后点击**加载**。

步骤 4 在 **IP 范围 (IP Range[s])** 字段中，指定要扫描或修改已加载列表的主机的 IP 地址。

注意：

- 对于带 IPv4 地址的主机，可指定多个 IP 地址，用逗号隔开，或者使用 CIDR 表示法。也可在 IP 地址前面添加感叹号 (!)，否定 IP 地址。
- 对于带 IPv6 地址的主机，请使用精确的 IP 地址。不支持地址范围。

步骤 5 在**端口 (Ports)** 字段中，指定要扫描的端口或修改已加载的列表。

可输入一个端口号、用逗号隔开的端口列表或者用连接号隔开的端口号范围。

步骤 6 点击**立即扫描 (Scan Now)**。

下一步做什么

- 或者，监控任务状态；请参阅*Cisco Secure Firewall Management Center* 管理指南中的查看任务消息。

Nmap 扫描结果

您可以监控正在进行的 Nmap 扫描，导入先前通过 Firepower 系统执行的扫描中的结果或在 Firepower 系统外执行的结果，以及查看和分析扫描结果。

您可查看作为弹出窗口中渲染页面的扫描结果（使用本地 Nmap 模块创建），也可下载原始 XML 格式的 Nmap 结果文件。

您还可在主机配置文件和网络映射中查看由 Nmap 检测到的操作系统和服务器信息。如果主机扫描为已过滤或已关闭端口上的服务器生成服务器信息，或者如果扫描收集无法包含在操作系统信息或服务器部分中的信息，主机配置文件会将这些结果纳入“Nmap 扫描结果”(Nmap Scan Results) 部分。

查看 Nmap 扫描结果

当 Nmap 扫描完成后，可以查看扫描结果表。

可以根据所查找的信息操作结果视图。您在访问扫描结果时看到的页面将随您所使用的工作流程而变化。可使用预定义的工作流程，其中包括扫描结果表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

可在 http://insecure.org 上下载 Nmap 结果，并使用 Nmap 1.01 DTD 查看。

还可清除扫描结果。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

步骤 2 在工具栏上，点击**扫描结果 (Scan Results)**。

步骤 3 有以下选项可供选择：

- 调整时间范围，如*Cisco Secure Firewall Management Center* 管理指南中的事件时间限制所述。
- 要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击 **(switch workflows)** 。
- 要查看作为弹出窗口中页面已渲染的扫描结果，请点击扫描作业旁的**查看**。
- 要保存扫描结果文件的副本，以便在任何文本编辑器中查看原始 XML 代码，请在扫描作业旁点击**下载 (Download)**。
- 要对扫描结果排序，请点击列标题。再次点击列标题以反转排列顺序。
- 要限制显示的列，请在要隐藏的列标题中点击 **关闭** (✕)。在显示的弹出窗口中，点击**应用 (Apply)**。

  提示
  要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击**已禁用列 (Disabled Columns)** 下的列名称。

- 要向下展开到工作流程中的下一个页面，请参阅*Cisco Secure Firewall Management Center* 管理指南中的使用向下钻取页面。
- 要配置扫描实例和补救，请点击工具栏中的**扫描工具** 并参阅管理 Nmap 扫描 ， 第 2552 页。
- 要在工作流程页面之内及在各工作流程页面之间导航，请参阅*Cisco Secure Firewall Management Center* 管理指南中的工作流程页面导航工具。
- 要导航至其他事件视图以查看关联的事件，请从**跳至 (Jump to)** 下拉列表中选择要查看的事件视图的名称。
- 要搜索扫描结果，请在相应字段中输入搜索条件。

相关主题

Nmap 扫描结果字段 ， 第 2560 页

Nmap 扫描结果字段

运行 Nmap 扫描时，防火墙管理中心 在数据库中收集扫描结果。下表介绍了扫描结果表中可以查看和搜索的字段。

表 155: 扫描结果字段

字段	说明
开始时间	生成结果的扫描的开始日期和时间。
结束时间	生成结果的扫描的结束日期和时间。
目标	生成结果的扫描的扫描目标的 IP 地址（或主机名，如果 DNS 解析已启用）。
扫描类型 (Scan Type)	要么是 Nmap，要么是第三方扫描工具的名称，指明生成结果的扫描的类型。
扫描模式 (Scan Mode)	生成结果的扫描的模式： • On Demand - 来自按需扫描的结果。 • 导入 - 来自不同系统上扫描的结果，和已导入 防火墙管理中心的结果。 • 预定 (Scheduled) - 来自作为预定任务运行的扫描的结果。
结果	扫描的结果。
域	扫描目标的域。此字段只存在于多域部署中。

导入 Nmap 扫描结果

您可以导入在系统外执行的 Nmap 扫描所创建的 XML 结果文件。您还可以导入先前从系统下载的 XML 结果文件。要导入 Nmap 扫描结果，结果文件必须采用 XML 格式，且兼容于 Nmap 1.01 DTD。有关创建 Nmap 结果的详细信息以及 Nmap DTD 的详细信息，请参阅 http://insecure.org 上的 Nmap 文档。

主机必须已存在于网络映射中，然后 Nmap 才能将其结果附加到主机配置文件。

过程

步骤 1 选择**策略** > **+ 显示更多** > **关联** > **扫描器**。

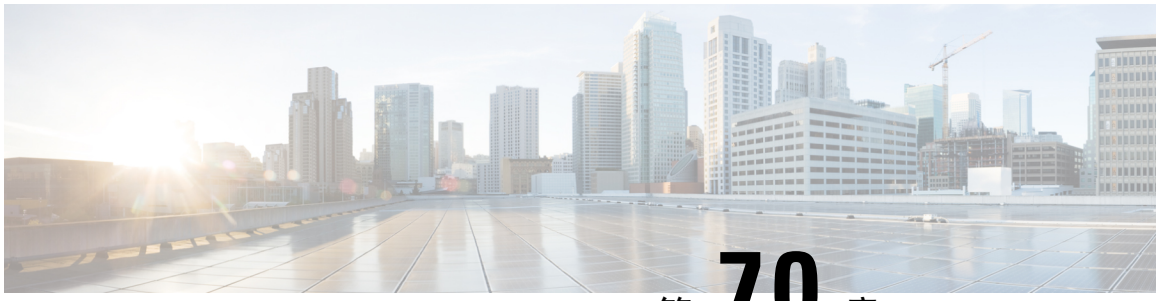
步骤 2 在工具栏上，点击 **Import Results**。

步骤 3 点击**浏览 (Browse)**，导航至结果文件。

步骤 4 返回“导入结果”(Import Results) 页面后，点击**导入 (Import)**，导入结果。

主机身份源的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense** 最低版本	详细信息
主机输入数据功能的安全性改进	6.5	任意	TLS 1.2 现在被用于 防火墙管理中心 和主机输入客户端之间的通信。该主题配置主机输入客户端，第 2543 页已使用此信息进行更新。



第 70 章

应用检测

以下主题介绍应用检测：

- 概述：应用检测， 第 2563 页
- 应用检测的要求和前提条件， 第 2569 页
- 自定义应用检测器， 第 2569 页
- 查看或下载检测器详细信息， 第 2577 页
- 检测器列表排序， 第 2578 页
- 过滤检测器列表， 第 2578 页
- 导航至其他检测器页面， 第 2580 页
- 激活和停用检测器， 第 2580 页
- 编辑自定义应用检测器， 第 2581 页
- 删除检测器， 第 2582 页

概述：应用检测

当系统分析 IP 流量时，它会尝试识别网络上的常用应用。应用感知对于应用控制至关重要。

系统检测的应用有三种类型：

- 应用协议（例如 HTTP 和 SSH），代表主机之间的通信
- 客户端（例如网络浏览器和邮件客户端），代表主机上运行的软件
- *Web* 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL

系统根据在检测器中指定的特征识别网络流量中的应用。例如，系统可以通过数据包报头中的ASCII模式识别应用。此外，安全套接字层(SSL)协议检测程序使用安全会话的信息来识别会话中的应用。

有两个应用检测器来源：

- 系统提供的检测器检测 Web 应用、客户端和应用协议。

  系统提供的应用检测器（和操作系统）的可用性取决于系统软件的版本和已安装的VDB版本。版本说明和公告包含关于新的和更新的检测器的信息。也可以导入专业服务开发的各个检测器。

- 自定义应用协议检测器由用户创建并检测 Web 应用、客户端和应用协议。

您还可以通过隐含应用协议检测来检测应用协议，此检测根据对客户端的检测暗示应用协议的存在。

如在网络发现策略中所定义，系统仅识别受监控网络中的主机上运行的应用协议。例如，如果内部主机访问未受监控的远程站点的 FTP 服务器，系统不会将应用协议识别为 FTP。另一方面，如果远程或内部主机访问正受监控主机上的 FTP 服务器，系统能够正确识别应用协议。

如果系统可以识别受监控主机用于连接到未受监控服务器的客户端，则系统会识别客户端的对应应用协议，但是不将该协议添加到网络映射中。请注意，客户端会话必须包括来自要发生应用检测的服务器的响应。

系统会确定其检测到的每个应用的特征；请参阅应用规则条件，第 1420 页。系统使用这些特征创建应用组，称为应用过滤器。应用过滤器用于执行访问控制以及限制报告和控制面板构件中使用的搜索结果和数据。

您还可以使用导出的 NetFlow 记录、Nmap 主动扫描和主机输入功能补充应用检测器数据。

相关主题

应用检测器基础知识，第 2564 页

应用检测器基础知识

Firepower 系统使用应用检测器来识别网络上的常用应用。使用“检测器”页面（**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**）查看检测器列表和自定义检测功能。

是否能修改检测器或更改其状态（活动或非活动）取决于其类型。系统仅使用活动检测器来分析应用流量。

注释 思科提供的检测器可能会随 Firepower 系统和 VDB 更新而更改。有关已更新的检测器的信息，请参阅版本说明和咨询。

注释 对于 Firepower 应用标识，不会特意列出端口。不会为任何思科应用报告应用的关联端口，因为大多数应用都与端口无关。我们平台的检测功能可以识别在网络中的任何端口运行的服务。

思科提供的内部检测器

内部检测器是一种特殊类别的检测器，适用于客户端、Web 应用和应用协议流量。内部检测器随系统更新一起提供，并且永远在线。

如果应用与旨在检测客户端相关活动的内部检测器匹配且不存在特定客户端检测器，则可以报告通用客户端。

思科提供的客户端检测器

客户端检测器用于检测客户端流量，并且通过 VDB 或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用客户端检测器。仅当导入客户端检测器后，才可以将其导出。

思科提供的 Web 应用检测器

Web 应用检测器用于检测 HTTP 流量负载中的 Web 应用，并且通过 VDB 或系统更新提供。Web 应用检测器永远在线。

思科提供的应用协议（端口）检测器

基于端口的应用协议检测器使用已知端口识别网络流量。此类检测器通过VDB或系统更新提供，或由思科专业服务提供用于导入。可以激活和停用应用协议检测器，还可查看检测器定义，以便将其用作自定义检测器的基础。

思科提供的应用协议 (Firepower) 检测器

基于 *Firepower* 的应用协议检测器用于使用 Firepower 应用指纹分析网络流量，并且通过 VDB 或系统更新提供。可以激活和停用应用协议检测器。

自定义应用检测器

自定义应用检测器基于模式。它们将检测来自客户端的数据包、Web应用或应用协议流量中的模式。对于已导入检测器和自定义检测器，您将拥有完全控制权。

在 Web 界面中识别应用协议

下表概述了系统如何识别检测到的应用协议：

表 *156:* 系统识别应用协议

标识	说明
应用协议名称	如果应用协议属于以下情况，防火墙管理中心将会使用应用协议名称来识别应用协议： • 由系统正确识别出 • 使用 NetFlow 数据识别出，并且 `/etc/sf/services` 中有端口应用协议关联 • 使用主机输入功能手动识别出 • 由 Nmap 或其他活动源识别出
`pending`	如果系统既不能正确识别也不能错误识别应用，防火墙管理中心会将应用协议识别为 `pending`。 大多数情况下，系统需要收集和分析更多的连接数据才能识别待处理应用。 在应用详细信息表、服务器表和主机配置文件中，只会对在其中检测到（而不是由检测到的客户端或 Web 应用流量推断）特定应用协议流量的应用协议显示 `pending` 状态。

标识	说明
unknown	在以下情况下，防火墙管理中心会将应用协议识别为 unknown： • 应用不匹配系统的任何检测器。 • 应用协议是使用 NetFlow 数据识别出的，但 /etc/sf/services 中没有端口应用协议关联。 • Snort 已关闭会话，但它仍存在于设备中。在这里，允许流量通过防火墙，但不会检测到应用。
空白	已检查检测到的所有可用数据，但没有识别出应用协议。在应用详细信息表、服务器表中和主机配置文件中，对于在其中没有检测到应用协议的非 HTTP 通用客户端数据流量，应用协议留空。

通过客户端检测进行隐含应用协议检测

如果系统可以识别受监控主机用于访问未受监控主机的客户端，防火墙管理中心会推断该连接使用与该客户端对应的应用协议。（由于系统仅跟踪监控网络上的应用，因此，连接日志通常不包含有关监控主机用于访问未受监控的服务器的连接的应用协议信息。）

此过程，或隐含应用协议检测，具有以下结果：

- 由于系统不会为这些服务器生成新的 TCP 端口或新的 UDP 端口事件，因此，服务器不会显示在服务器表中。此外，不能将对这些应用协议的检测作为条件来触发事件警报或关联规则。
- 由于应用协议未与主机关联，因此，不能查看主机配置文件中的详细信息，不能设置其服务器身份，也不能使用流量量变曲线或关联规则的主机配置文件限定条件中的信息。此外，系统不会根据此类检测将漏洞与主机关联。

但是，您可以触发有关连接中是否存在应用协议信息的关联事件。还可以使用连接日志中的应用协议信息创建连接跟踪程序和流量量变曲线。

主机限制和发现事件日志记录

如果系统检测到客户端、服务器或网络应用，它会生成发现事件，除非关联的主机已达到客户端、服务器或网络应用的最大数量。

主机配置文件最多为每个主机显示 16 个客户端、100 个服务器和 100 个网络应用。

请注意，依赖于客户端、服务器或网络应用检测的操作不受此限制的影响。例如，经配置要在服务器上触发的访问控制规则仍会记录连接事件。

应用检测的特殊注意事项

SFTP

为了检测 SFTP 流量，同一规则还必须检测 SSH。

Squid

在以下情况下，系统会积极识别 Squid 服务器流量：

- 系统检测从受监控网络上的主机到启用了代理身份验证的 Squid 服务器的连接；或
- 系统检测从受监控网络上的 Squid 代理服务器到目标系统（即，客户端正在其中请求信息或其他资源的目标服务器）的连接。

但是，在以下情况下，系统无法识别 Squid 服务流量：

- 受监控网络上的主机连接到已禁用代理身份验证的 Squid 服务器；或
- Squid 代理服务器被配置为从其 HTTP 响应中移除“通过：”报头字段

SSL 应用检测

系统提供可以使用安全套接字层 (SSL) 会话中的会话信息识别会话中的应用协议、客户端应用或 Web 应用的应用检测器。

如果系统检测到加密连接，它会将该连接标记为通用 HTTPS 连接或更为具体的安全协议，例如 SMTPS（如果适用）。如果系统检测到 SSL 会话，它会将 `SSL client` 添加到该会话的连接事件中的 **客户端 (Client)** 字段。如果识别到会话的 Web 应用，系统会为该流量生成发现事件。

对于 SSL 应用流量，托管设备还可以检测服务器证书中的公用名并将其与 SSL 主机模式的客户端或 Web 应用比对。当系统识别到特定客户端时，会将 `SSL client` 替换为该客户端的名称。

由于 SSL 应用流量已加密，因此系统只能使用证书中的信息（而不是加密数据流中的应用数据）进行标识。为此，SSL 主机模式有时只能识别作为应用编写者的公司，因此同一公司开发的 SSL 应用可能有相同的标识。

在某些情况下，例如 HTTPS 会话是从 HTTP 会话内部发起时，托管设备会从客户端数据包中的客户端证书检测服务器名称。

要启用 SSL 应用标识，必须创建监控响应方流量的访问控制规则。这些规则必须包含适用于 SSL 应用的应用条件或者使用来自 SSL 证书的 URL 的 URL 条件。对于网络发现，响应方 IP 地址不必位于要在网络发现策略中监控的网络上；访问控制策略配置决定是否识别流量。要识别 SSL 应用的检测，您可以在应用检测器列表中或在访问控制规则中添加应用条件时按 `SSL protocol` 标记进行过滤。

推荐的 Web 应用

Web 服务器有时会将流量推荐到其他网站，这些网站通常是广告服务器。为帮助您更好地理解网络上出现的推荐流量的情景，系统在推荐会话的事件的 **Web 应用 (Web Application)** 字段中列出推荐流量的 Web 应用。VDB 包含已知被推荐站点的列表。如果系统检测到来自这些站点之一的流量，

会将推荐站点连同该流量的事件一起存储。例如，如果通过Facebook访问的广告实际在Advertising.com上托管，则检测到的 Advertising.com 流量与 Facebook Web 应用关联。系统还可以检测到 HTTP 流量中的推荐 URL，例如当网站提供与另一站点的简单链接时；在这种情况下，推荐 URL 出现在 HTTP Referrer 事件字段。

在事件中，如果存在推荐应用，它将被列为流量的 Web 应用，而 URL 则是被推荐站点的 URL。在上述示例中，用于流量的连接事件的 Web 应用是 Facebook，但 URL 是 Advertising.com。在下列情况下，被推荐的应用可能显示为 Web 应用：未检测到推荐 Web 应用，主机推荐其本身，或者存在推荐链。在控制面板中，Web 应用的连接和字节数包括 Web 应用与该应用推荐的流量关联的会话数。

请注意，如果创建专门针对被推荐流量的规则，应该为被推荐应用（而不是推荐应用）添加条件。例如，要阻止从 Facebook 推荐的 Advertising.com 流量，可以向 Advertising.com 应用的访问控制规则添加应用条件。

Snort 3 中的应用检测

注释 Snort 3 现在与 Snort 2 相同，**如果** AC 策略中没有其他配置需要 AppID 来监控所有流量，则只会在网络发现策略过滤器中定义的特定网络子网上启用 AppID 检查。

在 Snort 3 中，默认情况下始终为所有网络启用应用检测。要禁用应用检测，请执行以下操作：

过程

步骤 1 选择 **策略** > **安全策略** > **访问控制**，点击编辑策略并删除应用规则。

步骤 2 选择 **策略** > **安全策略** > **解密**，点击删除以删除 SSL 策略。

步骤 3 选择 **策略** > **+ 显示更多** > **内容关联** > **网络发现**，点击删除以删除网络发现策略。

步骤 4 选择 **策略** > **安全策略** > **访问控制**，点击要编辑的策略的 **编辑** (✎)，然后点击**安全智能** > **URL** 选项卡以删除 URL 允许列表或阻止列表。

步骤 5 由于无法删除默认 DNS 规则，请选择**策略** > **安全策略** > **DNS**，点击编辑并取消选中“启用”复选框以禁用 DNS 策略。

步骤 6 在访问控制策略的**高级 (Advanced)** 设置下，禁用启用威胁情报导向器 *(Enable Threat Intelligence Director)* 和对 *DNS* 流量启用信誉实施 *(Enable reputation enforcement on DNS traffic)* 选项。

步骤 7 保存并部署访问控制策略。

应用检测的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 发现管理员

自定义应用检测器

如果在网络上使用自定义应用，您可以创建自定义的 Web 应用、客户端或应用协议检测器，它们可向系统提供识别应用所需的信息。应用检测器的类型由您在**协议 (Protocol)**、**类型 (Type)** 和**方向 (Direction)** 字段中进行的选择确定。

只有客户端会话包含来自服务器的响应器数据包，系统才能开始检测和识别服务器流量中的应用协议。请注意，对于 UDP 流量，系统将响应器数据包的来源指定为服务器。

如果已经在另一防火墙管理中心上创建了检测器，可将其导出后，再导入至此防火墙管理中心。然后，可根据自己的需求编辑已导入的检测器。您可导出和导入自定义检测器以及思科专业服务提供的检测器。但是，您**无法**导出或导入思科提供的任何其他类型检测器。

自定义应用检测器和用户定义的应用字段

可以使用以下字段配置自定义应用检测器和用户定义的应用。

自定义应用检测器字段：常规

使用以下字段配置基本和高级自定义应用检测器。

应用协议

要检测的应用协议。这可以是系统提供的应用或用户定义的应用。

如果要让应用免于执行主动身份验证（在身份规则中配置），则必须选择或创建带**用户代理排除项 (User-Agent Exclusion)** 标记的应用协议。

说明

应用检测器的说明。

名称

应用检测器的名称。

检测器类型

检测器的类型，**基本 (Basic)** 或**高级 (Advanced)**。基本应用检测器是在 Web 界面中作为一系列字段而创建的。高级应用检测器是在外部创建并作为自定义 .lua 文件上传的。

自定义应用检测器字段：检测模式

使用以下字段配置基本自定义应用检测器的检测模式。

方向

检测器应当检查的流量源，包括**客户端 (Client)** 或**服务器 (Server)**。

偏移

以字节为单位表示的在数据包中的位置，从数据包负载起始位置（系统应开始搜索模式的位置）开始。

因为数据包负载从 0 字节开始，请按以下方法计算偏移：将想要从数据包负载起始位置前移的字节数减去 1。例如，要查找数据包的第 5 个位中的模式，请在**偏移 (Offset)** 字段键入 `4`。

模式

与您选择的**类型 (Type)** 相关联的模式字符串。

端口

检测器应检查流量的端口。

协议

要检测的协议。选择的协议将确定是显示**类型 (Type)** 还是 **URL** 字段。

该协议（以及在某些情况下，您在**类型 [Type]** 和**方向 [Direction]** 字段中的后续选择）将确定您创建的应用检测器类型：Web 应用、客户端或应用协议。

检测器类型	协议	类型或方向
Web 应用	HTTP	**类型 (Type)** 为**内容类型 (Content Type)** 或 **URL**
	RTMP	任意
	SSL	任意
客户端	HTTP	**类型**为**用户代理**
	SIP	任意
	TCP 或 UDP	**方向 (Direction)** 为**客户端 (Client)**
应用协议	TCP 或 UDP	**方向 (Direction)** 为**服务器 (Server)**

类型

输入的模式字符串类型。您看到的选项由您已选择的**协议 (Protocol)** 确定。如果已选择 **RTMP** 作为协议，则系统将显示 **URL** 字段而非**类型 (Type)** 字段。



注释 如果选择**用户代理**作为**类型**，则系统自动将应用的**标记**设为**用户代理排除项**。

类型选择	字符串特征
Ascii	字符串使用 ASCII 编码。
公用名	字符串是服务器响应消息中 commonName 字段的值。
内容类型	字符串是服务器响应报头中 content-type 字段的值。
十六进制	字符串使用十六进制表示。
组织单位	字符串是服务器响应消息中 organizationName 字段的值。
SIP 服务器 (SIP Server)	字符串是消息报头中 From 字段的值。
SSL 主机 (SSL Host)	字符串是 ClientHello 消息中 server_name 字段的值。
URL	字符串是一个 URL。 注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 **cisco.com** 将匹配 **www.cisco.com/support** 和 **www.cisco.com**，但不匹配 **www.wearecisco.com**。
用户代理	字符串是 GET 请求报头中 user-agent 字段的值。它还可用于 SIP 协议，表示字符串是 SIP 消息报头中 user-agent 字段的值。

URL

来自 RTMP 数据包的 C2 消息内 swfURL 字段的完整 URL 或部分 URL。选择 **RTMP** 作为**协议 (Protocol)** 时，系统将显示此字段而非**类型 (Type)** 字段。



注释 检测器假设输入的字符串是完整的 URL 部分。例如，输入 **cisco.com** 将匹配 **www.cisco.com/support** 和 **www.cisco.com**，但不匹配 **www.wearecisco.com**。

用户定义的应用字段

使用以下字段在基本和高级自定义应用检测器内配置用户定义的应用。

业务相关性

应用被用于您的组织的业务运营中（而不是用于娱乐目的）的可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

类别

说明应用的最基本功能的应用通用分类。

说明

应用的说明。

名称

应用的名称。

风险

应用被用于违反您的组织安全策略的目的之可能性：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 或**非常低 (Very Low)**。选择最能描述应用的选项。

标签

提供有关应用的其他信息的一个或多个预定义标记。如果要让应用免于执行主动身份验证（在身份规则中配置），则必须为应用添加**用户代理排除项 (User-Agent Exclusion)** 标记。

配置自定义应用检测器

您可以配置基本或高级自定义应用检测器。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击**创建自定义检测器 (Create Custom Detector)**。

步骤 3 输入**名称 (Name)** 和**说明 (Description)**。

步骤 4 从应用下拉列表中选择**应用协议 (Application Protocol)**。您有以下选择：

- 如果是为现有应用协议创建检测器（例如，如果要检测非标准端口上的特定应用协议），请从下拉列表中选择应用协议。
- 如果是为用户定义的应用创建检测器，请按照创建用户定义的应用。，第 2573 页中概述的程序执行操作。

步骤 5 点击**检测器类型 (Detector Type)** 以选择**基本 (Basic)** 或 **高级 (Advanced)**。

步骤 6 点击**确定**。

步骤 7 配置 **检测模式** 或 **检测标准** 或 **加密可视性引擎进程分配**：

- 如果配置的是基本检测器，请指定预设**检测模式 (Detection Patterns)**，如指定基本检测器中的检测模式，第 2574 页中所述。

- 如果配置的是高级检测器，请指定自定义**检测条件 (Detection Criteria)**，如指定高级检测器中的检测条件，第 2575 页中所述。
- 如果要配置加密可视性引擎（EVE）检测器，请指定自定义EVE进程分配，如本章指定 *EVE* 进程分配部分中所述。

  注意
  高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

步骤 8 或者，使用**数据包捕获 (Packet Captures)** 测试新检测器，如测试自定义应用协议检测器，第 2577 页中所述。

步骤 9 点击**保存**。

注释
如果在访问控制规则中包含该应用，则检测器会自动激活，并且在使用时不能停用。

下一步做什么

- 激活检测器，如激活和停用检测器，第 2580 页中所述。

相关主题

自定义应用检测器和用户定义的应用字段，第 2569 页

创建用户定义的应用。

此处创建的应用、类别和标记在访问控制规则以及在应用过滤对象管理器中均可用。

注意 创建用户定义的应用会立即重启 Snort 进程，而无需执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。

过程

步骤 1 在**创建自定义应用检测器 (Create A Custom Application Detector)** 对话框中，点击**应用 (Application)** 字段旁边的 **添加** (+)。

步骤 2 键入**名称 (Name)**。

步骤 3 键入**说明 (Description)**。

步骤 4 选择**业务关联性**。

步骤 5 选择**风险**。

步骤 6 点击“类别”(Categories) 旁的**添加 (Add)** 以添加类别，并键入新的类别名称，或者从**类别 (Categories)** 下拉列表选择现有类别。

步骤 7 点击"标记"旁的**添加**以添加标记，并键入新的标记名称，或者从**标记**下拉列表选择现有标记。

注释
要为策略型路由关联自定义应用检测器域，您必须从 **标记** 列表中选择 NSG。

步骤 8 点击**确定**。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

自定义应用检测器和用户定义的应用字段，第 2569 页

指定基本检测器中的检测模式

可以配置自定义应用协议检测器以搜索应用协议数据包报头中的特定模式字符串。也可配置检测器，使其搜索多个模式，在这种情况下，应用协议流量必须匹配所有模式，以便检测器主动识别应用协议。

应用协议检测器可使用任何偏移搜索 ASCII 或十六进制模式。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。

过程

步骤 1 在**创建检测器 (Create Detector)** 页面上的**检测模式 (Detection Patterns)** 部分中，点击**添加 (Add)**。

步骤 2 从**应用 (Application)** 下拉列表中选择协议类型。

步骤 3 从**类型 (Type)** 下拉列表中选择模式类型。

步骤 4 键入与指定的**类型**相匹配的**模式**字符串。

步骤 5 或者，键入**偏移 (Offset)**（以字节为单位）。

步骤 6 或者，要根据其使用的端口识别应用协议流量，请在**端口**字段中键入 1 到 65535 之间的端口。要使用多个端口，请用逗号分隔它们。

步骤 7 点击**方向 (Direction)**：**客户端 (Client)** 或**服务器 (Server)**。

步骤 8 点击**确定**。

提示

如果要删除模式，请点击要删除的模式旁边的 **删除** ( ) 。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

指定高级检测器中的检测条件，第 2575 页

指定高级检测器中的检测条件

注意 高级自定义检测器很复杂，且需要具备外部知识才能构建有效的 .lua 文件。错误配置的检测器会对性能或检测能力造成负面影响。

注意 不要上传来自不可信来源的 .lua 文件。

自定义 .lua 文件包含自定义应用检测器设置。创建自定义 .lua 文件需要具备 lua 编程语言的高级知识和思科的 C-lua API 经验。思科强烈建议使用以下材料来准备 .lua 文件：

- lua 编程语言的第三方说明和参考资料
- 开源检测器开发人员指南： https://www.snort.org/downloads
- OpenAppID Snort 社区资源： http://blog.snort.org/search/label/openappid

注释 系统不支持引用系统调用或文件 I/O 的 .lua 文件。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。
- 通过下载和学习类似检测器的 .lua 文件，为创建有效的 .lua 文件做准备。有关下载检测器文件的详细信息，请参阅查看或下载检测器详细信息，第 2577 页。
- 创建包含自定义应用检测器设置的有效 .lua 文件。

过程

步骤 1 在高级自定义应用检测器的**创建检测器 (Create Detector)** 页面的**检测条件 (Detection Criteria)** 部分中，点击**添加 (Add)**。

步骤 2 点击**浏览...(Browse...)** 以导航至 `.lua` 文件并将其上传。

步骤 3 点击**确定**。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

相关主题

指定基本检测器中的检测模式，第 2574 页

指定 EVE 进程分配

您可以配置自己的自定义应用检测器，以将加密可视性引擎 (EVE) 检测到的进程映射到新应用或现有应用。

开始之前

- 开始配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“加密可视性引擎进程分配”(Encrypted Visibility Engine Process Assignments) 部分中，点击**添加 (Add)**。

步骤 2 输入 **进程名称** 和 **最小进程置信度** 值。

注释
您可以在 **进程名称** 字段中输入文本，这区分大小写。该值应与 EVE 检测到的确切进程名称匹配。**最小进程置信度** 可以是 0 到 100 之间的任何数字。这是连接事件中 **加密可视化进程置信度得分** 字段中显示的数字。

有关 **加密可视化进程置信度得分** 字段的信息，请参阅《Cisco Firepower 管理中心管理指南》中“连接和安全智能事件字段” 的部分。

步骤 3 点击**保存**。

步骤 4 在应用检测器列表页面中，激活您创建的检测器。有关详细信息，请参阅激活和停用检测器，第2580页。当您激活检测器时，检测器文件会被推送到 防火墙管理中心上注册的所有 FTD。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第2572页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

测试自定义应用协议检测器

如您拥有的数据包捕获 (pcap) 文件包含的数据包带有要检测的应用协议的流量，则可针对该 pcap 文件测试自定义的应用协议检测器。思科建议使用简单、干净的 pcap 文件，没有不必要的流量。

Pcap 文件必须为 256 KB 或更小；如果尝试针对较大的 pcap 文件测试检测器，防火墙管理中心会自动将其截断并测试不完整文件。在使用该文件测试检测器之前，必须修复 pcap 中无法确定的校验和。

开始之前

- 配置自定义应用协议检测器，如配置自定义应用检测器，第 2572 页中所述。

过程

步骤 1 在“创建检测器”(Create Detector) 页面上的“数据包捕获”(Packet Captures) 部分，点击**添加 (Add)**。

步骤 2 在弹出式窗口中浏览至 pcap 文件，然后点击**确定**。

步骤 3 要针对 pcap 文件的内容测试检测器，点击 pcap 文件旁的评估。系统显示消息，指示测试是否成功。

步骤 4 或者，重复第 1至 3 步，针对额外的 pcap 文件测试检测器。

提示
要删除 pcap 文件，点击想要删除的文件旁的 **删除** () 。

下一步做什么

- 继续配置自定义应用协议检测器，如配置自定义应用检测器，第2572页中所述。必须先保存并激活检测器，然后系统才能使用其分析流量。

查看或下载检测器详细信息

可以使用检测器列表来查看应用检测器详细信息（所有检测器）和下载检测器详细信息（仅自定义应用检测器）。

过程

步骤 1 要查看应用检测器详细信息，请执行以下任一操作：

- 参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html 上提供的相关 VDB 版本的 *Cisco Firepower* 应用检测器参考
- a. 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

  b. 过滤列表以查找特定检测器。

  c. 点击 **信息**()

步骤 2 要下载自定义应用检测器的检测器详细信息，请点击 **下载** （）。

如果控件呈灰显状态，则表明配置属于祖先域，或者您没有必要的权限。

检测器列表排序

默认情况下，Detectors 页面将按名称以字母顺序列出检测器。列标题旁边的向上或向下箭头表示页面按该列升序或降序排序。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击相应的列标题。

过滤检测器列表

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 展开检测器列表的过滤器组，第 2579 页中所述的其中一个过滤器组并选择过滤器旁边的复选框。要选择组中的所有过滤器，右键点击组名称，然后选择 **Check All**。

步骤 3 如果要移除某个过滤器，请点击 **删除**（）（位于**过滤器 [Filters]** 字段的过滤器名称中）或禁用过滤器列表中的过滤器。要移除组中的所有过滤器，右键点击组名称，然后选择 **Uncheck All**。

步骤 4 如果要移除所有过滤器，请点击已应用至检测器的过滤器列表旁边的**全部清除 (Clear alls)**。

检测器列表的过滤器组

可单独或组合使用多个过滤器组，以过滤检测器列表。

名称

查找名称或描述包含您键入的字符串的检测器。字符串可包含任何字母数字或特殊字符。

自定义过滤器 (Custom Filter)

查找与对象管理页面上创建的自定义应用过滤器匹配的检测器。

作者

按检测器的创建者查找检测器。可按以下内容过滤检测器：

- 创建或导入自定义检测器的任何个别用户
- 思科代表所有思科提供的检测器，单独导入的附加检测器除外（您是自己导入的任何检测器的作者）
- **任何用户**，代表非思科提供的所有检测器

状态

根据检测器的状态（即**活动 [Active]** 或**非活动 [Inactive]**）查找检测器。

类型

根据检测器类型查找检测器，如应用检测器基础知识，第 2564 页中所述。

协议

根据检测器检查的流量协议查找检测器。

类别

根据分配至所检测应用的类别查找检测器。

标记

根据分配至所检测应用的类别查找检测器。

风险

根据分配到所检测应用的风险查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

业务关联性 (Business Relevance)

根据分配至所检测应用的业务关联性查找检测器：**非常高 (Very High)**、**高 (High)**、**中 (Medium)**、**低 (Low)** 和**非常低 (Very Low)**。

导航至其他检测器页面

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 如果要查看下一页，请点击 **右箭头**（）。

步骤 3 如果要查看上一页，请点击 **左箭头**（）。

步骤 4 如果要查看另一页，请键入页码并按 Enter 键。

步骤 5 如果要跳到最后一页，请点击 **右端箭头**（）。

步骤 6 如果要跳到第一页，请点击 **左端箭头**（）。

激活和停用检测器

必须激活检测器，然后才能将其用于分析网络流量。默认情况下，思科提供的所有检测器均已激活。

可为每个端口激活多个应用检测器，以补充系统的检测能力。

在策略的访问控制规则中包含应用并部署策略时，如果该应用没有活动检测器，一个或多个检测器将会自动激活。类似地，在已部署策略中使用应用时，如果停用检测器会使该应用没有活动检测器，则不能停用检测器。

提示 为提高性能，请停用任何您不打算使用的应用协议、客户端或 Web 应用检测器。

注意 激活或停用系统或自定义应用检测器会立即重启 Snort 进程，而不会执行部署过程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击要激活或停用的检测器旁边的滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

注释
其他检测器可能需要某些应用检测器。如果停用其中一个检测器，系统会显示警告表明依赖于它的检测器也已被禁用。

编辑自定义应用检测器

使用以下程序修改自定义应用检测器。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击要修改的检测器旁边的 **编辑** ()。 如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对检测器进行更改，如配置自定义应用检测器 ， 第 2572 页中所述。

步骤 4 根据检测器的状态，您具有以下保存选择：

- 要保存非活动检测器，请点击**保存**。
- 要将非活动检测器另存为新的非活动检测器，请点击**另存为新项目**。
- 要保存活动检测器并立即开始使用，请点击**保存并重新激活**。

  注意
  保存和重新激活自定义应用检测器后，无需执行部署过程即可立即重启 Snort 进程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为 ， 第 174 页。

- 要将活动检测器另存为新的非活动检测器，请点击**另存为新项目**。

删除检测器

可以删除自定义检测器以及单独导入的由思科专业服务提供的附加检测器。不能删除思科提供的任何其他检测器，不过可以停用其中许多检测器。

注释 当检测器正在已部署的策略中使用时，不能删除该检测器。

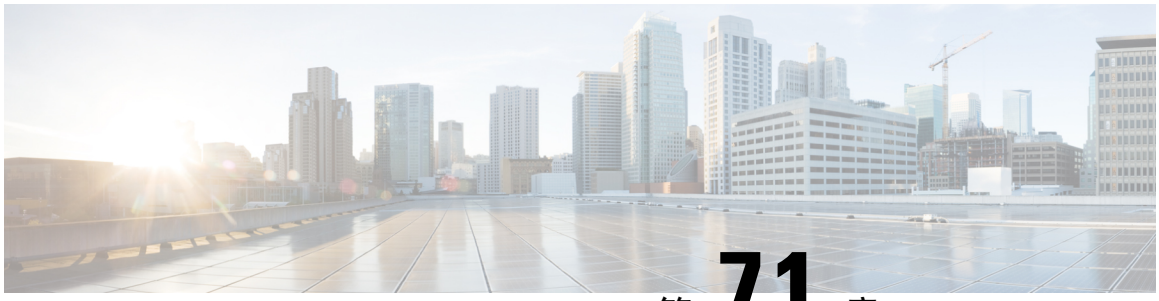
注意 删除已激活的自定义应用检测器将立即重启 Snort 进程，而无需执行部署流程。系统会提醒您，继续操作会重启 Snort 进程并允许您取消；重启发生在当前域或其任何子域中的任何托管设备上。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。

过程

步骤 1 选择**策略** > **+ 显示更多** > **高级** > **自定义应用检测器**。

步骤 2 点击要删除的检测器旁边的 **删除** ( )。 如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击**确定**。



第 71 章

网络发现策略

以下主题介绍如何创建、配置和管理网络发现策略：

- 概述：网络发现策略， 第 2583 页
- 网络发现策略的要求和前提条件， 第 2584 页
- 网络发现自定义， 第 2584 页
- 网络发现规则， 第 2585 页
- 配置高级网络发现选项， 第 2594 页
- 对网络发现策略进行故障排除， 第 2602 页

概述：网络发现策略

防火墙管理中心上的网络发现策略控制系统如何收集有关组织网络资产以及哪些网段和端口受监控的数据。

策略中的发现规则指定系统监控哪些网络和端口来根据流量中的网络数据生成发现数据，以及指定策略部署到的区域。在规则中，您可以配置是否发现主机、应用和非管理用户。可以创建规则来将网络和区域排除在发现范围外。您可以从 NetFlow 导出器配置数据发现，并且限制在网络上发现了用户数据的流量的协议。

网络发现策略包含一个配置为从观察到的所有流量发现应用的默认规则。该规则不排除任何网络、区域或端口，未配置主机和用户发现，并且规则未配置为监控 NetFlow 导出器。当托管设备注册到防火墙管理中心时，此策略默认部署到任何托管设备。要开始收集主机或用户数据，必须添加或修改发现规则并将策略重新部署到设备。

如果要调整网络发现范围，可以创建其他发现规则，并修改或移除默认规则。

请记住，每个托管设备的访问控制策略都定义面向该设备允许的流量，以及因此可使用网络发现监控的流量。如果使用访问控制阻止某些流量，则系统无法检查主机、用户和应用活动的该流量。例如，如果访问控制策略阻止对社交网络应用的访问，则系统无法在这些应用上提供任何发现数据。

如果在发现规则中启用基于流量的用户检测，则可以通过使用一组应用协议的流量中的用户登录活动来检测非管理用户。如有需要，可以禁用用于所有规则的特定协议中的发现。禁用某些协议有助于避免达到与 防火墙管理中心型号关联的用户限制，从而为来自其他协议的用户保留可用用户计数。

借助高级网络发现设置，可以管理记录哪些数据、如何存储发现数据、哪些危害表现 (IOC) 规则处于活动状态、哪些漏洞映射用于影响评估，以及如果源提供冲突发现数据将会发生什么情况。您还可以添加要监控的主机输入和 NetFlow 导出器的源。

网络发现策略的要求和前提条件

型号支持

任意。

支持的域

枝叶

用户角色

- 管理员
- 发现管理员

网络发现自定义

Firepower 系统收集的有关网络流量的信息对您最有价值，因为系统可以参考该信息来识别网络上最易受攻击和最重要的主机。

例如，如果网络上有多个运行自定义版本的 SuSE Linux 的设备，则系统无法识别操作系统，因此无法将漏洞映射至主机。不过，如果知道系统拥有 SuSE Linux 的漏洞列表，您可能想要为某个主机创建自定义的指纹，以便随后可使用该指纹来识别运行相同操作系统的其他主机。可将 SuSE Linux 漏洞列表的映射纳入指纹中，以便将该列表与匹配指纹的每个主机关联。

系统还允许使用主机输入功能，将来自第三方系统的主机数据直接输入至网络映射。不过，第三方操作系统或应用数据不会自动映射至漏洞信息。如果想要为使用第三方操作系统、服务器和应用协议数据的主机查看漏洞并执行影响关联，必须将来自第三方系统的供应商和版本信息映射至漏洞数据库 (VDB) 中列出的供应商和版本。您也可能想要持续维护主机输入数据。请注意，即使将应用数据映射到 Firepower 系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

如果系统无法识别网络主机上运行的应用协议，则可创建用户定义的应用协议检测器以便系统根据端口或模式识别应用。您还可以导入、激活和停用某些应用检测器，以便进一步自定义 Firepower 系统的应用检测功能。

还可使用 Nmap 主动扫描器的扫描结果替换操作系统和应用数据的检测结果，或者使用第三方漏洞来扩充漏洞列表。系统可以协调来自多个源的数据，从而确定应用的身份。

配置网络发现策略

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 配置策略的以下组件：

- 发现规则 - 请参阅配置网络发现规则，第 2585 页。
- 基于流量的用户检测 - 请参阅配置基于流量的用户检测，第 2593 页。
- 高级网络发现选项 - 请参阅配置高级网络发现选项，第 2594 页。
- 自定义操作系统定义（指纹）- 请参阅为客户端创建自定义指纹，第 2532 页和为服务器创建自定义指纹，第 2534 页。

网络发现规则

通过网络发现规则，您可以将为网络映射发现的信息定制为仅包含所需的特定数据。网络发现策略中的规则按顺序接受评估。您可以使用重叠的监控条件创建规则，但这样做可能会影响系统性能。

将主机或网络排除在监控范围外之后，被排除的主机或网络将不会显示在网络映射中，系统也不会为其报告事件。但是，在禁用本地 IP 的主机发现规则时，检测引擎实例会受到更高处理负载的影响，因为它会从每个流重新构建数据，而不是使用现有主机数据。

我们建议将负载均衡器（或负载均衡器上的特定端口）和NAT 设备排除在监控范围外。这些设备可能会创建过量并有误导性的事件，从而填充数据库并使防火墙管理中心过载。例如，受监控的NAT 设备可能会在短时间内显示其操作系统的多个更新。如果知道负载均衡器和 NAT 设备的 IP 地址，可以将它们排除在监控范围外。

提示 系统可通过检查网络流量识别许多负载均衡器和 NAT 设备。

此外，如果需要创建自定义服务器指纹，应暂时禁止监控用于与正在创建指纹的主机通信的 IP 地址。否则，网络映射和发现事件视图中将会出现大量关于该IP 地址代表的主机的不准确信息。创建指纹后，可以配置策略，以便再次监控该 IP 地址。

思科还建议 **不** 监控 NetFlow 导出器和托管设备的相同网段。尽管在理想情况下应使用不重叠的规则来配置网络发现政策，但系统不会丢弃托管设备生成的重复连接日志。但是，**不能**丢弃托管设备和 NetFlow 导出器均检测到的连接的重复连接日志。

配置网络发现规则

可以配置发现规则，以根据自身需求定制主机和应用数据的发现。

提示 在大多数情况下，我们建议将发现限制在 RFC 1918 中的地址。

开始之前

- 确保正在为要在其中发现网络数据的流量记录连接；请参阅*Cisco Secure Firewall Management Center* 管理指南中的连接日志记录最佳实践。
- 如果要收集导出的 NetFlow 记录，请按照将 NetFlow 导出器添加到网络发现策略，第 2599 页中所述添加 NetFlow Exporter。
- 如果要查看发现性能图，必须在发现规则中启用主机，用户和应用。请注意，这可能会影响性能。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**添加规则 (Add Rule)**。

步骤 3 如操作和发现的资产，第 2586 页中所述，为规则设置**操作 (Action)**。

步骤 4 设置可选的发现参数：

- 将规则操作限定于特定网络；请参阅限制受监控网络，第 2587 页。
- 将规则操作限定于特定区域中的流量；请参阅配置网络发现规则中的区域，第 2591 页。
- 将端口排除在监控范围外；请参阅排除网络发现规则中的端口，第 2590 页。
- 为 NetFlow 数据发现配置规则；请参阅配置用于 NetFlow 数据发现的规则，第 2588 页。

步骤 5 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

操作和发现的资产

配置发现规则时，必须为规则选择操作。规则操作的影响取决于规则是用于从托管设备还是NetFlow导出器发现数据。

下表说明了规则使用这两种方案中指定的操作设置发现的资产。

表 *157:* 发现规则操作

操作	选项	托管设备	NetFlow 导出器
排除	--	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。	将指定网络排除在监控范围外。如果用于连接的源主机或目标主机已被排除在发现范围外，会记录连接，但不会为排除的主机创建发现事件。
发现	主机数	根据发现事件将主机添加到网络映射。（可选操作；如果启用了用户发现，则为必要操作。）	根据 NetFlow 记录将主机添加到网络映射并记录连接。（必需）
发现	应用	根据应用检测程序将应用添加到网络映射。请注意，在没有发现应用的情况下，无法发现规则中的主机或用户。（必需）	根据 NetFlow 记录和 `/etc/sf/services` 中的端口应用协议关联将应用协议添加到网络映射。（可选）
发现	用户	将用户添加到用户表，并根据对网络发现策略中配置的用户协议进行的基于流量的检测记录用户活动。（可选）	n/a
记录 NetFlow 连接	--	n/a	仅记录 NetFlow 连接。不发现主机或应用。

如果要让规则监控托管设备流量，则应用日志记录为必要操作。如果要让规则监控用户，则主机日志记录为必要操作。如果要让规则监控导出的 NetFlow 记录，则您无法将其配置为记录用户，并且记录应用为可选操作。



注释 系统根据网络发现策略中的**操作 (Action)** 设置检测 NetFlow 记录中的连接。系统根据访问控制策略设置检测托管设备中的连接。

受监控网络

发现规则仅可发现流量中发向和来自指定网络中主机的受监控资产。发现规则执行发现的对象是至少有一个 IP 地址在指定网络范围内的连接，并仅对位于受监控网络范围内的 IP 地址生成事件。默认发现规则从所有观察到的流量中发现应用（`0.0.0.0/0` 表示所有 IPv4 流量，`::/0` 表示所有 IPv6 流量）。

如果将规则配置为处理 NetFlow 发现并仅记录连接数据，则系统还会记录发向和来自指定网络中 IP 地址的连接。请注意，网络发现规则是记录 NetFlow 网络连接的唯一方式。

另外，您也可以使用网络对象或对象组指定要监控的网络。

限制受监控网络

每个发现规则必须至少包含一个网络。

过程

步骤 1 选择策略 > + 显示更多 > 内容关联 > 网络发现。

步骤 2 点击添加规则 (Add Rule)。

步骤 3 如果还未打开，请点击 网络。

步骤 4 （可选）将网络对象添加到“可用网络”(Available Networks) 列表，如在配置发现规则期间创建网络对象，第 2589 页中所述。

如果修改网络发现策略中使用的网络对象，则更改对于发现不会生效，直至部署配置更改为止。

步骤 5 指定网络：

- 从可用网络 (Available Networks) 列表中选择网络。如果网络没有立即显示在列表中，请点击重新加载 ()。
- 将 IP 地址输入到“可用网络”(Available Networks) 标签下方的文本框中。

步骤 6 点击添加 (Add)。

步骤 7 点击保存。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

配置用于 NetFlow 数据发现的规则

系统可以使用来自 NetFlow 导出器的数据生成连接和发现事件，并将主机和应用数据添加到网络映射。

如果选择某个发现规则中的 NetFlow 导出器，该规则将被限制为为指定网络发现 NetFlow 数据。应先选择要监控的 NetFlow 设备，然后再配置规则行为的其他方面，因为在选择 NetFlow 设备时可用规则操作会变化。不能为监控 NetFlow 导出器配置端口排除。

开始之前

- 将支持 NetFlow 的设备添加到网络发现策略；请参阅将 NetFlow 导出器添加到网络发现策略，第 2599 页。

过程

步骤 1 选择策略 > + 显示更多 > 内容关联 > 网络发现。

步骤 2 点击添加规则 (Add Rule)。

步骤 3 选择 **NetFlow 设备**。

步骤 4 从 **NetFlow 设备 (NetFlow Device)** 下拉列表中，选择要监控的 NetFlow 导出器的 IP 地址。

步骤 5 指定要让系统托管设备收集的 NetFlow 数据类型：

- 仅连接 - 从操作 (Action) 下拉列表中选择 **Log NetFlow Connections**。
- 主机、应用和连接 - 从操作 (Action) 下拉列表中选择 **Discover**。系统会自动选中**主机 (Hosts)** 复选框并启用连接数据的收集。或者，可以选中**应用 (Application)** 复选框以收集应用数据。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

在配置发现规则期间创建网络对象

将新的网络对象添加到可重用网络对象和组列表中，即可将其添加到发现规则中显示的可用网络列表中。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 在**网络 (Networks)** 中，点击**添加规则 (Add Rule)**。

步骤 3 点击**可用网络 (Available Networks)** 旁边的 **添加** (+)。

步骤 4 按照创建网络对象，第 2660 页中所述创建网络对象。

步骤 5 按照配置网络发现规则，第 2585 页中所述完成添加网络发现规则。

端口排除

可以将特定端口排除在监控范围外，就像将主机排除在监控范围外一样。例如：

- 负载均衡器可在短时间内报告同一端口上的多个应用。可以配置网络发现规则，以便将该端口排除在监控范围外，例如排除处理 Web 场的负载均衡器上的端口 80。
- 组织可以使用采用特定端口范围的自定义客户端。如果来自该客户端的流量生成过多有误导性的事件，可以排除对这些端口的监控。同样，可以决定是否要监控DNS流量。在这种情况下，可以配置规则，使发现策略不监控端口 53。

添加要排除的端口时，可以决定是使用 Available Ports 列表中的可重用端口对象，将端口直接添加到源或目标排除列表，还是创建新的可重用端口然后将其移至排除列表。

注释 不能排除处理 NetFlow 数据发现的规则中的端口。

排除网络发现规则中的端口

不能排除处理 NetFlow 数据发现的规则中的端口。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**添加规则 (Add Rule)**。

步骤 3 点击 **Port Exclusions**。

步骤 4 或者，将端口对象添加到“可用端口”(Available Ports) 列表，如在配置发现规则期间创建端口对象，第 2590 页中所述。

步骤 5 使用以下任一方法将特定源端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到源 (Add to Source)**。
- 要排除来自特定源端口的流量而不添加端口对象，请在**所选源端口 (Selected Source Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号（从 1 到 65535 的值），然后点击**添加 (Add)**。

步骤 6 使用以下任一方法将特定目标端口排除在监控范围外：

- 从**可用端口 (Available Ports)** 列表中选择一个或多个端口，然后点击**添加到目标 (Add to Destination)**。
- 要排除来自特定目标端口的流量而不添加端口对象，请在**所选目标端口 (Selected Destination Ports)** 列表下，选择**协议 (Protocol)**，在**端口 (Port)** 中输入端口号，然后点击**添加 (Add)**。

步骤 7 点击**保存** 以保存所做的更改。

下一步做什么

- 部署配置更改；请参阅部署配置更改，第 180 页。

在配置发现规则期间创建端口对象

将新的端口对象添加到可在系统中任意位置使用的可重用端口对象和对象组列表，即可将其添加到发现规则中显示的可用端口列表中。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 在“网络”(Networks) 中，点击**添加规则 (Add Rule)**。

步骤 3 点击 **Port Exclusions**。

步骤 4 要将端口添加到可用端口列表，请点击 **添加** (+)。

步骤 5 输入**名称**。

步骤 6 在 **Protocol** 字段中，指定要排除的流量协议。

步骤 7 在**端口 (Port)** 字段中，输入要排除在监控范围外的端口。

可以指定单个端口、用破折线(-)分隔的一系列端口或者用逗号分隔的端口和端口范围列表。允许的端口值介于 1 到 65535 之间。

步骤 8 点击**保存**。

步骤 9 如果添加的端口没有立即显示在列表中，请点击 **刷新**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

网络发现规则中的区域

要提高性能，可以配置发现规则，以便规则中的区域包含物理连接到规则中的待监控网络的托管设备上的传感接口。

但是，系统可能并不总是告知您网络配置的更改情况。网络管理员可以通过路由或主机更改修改网络配置而无需告知您，这可能会导致您难以随时了解正确的网络发现策略配置。如果您不知道托管设备上的传感接口如何物理连接到您的网络，请将区域配置保留为默认设置。此默认设置会导致系统将发现规则部署到您的部署中的所有区域。（如果未排除任何区域，则系统会将发现策略部署到所有区域。）

配置网络发现规则中的区域

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**添加规则 (Add Rule)**。

步骤 3 点击 **区域**。

步骤 4 从**可用区域 (Available Zones)** 列表中选择一个或多个区域。

步骤 5 点击**保存** 以保存所做的更改。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

基于流量的检测身份源

基于流量的检测是系统唯一支持的未授权身份源。进行配置后，托管设备会检测您指定的网络上的 LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS 和 SMTP 登录。从基于流量的检测获取的数据仅可用于用户感知。与授权身份源不同，您可在网络发现策略中配置基于流量的检测，如配置基于流量的用户检测，第 2593 页中所述。

请注意以下限制：

- 基于流量的检测仅将用于 LDAP 连接的 Kerberos 登录解释为 LDAP 身份验证。托管设备无法检测使用协议（例如 SSL 或 TLS）的加密 LDAP 身份验证。
- 基于流量的检测只能检测使用 OSCAR 协议的 AIM 登录。无法检测使用 TOC2 的 AIM 登录。
- 基于流量的检测无法限制 SMTP 日志记录。这是因为未根据 SMTP 登录将用户添加到数据库；虽然系统会检测 SMTP 登录，这些登录不会被记录下来，除非数据库中包含已具有匹配邮件地址的用户。

基于流量的检测还会记录失败的登录尝试。如果登录尝试失败，不会将新用户添加到数据库的用户列表中。基于流量的检测功能检测到的登录失败活动的用户活动类型是**登录失败的用户 (Failed User Login)**。

注释 系统无法区分失败和成功的 HTTP 登录。要查看 HTTP 用户信息，您必须在基于流量的检测配置中启用**捕获登录失败尝试 (Capture Failed Login Attempts)**。

注意 使用网络发现策略 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。 在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测

基于流量的检测数据

设备使用基于流量的检测功能检测到登录时，它会将以下信息发送到 防火墙管理中心（这些信息将被记录为用户活动）：

- 识别出的登录用户名。
- 登录时间。
- 登录使用的 IP 地址，可能是用户的主机（用于 LDAP、POP3、IMAP 和 AIM 登录）、服务器（用于 HTTP、MDNS、FTP、SMTP 和 Oracle 登录）或会话发起方（用于 SIP 登录）的 IP 地址。
- 用户的邮件地址（用于 POP3、IMAP 和 SMTP 登录）。
- 检测到登录的设备名称。

如果之前已检测到该用户，防火墙管理中心会更新该用户的登录历史记录。请注意，防火墙管理中心可以使用 POP3 和 IMAP 登录中的邮件地址与 LDAP 用户 关联。举例来说，这意味着如果 防火墙管理中心检测到新的 IMAP 登录，且 IMAP 登录中的邮件地址与某个现有 LDAP 用户的邮件地址匹配，则 IMAP 登录不会创建新用户，而是会更新该 LDAP 用户的历史记录。

如果之前从未检测到该用户，防火墙管理中心会将该用户添加到用户数据库。唯一的 AIM、SIP 和 Oracle 登录始终会创建新用户记录，因为这些登录事件中没有 防火墙管理中心可与其他登录类型关联的数据。

在以下情况下，防火墙管理中心**不**会记录用户活动或用户身份：

- 网络发现策略被配置为忽略该登录类型
- 托管设备检测到 SMTP 登录，但用户数据库不包含之前使用匹配的邮件地址检测到的 LDAP、POP3 或 IMAP 用户

用户数据将被添加到用户表中。

基于流量的检测策略

可以限制在其中发现用户活动的协议，以减少检测到的用户的总数，以便将重点放在可能提供最完整用户信息的用户。限制协议检测有助于最大程度地减少用户名混乱以及预留 防火墙管理中心上的存储空间。

当选择基于流量的检测协议时，请注意以下事项：

- 如果通过协议（例如 AIM、POP3 和 IMAP）获取用户名，可能会由于承包商、访客及其他访客的网络访问而引入与组织无关的用户名。
- AIM、Oracle 和 SIP 登录可能会创建外来用户记录。之所以会发生这种情况，是因为这些登录类型没有与系统从 LDAP 服务器获取的任何用户元数据关联，也没有与托管设备会检测的其他类型登录中包含的任何信息关联。因此，防火墙管理中心无法将这些用户与其他类型的用户关联。

配置基于流量的用户检测

在网络发现规则中启用基于流量的用户检测时，将会自动启用主机发现。有关基于流量的检测的详细信息，请参阅基于流量的检测身份源，第 2592 页。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**用户 (Users)**。

步骤 3 请点击 **编辑** (✎)。

步骤 4 选中要检测登录的协议的复选框，或取消选中不希望检测登录的协议的复选框，然后选择是否**捕获失败的登录尝试**。

步骤 5 点击**保存**。

下一步做什么

注意 使用网络发现策略 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是直接通过而不进一步检查而，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 174 页。 在 HTTP、FTP 或 MDNS 协议上启用或禁用基于流量的非授权用户检测

- 配置网络发现规则以发现用户，如配置网络发现规则，第 2585 页中所述。
- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置高级网络发现选项

可以使用网络发现策略的”高级“(Advanced) 来配置策略范围的设置，以指定要检测的事件、发现数据的保留时间长度和更新频率、用于影响关联的漏洞映射，以及如何解决操作系统和服务器身份冲突。此外，还可以添加主机输入源和 NetFlow 导出器，以允许从其他源导入数据。

注释 发现和用户活动事件的数据库事件限制是在系统配置中设置。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击要修改的设置旁边的 **编辑** (✎) 或 **添加** (+)：

- “数据存储设置”(Data Storage Settings) - 更新设置，如配置网络发现数据存储，第 2601 页中所述。
- “事件日志记录设置”(Event Logging Settings) - 更新设置，如配置网络发现事件日志记录，第 2601 页中所述。
- “常规设置”(General Settings) - 更新设置，如配置网络发现常规设置，第 2595 页中所述。
- “身份冲突设置”(Identity Conflict Settings) - 更新设置，如配置网络发现身份冲突解决方法，第 2596 页中所述。
- “危害表现设置”(Indications of Compromise Settings) - 更新设置，如启用危害表现规则，第 2598 页中所述。
- “NetFlow 导出器”(NetFlow Exporters) - 更新设置，如将 NetFlow 导出器添加到网络发现策略，第 2599 页中所述。

- “操作系统和服务器身份源”(OS and Server Identity Sources) - 更新设置，如添加网络发现操作系统和服务器身份源， 第 2601 页中所述。
- “用于影响评估的漏洞”(Vulnerabilities to use for Impact Assessment) - 更新设置，如启用网络发现漏洞影响评估， 第 2597 页中所述。

步骤 4 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改， 第 180 页。

网络发现常规设置

常规设置控制系统更新网络映射的频率以及是否在发现过程中捕获服务器横幅。

捕获横幅

如果希望系统存储来自通告服务器供应商和版本的网络流量的报头信息（“横幅”），请选中此复选框。这些信息可提供有关收集的信息的其他上下文。可以通过访问服务器详细信息来访问为主机收集的服务器横幅。

更新间隔

系统更新信息（例如，上一次显示任何主机的 IP 地址的时间、使用应用的时间或应用的点击次数）的时间间隔。默认设置为 3600 秒（1 小时）。

请注意，为更新超时设置较小的时间间隔可在主机显示中提供更准确的信息，但会增加生成的网络事件数量。

配置网络发现常规设置

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**常规设置 (General Settings)** 旁边的 **编辑** (✎)。

步骤 4 更新设置，如网络发现常规设置， 第 2595 页中所述。

步骤 5 点击**保存**以保存常规设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改， 第 180 页。

网络发现身份冲突设置

系统通过将操作系统和服务器的指纹与流量模式进行匹配，从而确定在主机上运行的操作系统和应用。为了提供最可靠的操作系统和服务器身份信息，系统会核对来自多个源的指纹信息。

系统使用所有被动数据来推导操作系统身份并分配置信度值。

默认情况下，除非存在身份冲突，否则由扫描工具或第三方应用添加的身份数据会覆盖 Firepower 系统检测到的身份数据。可以使用 Identity Sources 设置按优先级对扫描程序和第三方应用指纹源进行评级。系统为每个源保留一个身份，但只有优先级最高的第三方应用或扫描程序源中的数据可用作当前身份。但请注意，用户输入数据会覆盖扫描程序和第三方应用数据，无论后者的优先级如何。

身份冲突是指系统检测到某个身份与来自“身份源”(Identity Sources) 设置中列出的活动扫描工具或第三方应用源或者来自 Firepower 系统用户的现有身份相冲突。默认情况下，身份冲突不会自动解决，必须通过主机配置文件，或者通过重新扫描主机或重新添加新的身份数据覆盖被动身份来解决冲突。但是，可以将系统设置为通过保留被动身份或主动身份来自动解决冲突。

生成身份冲突事件

指定在发生身份冲突时系统是否生成事件。

自动解决冲突

从**自动解决冲突 (Automatically Resolve Conflicts)** 下拉列表中，选择以下选项之一：

- **已禁用 (Disabled)**，如果要强制手动解决身份冲突
- **身份**，如果要在发生身份冲突时让系统使用被动指纹
- **保留主动身份 (Keep Active)**，如果要在发生身份冲突时让系统使用来自最高优先级主动源的当前身份

配置网络发现身份冲突解决方法

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**身份冲突设置 (Identity Conflict Settings)** 旁边的 **编辑** (✎)。

步骤 4 更新“编辑身份冲突设置”(Edit Identity Conflict Settings) 弹出窗口中的设置，如网络发现身份冲突设置，第 2596 页中所述。

步骤 5 点击**保存**以保存身份冲突设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

网络发现漏洞影响评估选项

可以配置系统如何对入侵事件执行关联影响。您具有以下选择：

- 如果要使用基于系统的漏洞信息执行影响关联，请选中**使用网络发现漏洞映射 (Use Network Discovery Vulnerability Mappings)** 复选框。
- 如果要使用第三方漏洞参考执行影响关联，请选中**使用第三方漏洞映射 (Use Third-Party Vulnerability Mappings)** 复选框。有关详细信息，请参阅《*Firepower* 系统主机输入 *API* 指南》。

可以同时选中这两个复选框或选中其中之一。如果系统生成入侵事件，且该事件涉及的主机所拥有的服务器或操作系统包含所选漏洞映射集中的漏洞，则该入侵事件将带有 Vulnerable（级别 1：红色）影响图标。对于没有供应商或版本信息的任何服务器，需要在 防火墙管理中心配置中启用漏洞映射。

如果取消选中这两个复选框，入侵事件将**不会**带有 Vulnerable（级别 1：红色）影响图标。

相关主题

映射第三方漏洞，第 2540 页

启用网络发现漏洞影响评估

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**用于影响评估的漏洞 (Vulnerabilities to use for Impact Assessment)** 旁边的 **编辑** (✎)。

步骤 4 更新“编辑漏洞设置”(Edit Vulnerability Settings) 弹出窗口中的设置，如网络发现漏洞影响评估选项，第 2597 页中所述。

步骤 5 点击**保存**保存漏洞设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

危害表现

系统使用网络发现策略中的 IOC 规则，以确定主机是否可能被恶意手段损害。当主机满足这些系统提供的规则中指定的条件时，系统将使用危害表现 (IOC) 进行标记。相关规则被称为 *IOC* 规则。每条 IOC 规则对应于一种类型的 IOC 标记。*IOC* 标记用于指定可能发生的危害的性质。

当发生以下情况时，防火墙管理中心可以标记涉及的主机和用户：

- 通过使用入侵、连接、安全智能和文件或恶意软件事件，系统将收集到的关于受监控网络及其流量的数据相关联，并确定潜在 IOC 已发生。
- 防火墙管理中心 可以通过 AMP 云从您的 Secure Endpoint 部署导入 IOC 数据。由于这些数据检查主机本身上的活动（例如，单个程序执行的操作），因此，通过这些数据可了解到纯网络数据无法洞察到的可能威胁。为了方便起见，防火墙管理中心会自动获取思科从 AMP 云开发的任何新 IOC 标记。

要配置此功能，请参阅启用危害表现规则，第 2598 页。

您还可以针对主机 IOC 数据和合规 allow 名单（决定 IOC 标记的主机）。

要调查和使用标记的 IOC，请参阅*Cisco Secure Firewall Management Center* 管理指南。

启用危害表现规则

要使系统检测和标记危害表现 (IOC)，必须先在网络发现策略中至少激活一个 IOC 规则。每个 IOC 规则对应于一种类型的 IOC 标记，所有 IOC 规则均由思科预定义；您不能创建原始规则。可根据网络和组织需要启用任何或全部规则。例如，如果使用诸如 Microsoft Excel 等软件的主机从未出现在监控网络上，可决定不启用与基于 Excel 的威胁相关的 IOC 标记。

提示 要禁用个别主机或其关联用户的 IOC 规则，请参阅*Cisco Secure Firewall Management Center* 管理指南中的 发现事件。

开始之前

由于 IOC 规则根据系统的其他组件以及Secure Endpoint 提供的数据触发，因此必须为要设置 IOC 标记的 IOC 规则正确许可并配置这些组件。启用与您将启用的 IOC 规则相关联的系统功能，例如入侵检测和防御 (IPS) 及高级恶意软件防护 (AMP)。如果未启用 IOC 规则的关联功能，将不会收集相关数据，规则也将无法触发。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击**危害表现设置 (Indications of Compromise Settings)** 旁边的 **编辑** (✎)。

步骤 4 要关闭或关闭整个 IOC 功能，请点击 **Enable IOC** 旁边的滑块。

步骤 5 要全局启用或禁用个别 IOC 规则，请点击相应规则的**启用 (Enabled)** 列中的滑块。

步骤 6 点击**保存**以保存 IOC 规则设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

将 NetFlow 导出器添加到网络发现策略

使用此程序添加NetFlow导出器。请注意，如果导出器当前正在发现规则中使用，则无法将其删除。

开始之前

- 查看前提条件：使用 NetFlow 数据的要求（原则），第 2523 页
- 配置 NetFlow 导出器：NetFlow 数据，第 2522 页

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **NetFlow 设备**旁边的 **添加** (+) 。

步骤 4 输入导出器的 **IP 地址**。

步骤 5 点击**保存**。

下一步做什么

- 配置网络发现规则以监控 NetFlow 流量：配置网络发现规则，第 2585 页
- 部署配置更改；请参阅 部署配置更改，第 180 页。

网络发现数据存储设置

发现数据存储设置包括主机限制和超时设置。

当达到主机限制时

Secure Firewall Management Center可以监控因而存储在网络映射中的主机数取决于其型号。**当达到主机限制时 (When Host Limit Reached)** 选项控制在达到主机限制后检测到新主机时发生的情况。您可以执行以下操作：

丢弃主机

系统丢弃保持非活动状态时间最长的主机，然后添加新主机。这是默认设置。

不插入新主机

系统不跟踪任何新发现的主机。仅在主机计数降至低于限制后，系统才会恢复跟踪新主机。如果管理员增加域的主机限制、手动从网络映射中删除主机，或者系统由于主机不活动而将其识别为超时，则可能会发生这种情况。

表 *158:* 达到多租户的主机限制

设置	已设置域主机限制？	已达到域主机限制	已达到祖先域主机限制
丢弃主机	是	丢弃受限制域中的最旧主机。	丢弃配置为丢弃主机的所有后代分叶域中的最旧主机。 如果无法丢弃任何主机，则不添加主机。
	否	不适用	丢弃配置为丢弃主机以及共享常规池的所有后代分叶域中的最旧主机。
不插入新主机	是/否	不添加主机。	不添加主机。

主机超时

系统因网络映射中的某一主机不活动而丢弃该主机之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。单个主机 IP 和 MAC 地址可以单独超时，但是，除非主机的所有关联地址都超时，否则该主机不会从网络映射中消失。

要避免主机提前超时，请确保主机超时值大于网络发现策略常规设置中的更新间隔。

服务器超时

系统因网络映射中的某一服务器不活动而丢弃该服务器之前经过的时间（以分钟为单位）。默认设置为七天（10,080 分钟）。

要避免服务器提前超时，请确保服务超时值大于网络发现策略常规设置中的更新间隔。

客户端应用超时

系统因网络映射中的某一客户端不活动而丢弃该客户端之前经过的时间（以分钟为单位）。默认设置为 10080 分钟（一周）。

为确保最佳性能，请将客户端超时值设置为超过网络发现策略常规设置中的更新间隔。

相关主题

主机限制，第 1986 页

配置网络发现数据存储

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **网络发现数据存储设置**旁的 **编辑** (✎) 。

步骤 4 更新“数据存储设置”(Data Storage Settings) 对话框中的设置，如网络发现数据存储设置，第 2599 页中所述。

步骤 5 点击**保存**以保存数据存储设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

配置网络发现事件日志记录

事件日志记录设置控制是否记录发现和主机输入事件。如果不记录事件，则无法在事件视图中检索事件，也不能将事件用于触发关联规则。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **事件日志记录设置**旁边的 **编辑** (✎) 。

步骤 4 选中或取消选中要在数据库中记录的发现和主机输入事件类型旁边的复选框，如在发现事件类型和主机输入事件类型 *Cisco Secure Firewall Management Center* 管理指南 的发现事件一节所述。

步骤 5 点击**保存** 以保存事件日志记录设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

添加网络发现操作系统和服务器身份源

在网络发现策略的“高级”中，可以添加新的主动源，或更改现有源的优先级或超时设置。

将扫描工具添加到此页面不会添加 Nmap 扫描工具已有的完整集成功能，但允许集成导入的第三方应用或扫描结果。

如果从第三方应用或扫描工具导入数据，请确保将源中的漏洞映射到网络中检测到的漏洞。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

步骤 2 点击**高级 (Advanced)**。

步骤 3 点击 **操作系统和服务器身份源** 旁边的 **编辑** (✎) 。

步骤 4 要添加新源，请点击 **Add Source**。

步骤 5 输入 **Name**。

步骤 6 从下拉列表中选择输入源**类型 (Type)**：

- 如果打算使用 AddScanResult 函数导入扫描结果，请选择**扫描工具 (Scanner)**。
- 如果不打算导入扫描结果，请选择**应用 (Application)**。

步骤 7 要指示从此源将某个身份添加到网络映射到删除该身份之间的持续时间，请从**超时 (Timeout)** 下拉列表中选择**小时数 (Hours)**、**天数 (Days)** 或**周数 (Weeks)**，并输入适当的持续时间。

步骤 8 或者：

- 要升级某个源并使用操作系统和应用身份以支持列表中该源下面的源，请选择该源并点击向上箭头。
- 要降级某个源并且只有列表中该源上面的源没有提供身份时才会使用操作系统和应用身份，请选择改源并点击向下箭头。
- 要删除某个源，请点击该源旁边的 **删除** (🗑) 。

步骤 9 点击**保存**以保存身份源设置。

下一步做什么

- 部署配置更改；请参阅 部署配置更改，第 180 页。

相关主题

映射第三方漏洞，第 2540 页

对网络发现策略进行故障排除

在对系统的默认检测功能进行任何更改之前，应分析哪些主机未被正确地识别以及原因，以便可以决定实施哪些解决方案。

托管设备是否正确布置？

如果诸如负载均衡器、代理服务器或NAT设备的网络设备位于托管设备和未识别或错误识别的主机之间，请将托管设备布置在更靠近错误识别的主机的位置，而不是使用自定义指纹技术。思科不建议在这种情况下使用自定义指纹技术。

未识别的操作系统是否拥有唯一的 TCP 堆栈？

如果系统识别的主机错误，应调查主机为何被错误地识别，以便帮助您决定：是创建和激活自定义指纹，还是用 Nmap 或主机输入数据替代发现数据。

⚠

注意 如果遇到错误识别的主机，请在创建自定义指纹之前联系支持代表。

如果主机正在运行的操作系统未被系统默认检测到，并且该操作系统不与检测到的现有操作系统共享识别性 TCP 堆栈特征，则应创建自定义指纹。

例如，如您拥有的 Linux 自定义版本带有系统无法识别的唯一 TCP 堆叠，则创建自定义指纹将让您受益，因为这可使系统识别并继续监控主机，而不必使用扫描结果或第三方数据，进而无需持续自行主动更新这些数据。

请注意，许多开源Linux发行版本使用相同的内核，同样，系统将使用Linux内核名称来识别它们。如为 Red Hat Linux 系统创建自定义指纹，可能会看到识别为 Red Hat Linux 的其他操作系统（如 Debian Linux、Mandrake Linux、Knoppix 等），因为相同的指纹与多个 Linux 发行版本匹配。

不应在每种情况下都使用指纹。例如，可能对主机的 TCP 堆叠做出了修改，以使其与另一操作系统类似或相同。例如，Apple Mac OS X 主机已修改，使其指纹与 Linux 2.4 主机相同，从而导致系统将其识别为 Linux 2.4 而不是 Mac OS X。如果为 Mac OS X 主机创建自定义指纹，可能会导致所有合法的 Linux 2.4 主机被错误地识别为 Mac OS X 主机。在这种情况下，如果 Nmap 正确地识别主机，应为该主机安排定期的 Nmap 扫描。

如果使用主机输入从第三方系统导入数据，则必须将第三方用于描述服务器和应用协议的供应商、产品和版本字符串映射到这些产品的思科定义。请注意，即使将应用数据映射到Firepower系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。

系统可以协调来自多个源的数据，以便确定操作系统或应用的当前标识。

对于 Nmap 数据，可安排定期 Nmap 扫描。对于主机输入数据，可定期运行用于导入的 Perl 脚本或命令行实用程序。然而，请注意，主动扫描数据和主机输入数据可能不会随发现数据的频率进行更新。

Firepower 系统能否识别所有应用？

如果主机已由系统正确识别，但有未识别的应用，则可创建用户定义的检测器来向系统提供端口和模式匹配信息以帮助识别应用。

是否已应用可修复漏洞的修补程序？

如果系统已正确识别主机，但未反映已应用的修补，则可使用主机输入功能导入修补程序信息。导入修补程序信息时，必须将修补程序的名称映射至数据库中的修补程序。

是否要跟踪第三方漏洞？

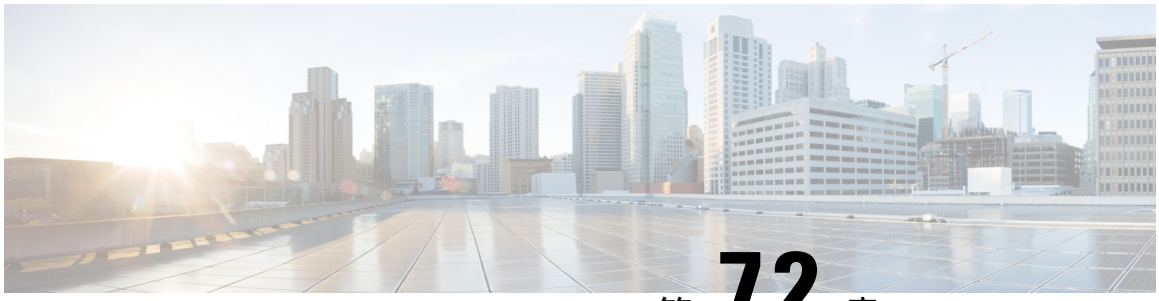
如果拥有要用于影响关联的第三方系统的漏洞信息，则可将服务器和应用协议的第三方漏洞标识符映射到思科数据库中的漏洞标识符，然后使用主机输入功能导入漏洞。有关使用主机输入功能的详细信息，请参阅《《*Firepower* 系统主机输入 *API* 指南》》。请注意，即使将应用数据映射到Firepower系统供应商和版本定义，导入的第三方漏洞也不用于客户端或 Web 应用的影响评估。



第 XIII 部分

对象和证书

- 对象管理， 第 2607 页
- 证书， 第 2743 页



第 72 章

对象管理

本章介绍如何管理可重用对象。

- 对象简介，第 2608 页
- 对象管理器，第 2610 页
- AAA 服务器，第 2620 页
- 访问列表，第 2625 页
- 地址池，第 2630 页
- 应用过滤器，第 2631 页
- AS 路径，第 2632 页
- BFD 模板，第 2632 页
- 密码套件列表，第 2634 页
- 社区列表，第 2634 页
- DHCP IPv6 池，第 2637 页
- 可分辨名称，第 2637 页
- DNS 服务器组，第 2640 页
- **加密可视性引擎例外列表**，第 2640 页
- 外部属性，第 2642 页
- 文件列表，第 2650 页
- FlexConfig，第 2654 页
- 地理定位，第 2655 页
- 接口，第 2655 页
- 密钥链，第 2656 页
- 网络，第 2658 页
- PKI，第 2661 页
- 策略列表，第 2680 页
- 端口，第 2682 页
- 前缀列表，第 2683 页
- 路由映射，第 2685 页
- 安全智能，第 2689 页
- Sinkhole，第 2700 页

- SLA 监控器， 第 2700 页
- 时间范围， 第 2702 页
- 时区， 第 2703 页
- 隧道区域， 第 2704 页
- URL， 第 2704 页
- 变量集， 第 2705 页
- VLAN 标记， 第 2720 页
- VPN， 第 2720 页
- 对象管理的历史记录， 第 2739 页

对象简介

为了提高灵活性和Web界面的易用性，系统会使用命名对象，命名对象是将名称与值相关联的可重用配置。当您要使用该值时，可使用命名对象来替代。系统支持在Web界面中的不同位置使用这些对象，包括许多策略和规则、事件搜索、报告、控制面板等等。系统提供许多代表常用配置的预定义对象。

使用对象管理器创建和管理对象。许多使用对象的配置也允许您根据需要即时创建对象。您也可以使用对象管理器进行以下操作：

- 查看使用网络、端口、VLAN或URL对象的策略、设置和其他对象；请参阅查看对象及其使用情况， 第 2614 页。
- 将对象分组，以用一个配置引用多个对象；请参阅对象组， 第 2615 页。
- 覆盖所选设备的对象值；请参阅 对象覆盖， 第 2617 页。

编辑在活动策略中使用的对象后，必须重新部署更改的配置，才能使更改生效。您无法删除活动策略正在使用的对象。

注释 当且仅当某个对象用于分配到某个托管设备的策略中时，该对象才会在托管设备上予以配置。如果从分配到给定设备的所有策略中删除某个对象，则该对象也会从下一次部署的设备配置中被删除，对其进行的后续更改不会在设备配置中反映出来。

对象类型

下表列出了您可以在系统中创建的对象，并指示是否可以对每个对象类型进行分组或配置以允许覆盖。

对象类型	是否可分组？	是否允许覆盖？
网络	是	是
端口	是	是

对象类型	是否可分组？	是否允许覆盖？
接口： • 安全区 • 接口组	否	否
隧道区域	否	否
应用过滤器	否	否
VLAN 标记	是	是
外部属性：安全组标记 (SGT) 和动态对象	否	否
URL	是	是
地理定位	否	否
时间范围	否	否
变量集	否	否
安全智能：网络、DNS 和 URL 列表和源	否	否
Sinkhole	否	否
文件列表	否	否
密码套件列表	否	否
可分辨名称	是	否
公钥基础设施 (PKI)： • 内部和受信任 CA • 内部和外部证书	是	否
密钥链	否	是
DNS 服务器组	否	否
SLA 监控器	否	否
前缀列表：IPv4 和 IPv6	否	是
路由映射	否	是
访问列表：标准和扩展	否	是
AS 路径	否	是

对象类型	是否可分组？	是否允许覆盖？
社区列表	否	是
策略列表	否	是
FlexConfig：文本和 FlexConfig 对象	否	是

对象和多租户

在多域部署中，您可以在全局域和后代域中创建对象，只能在全局域中创建的安全组标记 (SGT) 对象除外。系统会显示在当前域中创建的对象，您可以对其进行编辑。它还会显示在祖先域中创建的对象，但您无法对其进行编辑，除了安全区域和接口组。



注释 因为安全区域和接口组与在分叶级别配置的设备接口绑定，后代域中的管理员可以查看并编辑在祖先域中创建的 和组 。子域用户可以在祖先区域和组中添加和删除接口，但无法删除或重命名区域/组。

对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

对于支持分组的对象，可以将当前域中的对象与从祖先域中继承的对象分到一组。

对象覆盖允许您定义某些类型对象的设备特定或域特定值，包括网络、端口、VLAN 标记和 URL。在多域部署中，可以为祖先域中的对象定义默认值，但允许后代域中的管理员为该对象添加覆盖值。

对象管理器

可以使用对象管理器创建和管理对象和对象组。

对象管理器每页显示 20 个对象或对象组。如果有超过 20 个任何类型的对象或对象组，请使用位于页面底部的导航链接查看其他页面。您还可以转到特定页或点击 **刷新** ( ) 来刷新视图。

默认情况下，页面会按名称的字母顺序列示对象和对象组。您可以按名称或值对页面上的对象进行过滤。

导入对象

对象可以通过逗号分隔值文件导入。一次最多可以导入1000个对象。逗号分隔值文件的内容应依照特定的格式。每种对象类型的格式不同。只能导入几种类型的对象。请参阅下表以了解支持的对象类型以及相应的规则。

对象类型	规则

单个对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DN
	• 要导入条目，必须同时输入 NAME 和 DN 列条目。
	• 您可以将单个对象直接导入到现有的可分辨名称对象组中。

网络对象	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • TYPE
	  • 值
	  • 查询
	• 必须提供 NAME 和 VALUE 列条目才能导入主机、范围或网络对象类型的条目。
	• 对于 FQDN 对象，TYPE 列条目必须提及“fqdn”，而 LOOKUP 列条目必须指定为“ipv4”、“ipv6”或“ipv4_ipv6”。
	• 如果 FQDN 对象的 LOOKUP 列条目中未提供内容，则要使用 ipv4_ipv6 字段值来保存该对象。

对象类型	规则

端口	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• NAME 列条目为必填。
	• 对于“tcp”和“udp”协议类型，PORT 列条目为必填。
	• 对于“icmp”和“icmp6”协议类型，ICMPCODE 和 ICMPTYPE 列条目为必填。

URL	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • URL
	• 必须提供 NAME 和 URL 列条目才能导入条目。

VLAN 标记	• 列标题必须以大写字母表示。
	• 文件必须包含以下列标题：
	  • 名称
	  • DESCRIPTION
	  • 标记
	• 必须提供 NAME 和 TAG 列条目才能导入条目。

过程

步骤 1 选择**对象**。

步骤 2 从左侧窗格中选择以下对象类型之一：

- **可分辨名称 (Distinguished Name)** > **单个对象 (Individual Objects)** >
- **网络对象**
- **端口**
- **URL**
- **VLAN 标签**

步骤 3 从**添加 [对象类型] (Add [Object Type])** 下拉列表中选择**导入对象 (Import Object)**。

注释
如果您在上一步中选择了**单个对象 (Individual Objects)**，请点击**导入 (Import)**。

步骤 4 点击**浏览 (Browse)**。

步骤 5 在系统上找到并选择以逗号分隔的文件。

步骤 6 点击 **Open**。

注释
导入 **可分辨名称** 对象时，可以选中 **将导入的可分辨名称对象添加到下面的对象组 (Add imported Distinguished Name objects to the below object group)** 复选框，然后从下拉框中选择组名称，以将对象直接导入现有的可分辨名称对象组。

步骤 7 点击**导入 (Import)**。

编辑对象

过程

步骤 1 选择**对象**。

步骤 2 从列表中选择对象类型；请参阅对象简介，第 2608 页。

步骤 3 点击要编辑的对象旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 根据需要修改对象设置。

步骤 5 如果编辑的是变量集，请管理变量集中的变量；请参阅管理变量，第 2717 页。

步骤 6 对于可以配置为允许覆盖的对象：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。只可以为属于当前域的对象更改此设置。

- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 7 点击**保存**。

步骤 8 如果编辑的是变量集，并且该变量集正在被一个访问控制策略使用，请点击**是**以确认要保存更改。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

查看对象及其使用情况

您可以在“对象管理”(Object Management) 页面上查看对象的使用详细信息。防火墙管理中心 为许多对象类型提供此功能。但是，某些对象类型不受支持。

过程

步骤 1 选择**对象**。

步骤 2 选择以下支持的对象类型之一：

- 访问列表 > 扩展
- 访问列表 > 标准
- AS 路径
- 社区列表
- 接口
- 网络
- 策略列表
- 端口
- 前缀列表 > IPv4 前缀列表
- 前缀列表 > IPv6 前缀列表
- 路由映射
- SLA 监控器
- URL
- VLAN 标记

步骤 3 点击对象旁边的 **查找使用情况** (🔭) 图标。

“对象使用情况”(Object Usage) 窗口会显示使用对象的所有策略、对象和其他设置的列表。点击列出的任何项目，了解有关对象使用情况的详细信息。对于会用到对象的策略和一些其他设置，您可以点击相应的链接以访问相应的 UI 页面。

过滤对象或对象组

过程

步骤 1 选择**对象**。

步骤 2 在**过滤 (Filter)** 字段中输入过滤器条件。

页面会在您键入内容时进行更新，以显示匹配的项目。

您可以使用以下通配符：

- 星号 (*) 匹配零或重复出现的一个字符。
- 脱字符 (^) 匹配字符串开头的内容。
- 美元符号 ($) 匹配字符串结尾的内容。

步骤 3 选中**显示未使用的对象 (Show Unused Object)** 复选框，以查看系统中任何位置未使用的对象和对象组。

注释

- 如果对象是未使用的对象组的一部分，则该对象会被视为已使用。但是，如果选中**显示未使用的对象 (Show Unused Object)** 复选框，则会显示未使用的对象组。
- **显示未使用的对象 (Show Unused Object)** 复选框仅适用于网络、端口、URL 和 VLAN 标记对象类型。

对象组

将对象分组使得可以引用带有单个配置的多个对象。系统允许在 Web 界面中互用对象和对象组。例如，在任何要使用端口对象的地方，也可以使用端口对象组。

可以将网络、端口、VLAN 标记、URL 和 PKI 对象分组。网络对象组可以嵌套，即您可以将一个网络对象组添加到另一个网络对象组中，最高可达 10 个级别。

相同类型的对象和对象组不能具有相同的名称。

编辑策略中使用的对象组（例如，访问控制策略中使用的网络对象组）时，您必须重新部署已更改的配置以使更改生效。

删除组不会删除组中的对象，只会删除对象之间的相关性。此外，您也无法删除活动策略中正在使用的组。例如，无法删除用于已保存访问控制策略中的 VLAN 条件的 VLAN 标记组。

对可重用对象进行分组

过程

步骤 1 选择**对象**。

步骤 2 如果要分组的对象类型为**网络 (Network)**、**端口 (Port)**、**URL** 或 **VLAN 标记 (VLAN Tag)**：

a) 从对象类型列表中选择对象类型。

b) 从**添加（对象类型）(Add [Object Type])** 下拉列表中选择**添加组 (Add Group)**。

步骤 3 如果要分组的对象类型为**可分辨名称 (Distinguished Name)**：

a) 展开**可分辨名称 (Distinguished Name)** 节点。

b) 选择**对象组 (Object Groups)**。

c) 点击**添加可分辨名称 (Add Distinguished Name)**。

步骤 4 如果要分组的对象类型为 **PKI**：

a) 展开 **PKI** 节点。

b) 选择以下其中一个选项：

- **内部 CA 证书 (Internal CA Groups)**
- **受信任 CA 证书 (Trusted CA Groups)**
- **内部证书组 (Internal Cert Groups)**
- **外部证书组 (External Cert Groups)**

c) 点击**添加[对象类型]组 (Add [Object Type] Group)**。

步骤 5 在**名称 (Name)** 中输入唯一的名称。

步骤 6 从列表中选择一个或多个对象，然后点击**添加 (Add)**。

您还可以：

- 使用过滤器字段 (**搜索** ( )) 可搜索要包括的现有对象，在您键入时，该字段会更新以显示匹配项目。点击搜索字段上方的 **重新加载** ( )，或点击搜索字段中的 **清除** ( ) 以清除搜索字符串。
- 如果现有对象不符合您的需要，可点击 **添加** ( ) 快速创建对象。

步骤 7 或者对于**网络 (Network)**、**端口 (Port)**、**URL** 和 **VLAN 标记 (VLAN Tag)** 组：

- 输入**说明**。

- 选中**允许覆盖 (Allow Override)** 复选框，允许对此对象组进行覆盖；请参阅允许对象覆盖，第 2618 页。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象组，请部署配置更改；请参阅部署配置更改，第 180 页。

对象覆盖

通过对象覆盖，您可以为对象定义一个备选值，系统将为您指定的设备使用该值。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，您可能想要拒绝 ICMP 流量传送到公司的不同部门，每个部门连接到不同的网络。可以通过定义带有特定规则（包括一个称为“部门网络”的网络对象）的访问控制策略来实现。通过允许覆盖此对象，即可在每个相关设备上创建覆盖，指定该设备所连接的实际网络。

您可以将对象覆盖的目标对准特定域。在这种情况下，除非已在设备级覆盖该值，否则系统会将对象覆盖值用于目标域中的所有设备。

在对象管理器中，可以选择可覆盖的对象并为该对象定义设备级或域级覆盖列表。

只能使用具有以下对象类型的对象覆盖：

- 网络
- 端口
- VLAN 标记
- URL
- SLA 监控器
- 前缀列表
- 路由映射
- 访问列表
- AS 路径
- 社区列表
- 策略列表
- 证书注册 (PKI)

- 密钥链

如果可以覆盖对象，则系统会在对象管理器中为该对象类型显示**覆盖 (Override)** 列。此列的可能值包括：

- 绿色勾选标记 - 表示可为对象创建覆盖且尚未添加任何覆盖
- 红色 X - 表示无法为对象创建覆盖
- 数字 - 表示已添加到该对象的覆盖计数（例如，“2”表示已添加两个覆盖）

管理对象覆盖

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中进行选择；请参阅对象简介，第 2608 页。

步骤 3 点击要编辑的对象旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域且已配置为不允许覆盖，或者您没有修改对象的权限。

步骤 4 管理对象覆盖：

- 添加 - 添加对象覆盖；请参阅添加对象覆盖，第 2619 页。
- 允许 - 允许对象覆盖；请参阅允许对象覆盖，第 2618 页。
- 删除 - 在对象编辑器中，点击要删除的覆盖旁边的 **删除** ()。
- 编辑 - 编辑对象覆盖；请参阅编辑对象覆盖，第 2619 页。

允许对象覆盖

过程

步骤 1 在对象编辑器中，选中**允许覆盖**复选框。

步骤 2 点击**保存**。

下一步做什么

添加对象覆盖值；请参阅添加对象覆盖，第 2619 页。

添加对象覆盖

开始之前

允许对象覆盖；请参阅允许对象覆盖，第 2618 页。

过程

步骤 1 在对象编辑器中，展开**覆盖**部分。

步骤 2 点击**添加 (Add)**。

步骤 3 在**目标 (Targets)** 中，选择**可用设备和域 (Available Devices and Domains)** 列表中的域或设备，然后点击**添加 (Add)**。

步骤 4 在“覆盖”(Override) 选项卡中，输入**名称**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 输入覆盖值。

示例：

对于网络对象，请输入网络值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

编辑对象覆盖

可以修改说明和现有覆盖的值，但不可以修改现有目标列表。相反，您必须添加一个具有新目标的新覆盖，该覆盖将代替现有覆盖。

过程

步骤 1 在对象编辑器中，展开**覆盖**部分。

步骤 2 点击要修改的覆盖旁边的 **编辑** ()。

步骤 3 或者，修改**说明 (Description)**。

步骤 4 修改覆盖值。

步骤 5 点击**保存**保存覆盖。

步骤 6 点击保存保存对象。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

AAA 服务器

添加可重用的 AAA 服务器对象。

添加 RADIUS 服务器组

Radius 服务器组对象包含一个或多个对 RADIUS 服务器的引用。这些服务器用于对通过远程访问 VPN 连接登录的用户进行身份验证。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

开始之前

注释 不能覆盖 Radius 服务器组对象。

过程

步骤 1 选择对象 > **AAA 服务器** > **RADIUS 服务器组**。

将列出所有当前配置的 Radius 服务器组对象。使用过滤器缩小列表的范围。

步骤 2 选择并编辑某一已列出的 RADIUS 服务器组对象，或者添加一个新的 RADIUS 服务器组对象。

参阅RADIUS 服务器选项，第 2622 页和RADIUS 服务器组选项，第 2620 页以配置此对象。

步骤 3 点击保存

RADIUS 服务器组选项

导航路径

对象 > **AAA 服务器** > **RADIUS 服务器组**。选择并编辑已配置的 RADIUS 服务器组对象，或添加一个新的相应对象。

字段

- **名称**和**说明** - 输入名称，并可选择性地输入说明，以标识此 RADIUS 服务器组对象。
- **组记帐模式** - 将记帐消息发送到组中的 RADIUS 服务器的方法。选择**单个**，记帐消息会发送到组中的单个服务器，这是默认设置。或者，选择 **多个**，记帐消息将同时发送到组中的所有服务器。
- **重试间隔** - 两次尝试与 RADIUS 服务器联系之间的间隔。值范围为 1 秒至 10 秒。
- **领域**（可选）- 指定或选择此 RADIUS 服务器组与之关联的 Active Directory (AD) 领域。然后，在身份策略中选择此领域，以便在确定流量的 VPN 身份验证身份源时访问关联的 RADIUS 服务器组。此领域有效地提供了从身份策略到此 Radius 服务器组的桥接。如果没有与此 RADIUS 服务器组关联的领域，则无法访问 RADIUS 服务器组以确定身份策略中流量的 VPN 身份验证身份源。



注释 如果使用具有用户身份和 RADIUS 作为身份源的远程访问 VPN，则此字段为必填。

- **仅启用授权** - 如果此 RADIUS 服务器组未用于身份验证，但正在用于授权或记帐，请选中此字段以为 RADIUS 服务器组启用仅授权模式。

  在仅授权模式下，无需在 Access-Request 中包含 RADIUS 服务器密码。因此，为各个 RADIUS 服务器配置的密码将被忽略。

- **启用临时帐户更新**和**间隔** - 启用生成 RADIUS 临时记帐更新消息的功能，以便将新分配的 IP 地址通知 RADIUS 服务器。在“间隔”字段中设置定期记帐更新之间的间隔长度（以小时为单位）。有效范围是 1 至 120，默认值为 24。
- **启用动态授权**和**端口** - 为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务。在**端口**字段中指定用于 RADIUS CoA 请求的侦听端口。有效范围是 1024 至 65535，默认值为 1700。定义后，相应的 RADIUS 服务器组将注册用于 CoA 通知，并侦听相应端口以获取来自思科身份服务引擎 (ISE) 的 CoA 策略更新。
- **将可下载 ACL 与思科 AV 对 ACL 合并 (Merge Downloadable ACL with Cisco AV Pair ACL)** - 允许将可下载访问控制列表 (dACL) 与思科属性值 (AV) 对 ACL 合并。

  可下载 ACL 在 CiscoISE 中定义和更新访问控制列表，并允许将 ACL 下载到所有适用的控制器。有关在思科 ISE 中使用 dACL 的详细信息，请参阅《思科 *ISE* 管理员指南》中的“分段”一章中的“授权策略”部分。

  思科 AV 对 ACL 可用于为每个会话定义特定的身份验证、授权和审计元素。有关在思科 ISE 中使用 dACL 的详细信息，请参阅《思科 *ISE* 管理员指南》中的“分段”一章中的“授权配置文件设置”部分。

  如果选择**将可下载 ACL 与思科 AV 对 ACL 合并 (Merge Downloadable ACL with Cisco AV Pair ACL)**，则可以选择以下选项：

  - **在思科 AV 对 ACL 之后 (After Cisco AV Pair ACL)**表示可下载 ACL 条目应放置在思科 AV 对条目之后。

- **在思科 AV 对 ACL 之前 (Before Cisco AV Pair ACL)**表示可下载 ACL 条目应放置在思科 AV 对条目之前。

- **RADIUS 服务器** - 请参阅RADIUS 服务器选项，第 2622 页。

相关主题

添加 RADIUS 服务器组，第 2620 页

RADIUS 服务器选项

导航路径

对象 > **AAA 服务器** > **RADIUS 服务器组** 。选择并编辑某一已列出的 RADIUS 服务器组对象，或者添加一个新的 RADIUS 服务器组对象。然后在“RADIUS 服务器组”对话框中，选择并编辑某一已列出的 RADIUS 服务器，或者添加一个新的 RADIUS 服务器。

字段

- **IP 地址/主机名** — 标识将接收身份验证请求的 RADIUS 服务器的主机名或 IP 地址（IPv4 或 IPv6）的网络对象。只能选择一项，以向“RADIUS 服务器组”列表中添加其他服务器、添加其他 RADIUS 服务器。
- **启用 RADIUS 服务器的消息身份验证器**- 消息身份验证器可保护服务器到客户端的通信，它是 RADIUS 服务器和防火墙设备之间建立安全连接所必需的。禁用消息验证器可能会使防火墙暴露于潜在的攻击。

  您的 RADIUS 服务器必须支持并配置 Message-Authenticator。需要 Firewall Threat Defense 版本 7.2.10+、7.4.3+ 或 7.6.1+。对于 Firepower 4100/9300，此功能可能需要 FXOS 升级；有关最低版本，请参阅*Cisco Secure Firewall Threat Defense* 兼容性指南。
- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **密钥**和**确认密钥** - 用于在托管设备（客户端）与 RADIUS 服务器之间加密数据的共享密钥。

  该密钥是一个区分大小写的字母数字字符串，最多 127 个字符。允许使用特殊字符。

  在此字段中定义的密钥必须与 RADIUS 服务器上的密钥相匹配。在“确认”字段中再次数据该密钥。
- **记帐端口** - 在其上执行 RADIUS 记帐的端口。默认值为 1813。
- **超时** - 身份验证的会话超时。

  RADIUS 双因素身份验证的超时值必须为 60 秒或以上。默认超时值为 10 秒。
- **连接方式** - 使用路由查找或特定接口建立从设备到 RADIUS 服务器的连接。
  - 点击**路由 (Routing)** 单选按钮以使用路由表。
  - 点击**特定接口 (Specific Interface)** 单选按钮，然后从下拉列表中选择一个安全区/接口组或管理 接口（默认）。如果要使用管理，则必须明确选择它；它在使用路由查找时不可用。不能将任何其他仅管理接口指定为 RADIUS 源。 您也可以选择环回接口组。

- **重定向 ACL** - 从列表中选择重定向 ACL 或添加新 ACL。

  此为在设备中定义的用于决定重定向流量的 ACL 名称。此处的重定向 ACL 名称必须与 ISE 服务器中的 *redirect-acl* 名称相同。在配置 ACL 对象时，请确保对 ISE 和 DNS 服务器选择“阻止”操作，并对其余服务器选择“允许”操作。

相关主题

添加 RADIUS 服务器组，第 2620 页
RADIUS 服务器组选项，第 2620 页

添加单点登录服务器

开始之前

从 SAML 身份提供程序获取以下信息：

- 身份提供程序实体 ID URL
- 登录 URL
- 注销 URL
- 身份提供者证书，并使用 防火墙管理中心 Web 界面（设备 (Devices) > 证书 (Certificates)）在 Firewall Threat Defense 中注册证书**设备 > 证书**

有关详细信息，请参阅配置 SAML 单点登录身份验证，第 1625 页。

过程

步骤 1 选择**对象 > AAA服务器 > 单点登录服务器**。

步骤 2 点击 **添加单点登录服务器** 并提供以下详细信息：

- **名称**-SAML 单点登录服务器对象的名称。
- **身份提供程序实体 ID (Identity Provider Entity ID)** - 在 SAML IdP 中定义的用于唯一标识服务提供商的 URL。

  用于提供元数据 XML 的页面的 URL，元数据 XML 说明了 SAML 颁发者将如何响应请求。
- **SSO URL**-用于登录到 SAML 身份提供程序服务器的 URL。
- **注销 URL**-用于注销 SAML 身份提供程序服务器的 URL。
- **基本 URL (Base URL)** - 在身份提供程序身份验证完成后，将用户重定向回 Firewall Threat Defense 的 URL。这是为 Firewall Threat Defense 远程访问 VPN 配置的访问接口的 URL。
- **身份提供程序证书 (Identity Provider Certificate)** - 注册到 Firewall Threat Defense 以验证由 IdP 签名的消息的 IdP 的证书。

从列表中选择一个标识提供程序证书，或点击**添加**以创建新的证书注册对象。

注释
仅使用 CA 证书作为 IdP 证书；不允许使用自签名证书。

有关详细信息，请参阅管理 Firewall Threat Defense 证书，第 2744 页。

您必须在 Firewall Threat Defense上将所有 Microsoft Azure 注册应用 CA 证书注册为信任点。Microsoft Azure SAML 身份提供程序在 Firewall Threat Defense 上为初始应用配置。所有连接配置文件映射到配置的 MS Azure SAML 身份提供程序。对于每个 MS Azure 应用（默认设置除外），您可以在远程访问 VPN 的连接配置文件配置中选择所需的信任点（CA 证书）。

有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

- **服务提供商证书 (Service Provider Certificate)** - Firewall Threat Defense 证书，用于签署请求并与 IdP 建立信任圈。

  如果您尚未注册内部 Firewall Threat Defense 证书，请点击 + 添加并注册证书。有关详细信息，请参阅管理 Firewall Threat Defense 证书，第 2744 页。

- **请求签名**-选择用于对 SAML 单点登录请求签名的加密算法。

  签名从最弱到最强列出：SHA1，SHA256，SHA384，SHA512。选择“无”可禁用加密。

- **请求超时 (Request Timeout)** - 指定用户完成单点登录请求的 SAML 断言有效期。SAML IdP 有两个超时： *NotBefore* 和 *NotOnOrAfter*。Firewall Threat Defense 会验证其当前时间是否在（下限）*NotBefore* 和（上限）*NotBefore* 加上 *timeout* 和 *NotOnOrAfter* 中的较小者的时间范围内。因此，如果设置的超时长于 IdP 的 *NotOnOrAfter* 超时，则忽略指定的超时，并选择 *NotOnOrAfter* 超时。如果指定超时和 *NotBefore* 超时的总和小于 *NotOnOrAfter* 时间，则 Firewall Threat Defense 超时会覆盖超时。

  超时范围是 1-7200 秒，默认是 300 秒。

- **启用仅在内部网络上可访问的 IdP (Enable IdP only accessible on Internal Network)** - 如果 SAML IdP 位于内部网络上，请选择此选项。Firewall Threat Defense 会充当网关，并使用匿名 webvpn 会话在用户和 IdP 之间建立通信。

- **请求 IdP 在登陆重新进行身份验证**-选择此选项以在每次登录时对用户进行身份验证，即使之前的 IdP 会话有效。

- **允许覆盖**-选中此复选框以允许对此单点登录服务器对象进行覆盖。

步骤 3 点击**保存**。

相关主题

配置远程访问 VPN 的 AAA 设置，第 1555 页

访问列表

访问列表对象（也称为访问控制列表[ACL]），选择服务将应用到的流量。您可在配置特定功能（例如路由映射，对 Firewall Threat Defense 设备）时使用这些对象。对于识别为 ACL 所允许的流量，系统会提供服务，而“阻止”流量则会从服务中排除。从服务中排除流量未必意味着完全丢弃该流量。

您可以配置以下类型的 ACL：

- 扩展 - 根据源地址/端口和目标地址/端口识别流量。支持 IPv4 和 IPv6 地址（可以在给定规则中混用）。
- 标准 - 仅根据目标地址识别流量。仅支持 IPv4。

ACL 由一个或多个访问控制条目 (ACE) 或规则组成。ACE 的顺序非常重要。当评估 ACL 以确定数据包是否与“允许的”ACE 匹配时，该数据包会按照条目的列出顺序针对每个 ACE 进行测试。找到匹配项后，不再检查更多 ACE。例如，如果要“允许”10.100.10.1，但是“阻止”10.100.10.0/24 的其余地址，则允许条目必须在阻止条目之前。一般来说，将更具体的规则置于 ACL 的顶部。

与“允许”条目不匹配的数据包被视为受阻止。

以下主题介绍如何配置 ACL 对象。

配置扩展 ACL 对象

当要根据源和目标地址、协议和端口、应用组匹配流量时或者如果流量为IPv6，可使用扩展ACL对象。

过程

步骤 1 选择 **对象** > **访问列表** > **扩展**，然后从目录中选择 。

步骤 2 执行以下操作之一：

- 点击**添加扩展访问列表 (Add Extended Access List)** 以创建新的 ACL。
- 点击 **编辑** (✎) 以编辑现有对象。

步骤 3 在“新建扩展 ACL 访问列表对象”(New Extended Access List Object) 对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：

- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑** (✎) 以编辑现有条目。

b) 选择**操作 (Action)**，是允许（匹配）还是阻止（不匹配）流量条件。

注释
日志记录 (Logging)、**日志级别 (Log Level)** 以及**日志间隔 (Log Interval)** 选项仅用于访问规则（附加到接口或全局应用的 ACL）。由于 ACL 对象不用于访问规则，请将这些值保留其默认值。

c) 使用以下任一方法在**网络 (Network)** 选项卡上配置源和目标地址：

- 从“可用”(Available) 列表中选择所需的网络对象或组，然后点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。您可以通过点击列表上方的 + 按钮创建新对象。您可以混合使用 IPv4 和 IPv6 地址。
- 在源或目标列表下面的编辑框中输入地址并点击**添加 (Add)**。您可以指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）或子网（10.100.10.0/24 或 10.100.10.0 255.255.255.0 格式，或 2001:DB8:0:CD30::/60 这种 IPv6 格式）。

d) 点击**端口 (Port)** 选项卡并使用以下任一方法配置服务。

- 从可用列表中选择所需的端口对象，然后点击**添加到源 (Add to Source)** 或**添加到目标 (Add to Destination)**。您可以通过点击列表上方的 + 按钮创建新对象。对象可以指定 TCP/UDP 端口、ICMP/ICMPv6 消息类型或其他协议（包括“任意”[any]）。但是，通常留空的源端口只接受 TCP/UDP。您无法选择端口组。

  对于 TCP/UDP，请注意，如果同时指定了源和目标字段，则必须在两者中使用相同的协议。例如，您不能指定 UDP 源端口和 TCP 目标端口。
- 在源或目标列表下面的编辑框中输入或选择端口或协议并点击**添加 (Add)**。

注释
要获取适用于所有 IP 流量的条目，请选择指定“所有”协议的目标端口对象。

e) 点击**应用 (Application)** 选项卡，然后选择要为直接互联网访问策略分组的应用。

重要事项
- 不能为集群设备配置应用。因此，此选项卡不适用于集群设备。
- 仅在策略型路由选择中使用带有应用的扩展 ACL。请勿在其他策略中使用它，因为其行为未知且不受支持。确保为策略型路由选择迁移领域/ISE 配置，该路由选择在扩展 ACL 中使用用户身份和 SGT。

注释
- **可用应用** 列表显示一组固定的预定义应用。此列表是访问控制策略上可用的应用的子集，因为只有第一个数据包（FQDN 终端解析为 IP 地址和端口）可以检测到这些应用。应用定义通过 VDB 更新进行更新，并在后续部署期间推送到 Firewall Threat Defense 。
- 不支持用户定义的自定义应用或应用组。
- 目前， 防火墙管理中心 既不支持用户定义的自定义应用或应用组，也不允许您修改预定义的应用列表。
- 您可以使用应用过滤器下提供的**应用过滤器 (Application Filters)** 来优化此列表。

f) 点击**用户 (Users)** 选项卡，然后选择要为策略型路由 (PBR) 分类的用户、用户组或两者。

重要事项
仅对策略型路由中的用户使用用户、用户组或两者扩展ACL。请勿在其他策略中使用它，因为其行为未知且不受支持。

注释
- **可用领域 (Available Realms)** 列表会显示已配置的 Active Directory/LDAP 领域。有关创建和管理领域的信息，请分别参阅创建 LDAP 领域或 Active Directory 领域和领域目录，第 2019 页和管理领域，第 2048 页。

  注释
  不支持本地领域和 Azure AD 领域。

- **可用用户 (Available Users)** 列表会显示所选 AD/LDAP 领域的已下载用户和用户组。要下载用户、用户组或两者，请导航至**集成 (Integrations)** > **其他集成 (Other Integrations)** > **领域 (Realms)**，然后对相关的 Active Directory/LDAP 领域点击**下载 (Download)**。

  注释
  威胁防御最多可支持 512 个用户组和 64000 个用户 IP 映射。

- 在用户登录或注销和组成员身份更改期间，用户到 IP 的映射和用户组成员身份信息将更新并从 防火墙管理中心 推送到 Firewall Threat Defense 。

g) 点击**安全组标记 (Security Group Tag)**选项卡，然后选择要为直接互联网访问策略分类的源 SGT 标记。

重要事项
仅对策略型路由中的 SGT 使用扩展 ACL。请勿在其他策略中使用它，因为其行为未知且不受支持。

注释
- **可用安全组标记 (Available Security Group Tags)** 列表会显示已配置的安全组标记。您可以选择使用 ISE SGT 或创建自定义 SGT。
- 要使用 ISE SGT，请确保通过已订用的**会话目录主题** 和 SXP 主题将 ISE 与 防火墙管理中心 集成。有关 ISE 集成的更多信息，请参阅配置思科身份服务引擎 (Cisco ISE)身份源的方法，第 2092 页。

  注释
  支持的 ISE 版本包括 3.2、3、1、3.0 和 2.7 修补程序 2+。

- 有关创建自定义 SGT 的信息，请参阅创建安全组标记对象，第 2649 页。

h) 选择所需的应用，然后点击**添加到规则 (Add to Rule)**。

注释
- 请勿在扩展 ACL 对象中配置目标网络和应用。

- 每个访问控制条目中的所选应用（Nertwork 服务对象）组成一个网络服务组 (NSG)，此组部署在 Firewall Threat Defense上。NSG 用于直接互联网访问，根据与所选应用组的匹配对流量进行分类。

i) 点击**添加 (Add)** 以将条目添加到对象。
j) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ，第 2618 页。

步骤 5 点击**保存**。

配置服务访问对象

服务访问对象定义了流量访问 Firewall Threat Defense 设备上的远程访问 VPN 等服务必须满足的条件。此对象定义的条件是指多个按顺序执行的规则。每个服务访问规则都有一个“允许”或“拒绝”操作以及一组匹配标准，如国家、洲或用户定义的地理位置对象。这些规则管理基于不同地理位置的访问，确保只有来自批准区域的流量才能访问指定的服务。如果流量与任何规则都不匹配，则实施默认操作。

开始之前

- 配置地理位置对象。有关详细信息，请参阅地理定位 ，第 2655 页。
- 配置远程访问 VPN 策略。有关详细信息，请参阅创建新的远程访问 VPN 策略 ，第 1542 页。

过程

步骤 1 选择**对象** > **访问列表** > **服务访问**。

步骤 2 点击**添加服务访问对象 (Add Service Access Object)** 以创建一个新对象。

步骤 3 在**添加服务访问对象 (Add Service Access Object)** 对话框中，配置以下参数：

a) 在**名称 (Name)**字段中，输入对象的名称。
b) 点击**添加规则 (Add Rule)**，为此对象创建服务访问规则。在**添加服务访问规则 (Add Service Access Rule)** 对话框中，配置以下参数：

1. 从下拉列表中选择**允许 (Allow)** 或**拒绝 (Deny)** 操作。
2. 从**可用国家/地区 (Available Countries)** 中，选择国家/地区、大洲或用户定义的地理位置对象，然后将其移至**所选地理位置 (Selected Geolocation)** 列表。
3. 点击**添加 (Add)**。

创建服务访问规则后，会为规则分配一个序列号。此数字决定规则的执行顺序。您无法对这些规则重新排序。

步骤 4 从**默认操作 (Default Action)** 下拉列表中，选择**允许所有国家/地区 (Allow All Countries)** 或**拒绝所有国家/地区 (Deny All Countries)**。

步骤 5 （可选）选中**允许覆盖 (Allow Overrides)** 复选框，然后点击 **+** 为设备的服务访问对象配置覆盖。

注释
为设备或域定义覆盖后，系统在设备或域上配置该对象时，就会使用覆盖值而不是原始对象中定义的值。

步骤 6 （可选）在**添加服务访问覆盖 (Add Service Access Override)** 对话框中，配置以下参数：

a) 从**目标设备和域 (Target Devices and Domains)** 下拉列表中，选择覆盖所需的设备或域。
b) 验证是否需要现有规则。否则，请将其删除。
c) 点击**添加规则 (Add Rule)**，为此对象覆盖创建服务访问规则。
   1. 从下拉列表中选择**允许 (Allow)** 或**拒绝 (Deny)** 操作。
   2. 从**可用国家/地区 (Available Countries)** 中，选择国家/地区、大洲或用户定义的地理位置对象，然后将其移至**所选地理位置 (Selected Geolocation)** 列表。
   3. 点击**添加 (Add)**。
d) 从**默认操作 (Default Action)** 下拉列表中，选择**允许所有国家/地区 (Allow All Countries)** 或**拒绝所有国家/地区 (Deny All Countries)**。
e) 点击**添加 (Add)**。

步骤 7 点击**保存**。

下一步做什么

在远程访问 VPN 策略中配置服务访问对象。有关详细信息，请参阅配置远程访问 VPN 的访问接口，第 1571 页。

配置标准 ACL 对象

当要仅根据目标 IPv4 地址匹配流量时，请使用标准 ACL 对象。否则，请使用扩展 ACL。

过程

步骤 1 从目录中选择 **对象** > **访问列表** > **标准**。

步骤 2 执行以下操作之一：

- 点击 **添加标准访问列表** 以创建新对象。

- 点击 **编辑** (✎) 以编辑现有对象。

步骤 3 在“新建标准ACL 访问列表对象”对话框中，输入对象的名称（不允许使用空格），并配置访问控制条目：

a) 执行以下操作之一：

- 点击**添加 (Add)** 以创建新条目。
- 点击 **编辑** (✎) 以编辑现有条目。

b) 对于每个访问控制条目，请配置以下属性：

- **操作 (Action)** - 是允许（匹配）还是阻止（不匹配）流量标准。
- **网络 (Network)** - 添加用于识别流量目标的 IPv4 网络对象或组。

c) 点击**添加 (Add)** 以将条目添加到对象。

d) 如有必要，请点击并拖动条目，以按照规则顺序将其上移或下移到所需位置。

重复该过程以创建或编辑对象中的其他条目。

步骤 4 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 5 点击**保存**。

地址池

您可以为 IPv4 和 IPv6 配置 IP 地址池，该地址池可用于集群的诊断接口，或 用于 VPN 远程访问配置文件。 对于单个接口模式下的集群，还可以配置 MAC 地址池。

过程

步骤 1 选择**对象** > **地址池** 。

步骤 2 点击 **IPv4 池 (IPv4 Pools)**，然后点击**添加 IPv4 池 (Add IPv4 Pools)** 并配置以下字段：

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IP 地址** - 输入池中可用地址的范围。在开始地址和结束地址之间使用虚线十进制符号和破折号，例如：10.10.147.100-10.10.147.177。
- **掩码** - 标识此 IP 地址池所属的子网。
- **允许覆盖** - 选中此复选框可启用对象覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 2617 页。

步骤 3 点击**保存**。

步骤 4 点击 **IPv6 池 (IPv6 Pools)**，然后点击**添加 IPv6 池 (Add IPv6 Pools)** 并配置以下字段。

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **IPv6 地址** - 输入配置的池中可用的第一个 IP 地址和前缀长度（以位为单位）。例如：2001:DB8::1/64。
- **地址数量** - 标识地址池中从开始 IP 地址开始的 IPv6 地址的数量。
- **允许覆盖** - 选中此复选框可启用覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 2617 页。

步骤 5 点击**保存**。

步骤 6 点击 **MAC 地址池 (MAC Address Pool)**，然后点击**添加 MAC 地址池 (Add MAC Address Pool)** 并配置以下字段。

对于单个接口模式下的集群，可以为接口配置 MAC 地址池。为接口手动配置 MAC 地址并不常见，但如果您有特殊需求，则此池用于为每个接口分配唯一的 MAC 地址。请参阅配置 MAC 地址，第 820 页。

- **名称** - 输入地址池的名称。最多可包含 64 个字符
- **说明** - 为该池添加可选说明。
- **MAC 地址范围 (MAC Address Range)** - 输入池中可用的 MAC 地址的范围。在开始地址和结束地址之间使用短划线，例如：000C.F142.4CD1-000C.F142.4CD7。
- **允许覆盖** - 选中此复选框可启用覆盖。点击展开箭头可显示**覆盖**表。您可以通过点击**添加**来添加新的覆盖。有关详细信息，请参阅对象覆盖，第 2617 页。

应用过滤器

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以在对象管理器中，以系统提供的过滤器的组合为基础或以应用的自定义组合为基础，创建并管理可重复使用的用户定义的应用过滤器。

您可以在允许应用匹配的各种策略（例如访问控制、QoS、智能应用绕行和解密）中选择自定义应用过滤器。

- 要创建过滤器，请使用系统提供的过滤器查找应用，选择这些应用，然后点击**添加到规则**。
- 要从过滤器中删除应用，请点击应用旁边的删除图标。
- 点击应用旁边的信息图标可查看应用的相关信息。

有关应用特征的详细信息，请参阅应用规则条件，第 1420 页。

AS 路径

AS 路径是用于设置 BGP 的必需属性。它是 AS 编号序列，通过其可以访问网络。AS-PATH 是形成供数据包传播的定向路由的源和目标路由器之间的中间 AS 编号序列。相邻自治系统 (ASes) 使用 BGP 交换和更新有关如何到达不同的 AS 前缀的消息。在每个路由器制定有关目标的最佳路由的新本地决策后，它会将该路由或路径信息以及随附的距离指标和路径属性发送到其每个对等体。由于此信息通过网络传播，因此路径沿线的每个路由器会将其唯一 AS 编号预置到 BGP 消息中的 ASes 列表。此列表是路由的AS-PATH。AS-PATH 以及 AS 前缀通过网络为单向传输路由提供特定处理。使用“配置 AS 路径”(Configure AS Path) 页面创建、复制和编辑自治系统 (AS) 路径策略对象。您可以创建 AS 路径对象以在配置路由映射、策略映射、BGP 邻居过滤时使用。AS 路径过滤器使您能够通过使用正则表达式来过滤路由更新消息。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 选择 **对象** > **AS 路径**，然后从目录中选择 。

步骤 2 点击**添加 AS 路径 (Add AS Path)**。

步骤 3 在**名称 (Name)** 字段中输入 AS 路径对象的名称。有效值介于 1 与 500 之间。

步骤 4 点击**新建 AS 路径对象 (New AS Path Object)** 窗口上的**添加 (Add)**。

a) 从**操作 (Action)** 下拉列表中选择“允许”(Allow) 或“阻止”(Block) 选项以指示重新分发访问。

b) 在**正则表达式 (Regular Expression)** 字段中指定用于定义 AS 路径过滤器的正则表达式。

c) 点击**添加 (Add)**。

步骤 5 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 6 点击**保存**。

BFD 模板

BFD 模板指定一组 BFD 间隔值。BFD 模板中配置的 BFD 间隔值并不是特定于单个接口。此外，还可以为单跳和多跳会话配置身份验证。默认情况下，Echo 模式为禁用状态。您可以仅在单跳上启用回应。

过程

步骤 1 选择**对象** > **BFD 模板**。

步骤 2 点击**添加 BFD 模板 (Add BFD Template)** 或**编辑 (Edit)**。

注释
如果您正在编辑模板，则无法修改其名称和类型。

步骤 3 在 **Template** 选项卡上，配置以下选项：

- **Template Name** - 此 BFD 模板的名称。必须分配一个名称，才能配置模板中的其余参数。模板名称不能包含空格，并且不能仅包含数字。
- **类型 (Type)** - 点击**单跳 (Single-Hop)** 或**多跳 (Multi-Hop)** 单选按钮。
- **Enable Echo** -（可选）为单跳模板启用回应。

如果未协商回应功能，BFD控制数据包将以高速率发送以符合检测时间。如果已协商回应功能，BFD控制数据包将以较慢的协商速率发送，而自定向的回应数据包将以高速率发送。如果可能，我们建议您使用回应模式。

步骤 4 在**间隔**选项卡上，配置以下选项：

a) 从**间隔类型 (Interval Type)** 下拉列表中选择**微秒 (Microseconds)** 或**毫秒 (Milliseconds)**。
b) 在**倍数 (Multiplier)** 字段中，输入用于计算抑制时间的值。此值表示在BFD 声明对等体不可用并通知第 3 层 BFD 对等体相关故障之前必须错过来自该 BFD 对等体的连续 BFD 控制数据包数。范围为 3 到 50。默认值为 3。
c) 在**最小传输 (Minimum Transmit)** 字段中，输入最小传输间隔功能。范围介于 50 到 999 毫秒或 50000 到 999000 毫秒之间。
d) 在**最小接收 (Minimum Receive)** 字段中，输入最小接收间隔功能。范围介于 50 到 999 毫秒或 50000 到 999000 毫秒之间。

步骤 5 在 **Authentication** 选项卡上，配置以下选项：

- **身份验证类型 (Authentication Type)** - 从下拉列表中选择 **NONE**、**md5**、**meticulous-sha-1**、**meticulous-md5** 或 **sha-1**。
- **加密密码 (Encrypted Password)** -（可选）启用身份验证密码加密。
- **密码 (Password)** - 必须使用进行身份验证的路由协议在数据包中发送和接收的身份验证密码。有效值是包含 1 到 29 个大小写字母数字字符的字符串，但第一个字符不能为数字或数字后接空格。例如，“1password”或“0 password”无效。
- **Key ID** - 匹配密钥值的共享密钥 ID。范围为 0 到 255。

步骤 6 点击**确定**。

步骤 7 点击 **Apply** 以保存 BFD 模板配置。

密码套件列表

密码套件列表是由多个密码套件组成的对象。每个预定义密码套件值代表用于协商 SSL 或 TLS 加密会话的一个密码套件。您可以在 SSL 规则中使用密码套件和密码套件列表根据协商 SSL 会话的客户端和服务器是否使用该加密套件来控制加密流量。如果将密码套件列表添加到 SSL 规则，使用该列表中的任何密码套件协商的 SSL 会话都匹配该规则。

注释 虽然密码套件和密码套件列表在 Web 界面中可使用的位置相同，但不能添加、修改或删除密码套件。

创建密码套件列表

过程

步骤 1 从对象类型列表中选择 URL。**对象** > **密码套件列表**

步骤 2 点击 **Add Cipher Suites**。

步骤 3 输入 **Name**。

步骤 4 从**可用密码 (Available Ciphers)** 列表中选择一个或多个密码套件。

步骤 5 点击**添加 (Add)**。

步骤 6 或者，点击**所选密码 (Selected Ciphers)** 列表中要删除的任何密码套件旁边的 **删除** ()。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

社区列表

社区是可选的过渡BGP属性。社区是指一组共享某个通用属性的目标。它用于路由标记。BGP社区属性是可分配给特定前缀并通告到其他邻居的数值。社区可用于标记共享通用属性的一组前缀。上游提供商可以使用这些标记应用通用路由策略，例如过滤或分配特定本地首选项或者修改其他属性。使用“配置社区列表”页面创建、复制和编辑社区列表策略对象。您可以创建社区列表对象以在配置路由映射或策略映射时使用。您可以使用社区列表创建要在路由映射的匹配子句中使用的社区组。社区列表是匹配语句的有序列表。目标根据规则进行匹配，直至找到匹配项为止。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 选择 **对象** > **社区列表**，然后从目录中选择 。

步骤 2 点击**添加社区列表 (Add Community List)**。

步骤 3 在**名称**字段中，指定社区列表对象的名称。

步骤 4 点击**新建社区列表对象 (New Community List Object)** 窗口上的**添加 (Add)**。

步骤 5 选择**标准**单选按钮以指示社区规则类型。

标准社区列表用于指定已知的社区和社区编号。

注释
不能在同一社区列表对象中同时具有使用“标准”和使用“扩展”社区规则类型的条目。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。
b) 在**社区**字段中，指定社区号。有效值可以从 1 到 4294967295 或者从 0:1 到 65534:65535。
c) 选择相应的**路由类型**。

- **互联网** - 选择指定互联网已知社区。系统向所有对等体（内部和外部）通告具有此社区的路由。
- **无通告** - 选择指定不通告已知社区。系统不向任何对等体（内部或外部）通告具有此社区的路由。
- **无导出** - 选择指定不导出已知社区。系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。

步骤 6 选择**扩展**单选按钮以指示社区规则类型。

扩展的社区列表通过正则表达式用于过滤社区。正则表达式用于指定要与社区属性匹配的模式。

a) 从**操作**下拉列表中选择“允许”或“阻止”选项以指示重新分发访问。
b) 在**表达式**字段中指定正则表达式。

步骤 7 点击**添加 (Add)**。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖 ， 第 2618 页。

步骤 9 点击**保存**。

扩展社区

扩展社区是一组更大的共享某个通用属性的目的。BGP 扩展社区列表具有可用于标记共享通用属性的一组前缀的属性。这些标记用在路由映射的 match 子句中，用于过滤路由以实现虚拟路由器之间的路由泄漏。您还可以使用扩展社区列表定义策略列表对象以进行过滤。扩展社区列表是匹配语句的有序列表。路由会根据规则进行匹配，直到找到具有指定路由目标（标准）或正则表达式（扩展）的匹配项。使用“扩展社区”页面创建和编辑扩展社区列表策略对象。

注释 扩展社区列表仅适用于配置路由的导入或导出。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 选择**对象** > **社区列表** > **扩展社区**。

步骤 2 点击**添加扩展社区列表 (Add Extended Community List)**。

步骤 3 在**名称**字段中，指定扩展社区列表对象的名称。名称的长度不能超过 80 个字符。

步骤 4 选择扩展社区规则类型：

- 点击**标准 (Standard)** 单选按钮，指定一个或多个路由目标。
- 点击**扩展 (Expanded)**单选按钮，指定正则表达式。

注释
在同一个扩展社区列表对象中不能同时具有使用“标准”和“扩展”扩展社区规则类型的条目。

步骤 5 点击**添加 (Add)**。

步骤 6 如果已选择**标准**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配路由目标的路由，请选择**允许**； 如果要拒绝具有在此处指定的匹配路由目标的路由，请选择**阻止**。

c) 在**路由目标**字段中，指定路由目标。

- 您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如 *1:2,1:4,1:6*。
- 有效值可以是 1:1 到 65534:65535。
- 一个条目中最多可以包含 8 个路由目标。
- 不能跨多个条目设置多余的路由目标。例如，假设要使用 *1:200,100:100,1:300* 路由目标配置 *seq1*，并使用 *1:300,100:100,1:200* 路由目标配置 *seq2*。这会导致设置多余的路由目标，且无法部署。

步骤 7 如果已选择**扩展**作为扩展社区规则类型，请指定以下内容：

a) 在**序列号**字段中，输入希望规则执行的顺序。

序列号在列表中必须唯一。

b) 在**操作**下拉列表中，如果要允许具有此处指定的匹配正则表达式的路由，请选择**允许**； 如果要拒绝具有此处指定的匹配正则表达式的路由，请选择**阻止**。

c) 在**表达式**字段中指定正则表达式。

- 可以在单个条目中添加单个路由目标或一组以空格分隔的路由目标。例如，*^((16)|(18)):(.)$*。
- 最多可以向一个条目中添加 16 个正则表达式。
- 不能跨多个条目设置多余的正则表达式。例如，假设要使用 *^((16) | (18)):(.)$ ^4_[0-9]*$* 路由目标配置 *seq1*，并使用 *^4_[0-9]*$ ^((16) | (18)):(.)$* 路由目标配置 *seq2*。这会导致设置多余的正则表达式，且无法部署。

有关 BGP 正则表达式的详细信息，请参阅此处。

步骤 8 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 9 点击**保存 (Save)**。

可以在路由映射对象或策略列表对象的 match 子句中引用扩展社区列表：

- 在路由映射对象中，扩展社区列表的名称显示在**添加路由映射条目** > **Match 子句** > **BGP** > **社区列表** > **添加扩展社区列表**对话框中。有关在路由映射中配置 BGP 设置的详细信息，请参阅路由映射，第 2685 页。
- 在策略列表对象中，扩展社区列表的名称显示在**添加策略列表** > **社区规则** > **添加扩展社区列表**对话框中。有关在策略列表中配置 BGP 设置的详细信息，请参阅策略列表，第 2680 页。

DHCP IPv6 池

对于结合前缀授权功能 (启用 IPv6 前缀授权客户端，第 804 页) 使用无状态地址自动配置 (SLAAC) 的客户端，可以通过定义 DHCP IPv6 池并将其分配给 DHCPv6 服务器来配置 Firewall Threat Defense，以便在它们向 Firewall Threat Defense 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 Firewall Threat Defense 的前缀。

要添加池，请参阅 创建 DHCP IPv6 池，第 960 页。

可分辨名称

每个可分辨名称对象代表的公共密钥的使用者或颁发者的可分辨名称。您可在 TLS/SSL 规则中使用可分辨名称对象和对象组根据协商 TLS/SSL 会话的客户端和服务器是否使用将该可分辨名称作为使用者或颁发者的服务器证书来控制加密流量。

（可分辨名称组是现有可分辨名称对象的命名集合。）

可分辨名称可以包含国家/地区代码、公用名、组织和组织单位，但通常只会包含一个公用名。例如，`https://www.cisco.com` 的证书中的公用名为 `cisco.com`。（但情况并非总是这么简单；可分辨

名称 (DN) 规则条件，第 1926 页显示了如何查找常用名称。）证书可以包含多个可在规则条件中用作 DN 的使用者可选名称 (SAN)。有关 SAN 的详细信息，请参阅 RFC 5280 第 4.2.1.6 节。

引用通用名称的可分辨名称对象的格式为 `CN=name`。如果添加不带 `CN=` 的 DN 规则条件，系统会在名称前面加上 `CN=`，再保存对象。

如 可分辨名称 (DN) 规则条件，第 1926 页 中进一步所述，系统尽可能使用服务器名称指示 (SNI) (Server Name Indication [SNI]) 来匹配 TLS/SSL 规则中的 DN。

还可以添加带有下表中列出的每个属性（用逗号隔开）的一个可分辨名称。

表 *159:* 可分辨名称属性

属性	说明	允许的值
C	国家/地区代码	两个字母字符
CN	公用名称	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
O	组织	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格
OU	组织单位	最多 64 个字母数字、斜杠 (/)、连字符 (-)、引号 (")、星号 (*) 字符或空格

有关 DN 规则条件的重要说明

- 系统首次检测新服务器的加密会话时，DN 数据不可用于 ClientHello 处理，因为这可能会导致首个会话不解密。

  如果服务器请求 TLS 1.3，则 TLS 服务器身份发现的设置可以确保在做出 解密策略 决策之前知道服务器证书，从而提供帮助。有关详细信息，请参阅TLS 服务器身份发现，第 2459 页。

- 如果还选择了**解密 - 已知密钥 (Decrypt - Known Key)** 操作，则无法配置可分辨名称条件。由于该操作要求选择服务器证书来解密流量，因此证书已经与流量相匹配。

通配符示例

可以定义一个或多个星号 (*) 作为属性中的通配符。在通用名称属性中，您可以为每个域名标签定义一个或多个星号。通配符仅在该标签中匹配，但您可以使用通配符定义多个标签。请参阅下表中的示例。

表 *160:* 公用名属性通配符示例

属性	匹配	不匹配
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com

属性	匹配	不匹配
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com



注释 DN 对象 `CN=amp.cisco.com` 与 `CN=auth.amp.cisco.com` 不匹配，因此我们建议要在这些情况下使用通配符。

有关详细信息和示例，请参阅可分辨名称 (DN) 规则条件，第 1926 页。

相关主题

可分辨名称 (DN) 规则条件，第 1926 页

创建可分辨名称对象

过程

步骤 1 选择**对象**。

步骤 2 展开**可分辨名称 (Distinguished Name)** 节点，然后选择**单个对象 (Individual Objects)**。

步骤 3 点击 **Add Distinguished Name**。

步骤 4 输入 **Name**。

步骤 5 在 **DN** 字段中，输入可分辨名称或公用名的值。您有以下选择：

- 如果添加可分辨名称，则可包括可分辨名称，第 2637 页中列出的每个属性（以逗号隔开）。
- 如果添加公用名，则可包括多个标签和通配符。

步骤 6 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

DNS 服务器组

域名系统 (DNS) 服务器会将完全限定域名 (FQDN)（例如 www.example.com）解析为 IP 地址。

创建 DNS 服务器组对象

过程

步骤 1 从对象类型列表中选择网络 (Network)。**对象** > **DNS 服务器组**

步骤 2 点击**添加 DNS 服务器组**。

步骤 3 输入 **Name**。

步骤 4 或者，输入用于附加到非完全限定主机名的**默认域**。

此设置仅用于默认服务器组。

步骤 5 默认的**超时**和**重试次数**值已预填。如有必要，可更改这些值。

- 重试次数 - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。
- 超时 (Timeout) - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。

步骤 6 输入将属于此组的 **DNS 服务器**，可为 IPv4 或 IPv6 格式的逗号分隔条目。

一个组最多可包含 6 个 DNS 服务器。

步骤 7 点击**保存**。

下一步做什么

在 DNS 服务器组中配置的 DNS 服务器应当分配到 DNS 平台设置中的接口对象。有关详细信息，请参阅DNS，第 977 页。

加密可视性引擎例外列表

您可以创建加密可视性引擎 (EVE) 例外列表来绕过 EVE 的阻止操作，从而确保可信连接和服务的连续性。您可以将进程名称、源和目标 IP 地址/FQDN 以及动态对象等属性添加到异常规则中。例如，

您可能希望绕过受信任网络的EVE阻止判定。根据威胁置信度，绕过网络中的所有连接都免于执行EVE 阻止判定。

过程

步骤 1 选择**对象** > **EVE 例外列表**。

步骤 2 在**加密可视性引擎（EVE）例外列表**窗口中，点击 **+添加例外规则**，并添加所需属性。

a) 在**进程名称**选项卡下，输入 EVE 识别的进程名称，然后点击窗口右侧的 **+添加**。

可以将多个进程名称添加到同一例外规则。基于进程名称的 EVE 例外列表仅适用于 EVE 识别的进程名称，这些进程名称区分大小写和空格。

b) 在**网络对象 (Network Objects)** 选项卡下，执行以下操作之一：

- 在**选定源网络**或**选定目标网络**下，手动输入 IP 地址，然后点击 + 图标以将其添加到所选网络列表中。
- 要创建新的网络对象，请点击 **+创建网络对象**。
  1. 输入**名称**和可选的**说明**。
  2. 选择所需的网络类型 - **主机**、**范围**、**网络**或 **FQDN**。如果选择**主机**、**范围**或**网络**，请输入相关的 IP 地址。如果选择 **FQDN**，请输入完全限定域名 (**FQDN**)，并从**查找**下拉列表中选择所需选项。
  3. 如果要允许配置覆盖，请选中**允许覆盖**复选框。
  4. 点击**添加 (Add)**。

c) 在**动态属性**选项卡下，从**可用动态属性**列表中选择所需的动态属性，并使用 > 按钮将其添加到**选定目标动态属性**列表中。

有关创建动态对象或使用动态对象的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的首次创建动态对象或使用动态对象部分。

d) 要创建新的动态属性，请点击 **+创建动态属性**。

1. 输入**名称**和可选的**说明**。
2. 点击**添加 (Add)**。可以使用思科安全动态属性连接器 (CSDAC) 或管理中心 API 配置此对象。

e) （可选）在所有选项卡的**注释**字段中，可以输入将所需网络对象和动态属性添加到 EVE 例外规则的原因。

步骤 3 点击**保存**，然后部署访问控制策略。

注释 当连接匹配例外规则时，它会绕过EVE的阻止判定。您可以在**连接事件**或**统一事件**页面中查看EVE的操作。**原因 (Reason)** 列标题显示 **EVE 已豁免 (EVE Exempted)**，用于识别此类绕过 EVE 的流量。

外部属性

动态对象

动态对象 是指定使用 REST API 调用或使用 Dynamic Attributes Connector检索的一个或多个 IP 地址的对象，该对象能够从云源更新 IP 地址。这些动态对象可在访问控制 或 DNS 规则中使用，而无需将动态更改部署到对象。

注释 与大多数其他对象不同，动态对象不必部署到托管设备即可生效。只需将动态对象添加到访问控制规则的 **动态属性** 选项卡页面即可； Dynamic Attributes Connector推送后，对象值会尽快在托管设备上自动更新。

有以下几种动态对象：

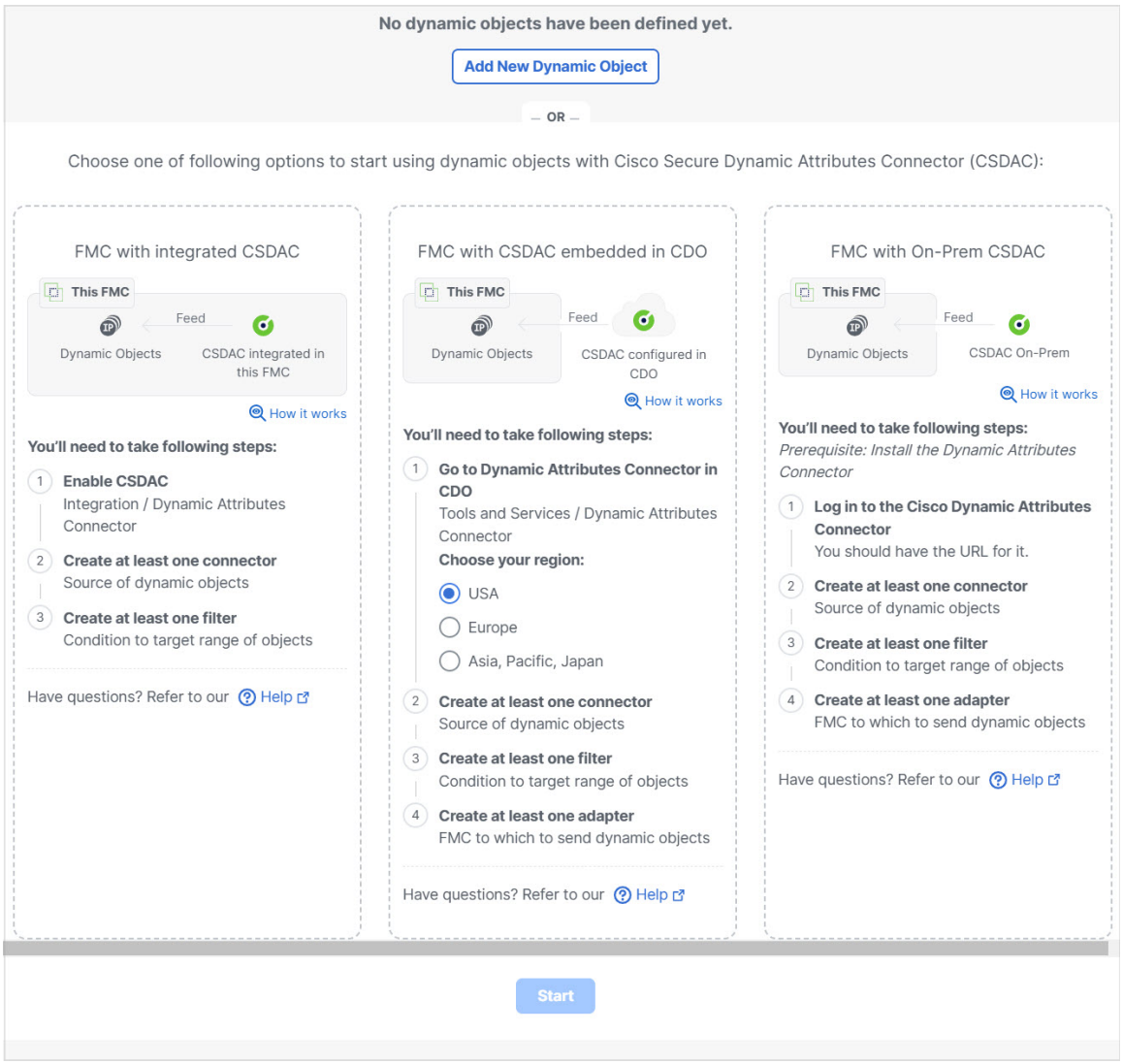
- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到 防火墙管理中心，并且还会定期更新。
- API 创建的动态对象：
  - 是 IP 地址，有或没有或无类域间路由 (CIDR)，可以在访问控制规则中使用，与网络对象很相似。
  - 不支持完全限定域名或地址范围。
  - 必须使用 API 进行更新。

有关动态对象的详细信息，请参阅 关于 API 创建的动态对象 ， 第 2647 页。

首次创建动态对象

如果尚未配置任何动态对象，则 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)** 如下所示的页面显示。

如果您已经创建了一些动态对象，请参阅 处理动态对象 ， 第 2647 页。



要使用此页面，请执行以下操作：

- 点击表示您计划如何部署 dynamic attributes connector的部分。
- 点击 **工作原理** 以查看图表并获取有关该类型部署的更多帮助。

  以下主题提供更多信息。

  - 使用嵌入式 Dynamic Attributes Connector创建动态对象 ，第 2644 页
  - 使用 Security Cloud Control创建动态对象 ，第 2645 页
  - 在本地创建动态对象 Dynamic Attributes Connector ，第 2646 页

- 点击 **开始** 打开相关应用，如下所示：

- 如果您点击了 **具有集成 CSDAC 的 FMC** 方法，则 **开始** 会将您带到可以启用和配置 Dynamic Attributes Connector的位置 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)** 。

  有关详细信息，请参阅启用 dynamic attributes connector ， 第 2116 页。

- 如果您点击了 **嵌入了 CSDAC 的 FMC** Security Cloud Control方法，则**开始**会启动 Security Cloud Control。

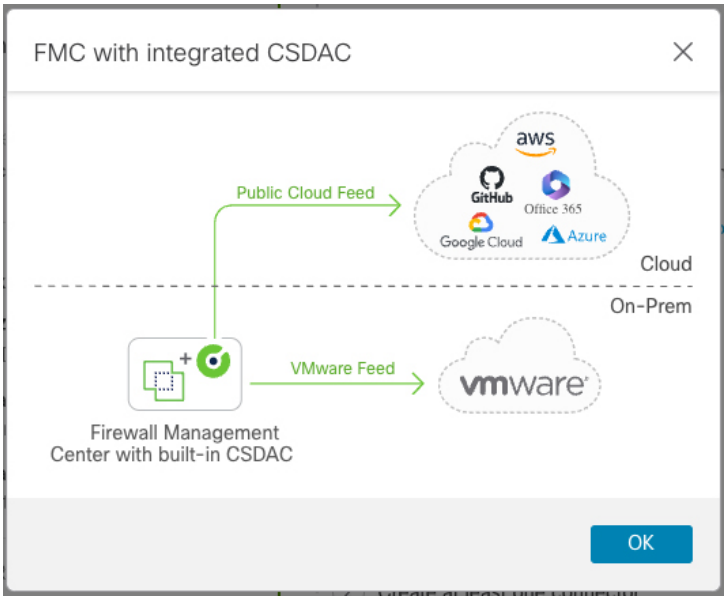
  有关更多信息，请参阅 使用 *Security Cloud Control*中的云交付防火墙管理中心管理防火墙威胁防御 。

- 如果您点击了 **使用本地 CSDAC 的 FMC**方法，则 **开始** 可让您下载 Dynamic Attributes Connector，如果您尚未这样做。

  有关详细信息，请参阅《*Cisco Secure Dynamic Attributes Connector* 配置指南》。

使用嵌入式 Dynamic Attributes Connector创建动态对象

如果您指定使用提供的 Secure Firewall Management Center配置 Dynamic Attributes Connector ， 系统将显示以下页面。 Secure Firewall Management Center 已经集成了 Dynamic Attributes Connector (**集成** > **动态属性连接器**)。



要使用此部署类型：

1. 启用 Dynamic Attributes Connector ， 如 启用 dynamic attributes connector ， 第 2116 页中所述。
2. 配置从云服务检索 IP 地址的连接器。

   有关详细信息，请参阅创建连接器 ， 第 2340 页。
3. 配置动态属性过滤器，用于确定要发送到管理中心的 IP 地址。

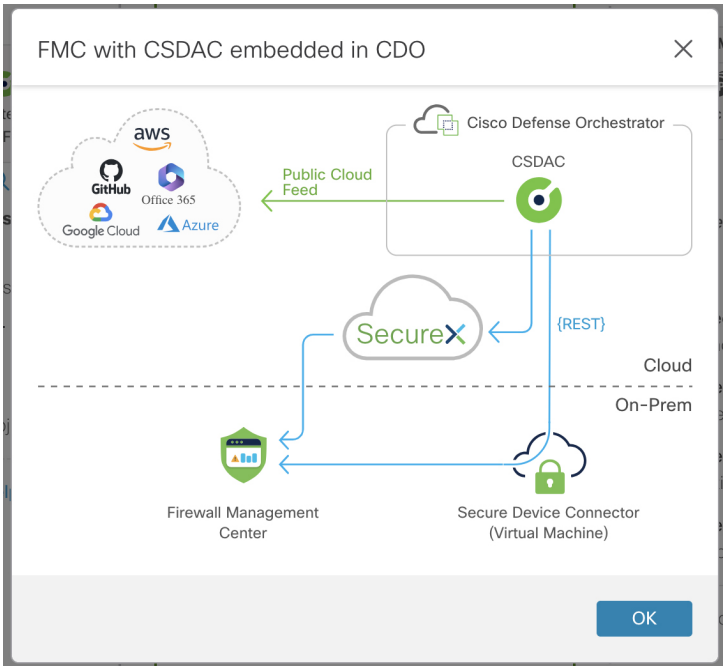
有关详细信息，请参阅创建动态属性过滤器，第 2164 页。

4. 查看 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**的动态对象。
5. 在访问控制规则中使用动态对象（**策略** > **安全策略** > **访问控制**，然后点击 **动态属性** 选项卡）。

   您也可以在 DNS 规则中使用这些对象。

使用 Security Cloud Control创建动态对象

如果您指定使用提供的 Security Cloud Control配置 Dynamic Attributes Connector，系统将显示以下页面。



上图包含有关本指南中未讨论的配置 Security Cloud Control 的详细信息。有关更多详细信息，请参阅 Secure Device Connector (SDC) 或 SecureX 和 Security Cloud Control。

要使用此部署类型：

1. 配置从云服务检索 IP 地址的连接器。

   有关详细信息，请参阅创建连接器，第 2340 页。

2. 配置动态属性过滤器，用于确定要发送到管理中心的 IP 地址。

   有关详细信息，请参阅创建动态属性过滤器，第 2164 页。

3. 配置适配器，将 IP 地址发送到 Secure Firewall Management Center 或 云交付的防火墙管理中心。

   有关详细信息，请参阅 思科安全云控制：用于 *Cisco Secure Firewall Threat Defense* 的云交付防火墙管理中心中有关创建适配器的部分。

4. 登录到您定义为适配器的 Secure Firewall Management Center 。

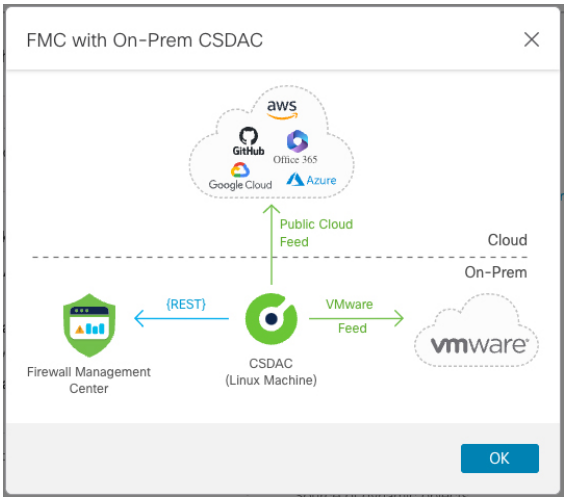
如果 Secure Firewall Management Center 由 Security Cloud Control 管理，请点击**云交付 FMC**。

5. 查看 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**的动态对象。
6. 在访问控制规则中使用动态对象（**策略** > **安全策略** > **访问控制**，然后点击 **动态属性** 选项卡）。

   您也可以在 DNS 规则中使用这些对象。

在本地创建动态对象 Dynamic Attributes Connector

如果您已指示将本地部署 Dynamic Attributes Connector 配置为将动态对象发送到 Secure Firewall Management Center 或 云交付的防火墙管理中心，则会显示以下页面。



要使用此部署类型：

1. 在支持的 Linux 虚拟机上安装 Dynamic Attributes Connector 。
2. 配置从云服务检索 IP 地址的连接器。

   有关详细信息，请参阅 *《Cisco Secure Dynamic Attributes Connector 配置指南》*中有关创建连接器的部分。
3. 配置适配器，将 IP 地址发送到 Secure Firewall Management Center 或 云交付的防火墙管理中心。

   有关详细信息，请参阅 *《Cisco Secure Dynamic Attributes Connector 配置指南》*中有关创建适配器的部分。
4. 配置动态属性过滤器，用于确定要发送到管理中心的 IP 地址。

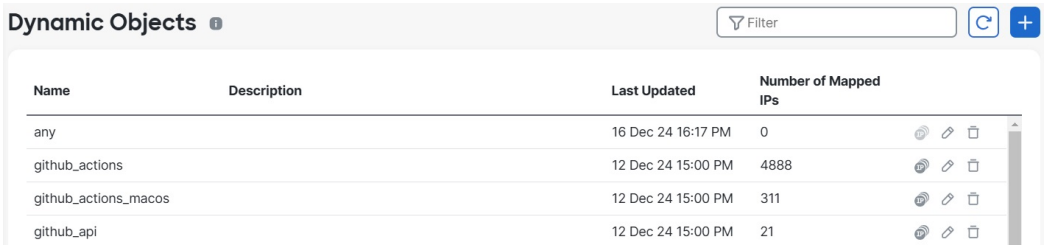
   有关详细信息，请参阅 *《Cisco Secure Dynamic Attributes Connector 配置指南》*中有关配置动态属性过滤器的部分。
5. 查看 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**的动态对象。
6. 在访问控制规则中使用动态对象（**策略** > **安全策略** > **访问控制**，然后点击 **动态属性** 选项卡）。

   您也可以在 DNS 规则中使用这些对象。

有关详细信息，请参阅《*Cisco Secure Dynamic Attributes Connector* 配置指南》。

处理动态对象

如果您已配置一些动态对象，则 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)** 处的可用页面将显示如下。

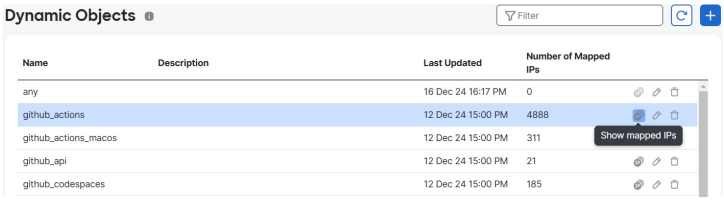


此页面显示有关每个动态对象的信息，并允许您查看或下载与该对象关联的 IP 地址。有关详细信息，请参阅动态对象映射，第 2647 页。

动态对象映射

如果使用 API 或使用 dynamic attributes connector配置动态对象，则连接器会定期向 防火墙管理中心 发送与动态属性过滤器匹配的 IP。

要查看或下载这些 IP 地址的当前列表，请点击 **显示映射 ID**，如下图所示。



IP 地址随时间动态添加，因此您应考虑定期执行此操作，尤其是在访问控制规则未按预期运行的情况下。

相关主题

- 关于 API 创建的动态对象，第 2647 页
- 关于 dynamic attributes connector，第 2325 页

关于 API 创建的动态对象

动态对象 是指定使用 REST API 调用或使用 Dynamic Attributes Connector检索的一个或多个 IP 地址的对象，该对象能够从云源更新 IP 地址。这些动态对象可在访问控制 或 DNS 规则中使用，而无需将动态更改部署到对象。

有关 dynamic attributes connector 的详细信息，请参阅《思科安全动态属性配置指南》（指南链接）。

动态对象和网络对象之间的差异如下：

- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到 防火墙管理中心，并且还会定期更新。
- API 创建的动态对象：
  - 是 IP 地址，有或没有或无类域间路由 (CIDR)，可以在访问控制规则中使用，与网络对象很相似。
  - 不支持完全限定域名或地址范围。
  - 必须使用 API 进行更新。

相关主题

添加或编辑 API 创建的动态对象 ，第 2648 页

添加或编辑 API 创建的动态对象

此过程讨论如何添加或编辑 动态对象， 动态对象是一组使用 API 的 IP 地址，可以在访问控制规则中使用或不使用无类域间路由 (*CIDR*)，就像网络对象一样。

注释 如果使用 Dynamic Attributes Connector ，则无需执行此过程，因为它会自动为您创建动态对象。

开始之前

有关使用对象服务 REST API 为 IP 对象填充地址的信息，请参阅 *Firepower* 管理中心 *REST API* 快速入门指南 。动态对象不需要部署。

过程

步骤 1 点击 **对象**。

步骤 2 点击**外部属性 (External Attributes)** > **动态对象 (Dynamic Objects)**。

步骤 3 点击**添加动态对象 (Add Dynamic Object)** 或 **编辑** ()。

步骤 4 输入对象的**名称**和可选的**说明**。

步骤 5 在**类型 (Type)** 列表中，点击 **IP**。

下一步做什么

如有必要，请使用 API 来更新动态对象。不需要部署。

安全组标记

安全组标记 (SGT) 对象指定单个 (SGT) 值。您可以使用规则中的 SGT 对象来控制具有**并非**由思科 ISE 分配的 SGT 属性的流量。您不能分组或覆盖 SGT 对象。

相关主题

从自定义 SGT 自动过渡到 ISE SGT
自定义 SGT 条件
ISE SGT 与自定义 SGT 规则条件

创建安全组标记对象

您只能在全局域中创建这些对象。要在经典设备上使用对象，您必须拥有控制许可证。对于智能许可设备，任何许可证均可。

开始之前

- 禁用 ISE/ISE-PIC 连接。如果使用 ISE/ISE-PIC 作为身份源，则不能创建自定义 SGT 对象。

  点击**集成** > **身份** > **身份源**，选择**无**，然后点击**保存**。

- 有关身份源的使用准则，请参阅ISE/ISE-PIC 准则和限制，第 2081 页。

过程

步骤 1 请点击 **对象**。
步骤 2 点击**外部属性 (External Attributes)** > **安全组标记 (Security Group Tag)**。
步骤 3 点击**添加安全组标记 (Add Security Group Tag)**。
步骤 4 输入 **Name**。
步骤 5 输入**说明 (Description)**（可选）。
步骤 6 在**标记 (Tag)** 字段中，输入单个 SGT。
步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

文件列表

如果使用恶意软件防护，而 AMP 云错误地识别某个文件的处置情况，则您可以将该文件添加到文件列表，以便将来能够更好地检测该文件。这些文件使用 SHA-256 散列值进行指定。每个文件列表最多可以包含 10000 个唯一的 SHA-256 值。

文件列表有两种预定义类别：

干净的列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了干净处置情况。

自定义检测列表

如果将某个文件添加到此列表，则系统视为 AMP 云为其分配了恶意软件处置情况。

由于您手动指定这些列表中包含的文件的阻止行为，系统不会在 AMP 云中查询这些文件的处置情况。您必须配置文件策略中的规则（通过**恶意软件云查找 [Malware Cloud Lookup]** 或**阻止恶意软件 [Block Malware]** 操作）和匹配的文件类型才能计算文件的 SHA 值。

⚠

注意 请**勿**在干净的列表中包含恶意软件。干净的列表会覆盖 AMP 云和自定义检测列表。

文件列表的源文件

可通过上传包含 SHA-256 值和描述的列表的逗号分隔值 (CSV) 源文件将多个 SHA-256 值添加到文件列表。防火墙管理中心验证内容并使用有效的 SHA-256 值填充文件列表。

源文件必须为具有 .csv 文件扩展名的简单文本文件。所有标题必须以井号 (#) 开头；标题将被视为注释，不会上传。每个条目都应包含一个 SHA-256 值，后跟说明并以 LF 或 CR+LF 换行字符结尾。系统将会忽略条目中的任何其他信息。

请注意以下提示：

- 从文件列表删除源文件也会从该文件列表删除所有相关的 SHA-256 散列值。
- 如果成功上传源文件导致文件列表包含超过 10000 个不同的 SHA-256 值，则不能将多个文件上传到该文件列表。
- 上传时，系统会截去描述中超过 256 个字符的字符，仅保留前 256 个字符。如果描述包括逗号，必须使用转义字符 (\,)。如果未包含描述，将会改为使用源文件名。
- 所有非重复的 SHA-256 值都将被添加到文件列表。如果文件列表包含 SHA-256 值，并且上传了包括该值的源文件，新上传的值不会修改现有 SHA-256 值。查看与 SHA-256 值相关的捕获的文件、文件事件或恶意软件事件时，所有威胁名称或描述都来源于单个 SHA-256 值。
- 系统不会在源文件中上传无效的 SHA-256 值。
- 如果多个上传的源文件包括相同 SHA-256 值的条目，系统将使用最新的值。

- 如果源文件包括相同 SHA-256 值的多个条目，系统将使用最后一个。
- 不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。
- 与源文件相关的条目数是指不同的 SHA-256 值的数量。如果从文件列表删除某个源文件，文件列表包含的 SHA-256 条目总数将会减少等于该源文件中有效条目的数量。

将单个 SHA-256 值添加到文件列表

您必须有此程序的 恶意软件防御 许可证。

可以提交文件的 SHA-256 值以将其添加到文件列表。不能添加重复的 SHA-256 值。

开始之前

- 在事件视图中右键点击某个文件或恶意软件事件，在情景菜单中选择**显示全文 (Show Full Text)**，然后复制完整的 SHA-256 值以粘贴到列表中。

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉列表中选择 `Enter SHA Value`。

步骤 5 在 **Description** 字段中输入源文件的描述。

步骤 6 在 **SHA-256** 字段中输入或粘贴文件的完整值。系统不支持匹配部分值。

步骤 7 点击**添加 (Add)**。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将单个文件上传到文件列表

您必须有此程序的 恶意软件防御 许可证。

如果要将文件副本添加到文件列表，则可将文件上传到Secure Firewall Management Center进行分析；系统会计算文件的SHA-256值并将文件添加到列表。系统不对用于SHA-256计算的文件大小强制实施任何限制。

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要添加文件的干净列表或自定义检测列表旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择**计算 SHA (Calculate SHA)**。

步骤 5 或者，在**说明 (Description)** 字段中输入文件的说明。如果不输入说明，在上传时文件名将被用作说明。

步骤 6 点击**浏览 (Browse)**，然后选择要上传的文件。

步骤 7 点击**计算并添加 SHA (Calculate and Add SHA)**。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

将源文件上传到文件列表

您必须有此程序的 恶意软件防御 许可证。

过程

步骤 1 选择**对象**。

步骤 2 点击 **File List**。

步骤 3 点击要从源文件向其添加值的文件列表旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 从**添加方式 (Add by)** 下拉菜单中，选择 `List of SHAs`。

步骤 5 或者，在**说明 (Description)** 字段中输入源文件的说明。如果不输入说明，系统将会使用文件名。

步骤 6 点击**浏览 (Browse)** 浏览到源文件，然后点击**上传并添加列表 (Upload and Add List)**。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

注释 在部署策略后，系统不再查询 AMP 云以查找列表中的文件。

编辑文件列表中的 SHA-256 值

您必须有此程序的 恶意软件防御 许可证。

可以编辑或删除文件列表中的各个 SHA-256 值。请注意，不能在对象管理器中直接编辑源文件。要进行更改，必须首先直接修改源文件，删除系统中的副本，然后上传修改后的源文件。

过程

步骤 1 选择**对象**。

步骤 2 点击 **File List**。

步骤 3 点击要修改文件的干净列表或自定义检测列表旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 您可以执行以下操作：

- 点击要更改的 SHA-256 值旁边的 **编辑** ()，并根据需要修改 **SHA-256** 或**说明 (Description)** 值。
- 点击要删除的 SHA-256 值旁边的 **删除** ()。

步骤 5 点击**保存**以更新列表中的文件条目。

步骤 6 点击**保存**以保存文件列表。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

注释 在部署配置更改后，系统不再查询 AMP 云以查找列表中的文件。

从文件列表下载源文件

您必须有此程序的 恶意软件防御 许可证。

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**文件列表 (File List)**。

步骤 3 点击要下载源文件的干净列表或自定义检测列表旁边的 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 点击要下载的源文件旁边的 **视图** ()。

步骤 5 点击**下载 SHA 列表 (Download SHA List)** 并按照提示保存源文件。

步骤 6 点击**关闭 (Close)**。

FlexConfig

可以使用 FlexConfig 策略中的 FlexConfig 策略对象为 Firewall Threat Defense设备上您不能使用 Secure Firewall Management Center另行配置的功能提供自定义配置。有关 FlexConfig 策略的更多信息，请参阅FlexConfig 策略概述， 第 1041 页。

可为 FlexConfig 配置以下类型的对象。

文本对象

文本对象定义了在 FlexConfig 对象中用作变量的自由形式的文本字符串。这些对象可以具有单个值，或是多个值的列表。

有几种预定义文本对象可以用于预定义 FlexConfig 对象。如果使用相关联的 FlexConfig 对象，则只需编辑文本对象的内容，即可自定义 FlexConfig 对象配置给定设备的方式。在编辑预定义对象时，为您配置的每台设备创建设备覆盖，而不是直接更改这些对象的默认值，通常是更好的选择。这有助于避免如果另一个用户希望将同一 FlexConfig 对象用于一组不同的设备可能导致的意外后果。

有关配置文本对象的信息，请参阅配置 FlexConfig 文本对象， 第 1067 页。

FlexConfig 对象

FlexConfig 对象包括设备配置命令、变量和脚本语言指令。在配置部署过程中，将处理这些指令，以创建一系列带有自定义参数的配置命令，用于配置目标设备上的特定功能。

这些指令要么是在系统配置常规 防火墙管理中心策略和设置中定义的功能之前（预置）进行配置，要么是在此之后（附加）进行配置。必须将任何取决于 Secure Firewall Management Center 配置的对象（例如网络对象）的 FlexConfig 附加到配置部署，否则在所需 FlexConfig 参考所需对象之前，不会配置这些对象。

有关配置 FlexConfig 对象的更多信息，请参阅配置 FlexConfig 对象，第 1063 页。

地理定位

配置的每个地理定位对象代表系统识别为受监控网络上流量的源或目标的一个或多个国家/地区或大洲。可在系统 Web 界面中的不同位置使用地理定位对象，包括访问控制策略、SSL 策略、远程访问 VPN 和事件搜索。例如，可编写阻止流向或来自某些国家/地区的流量的访问控制规则。

要确保使用最新信息来过滤网络流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

创建地理位置对象

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**地理位置 (Geolocation)**。

步骤 3 点击 **Add Geolocation**。

步骤 4 输入 **Name**。

步骤 5 选中要包括到地理定位对象中的国家/地区和大洲的相应复选框。选中大洲会选中该大洲的所有国家/地区，以及 GeoDB 更新将来可能添加到该大洲下的所有国家/地区。取消选中大洲下的任意国家/地区会取消选中该大洲。您可以选择国家/地区和大洲的任意组合。

步骤 6 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

接口

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以将“内部”接口分配到“内部”区域，而将“外部”接口分配到“外部”区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。某些策略仅支持安全区域，而其他策略则支持区域和组。

有关接口对象的详细信息，请参阅安全区域和接口组，第 713 页。

要添加接口对象，请参阅创建安全区域和接口组对象，第 715 页。

密钥链

为了增强设备的数据安全和防护，引入了用于对持续时间为 180 天以内的 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。轮换密钥仅适用于 OSPFv2 协议。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

注释 身份验证仅使用 MD5 加密算法。

密钥生存期

为了维持稳定的通信，每个设备会将密钥链身份验证密钥存储起来，并对某个功能同时使用多个密钥。密钥链管理基于密钥的发送和接受生存期，提供了一种安全机制来处理密钥滚动。设备使用密钥生存期来确定密钥链中的哪些密钥处于活动状态。

密钥链中的每个密钥具有两个生存期：

- 接受生存期 - 设备在与另一设备进行密钥交换期间接受密钥的时间间隔。
- 发送生存期 - 设备在与另一设备进行密钥交换期间发送密钥的时间间隔。

在密钥发送生存期内，设备会将路由更新数据包与密钥一起发送。当发送的密钥不在设备上密钥的接受生存期内时，设备将不会接受来自其他设备的通信。

如果未配置生存期，则相当于配置没有时间线的 MD5 身份验证密钥。

密钥选择

- 当密钥链含有多个有效密钥时，OSPF 会选择生存期最长的密钥。
- 首选具有无限生存期的密钥。
- 如果密钥生存期相同，则首选密钥 ID 较高的密钥。

创建密钥链对象

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**密钥链**。

步骤 3 点击**添加密钥链**。

步骤 4 在“添加密钥链对象”对话框的**名称**字段中输入密钥链的名称。

该名称必须以下划线或字母开头，后跟字母数字字符或特殊字符（-、_、+、.）。

步骤 5 要向密钥链添加密钥，请点击**添加 (Add)**。

步骤 6 在**密钥 ID** 字段中指定密钥标识符。

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

步骤 7 **算法**字段和**密码加密类型**字段分别显示支持的算法和加密类型，即 MD5 和明文。

步骤 8 在**加密密钥字符串**字段中输入密码，然后在**确认加密密钥字符串**字段中重新输入该密码。

- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

步骤 9 要设置设备与其他设备进行密钥交换期间接受/发送密钥的时间间隔，请在**接受生存期**和**发送生存期**字段中提供生存期值：

注释
“日期时间”值默认为 UTC 时区。

结束时间可为持续时间，即接受/发送生存期结束时的绝对时间或永不到期。默认结束时间为日期时间。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于相应的结束生存期。

步骤 10 点击**添加 (Add)**。

重复步骤 5 到 10 以创建密钥。为具有重叠生存期的密钥链创建至少两个密钥。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。

步骤 11 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 12 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

网络

网络对象表示一个或多个 IP 地址。您可以在多个位置使用网络对象和组合，包括访问控制策略、网络变量、身份规则、网络发现规则、事件搜索、报告、身份识别等等。

当配置需要网络对象的选项时，系统会自动过滤列表，以仅显示对于该选项有效的那些对象。例如，某些选项需要主机对象，而其他选项则需要子网。

网络对象可以是以下类型之一：

主机

单个 IP 地址。

IPv4 示例：

```
209.165.200.225
```

IPv6 示例：

`2001:DB8::0DB8:800:200C:417A` 或 `2001:DB8:0:0:0DB8:800:200C:417A`

范围

IP 地址范围。

IPv4 示例：

```
209.165.200.225-209.165.200.250
```

IPv6 示例：

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

网络

地址块，也称为子网。

IPv4 示例：

```
209.165.200.224/27
```

IPv6 示例：

```
2001:DB8:0:CD30::/60
```



注释 “安全智能”会忽略使用 `/0` 掩码的 IP 地址块。

FQDN

单个完全限定域名 (FQDN)。您可以将 FQDN 解析限制为仅 IPv4 地址，仅 IPv6 地址或 IPv4 和 IPv6 地址。FQDN 必须以数字或字母开头和结尾。FQDN 中仅允许使用字母、数字和短划线作为内部字符。

例如：

```
www.example.com
```

注释 您可在访问控制规则和预过滤规则中使用 FQDN 对象， 或手动 NAT 规则，仅限 。规则匹配通过 DNS 查找获取的 FQDN IP 地址。要使用 FQDN 网络对象，请确保已分别在 DNS 服务器组，第 2640 页和DNS，第 977 页中配置 DNS 服务器设置和 DNS 平台设置。

您不能在身份规则中使用 FDQN 网络对象。

组

一组网络对象或其他网络对象组。您可以通过将一个网络对象组添加到另一个网络对象组创建嵌套组。最多可以嵌套 10 个级别的组。

注释 在网络对象中最多可以添加 100 个网络文字。此外，每个嵌套网络对象组最多可以包含 100 个网络文字。

网络通配符掩码

您可以从网络通配符掩码 **对象** 页面创建和管理通配符掩码对象。

您可以创建具有扩展子网 IP 地址的网络对象。现有网络对象已扩展为支持网络和网络通配符对象。使用通配符掩码的网络对象在网络对象列表页面的**类型 (Type)** 列中列为**网络通配符**。

通配符掩码是不连续的位掩码的 IP 地址。可以使用连续掩码为通配符网络对象创建标准网络对象和不连续的掩码。

IP 地址示例	网络通配符？	对象类型
192.0.0.0/8	不支持	网络
10.10.0.0/255.255.0.0	不支持	网络
10.10.0.10/255.255.0.255	是	网络通配符
72.0.240.10/255.255.240.255	是	网络通配符

注释 只有在配置以下策略时才允许使用网络通配符对象以及包含网络通配符对象的对象组：

- 预过滤器策略
- 访问控制策略
- NAT 策略

准则和限制

- 要创建网络通配符对象，请在 防火墙管理中心 UI 中依次选择**对象** > **网络**并点击**添加网络**，然后点击**添加对象**。选择**网络 (Network)** 选项并输入扩展子网掩码形式的值。示例：10.0.10.10/255.255.0.255。
- 支持对象覆盖、组对象支持、组对象覆盖、通配符文本和通配符对象导入。
- 仅 IPv4 地址支持网络通配符对象。
- 防火墙管理中心 和 Firewall Threat Defense 7.1 及更高版本可支持网络通配符对象。
- 仅 Snort-3 支持网络通配符对象。

创建网络对象

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**网络 (Network)**。

步骤 3 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 4 或者，您可以克隆现有网络对象，然后编辑参数以创建新的网络对象。点击要克隆的现有网络对象上的**克隆**图标。

步骤 5 输入 **Name**。

步骤 6 输入**说明 (Description)**（可选）。

步骤 7 在**网络**字段中，选择所需选项，然后输入适当的值；请参阅网络，第 2658 页。

注释
在网络对象中最多可以添加 100 个网络文字。此外，每个嵌套网络对象组最多可以包含 100 个网络文字。

步骤 8 （仅限 FQDN 对象）从**查找**下拉菜单中选择 DNS 解析以确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。

步骤 9 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 10 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

导入网络对象

有关导入网络对象的详细信息，请参阅导入对象，第 2610 页。

PKI

用于 SSL 应用的 PKI 对象

PKI 对象代表支持您的部署所需的公钥证书和配对的私钥。内部和可信 CA 对象包括证书颁发机构 (CA) 证书；内部 CA 对象还包括与证书配对的私钥。内部和外部证书对象包括服务器证书；内部证书对象还包括与证书配对的私钥。

如果使用可信证书颁发机构对象和内部证书对象来配置与 ISE/ISE-PIC 的连接，则可使用 ISE/ISE-PIC 作为身份源。

如果使用内部证书对象来配置强制网络门户，在连接到用户的 Web 浏览器时，系统可验证强制网络门户设备的身份。

如果使用可信证书颁发机构对象来配置领域，则可配置与 LDAP 或 AD 服务器的安全连接。

如果在 SSL 规则中使用 PKI 对象，可以匹配使用以下证书加密的流量：

- 外部证书对象中的证书
- 由受信任 CA 对象中的 CA 签名的证书或在 CA 的信任链中的证书

如果在 SSL 规则中使用 PKI 对象，可以解密：

- 传出流量（通过对带有内部 CA 对象的服务器证书进行重签）
- 传入流量（使用内部证书对象中的已知私钥）

可以手动输入证书和密钥信息，上传包含这些信息的文件，在某些情况下，还可以生成新的 CA 证书和私有密钥。

在对象管理器中查看 PKI 对象列表时，系统会将证书的使用者可分辨名称显示为对象值。将指针悬停在该值上可查看证书使用者的完整可分辨名称。要查看其他证书的详细信息，请编辑 PKI 对象。



注释 防火墙管理中心和托管设备在保存存储在内部 CA 对象和内部证书对象中的所有私钥之前，会使用随机生成的密钥对它们进行加密。如果上传受密码保护的私钥，设备会使用用户提供的密码对该密钥解密，然后用随机生成的密钥对其加密，再进行保存。

用于证书注册的 PKI 对象

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅PKI 基础设施与数字证书，第 1435 页。

内部证书颁发机构对象

配置的每个内部证书颁发机构 (CA) 对象代表组织控制的 CA 的 CA 公共密钥证书。此类对象由对象名称、CA 证书和配对私钥组成。您可以在 SSL 规则中使用内部 CA 对象和组通过使用内部 CA 对服务器证书进行重新签名来解密传出加密流量。



注释 如果在**解密 - 重新签名 (Decrypt - Resign)** SSL 规则中引用内部 CA 对象，且该规则与加密会话相匹配，在协商 SSL 握手时，用户的浏览器可能会警告证书不可信。要避免此问题，请将内部 CA 对象证书添加到受信任根证书的客户端或域列表。

可以通过以下方式创建内部 CA 对象：

- 导入现有基于 RSA 或基于椭圆曲线的 CA 证书和私有密钥
- 生成新的基于 RSA 的自签 CA 证书和私有密钥
- 生成未签名的基于 RSA 的 CA 证书和私有密钥。使用内部 CA 对象之前，必须向另一个 CA 提交证书签名请求 (CSR) 以对证书进行签名。

创建包含签名证书的内部 CA 对象后，可以下载 CA 证书和私钥。系统使用用户提供的密码对下载的证书和私钥进行加密。

无论是系统生成还是用户创建的内部 CA 对象名称，您都只能修改其名称，但不能修改其他对象属性。

不能删除正在使用的内部 CA 对象。此外，在编辑用于 SSL 策略的内部 CA 对象后，相关联的访问控制策略已过时。必须重新部署访问控制策略才能使更改生效。

CA 证书和私钥导入

可以通过导入 X.509 v3 RSA 证书和私有密钥来配置内部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果私有密钥文件受密码保护，您可以提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

注释 如果配置具有 **Decrypt - Resign** 操作的规则，除了任何配置的规则条件之外，该规则还根据引用的内部 CA 证书的加密算法类型匹配流量。例如，必须上传一个基于椭圆曲线的 CA 证书，以解密用基于椭圆曲线的算法进行加密的出站流量。

导入 CA 证书和私钥

过程

步骤 1 选择**对象**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**导入 CA**。

步骤 4 输入 **Name**。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。

步骤 7 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

生成新的 CA 证书和私钥

可以通过提供识别信息生成基于 RSA 的自签 CA 证书和私有密钥来配置内部 CA 对象。

生成的 CA 证书有效期为十年。有效期起始日期为生成一周之前。

过程

步骤 1 选择**对象**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 点击**生成 CA (Generate CA)**。

步骤 4 输入 **Name**。

步骤 5 输入标识属性。

步骤 6 点击 **Generate self-signed CA**。

新签名证书

可以通过从 CA 获取签名证书来配置内部 CA 对象。这包括两个步骤：

- 提供识别信息以配置内部 CA 对象。这会生成未签名证书和配对私钥，并创建向您指定的 CA 发出的证书签名请求 (CSR)。
- 在 CA 颁发签名证书后，请上传证书到内部 CA 对象，用以替换未签名证书。

仅当内部 CA 对象包含签名证书时，才能在 SSL 规则中引用该对象。

创建未签名的 CA 证书和 CSR

过程

步骤 1 选择**对象**。
步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。
步骤 3 点击**生成 CA (Generate CA)**。
步骤 4 输入 **Name**。
步骤 5 输入标识属性。
步骤 6 点击 **Generate CSR**（**生成 CSR**）。
步骤 7 复制 CSR 以将其提交到 CA。
步骤 8 点击**确定**。

下一步做什么

- 必须上传由 CA 颁发的签名证书，如 中所述 上传为响应 CSR 而颁发的签名证书，第 2664 页

上传为响应 CSR 而颁发的签名证书

上传之后，签名证书可在 SSL 规则中引用。

过程

步骤 1 选择**对象**。
步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。
步骤 3 点击包含等待 CSR 的未签名证书的 CA 对象旁边的 **编辑** ()。

步骤 4 点击 **Install Certificate**。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果上传的文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击**保存**以将签名证书上传到 CA 对象。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

CA 证书和私钥下载

可以通过下载包含内部 CA 对象中的证书和密钥信息的文件来备份或传输 CA 证书和配对私钥。

注意 系统始终将下载的密钥信息存储在安全的位置。

系统在保存密钥信息之前，会使用随机生成的密钥对存储在内部 CA 对象中的私钥进行加密。如果从内部 CA 下载证书和私钥，系统在创建包含证书和私钥信息的文件之前，会首先对这些信息进行解密。然后，您必须提供系统用于加密下载文件的密码。

注意 作为系统备份一部分下载的私钥将被解密，然后存储在未加密的备份文件中。

下载 CA 证书和私钥

可以同时为当前域和祖先域下载 CA 证书。

过程

步骤 1 选择**对象**。

步骤 2 展开 **PKI** 节点，然后选择**内部 CA (Internal CAs)**。

步骤 3 在要下载其证书和私钥的内部 CA 对象旁边，点击 **编辑** ()。

步骤 4 点击**下载**。

步骤 5 在**密码 (Password)** 和**确认密码 (Confirm Password)** 字段中输入加密密码。

步骤 6 点击**确定**。

受信任证书颁发机构对象

配置的每个受信任证书颁发机构 (CA) 对象代表属于受信任 CA 的 CA 公钥证书。此类对象由对象名称和 CA 公共密钥证书组成。您可以在以下位置使用外部 CA 对象和组：

- SSL 策略，用于控制使用由受信任 CA 或信任链中的任何 CA 签名的证书加密的流量。
- 领域配置，用于建立与 LDAP 或 AD 服务器的安全连接。
- 您的 ISE/ISE-PIC 连接。为 **pxGrid 服务器 CA (pxGrid Server CA)** 和 **MNT 服务器 CA (MNT Server CA)** 对象选择受信任证书颁发机构对象。

创建受信任 CA 对象后，可以修改名称和添加证书撤销列表 (CRL)，但不能更改其他对象属性。可添加到对象的CRL数量没有限制。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

不能删除正在使用的可信 CA 对象。此外，在编辑正在使用的受信任 CA 对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

受信任的 CA 对象

您可以通过上传 X.509 v3 CA 证书来配置外部 CA 对象。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书采用PEM格式编码，还可以复制并粘贴信息。

仅当文件包含适当的证书信息时，才可以上传 CA 证书；系统在保存对象之前会对证书进行验证。

添加受信任 CA 对象

过程

步骤 1 选择**对象**。

步骤 2 展开 **PKI** 节点，然后选择**受信任 CA (Trusted CAs)**。

步骤 3 点击 **Add Trusted CAs**。

步骤 4 输入 **Name**。

步骤 5 点击**浏览 (Browse)** 上传 DER 或 PEM 编码的 X.509 v3 CA 证书文件。

步骤 6 如果文件受密码保护，请选中**已加密，密码为：(Encrypted, and the password is:)** 复选框并输入密码。

步骤 7 点击保存。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

受信任 CA 对象中的证书撤销列表

您可以将 CRL 上传到受信任 CA 对象。如果在 SSL 策略中引用受信任 CA 对象，则可以根据颁发会话加密证书的 CA 随后是否会撤销证书来控制加密流量。可以上传采用下列其中一种受支持格式编码的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

添加CRL后，可以查看已撤销证书的列表。要修改已上传到对象的CRL，必须删除该对象并重新创建对象。

只能上传包含适当 CRL 的文件。可添加到受信任 CA 对象的 CRL 数量没有限制。但是，每次上传 CRL 之后，必须先保存对象再添加另一个 CRL。

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

向受信任 CA 对象添加证书撤销列表

注释 在 ISE/ISE-PIC 集成配置中使用对象时，将 CRL 添加到该对象没有任何作用。

过程

步骤 1 选择对象。

步骤 2 展开 **PKI** 节点，然后选择受信任 **CA (Trusted CAs)**。

步骤 3 点击可信 CA 对象旁边的 编辑 ()。

如果显示视图 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 4 点击添加 **CRL (Add CRL)** 上传 DER 或 PEM 编码的 CRL 文件。

步骤 5 点击确定。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

外部证书对象

您配置的每个外部证书对象都表示一个不属于贵组织的服务器公钥证书。该对象由对象名称和证书组成。可以在 SSL 规则中使用外部证书对象和对象组来控制使用服务器证书加密的流量。例如，您可以上传您信任的自签服务器证书，但不能使用可信 CA 证书进行验证。

您可以通过上传 X.509 v3 服务器证书来配置外部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

仅当文件包含适当的服务器证书信息时，才可以上传文件；系统在保存对象之前会对文件进行验证。如果证书采用 PEM 格式编码，还可以复制并粘贴信息。

添加外部证书对象

过程

步骤 1 选择**对象**。

步骤 2 展开 **PKI** 节点，然后选择**外部证书 (External Certs)**。

步骤 3 点击 **Add External Cert**。

步骤 4 输入 **Name**。

步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。

步骤 6 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

内部证书对象

您配置的每个内部证书对象都代表一个属于您组织的服务器公共密钥证书。此类对象由对象名称、公共密钥证书和配对私钥组成。您可以在以下位置使用内部证书对象和组：

- SSL 规则，用于通过已知私钥解密传入到您的组织其中一台服务器的流量。
- 您的 ISE/ISE-PIC 连接。为 **MC 服务器证书 (MC Server Certificate)** 字段选择内部证书对象。

- 强制网络门户配置，用于在连接到用户的 Web 浏览器时对强制网络门户设备的身份进行身份验证。为**服务器证书 (Server Certificate)** 字段选择内部证书对象。

可以通过上传基于 X.509 v3 RSA 或基于椭圆曲线的服务器证书和配对的私有密钥来配置内部证书对象。可以上传采用下列其中一种受支持格式的文件：

- 可分辨编码规则 (DER)
- 隐私增强电子邮件 (PEM)

如果文件受密码保护，必须提供解密密码。如果证书和密钥采用 PEM 格式编码，还可以复制并粘贴信息。

如果要上传文件，文件中必须包含正确的证书或密钥信息，并且可以相互配对。系统在保存对象前将验证配对。

创建内部证书对象后，可以修改名称，但不能修改其他对象属性。

不能删除正在使用的内部证书对象。此外，在编辑正在使用的内部证书对象后，关联的访问控制策略会过期。必须重新部署访问控制策略才能使更改生效。

添加内部证书对象

过程

步骤 1 选择**对象**。
步骤 2 展开 **PKI** 节点，然后选择**内部证书 (Internal Certs)**。
步骤 3 点击 **Add Internal Cert**。
步骤 4 输入 **Name**。
步骤 5 在 **Certificate Data** 字段上方，点击 **Browse** 上传 DER 或 PEM 编码的 X.509 v3 服务器证书文件。
步骤 6 在 **Key** 字段上方，点击 **Browse** 上传 DER、PEM 编码的配对私有密钥文件。
步骤 7 如果上传的私有密钥文件受密码保护，请选中**已加密，密码为:** 复选框并输入密码。
步骤 8 点击**保存**。

证书注册对象

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

证书注册对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。这些活动发生在您的私有密钥基础设施 (PKI) 中。

证书注册对象还可能包括证书撤销信息。有关 PKI、数字证书和证书注册的详细信息，请参阅PKI 基础设施与数字证书，第 1435 页。

如何使用 证书注册对象

证书注册对象用于将托管设备注册到PKI基础设施中，并通过执行以下操作在支持VPN连接的设备上创建信任点（CA 对象）：

1. 在证书注册对象中定义用于CA身份验证和注册的参数。指定共享参数，并使用覆盖功能为不同的设备指定唯一的对象设置。
2. 在需要身份证书的每个托管设备上关联并安装此对象。在设备上，它将成为信任点。

   当证书注册对象与某个设备关联并安装至该设备后，证书注册过程会立即开始。对于自签名、SCEP， EST， 和 PKCS12 文件注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。
3. 在您的 VPN 配置中指定创建的信任点。

管理证书注册对象

要管理 证书注册对象，请转到 **对象** > **PKI** > **证书注册**。系统将显示以下信息：

- 现有证书注册对象会在**名称**列中列出。

  使用搜索字段（放大镜）过滤列表。
- 每个对象的注册类型显示在**类型**列中。可以使用以下注册方法：
  - **自签名** - 托管设备将生成其自己的自签名根证书。
  - **EST**-设备使用安全传输注册从 CA 获取身份证书。
  - **SCEP** -（默认）简单证书注册协议 (SCEP) 供设备用于从 CA 获取身份证书。
  - **手动** - 注册过程由管理员手动执行。
  - **PKCS12 文件** - 在支持 VPN 连接的 威胁防御托管设备上导入 PKCS12 文件。PKCS#12、PFX 或 P12 文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。
  - **ACME**— 自动证书管理环境 (ACME) 协议是一种开放、标准化的协议，旨在自动执行 SSL 和 TLS 证书的颁发、续订和管理。 管理中心 会与支持 ACME 的 CA 服务器通信，在完成域验证后，ACME 服务器会向该设备颁发 SSL 或 TLS 证书。
- **覆盖 (Override)** 列指示对象是允许覆盖（绿色复选标记）还是不允许覆盖（红色的 X）。如果显示一个数字，则它是现有的覆盖数。

  使用“覆盖”选项自定义作为VPN配置一部分的每个设备的对象设置。覆盖将使每个设备的信任点详细信息都是唯一的。通常，在VPN配置中，为每个设备覆盖“公用名”或“使用者”。

  有关覆盖任意类型对象的详细信息和操作步骤，请参阅对象覆盖，第 2617 页。
- 点击编辑图标（铅笔）可**编辑**之前创建的证书注册对象。只有在注册对象未与任何托管设备关联时，才能进行编辑。请参阅有关编辑证书注册对象的添加说明。您可以对失败的注册对象进行编辑。

- 点击删除图标（垃圾桶）可**删除**之前创建的证书注册对象。如果证书注册对象已与任意托管设备关联，则无法将其删除。

按 (+)**添加证书注册 (Add Cert Enrollment)** 打开**添加证书注册 (Add Cert Enrollment)** 对话框并配置 证书注册对象，请参阅添加证书注册对象，第 2671 页。然后在每个托管前端设备上安装证书。

相关主题

使用自签注册安装证书，第 2747 页
使用 EST 注册安装证书，第 2748 页
使用 SCEP 注册安装证书，第 2749 页
使用手动注册安装证书，第 2750 页
使用 PKCS12 文件安装证书，第 2751 页

添加证书注册对象

您可以将这些对象与 Firewall Threat Defense 设备一起使用。您必须具有管理员或网络管理员权限才能执行此任务。

过程

步骤 1 打开**添加证书注册**对话框：

- 直接从对象管理 (Directly from Object Management)：在 **对象** > **PKI** > **证书注册**，然后点击 **添加证书注册**。
- 在配置托管设备时：在**设备 (Devices)** > **证书 (Certificates)** 屏幕中，选择**添加 (Add)** > **添加新证书 (Add New Certificate)**，然后点击证书注册 (Certificate Enrollment) 字段的 (+)。**设备** > **证书** (+)

步骤 2 输入此注册对象的**名称 (Name)** 和**说明 (Description)**（后者为可选项）。

注册完成后，此名称将成为信任点在其关联的托管设备上的名称。

步骤 3 点击 **CA 信息**选项卡。

步骤 4 选择**注册类型**。

- **自签名证书** - 作为 CA 的托管设备将生成其自己的自签名根证书。此窗格中不需要其他信息。

  注释
  注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **EST**-在安全传输协议上注册。指定EST信息。请参阅证书注册对象 EST选项，第 2673 页。
- **SCEP** - （默认）简单证书注册协议。指定 SCEP 信息。请参阅证书注册对象 SCEP 选项，第 2674 页。
- **手动**
  - **仅 CA (CA Only)** - 选中此复选框可仅从所选 CA 创建 CA 证书。不会为此证书创建身份证书。

如果不选中此复选框，则CA证书不是强制性的。您可以在没有CA证书的情况下生成CSR并获取身份证书。

- **CA 证书 (CA Certificate)** - 在框中粘贴 PEM 格式的 CA 证书。您也可以通过从其他设备复制 CA 证书来获取该证书。

  如果选择不使用 CA 证书生成 CSR，则可以将此框留空。

- **PKCS12 文件** - 在支持VPN连接的Firewall Threat Defense托管设备上导入PKCS12文件。PKCS#12或PFX文件将服务器证书、中间证书和私钥保存在一个加密文件中。输入**口令**值进行解密。
- **ACME**—ACME 协议是一种开放式标准化协议，旨在自动执行 SSL 和 TLS 证书的颁发、续订和管理。 管理中心 会与支持 ACME 的 CA 服务器通信，在完成域验证后，ACME 服务器会向该设备颁发 SSL 或 TLS 证书。请参阅证书注册对象 ACME 选项，第 2675 页。

步骤 5 **跳过 CA 证书基本限制中的 CA 标志检查 (Skip Check for CA flag in basic constraints of the CA Certificate)** - 如果要跳过检查信任证书中的基本限制扩展和 CA 标志，请选中此复选框。

步骤 6 **验证使用 (Validation Usage)** - 选择在 VPN 连接期间验证证书的选项：

- **IPsec 客户端** - 验证 IPsec 站点间 VPN 连接的客户端证书。
- **SSL 客户端**-在远程访问 VPN 连接尝试期间验证 SSL 客户端证书。
- **SSL 服务器**-选择以验证 SSL 服务器证书，例如作为 Cisco Umbrella 服务器证书。

步骤 7 （可选） 打开**证书参数 (Certificate Parameters)** 选项卡并指定证书内容。请参阅证书注册对象 证书参数，第 2677 页。

此类信息会置于证书中，从路由器接收证书的任何一方均可访问这些信息。

步骤 8 （可选） 打开**密钥 (Key)** 选项并指定密钥信息。请参阅证书注册对象 密钥选项，第 2678 页。

步骤 9 （可选） 点击**撤销**选项卡并指定撤销选项：请参阅证书注册对象 撤销选项，第 2680 页。

步骤 10 如有需要，**允许覆盖 (Allow Overrides)** 此对象。

每次修改 PKCS12 证书注册对象以允许覆盖时，您必须在证书被覆盖的设备上更新证书的 **口令** 。

有关对象覆盖的完整说明，请参阅对象覆盖，第 2617 页。

步骤 11 点击**保存**。

下一步做什么

关联注册对象并将其安装到某设备上，以在该设备上创建一个信任点。

相关主题

使用自签注册安装证书 ，第 2747 页
使用 EST 注册安装证书，第 2748 页
使用 SCEP 注册安装证书，第 2749 页
使用手动注册安装证书，第 2750 页

使用 PKCS12 文件安装证书，第 2751 页

添加证书注册

过程

步骤 1 输入**名称**。

步骤 2 将证书信息粘贴到 PEM 格式的 **IdP 证书** 字段中。

注释
如果证书依赖于根证书或中间证书，则必须安装从属证书。请参阅证书，第 2743 页。

步骤 3 点击**保存**。

证书注册对象 EST选项

Secure Firewall Management Center 导航路径

对象 > PKI > 证书注册。点击**添加证书注册 (Add Cert Enrollment)** 来打开**添加证书注册 (Add Cert Enrollment)** 对话框，然后选择 **CA 信息 (CA Information)** 选项卡。

字段

注册类型-设置为 **EST**。

注释

- EST 注册类型不支持 EdDSA 密钥。
- 不支持 EST 在证书过期时自动注册设备的功能。

注册 URL (Enrollment URL) - 设备应尝试注册到的 CA 服务器的 URL。

使用 **https://CA_name:port** 形式的 HTTPS URL，其中 *CA_name* 是 CA 服务器的主机 DNS 名称或 IP 地址。 端口 号为必填项。

用户名-用于访问 CA 服务器的用户名。

密码/确认密码-访问 CA 服务器的密码。

指纹-当使用 EST 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接联系服务器获取 CA 的指纹。

源接口-与 CA 服务器交互的接口。默认情况下，显示诊断接口。要将数据接口配置为源接口，请选择相应的安全区域或接口组对象。

忽略 EST 服务器证书验证-默认情况下，EST 服务器证书验证已完成。如果要忽略 Firewall Threat Defense 验证 EST 服务器证书，请选中此复选框。

证书注册对象 SCEP 选项

Secure Firewall Management Center 导航路径

对象 > **PKI** > 证书注册。点击**添加证书注册 (Add Cert Enrollment)** 来打开**添加证书注册 (Add Cert Enrollment)** 对话框，然后选择 **CA 信息 (CA Information)** 选项卡。

字段

注册类型 (Enrollment Type) - 设置为 **SCEP**。

注册 URL (Enrollment URL) - 设备应尝试注册到的 CA 服务器的 URL。

使用 **http://CA_name:port** 形式的 HTTP URL，其中 CA_name 是 CA 服务器的主机 DNS 名称或 IP 地址。端口 号为必填项。

注释 如果使用主机名/FQDN 引用 SCEP 服务器，请使用 FlexConfig 对象配置 DNS 服务器。

如果 CA 中的 CA cgi-bin 脚本位置不是默认位置 (/cgi-bin/pkiclient.exe)，则您也必须将非标准脚本位置包含在 http://CA_name:port/script_location 形式的 URL 中，其中 script_location 是 CA 脚本的完整路径。

质询密码/确认密码 (Challenge Password/Confirm Password) - CA 服务器验证设备身份时所使用的密码。您可以通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取密码：**http://URLHostName/certsrv/mscep/mscep.dll**。从 CA 服务器获取的密码在获取后 60 分钟内有效。因此，创建密码后请务必尽快部署。

重试时间段 (Retry Period) - 各证书请求尝试之间的时间间隔（以分钟为单位）。值可以是 1 到 60 分钟。默认值为 1 分钟。

重试计数 (Retry Count) - 若首次请求后未发出证书，应进行重试的次数。值可以是 1 到 100。默认值为 10。

CA 证书源 (CA Certificate Source) - 指定获取 CA 证书的方式。

- **使用 SCEP 检索**（默认选项，也是唯一受支持的选项）- 使用简单证书注册流程 (SCEP) 从 CA 服务器检索证书。使用 SCEP 在设备和 CA 服务器之间建立连接。在开始注册过程之前，请确保存在从设备到 CA 服务器的路由。

指纹 - 当使用 SCEP 检索 CA 证书时，您可以为 CA 服务器输入指纹。使用指纹验证 CA 服务器证书的真实性有助于防止未经授权的第三方使用虚假证书替代真证书。输入十六进制格式的 CA 服务器**指纹 (Fingerprint)**。如果您输入的值与证书的指纹不匹配，则证书将被拒绝。通过直接连接 CA 服务器或通过在网络浏览器中输入以下地址获取 CA 的指纹：**http://<URLHostName>/certsrv/mscep/mscep.dll**。

证书注册对象 ACME 选项

Secure Firewall Management Center 导航路径

对象 > 对象管理，然后从导航窗格中选择 **PKI** > **Cert 注册**。点击**添加证书注册 (Add Cert Enrollment)** 来打开**添加证书注册 (Add Cert Enrollment)** 对话框，然后选择 **CA 信息 (CA Information)** 选项卡。

ACME 证书的工作原理

1. Firewall Threat Defense 设备通过源接口请求特定域或域列表的 ACME 证书。
2. ACME 服务器通过 Firewall Threat Defense 设备身份验证接口的端口 80 验证域所有权。对于域验证， Firewall Threat Defense 设备使用基于 HTTP 的质询机制 (HTTP-01)。

注释 Firewall Threat Defense 在注册质询响应过程中短暂打开端口 80，仅提供 ACME 质询数据；注册成功或失败后，端口将立即关闭。

3. 在域验证后，ACME 服务器会向设备颁发 SSL 或 TLS 证书。

注释 对于证书注册请求中的每个 FQDN，系统会重复这些阶段。

字段

注册类型 - 选择 **ACME**。

注册 URL (Enrollment URL) - 输入 ACME 服务器的 URL。

默认 URL 是 Let's Encrypt 服务的 URL： https://acme-v02.api.letsencrypt.org/directory。

在**身份验证协议 (Authentication Protocol)** 字段中，**HTTP-01** 是用于验证域所有权的预定义协议。

身份验证接口 (Authentication Interface) - 选择包含 ACME 服务器与 设备通信以验证域所有权的接口的安全区域或接口组。点击 + 以添加接口组或安全区域。

源接口 (Source Interface) - 选择具有接口的安全区域或接口组，设备通过该接口与 ACME 服务器进行交互，从而请求和接收已注册的 ACME 证书。点击 + 以添加接口组或安全区域。

CA 纯证书 (CA only Certificate) - 选择手动安装的用于对 ACME 服务器进行身份验证的仅 CA 证书。

自动注册 (Auto Enroll) - 选中此复选框，以根据配置的生命周期启用 ACME 证书的自动注册。

生命周期 (Lifetime) - 输入ACME 证书使用期限的百分比，之后会自动启动证书重新注册。默认值为 70%。例如，如果证书的生命周期为 100 天且此字段设置为 80，则将在第 81 天触发自动续约。

重新生成密钥 (Regenerate Key) - 选中此复选框以为每个 ACME 注册重新生成新密钥。如果取消选中此复选框，系统将使用先前的密钥进行注册。

使用 ACME 证书的前提条件

一般前提条件

- 确保 Firewall Threat Defense 设备为 10.0 及更高版本。
- 在 Firewall Threat Defense 平台设置中配置 DNS，以解析 ACME 服务器的域名。
- 确保您的域映射到公共 IP 地址。为设备接口配置此 IP 地址，并将其设置为 ACME 证书注册中的身份验证接口。
- 在设备上注册 ACME CA 证书（一种手动安装的仅 CA 证书，用于对 ACME 服务器进行身份验证）。
  - 如果使用 Let’s Encrypt 作为 ACME 服务器，必须从 https://letsencrypt.org/certificates/ 获取互联网安全研究组 (ISRG) 根证书，并将其作为手动仅 CA 证书在设备上注册。例如，您可以使用 https://letsencrypt.org/certs/isrgrootx1.pem.txt 中的根证书。
  - 如果为任何设备配置对象覆盖，请确保也在该设备上注册 ACME CA 证书。
- 为 ACME 服务器和 Firewall Threat Defense 设备配置相同的 NTP 服务器。

ACME 服务器的前提条件

- 确保您可以访问 ACME 服务器，如 Let's Encrypt 或任何其他公网或本地 ACME 服务器。
- 确保 Firewall Threat Defense 设备可以访问 ACME 服务器。
- 确保 ACME 服务器可以验证域名和备用 FQDN。
- 如果身份验证接口与源接口不同，请确保从设备的源接口可以访问 ACME 服务器。

VPN 负载均衡的前提条件

为 VPN 负载均衡组配置 ACME 注册对象时，请确保在**备用 FQDN** 字段中包含控制器和成员 FQDN。请注意，ACME 证书不支持通配符证书。

使用 ACME 证书的限制

- ACME 证书不支持：
  - 站点间 VPN
  - 融合模式下的管理接口
  - DNS 身份验证 (DNS-01)；仅支持 HTTP-01
  - 域覆盖
  - 通配符证书：此类证书通过在域名字段中使用通配符 (*) 保护单个域和多个子域。
  - 集群

- ACME 证书仅支持 RSA 密钥的 2048、3072 和 4096 密钥大小，以及 ECDSA 密钥的 256、384 和 521 密钥大小。
- ACME 注册与控制平面 ACL 不兼容。

  将 Let's Encrypt 与控制平面 ACL 配合使用时：

  1. 在 ACME 登记之前禁用 ACL，以允许端口 80 访问。
  2. 注册 ACME 证书。
  3. 验证登记。
  4. 重新启用 ACL。

  将 ACME 服务器（而非 Let's Encrypt）与控制平面 ACL 配合使用时，请在 ACL 中包含服务器的 FQDN。

证书注册对象 证书参数

在发送到 CA 服务器的证书请求中指定其他信息。此类信息会置于证书中，从路由器接收证书的任何一方均可查看这些信息。

Secure Firewall Management Center 导航路径

对象 > **PKI** > **证书注册**。点击**添加证书注册 (Add Cert Enrollment)** 打开**添加证书注册 (Add Cert Enrollment)** 对话框，然后选择**证书参数 (Certificate Parameters)** 选项卡。

字段

使用标准 LDAP X.500 格式输入所有信息。

- **包含 FQDN (Include FQDN)** - 是否将设备的完全限定域名 (FQDN) 包含在证书请求中。选项如下：
  - **将设备主机名用作 FQDN**
  - **请不要在证书中使用 FQDN**
  - **自定义 FQDN (Custom FQDN)** - 选择此选项，然后在显示的**自定义 FQDN (Custom FQDN)** 字段中指定 FQDN。
- **包含设备的 IP 地址 (Include Device's IP Address)** - 将接口的 IP 地址包含在证书请求中。
- **公用名 (CN)(Common Name [CN])** - 要包含在证书中的 X.500 公用名。



注释 注册自签名证书时，必须在证书参数中指定公用名称 (CN)。

- **组织单位 (OU)** - 要包含在证书中的组织单位名称（例如部门名称）。

- **组织 (O) (Organization [O])** - 要包含在证书中的组织或公司名称。
- **位置 (L) (Locality [L])** - 要包含在证书中的位置。
- **州/省 (ST) (State [ST])** - 要包含在证书中的州或省。
- **国家/地区代码 (C) (County Code [C])** - 要包含在证书中的国家/地区。这些代码符合 ISO 3166 国家/地区缩写规范，例如“US”表示美国。
- **邮件 (E) (Email [E])** - 要包含在证书中的邮件地址。
- **包含设备的序列号 (Include Device’s Serial Number)** - 是否将设备的序列号包含在证书中。CA 使用序列号对证书进行验证，或者之后将证书与特定设备相关联。如有疑问，请含序列号，因为这对调试用途非常有用。

证书注册对象 密钥选项

Secure Firewall Management Center 导航路径

对象 > **PKI** > 证书注册，点击 添加证书注册 **(Add Cert Enrollment)** 打开添加证书注册 **(Add Cert Enrollment)** 对话框，然后选择密钥 **(Key)** 选项卡。

字段

- 密钥类型-RSA、ECDSA、EdDSA。

注释

- 对于 EST 注册类型，请勿选择 EdDSA 密钥，因为它不受支持。
- EdDSA 仅在站点间 VPN 拓扑中受支持。
- EdDSA 不支持作为远程访问 VPN 的身份证书。

- **密钥名称**-如果要与证书关联的密钥对已存在，则此字段指定该密钥对的名称。如果密钥对不存在，则此字段指定要分配给将在注册期间生成的密钥对的名称。如果您不指定名称，系统将使用完全限定域名 (FQDN) 密钥对。
- **密钥大小 (Key Size)** - 如果密钥对不存在，可定义所需的密钥大小（模数，以位为单位）。建议大小为 2048 位。模数越大，密钥越安全。但是，生成模数较大的密钥需要更长的时间（模数大于 512 位时需要一分钟或更长时间），而且交换时的处理时间也更长。

重要事项

- 在 防火墙管理中心 和 Firewall Threat Defense 7.0 及更高版本上，您无法使用 RSA 加密算法注册使用 RSA 密钥大小小于 2048 位的密钥和密钥。但是，您可以使用 具有弱加密的 PKI 证书注册 ，以允许使用具有 RSA 加密算法和较小密钥大小的 SHA-1 的证书。
- 对于 Firewall Threat Defense 7.0，您无法生成大小小于 2048 位的 RSA 密钥，即使启用了弱加密选项也是如此。

- **高级设置** -如果不希望在 IPsec 远程客户端证书的密钥使用和扩展密钥使用扩展中验证值，请选择 **忽略 IPsec 密钥使用** 。您可以抑制对 IPsec 客户端证书的密钥用法检查。默认情况下不启用此选项。

注释 对于站点间 VPN 连接，如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须为所选对象选择 **忽略 IPsec 密钥使用** 选项。否则，终端无法完成站点间 VPN 连接。

使用弱加密的 PKI 证书注册

SHA-1 散列签名算法和 RSA 密钥大小（小于 2048 位用于认证）在 防火墙管理中心 和 Firewall Threat Defense7.0 及更高版本上不受支持。可以用过RSA密钥（大小小于 2048 位）来注册证书。

要在管理 Firewall Threat Defense运行低于 7.0 版本的 防火墙管理中心 7.0 上覆盖这些限制，您可以在 Firewall Threat Defense上使用启用弱加密选项。我们不建议允许使用弱加密密钥，因为此类密钥不如具有更大密钥大小的密钥安全。

注释 Firewall Threat Defense 7.0 或更高版本不支持生成大小小于 2048 位的RSA密钥，即使您允许使用弱加密。

要在设备上启用弱加密，请导航至 **设备** > **证书**页面。点击针对 Firewall Threat Defense 设备提供的 **启用弱加密**（ 按钮。当弱加密选项启用时，按钮更改为 。默认情况下，弱加密选项已禁用。

注释 当由于弱密码使用导致证书注册失败时， 防火墙管理中心 会显示警告消息，提示您启用弱加密选项。同样，当您启用启用弱加密按钮时， 防火墙管理中心 会在设备上启用弱加密配置之前显示警告消息。

将早期版本升级到 Firewall Threat Defense 7.0

当您升级到 Firewall Threat Defense 7.0 时，现有证书配置会保留。但是，如果这些证书的 RSA 密钥小于 2048 位，并使用 SHA-1 加密算法，则无法用于建立 VPN 连接。您必须获取 RSA 密钥大小大于 2048 位的证书，或者为 VPN 连接启用允许弱加密选项。

证书注册对象 撤销选项

通过选择和配置相关方法指定是否检查证书的撤销状态。撤销检查默认处于关闭状态，不选中任何一种方法（CRL 或 OCSP）。

Secure Firewall Management Center 导航路径

按 对象 > **PKI** > 证书注册添加证书注册 **((+) Add Cert Enrollment)** 打开添加证书注册 **(Add Cert Enrollment)** 对话框，然后选择撤销 **(Revocation)** 选项卡。 (+)

字段

- 启用证书撤销列表 **(Enable Certificate Revocation Lists)** - 选中可启用 CRL 检查。
  - 使用来自证书的 **CRL** 分发点 **(Use CRL distribution point from the certificate)** - 选中可获取来自证书的撤销列表分发 URL。
  - 使用已配置的静态 **URL (Use static URL configured)** - 选中可添加静态的预定义的撤销列表分发 URL。然后添加 URL。

    CRL 服务器 **URL (CRL Server URL)** - 可从中下载 CRL 的 LDAP 服务器的 URL。

    URL 必须以 **`http://`** 开头。在 URL 中包含端口号。将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

- 启用在线证书状态协议 **(Enable Online Certificate Status Protocol) (OCSP)** - 选中可启用 OCSP 检查。

  OCSP 服务器 **URL (OCSP Server URL)** - 需要进行 OCSP 检查时，用以检查撤销的 OCSP 服务器的 URL。

  URL 必须以 **`http://`** 开头。将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

- 如果撤销信息无法访问，请考虑证书是否有效 **(Consider the certificate valid if revocation information cannot be reached)** - 默认处于选中状态。如果您不想允许此操作，请取消选中此字段。

策略列表

使用“配置策略列表”页面创建、复制和编辑策略列表策略对象。您可以创建策略列表对象以在配置路由映射时使用。当在路径映射中引用策略列表时，将评估并处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他预先存在的匹配共存，

并设置在同一路径映射内部、策略列表外部配置的语句。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 选择**对象** > **策略列表**。

步骤 2 点击**添加策略列表**。

步骤 3 在**名称**字段中输入策略列表对象的名称。对象名称不区分大小写。

步骤 4 从**操作**下拉列表中选择是允许还是阻止匹配条件的访问。

步骤 5 点击**接口**选项卡以分发使其下一跳脱离其中一个指定接口的路由。

在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域。对于不在区域中的接口，您可以在**所选区域/接口 (Selected Zone/Interface)** 列表下方的字段中键入接口名称，然后点击**添加 (Add)**。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 6 点击**地址**选项卡以重新分发任何具有标准访问列表或前缀列表允许的目标地址的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 7 点击**下一跳**选项卡，重新分发具有指定访问列表或前缀列表传递的下一跳路由器地址的任何路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 8 点击**路由源**选项卡，重新分发在访问列表或前缀列表指定的地址由路由器和接入服务器通告的路由。

选择是否使用**访问列表**或**前缀列表**进行匹配，然后输入或选择要用于匹配的标准访问列表对象或前缀列表对象。

步骤 9 点击 **AS 路径**选项卡以匹配 BGP 自治系统路径。如果指定多条 AS 路径，则路由可以匹配任一 AS 路径。

步骤 10 点击**社区规则**选项卡，以支持将BGP社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。

a) 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**(✎)。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加 (Add)**，然后点击**确定 (OK)**。

要使 BGP 社区与指定社区完全匹配，请选中**完全匹配指定社区**复选框。

b) 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**(✎)。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加 (Add)**，然后点击**确定 (OK)**。

注释
扩展社区列表仅适用于配置路由的导入或导出。

步骤 11 点击**指标与标记**选项卡以匹配路由的指标和安全组标记。

a) 在**指标**字段中输入用于匹配的指标值。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在 0 到 4294967295 之间。
b) 在**标记**字段中输入用于匹配的标记值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。

步骤 12 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 13 点击**保存**。

端口

端口对象以略有不同的方式代表不同协议：

TCP 和 UDP

代表传输层协议（协议号括在括号内，加上一个可选的关联端口或端口范围）的端口对象。例如：`TCP(6)/22`。

ICMP 和 ICMPv6 (IPv6-ICMP)

代表互联网层协议再加上可选类型和代码的端口对象。例如：`ICMP(1):3:3`。

您可以按类型和代码（如果适用）来限制 ICMP 或 IPV6-ICMP 端口对象。有关 ICMP 类型和代码的详细信息，请参阅：

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

其他

可以代表不使用端口的其他协议的端口对象。

系统为已知端口提供默认端口对象。您无法修改或删除这些默认对象。除默认对象以外，还可以创建自定义端口对象。

可在系统 Web 界面中的不同位置使用端口对象和对象组，包括访问控制策略、身份规则、网络发现规则、端口变量和事件搜索。例如，如果您的组织使用的自定义客户端使用特定范围的端口并导致系统生成过多误导事件，可以配置网络发现策略来排除对这些端口的监控。

使用端口对象时，请遵循以下准则：

- 不能为访问控制规则中的源端口条件添加除 TCP 或 UDP 以外的任何协议。此外，在规则中设置源端口条件和目标端口条件时，不能混用传输协议。
- 如果要将不受支持的协议添加到用于源端口条件的端口对象组，则在部署配置时使用该协议的规则不会在托管设备上生效。
- 如果创建同时包含 TCP 和 UDP 端口的端口对象，然后将其添加为规则的源端口条件，则不能添加目标端口，反之亦然。

创建端口对象

过程

步骤 1 选择**对象**。

步骤 2 从对象类型列表中选择**端口 (Port)**。

步骤 3 从**添加端口 (Add Port)** 下拉列表中选择**添加对象 (Add Object)**。

或者，您可以克隆现有端口对象，然后编辑参数以创建新端口对象。点击要克隆的现有端口对象上的 **克隆** 图标。

步骤 4 输入 **Name**。

步骤 5 选择**协议 (Protocol)**。

步骤 6 根据选择的协议，按**端口 (Port)** 进行限制，或者选择 ICMP **类型 (Type)** 和**代码 (Code)**。

可输入 `1` 到 `65535` 之间的端口。使用连字符指定端口范围。如果选择与**所有 (All)** 协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 7 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 8 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

导入端口对象

有关导入端口对象的详细信息，请参阅导入对象，第 2610 页。

前缀列表

您可以为 IPv4 和 IPv6 创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

配置 IPv6 前缀列表

使用“配置 IPv6 前缀列表”(Configure IPv6 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 从目录中选择 **对象** > **前缀列表** > **IPv6 前缀列表**。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击 **新建前缀列表对象 (New Prefix List Object)** 窗口上的 **添加 (Add)** 。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv6 地址。掩码长度必须是介于 1 和 128 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 12 点击**保存**。

配置 IPv4 前缀列表

使用“配置 IPv4 前缀列表”(Configure IPv4 Prefix list) 页面创建、复制和编辑前缀列表对象。您可以创建前缀列表对象以在配置路由映射、策略映射、OSPF 过滤或 BGP 邻居过滤时使用。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 从目录中选择 **对象** > **前缀列表** > **IPv4 前缀列表** 。

步骤 2 点击**添加前缀列表 (Add Prefix List)**。

步骤 3 在**新建前缀列表对象 (New Prefix List Object)** 窗口上的**名称 (Name)** 字段中输入前缀列表对象的名称。

步骤 4 点击**添加 (Add)**。

步骤 5 从**操作 (Action)** 下拉列表中选择相应的操作（“允许”[Allow] 或“阻止”[Block]），以指示重新分发访问。

步骤 6 在**序列号 (Sequence No.)** 字段中输入用于指示新前缀列表条目在已为此对象配置的前缀列表条目列表中将具有的位置的唯一编号。如果保留为空白，则序列号将默认为比当前使用中的最大序列号大 5。

步骤 7 在 **IP 地址 (IP address)** 字段中指定 IP 地址/掩码长度格式的 IPv4 地址。掩码长度必须是介于 1 和 32 之间的有效值。

步骤 8 在**最小前缀长度 (Minimum Prefix Length)** 中输入最小前缀长度。该值必须大于掩码长度并小于或等于“最大前缀长度”(Maximum Prefix Length)（如果指定）。

步骤 9 在**最大前缀长度 (Maximum Prefix Length)** 字段中输入最大前缀长度。该值必须大于或等于“最小前缀长度”(Minimum Prefix Length)（如果存在），或者大于掩码长度（如果未指定“最小前缀长度”[Minimum Prefix Length]）。

步骤 10 点击**添加 (Add)**。

步骤 11 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 12 点击**保存**。

路由映射

在将路由重新分发到任何路由过程中时，将会使用路由映射。在为路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。配置路由映射，以创建路由映射对象的新路由映射条目或编辑现有路由映射条目。

您可以将此对象与 Firewall Threat Defense 设备一起使用。

开始之前

路由映射可以使用其中一个或多个对象；不必添加所有对象。根据需要创建并使用其中任何对象，以配置路由映射。

- 添加 ACL。
- 添加前缀列表。
- 添加 AS 路径。

- 添加社区列表。
- 添加扩展社区列表。



注释 扩展社区列表仅适用于配置路由的导入或导出。

- 添加策略列表。

过程

步骤 1 选择**对象** > **路由地图**。

步骤 2 点击**添加路由映射**。

步骤 3 点击**新建路由映射对象 (New Route Map Object)** 窗口上的**添加 (Add)** 。

步骤 4 在**序列号**字段中，输入 0 到 65535 之间的数字，该数字指示新路由映射条目在已为此路由映射对象配置的路由映射条目列表中的位置。

注释
建议至少以 10 为间隔对子句进行编号，以便将来想要插入子句时保留编号空间。

步骤 5 从**从重新分发 (Redistribution)** 下拉列表中选择相应的操作，即“允许”(Allow) 或“阻止”(Block)，以指示重新分发访问。

步骤 6 点击**匹配子句 (Match Clause)** 选项卡以根据在目录中选择的以下条件来匹配（路由/流量）：

- **安全区域 (Security Zones)** - 根据（入口/出口）接口匹配流量。可以选择区域并添加这些区域，或者键入接口名称并添加这些接口。
- **IPv4** - 根据以下条件匹配 IPv4（路由/流量）；选择该选项卡可定义条件。
  1. 点击**地址**选项卡以根据路由地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的ACL对象或前缀列表对象。
  2. 点击**下一跳**选项卡以根据路由的下一跳地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
  3. 点击**路由源**选项卡以根据路由的通告源地址来匹配路由。对于 IPv4 地址，请从下拉列表中选择要使用访问列表还是前缀列表进行匹配，然后输入或选择要用于匹配的 ACL 对象或前缀列表对象。
- **IPv6** - 根据路由的路由地址、下一跳地址或通告源地址来匹配 IPv6（路由/流量）。
- **BGP** - 根据以下条件来匹配 BGP（路由/流量）；选择该选项卡可定义条件。
  1. 点击 **AS 路径**选项卡以支持将 BGP 自治系统路径访问列表与指定的路径访问列表相匹配。如果指定多个路径访问列表，则路由可以匹配任一路径访问列表。

2. 点击**社区列表**选项卡以支持将 BGP 社区或扩展社区分别与指定的社区列表对象或扩展社区列表对象相匹配。

   - 要为规则指定社区列表，请点击**选定社区列表**字段中的给定**编辑**(✎)。社区列表显示在**可用社区列表**下。选择所需列表，点击**添加 (Add)**，然后点击**确定 (OK)**。有关如何创建社区列表对象的信息，请参阅社区列表，第 2634 页
   - 要添加扩展社区列表，请点击**选定扩展社区列表**字段中的给定**编辑**(✎)。扩展社区列表显示在**可用扩展社区列表**下。选择所需列表，点击**添加 (Add)**，然后点击**确定 (OK)**。有关如何创建扩展社区列表对象的信息，请参阅扩展社区，第 2635 页。

   要使 BGP 社区与指定社区列表对象完全匹配，请选中**完全匹配指定社区**复选框。此选项不适用于扩展社区列表。

   注释
   如果指定多个规则，系统会根据规则验证路由，直到满足某个匹配允许或拒绝条件为止。出站路由映射中将不会通告与至少一个匹配社区不匹配的路由。

3. 点击**策略列表**选项卡以配置路由映射来评估和处理 BGP 策略。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

- **其他 (Others)** - 根据以下条件来匹配路由或流量。

1. 在**指标路由值**字段中输入要用于匹配的指标值，以支持匹配路由的指标。可以输入多个以逗号分隔的值。通过此设置可匹配具有指定指标的任何路由。指标值范围可以在0到4294967295之间。
2. 在**标签值**字段中输入要用于匹配的标签值。可以输入多个以逗号分隔的值。通过此设置可匹配任何具有指定安全组标记的路由。标记值范围在 0 到 4294967295 之间。
3. 选中相应的**路由类型**选项以启用路由类型匹配。有效路由类型为 External1、External2、Internal、Local、NSSA-External1 和 NSSA-External2。可以从列表中选择多个路由类型。

步骤 7 点击**设置子句**选项卡以根据在目录中选择的以下条件来设置路由/流量：

- **指标值 (Metric Values)** - 设置“带宽”(Bandwith)、所有值或无任何值。

1. 在**带宽**字段中以千位/秒为单位输入指标值或带宽。有效值是范围从 0 到 4294967295 的整数值。
2. 从**指标类型**下拉列表中选择指定目标路由协议的指标类型。有效值为：internal、type-1 或 type-2。

- **BGP 子句 (BGP Clauses)** - 根据以下条件设置 BGP 路由；选择该选项卡以定义条件。

1. 点击 **AS 路径**选项卡以修改 BGP 路由的自治系统路径。
   1. 在**预置 AS 路径**字段中输入 AS 路径编号，以将任意自治系统路径字符串预置到 BGP 路由。通常本地 AS 编号预置多次，从而增加自治系统路径长度。如果指定多个 AS 路径编号，则路径可以预置任一 AS 编号。

2. 在**将最后一个 AS 预置到 AS 路径**字段中输入 AS 路径编号，来为 AS 路径预置最后一个 AS 编号。为 AS 编号输入 1 到 10 之间的值。
3. 选中**将路由标签转换为 AS 路径**复选框以将路由的标签转换为自治系统路径。

2. 点击**社区列表 (Community List)** 选项以设置社区属性。

   在**特定社区**下：

   1. 点击**无** 单选按钮以从用于传递路由映射的前缀中删除社区属性。
   2. 点击**特定社区**单选按钮以输入社区编号（如果适用）。有效值范围为 1 至 4294967295。
   3. 选中**添加到现有社区**以将社区添加到已经现有的社区。
   4. 选中 **Internet**、**无通告**或**无导出**复选框以使用已知社区之一。

   在**特定扩展社区**下的**路由目标**字段中，输入 *ASN:nn* 格式的路由目标编号：

   - 您可以输入在 1:1 到 65534:65535 范围内的值。

     您可以在单个条目中添加单个路由目标或一组以逗号分隔的路由目标。例如*1:2,1:4,1:6*。
   - 一个条目中最多可以包含 8 个路由目标。
   - 路由映射中不能包含多余的路由目标条目。

3. 点击**其他**选项卡以设置其他属性。
   1. 选中**设置自动标签**复选框以自动计算标签值。
   2. 在**设置本地首选项**字段中输入自治系统路径的首选项值。输入 0 到 4294967295 之间的值。
   3. 在**设置权重**字段中输入路由表的 BGP 权重。输入 0 到 65535 之间的值。
   4. 选择指定 BGP 源代码。有效值为**本地 IGP** 和**不完整**。
   5. 在“IPv4 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv4 地址。它不需要是相邻路由器。如果指定多个 IPv4 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv4 前缀列表。
   6. 在“IPv6 设置”部分中，指定数据包输出到的下一跳的下一跳 IPv6 地址。它不需要是相邻路由器。如果指定多个 IPv6 地址，则数据包可以在任一 IP 地址输出。

      选择在**前缀列表**下拉列表中指定 IPv6 前缀列表。

步骤 8 点击**添加 (Add)**。

步骤 9 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。

步骤 10 点击**保存**。

安全智能

安全情报是一种流量过滤机制

- 使用 IP 地址、域名和 URL 的集合快速过滤与条目匹配的流量
- 要求具备 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（其他所有设备类型），以及
- 通过归类为 DNS、网络及 URL 的列表和源运作。

安全情报组件

安全情报列表和源是 IP 地址、域名的集合。您可以将它们用于快速过滤与列表或源中条目匹配的流量。

- 列表是一个可手动管理的静态集合。
- 源是按一定间隔通过 HTTP 或 HTTPS 更新的动态集合。

安全智能列表/源分组为：

- DNS （域名）
- 网络 （IP 地址）
- URL

系统提供的源：

思科提供以下源作为安全情报对象：

- 安全智能源定期更新来自以下方面的最新威胁智能：Talos
  - Cisco-DNS-and-URL-Intelligence-Feed（在 DNS 列表和源下）
  - Cisco 智能馈送（对于 IP 地址，在网络列表和馈送下）

  虽然无法删除系统提供的源，但可以更改其更新频率（或禁用更新）。
- Cisco-TID-Feed（在网络列表和源下）

  此源不在访问控制策略的“安全智能”选项卡中使用。

  但须启用并配置 Cisco Secure Firewall 威胁智能导向器 方可使用此源。该源是 TID 可观测数据的集合。

  使用此对象配置向 TID 元素发布数据的频率。

  有关详细信息，请参阅威胁情报导向器，第 2411 页。

预定义全局阻止列表与不排除列表：

系统包含域 (DNS)、IP 地址（网络）和 URL 的预定义全局阻止列表与不排除列表。

这些列表在您填充之前为空。要构建这些列表，请参阅 全局和域安全智能列表，第 2690 页。

默认情况下，访问控制和 DNS 策略使用这些名单作为安全智能的一部分。

自定义源：

您可以使用第三方源，或者，利用自定义内部源，您可以在具有多个 Secure Firewall Management Center 设备的大型部署中轻松维护企业级阻止列表。

请参阅自定义安全智能源，第 2696 页。

自定义列表：

自定义列表可扩充和微调源和全局列表。

请参阅自定义安全智能列表，第 2698 页。

安全情报列表和源的使用位置：

- IP 地址和地址块 - 用于访问控制策略的阻止列表和不阻止列表，作为安全智能的一部分。
- 域名 - 用于 DNS 策略的阻止列表和不阻止列表，作为安全智能的一部分。
- URL - 用于访问控制策略的阻止列表和不阻止列表，作为安全智能的一部分。此外，您还可以在访问控制和 QoS 规则中使用 URL 列表，这些规则的分析和处理阶段发生在安全智能之后。

如何修改安全智能对象

要添加或删除阻止列表、不阻止列表、源或 Sinkhole 对象中的条目，请执行以下操作：

对象类型	编辑功能	编辑后是否需要重新部署？
自定义阻止和不阻止列表	使用对象管理器上传新列表和替代列表。	不支持
默认（但自定义填充）阻止列表和不阻止列表：全局、后代和特定域	使用上下文菜单来添加条目或使用对象管理器删除条目。	不支持
系统提供的情报源	使用对象管理器禁用或更改更新频率。	否
自定源	使用对象管理器进行全面修改。	否
Sinkhole	使用对象管理器进行全面修改。	支持

全局和域安全智能列表

防火墙管理中心 包括“全局阻止”和“不阻止”列表，使您能够使用安全智能持续阻止特定连接或禁止阻止特定连接，从而允许您配置的其他威胁检测流程对这些连接进行评估。

例如，如果注意到入侵事件中的一组可路由IP地址涉及漏洞攻击尝试，可以立即阻止这些IP地址。虽然更改可能需要几分钟时间才能完成传播，但您无需重新部署。

默认情况下，访问控制和DNS策略使用这些适用于所有安全区域的全局列表。您可以为每个策略选择不使用这些列表。



注释 这些选项仅适用于安全智能。安全智能无法阻止已使用快速路径的流量。同样，安全智能也不会自动将受信任或快速路径匹配流量列入不阻止列表。有关详细信息，请参阅关于安全智能，第1729页。

安全智能列表和多租户

多租户地址：

- 域列表 - 内容只适用于特定子域的阻止列表和不阻止列表。全局列表是全局域的域列表。
- 后代域列表 - 汇聚当前域的后代的域列表的阻止列表和不阻止列表。

域列表

除了能够访问（但不能编辑）全局列表之外，每个子域都具有自己的命名列表，命名列表的内容只应用于该子域。例如，名为 Company A 的子域拥有：

- 域阻止列表-公司 A 和域不阻止列表-公司 A
- DNS 域阻止列表-公司 A，DNS 的域不阻止列表-公司 A
- URL 域阻止列表-公司 A，URL 的域不阻止列表-公司 A

当前或以上域中的任何管理员都可以填充这些列表。您可以用情景菜单将当前及所有后代域中的项目列入阻止列表和不阻止列表。但只有关联域中的管理员可以删除域列表中的项目。

例如，全局管理员可以选择将全局域和公司 A 的域中的相同 IP 地址列入阻止列表，但不能在公司 B 的域中将其列入阻止列表。此操作会将 IP 地址添加到：

- 全局阻止列表（只有全局管理员可以将其删除）
- 域阻止列表 - 公司 A（只有公司 A 管理员可以将其删除）

后代域列表

后代域列表是汇聚当前域的后代的域列表的不阻止列表和阻止列表。分叶域没有后代域列表。

后代域列表很有用，因为较高级别的域管理员可以执行通用安全智能设置，但仍允许子域用户将其自己部署中的项目列入阻止列表和不阻止列表。

例如，全局域具有以下后代域列表：

- 后代阻止列表 - 全局、后代不阻止列表 - 全局
- 后代 DNS 阻止列表 - 全局、后代 DNS 不阻止列表 - 全局

- 后代 URL 阻止列表 - 全局、后代 URL 不阻止列表 - 全局



注释 后代域列表不显示在对象管理器中，因为它们是象征性汇聚，不是手动填写列表。它们显示在您可以使用它们的位置：访问控制策略和 DNS 策略。

将条目添加到全局安全智能列表

查看事件和控制面板时，您可以通过将这些事件中显示的 IP 地址、域和 URL 添加到预定义的阻止列表，立即阻止这些流量。

同样，如果安全智能阻止了您希望在安全智能阻止之后由威胁检测进程评估的流量，则可以将事件中的 IP 地址、域和 URL 添加到预定义的“不阻止”列表。

在威胁检测的安全智能阶段，将根据这些列表中的条目评估流量。

有关这些列表的详细信息，请参阅 全局和域安全智能列表，第 2690 页。

开始之前

由于将条目添加到安全智能列表会影响访问控制，因此必须具有以下其中一种角色：

- 管理员
- 角色的组合：网络管理员或访问管理员，加上安全分析师和安全审批人
- 同时具有“修改访问控制策略”(Modify Access Control Policy) 和“将配置部署到设备”(Deploy Configuration to Devices) 权限的自定义角色

如果适用，请验证这些列表是否用于您期望使用它们的策略中。

过程

步骤 1 导航至包含要始终使用安全智能阻止或免于安全智能阻止的 IP 地址、域或 URL 的事件。

步骤 2 右键点击 IP 地址、域或 URL，然后选择相应的选项：

项目类型	上下文菜单选项
IP 地址	将 IP 添加到阻止列表 将 IP 添加到不阻止列表 这些选项将 IP 地址添加到相应的网络列表。
URL	将 URL 添加到 URL 的全局阻止列表 将 URL 添加到 URL 的全局不阻止列表

项目类型	上下文菜单选项
URL 字段中的 URL 域	将域添加到 URL 的全局阻止列表 将域添加到 URL 的全局不阻止列表
DNS 查询字段中的域	将域添加到 DNS 的全局阻止列表 将域添加到 DNS 的全局不阻止列表

下一步做什么

您无需重新部署即可使这些更改生效。

如果要从列表中删除项目，请参阅从全局安全智能列表中删除条目，第 2693 页。

从全局安全智能列表中删除条目

注释 要向这些列表中添加条目，请参阅将条目添加到全局安全智能列表，第 2692 页。

过程

步骤 1 选择**对象 (Objects)** > **安全智能 (Security Intelligence)**。

步骤 2 点击适当的选项：

- **网络列表和源**（对于 IP 地址）
- **DNS 列表和源**（用于域名）
- **URL 列表和源**

步骤 3 点击“全局阻止”(Global Block) 或“全局不阻止”(Global Do-Not-Block) 列表旁边的铅笔。

步骤 4 点击要删除的条目旁边的垃圾桶按钮。

安全智能的列表和源更新

列表和源更新会将现有列表或源文件替换为新文件的内容。现有文件和新文件的内容不会合并。

如果系统下载损坏的源或具有无法识别的条目的源，则系统会继续使用旧源数据（除非是第一次下载）。但是，如果系统可以识别即便源中的一个条目，也会使用其可识别的条目。

默认情况下，各个源每两小时更新一次管理中心，您可以修改频率。管理中心收到的任何更新都会立即传递到托管设备。此外，托管设备每 30 分钟轮询一次 防火墙管理中心 以了解更改。您无法修改此频率。

注释 对于 Cisco Secure Firewall 200，更新每天下载一次，而不是每 30 分钟一次。

要修改源更新间隔，请参阅更改安全智能源的更新频率 ， 第 2694 页。

更改安全智能源的更新频率

您可以指定 防火墙管理中心更新安全智能源的间隔。

有关源更新的详细信息，请参阅安全智能的列表和源更新 ， 第 2693 页。

过程

步骤 1 选择**对象**。

步骤 2 展开**安全智能 (Security Intelligence)** 节点，然后选择要更改其频率的源类型。

系统提供的 URL 源与 **DNS 列表和源**下的域源合并。

步骤 3 在要更新的源旁边，点击 **编辑** ()。

如果显示**视图** ()，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 4 编辑 **Update Frequency**。

步骤 5 点击**保存**。

自定义安全智能列表和源

自定义列表和源：要求

列表和源格式

每个列表或源必须是不大于 500 MB 的简单文本文件。列表文件必须包括 .txt 扩展名。每行包括一个条目或注释：一个 IP 地址、一个 URL、一个域名。

提示 可包含的条目数受该文件的最大大小限制。例如，没有注释、平均 URL 长度为 100 个字符（包括 Punycode 或百分比 Unicode 表示和换行符）的 URL 列表可包含 524 万个以上条目。

在 DNS 列表条目中，您可以为域标签指定星号 (*) 通配符。所有标签都与通配符匹配。例如，条目 `www.example.*` 与 `www.example.com` 和 `www.example.co` 均匹配。

如果在源文件中添加注释行，则其必须以井号 (#) 字符开头。如果上传具有注释的源文件，则系统会在上传期间删除注释。您下载的源文件包含不带注释的所有条目。

源要求

配置源时，可使用 URL 指定位置；但 URL 不能使用 Punycode 编码。

对于 30 分钟或更短的源更新间隔，必须指定 MD5 URL。这可以防止频繁下载未更改的源。如果源服务器未提供 MD5 URL，则必须使用至少 30 分钟的下载间隔。

如果您使用 MD5 校验和，校验和必须存储在仅带有该校验和的简单文本文件中。不支持注释。

URL 列表和源：URL 语法和匹配条件

安全智能URL列表和源（包括全局阻止列表和不阻止列表中的自定义列表和源和条目）可以包括以下内容，它们具有所述的匹配行为：

- 主机名

  例如，**www.example.com**。

- URL

  example.com 匹配 **example.com** 和所有子域，包括 **www.example.com**、**eu.example.com**、**example.com/abc** 和 **www.example.com/def** -- 但不包括 **example.co.uk** 或 **examplexyz.com** 或 **example.com.malicious-site.com**

  当 URL 源或列表包含单个条目时，所有以这些域结尾的 URL 都会被识别并阻止。

  示例：当以下 URL 源 - **www.netflix.com, www.amazon.*、org、edu、www.hulu.*** 被添加到全局“阻止列表”时，将阻止以下内容：http://www.amazon.in、http://www.rajiv.org/、http://www.edu.edu/、http://www.edu.org/、http://org.org/ 和 http://edu.edu。

  您也可以包括整个 URL 路径，例如 **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**



注释 您可以创建自定义URL、网络和DNS源，其中，您可以在URL中添加用户名和密码，例如：
https://admin:password@server.domain.com/list.txt

但是，如果密码包含特殊字符，例如冒号 (:) 或 @ 符号，则传输将失败。确保您的密码不包含任何特殊字符。或者，您可以在 URL 中使用编码密码。

- URL 末尾的斜杠，用于指定精确匹配项

  example.com/ 仅匹配 **example.com**；它不匹配 **www.example.com** 或任何其他 URL。

- 表示 URL 中任何域的通配符 (*)

星号可以表示由点分隔的完整域字符串，但不能表示部分域字符串，也不能表示URL中第一个斜杠后面的任何部分。

有效示例：

- ***.example.com**
- **www.*.com**
- **example.***

  （例如，这将匹配 **example.com** 和 **example.org** 和 **example.de**，但不匹配 **example.co.uk**）
- ***.example.***
- **example.*/**

无效示例：

- **example*.com**
- **example.com/***

- IP 地址 (IPv4)

  对于 IPv6 地址，或者要使用范围或 CIDR 表示法，请使用安全智能网络对象。

  您可以包含一个或多个表示八位组的通配符，例如 10.10.10.* 或 10.10.*.*。

另请参阅自定义安全智能列表，第 2698 页。

自定义安全智能源

自定义或第三方安全智能源允许您使用互联网上其他定期更新且信誉良好的不阻止列表和阻止列表来扩充系统提供的智能源。也可以设置内部源；如果要使用一个源列表来更新部署中的多个 Secure Firewall Management Center 设备，这将会很有用。

注释 您不能通过在安全智能源中使用 /0 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 any。

您也可以将系统配置为使用MD5校验和来确定是否下载更新的源。如果校验和自上次系统下载源以来没有更改，则系统无需重新下载该源。您可能希望将MD5校验和用于内部源，尤其是那些很大的内部源。

注释 在下载自定义源时，系统不执行对等 SSL 证书验证，系统也不支持使用证书捆绑包或自签证书来验证远程对等设备。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

手动更新安全智能源会更新所有源，包括智能源。

请参阅 自定义列表和源：要求，第 2694 页完成要求

创建安全智能源

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择 **对象 (Objects)** > **安全智能 (Security Intelligence)** 节点，然后选择要添加的源类型。

步骤 2 点击适合您在上方所选源类型的选项：

- **添加网络列表和源**（对于 IP 地址）
- **添加 DNS 列表和源 (Add DNS Lists and Feeds)**
- **添加 URL 列表和源 (Add URL Lists and Feeds)**

步骤 3 为源输入**名称 (Name)**。

步骤 4 从**类型 (Type)** 下拉列表中选择**源 (Feed)**。

步骤 5 输入**源 URL (Feed URL)**。

步骤 6 输入 **MD5 URL**。

这用于确定自上次更新以来源内容是否已更改，因此系统不会下载未更改的源。

小于 30 分钟的更新间隔需要 MD5 URL。

如果源服务器未提供 MD5 URL，则必须选择至少 30 分钟的间隔。

步骤 7 选择**更新频率 (Update Frequency)**。

步骤 8 点击**保存**。

除非已禁用源更新，否则系统会尝试下载并验证源。

手动更新安全智能源

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

开始之前

必须至少将一个设备添加到管理中心。

过程

步骤 1 选择**对象 (Objects)** > **安全智能 (Security Intelligence)**。

步骤 2 点击**更新源 (Update Feeds)**，然后确认。

步骤 3 点击**确定**。

Secure Firewall Management Center下载和验证源更新后，会将任何更改通知其托管设备。您的部署开始使用更新的源过滤流量。

自定义安全智能列表

安全智能列表是手动上传到系统的IP地址和地址块、URL或域名的简单静态列表。如果要扩充和微调单个Secure Firewall Management Center的托管设备的源或其中一个全局列表，自定义列表很有用。

例如，如果信誉良好的源错误地阻止对重要资源的访问，但整体来说对组织有用，您即可创建仅包含分类不当的 IP 地址的自定义不阻止列表，而不是从访问控制策略的阻止列表中删除 IP 地址源对象。



注释 您不能通过在安全智能列表中使用 `/0` 网络掩码，将地址块列入阻止列表或不阻止列表。如果要监控或阻止策略所针对的所有流量，请分别使用包含**监控 (Monitor)** 或**阻止 (Block)** 规则操作的访问控制规则，并对**源网络 (Source Networks)** 和**目标网络 (Destination Networks)** 使用默认值 `any`。

有关列表条目格式，请注意以下事项：

- 地址块的网络掩码可以是 `0` 到 `32` 之间或 `0` 到 `128` 之间的整数（分别适用于 IPv4 和 IPv6）。
- 域名中的 Unicode 必须使用 Punycode 格式进行编码，并且不区分大小写。
- 域名中的字符不区分大小写。
- URL 中的 Unicode 应使用百分比编码格式进行编码。
- URL 子目录中的字符区分大小写。
- 以井号 (`#`) 开头的列表条目被视为注释。
- 请参阅 自定义列表和源：要求，第 2694 页中的其他格式要求。

有关匹配的列表条目，请注意以下事项：

- 如果在 URL 或 DNS 列表中存在较高级别的域，则系统与子级别域匹配。例如，如果将 `example.com` 添加到 DNS 列表，则系统与 `www.example.com` 和 `test.example.com` 均匹配。
- 系统不对 DNS 或 URL 列表条目执行 DNS 查找（正向或反向）。例如，如果向 URL 列表中添加 `http://192.168.0.2`，并且其解析为 `http://www.example.com`，则系统仅与 `http://192.168.0.2` 匹配，而与 `http://www.example.com` 不匹配。

将新的安全智能列表上传到 Secure Firewall Management Center

要修改安全智能列表，必须更改源文件并上传新副本。不能使用 Web 界面来修改文件内容。如果您无法访问源文件，可以从系统下载副本。

过程

步骤 1 选择 对象 (Objects) > 安全智能 (Security Intelligence) 节点，然后选择列表类型。

步骤 2 点击适合您在上方所选列表的选项：

- 添加网络列表和源（对于 IP 地址）
- 添加 DNS 列表和源 (Add DNS Lists and Feeds)
- 添加 URL 列表和源 (Add URL Lists and Feeds)

步骤 3 输入 Name。

步骤 4 从类型 (Type) 下拉列表中，选择列表 (List)。

步骤 5 点击浏览 (Browse) 浏览到列表 .txt 文件，然后点击上传 (Upload)。

步骤 6 点击保存。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全智能列表中删除条目，第 2693 页。

更新安全智能列表

过程

步骤 1 选择 对象 (Objects) > 安全智能 (Security Intelligence) 节点，然后选择列表类型。

步骤 2 在要更新的列表旁边，点击 编辑 ()。

如果显示视图 ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 如果需要对要编辑的列表保留副本，请点击下载，然后按照浏览器的提示将该列表另存为文本文件。

步骤 4 根据需要对列表进行更改。

步骤 5 在“安全智能”弹出窗口中，点击浏览以浏览到修改后的列表，然后点击上传。

步骤 6 点击保存。

下一步做什么

您无需重新部署这些更改即可生效。如果要从列表中删除条目，请参阅从全局安全智能列表中删除条目，第 2693 页。

Sinkhole

Sinkhole 对象代表为 Sinkhole 中所有域名提供非可路由地址的 DNS 服务器或没有解析到服务器的 IP 地址。您可以在 DNS 策略规则中引用 Sinkhole 对象，以将匹配流量重定向到 Sinkhole。您必须为对象同时分配 IPv4 地址和 IPv6 地址。

创建 Sinkhole 对象

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **Sinkhole**。

步骤 2 点击**添加 Sinkhole (Add Sinkhole)**。

步骤 3 输入 **Name**。

步骤 4 输入 Sinkhole 的 **IPv4 地址 (IPv4 Address)**和 **IPv6 地址 (IPv6 Address)**。

步骤 5 您有以下选择：

- 如果要将流量重定向到 Sinkhole 服务器，请选择**记录与 Sinkhole 的连接 (Log Connections to Sinkhole)**。
- 如果要将流量重定向到非解析 IP 地址，请选择**阻止并记录与 Sinkhole 的连接 (Block and Log Connections to Sinkhole)**。

步骤 6 如果要将危害表现 (IoC) 类型分配给 Sinkhole，请从**类型 (Type)** 下拉列表中选择一种类型。

步骤 7 点击**保存**。

SLA 监控器

每个互联网协议服务级别协议 (SLA) 监控器定义受监控地址的连接策略，并跟踪地址路由的可用性。通过发送 ICMP 回应请求并等待响应，定期检查路由的可用性。如果请求超时，路由将从路由表中删除并使用备份路由来替换。SLA 监控作业在部署后立即开始并持续运行，除非您从设备配置移除 SLA 监控器（即，监控器并未过期）。互联网协议服务级别协议 (SLA) 监控器对象用在 IPv4 静态路由策略的“路由跟踪”字段中。IPv6 路由无法选择通过路由跟踪使用 SLA 监控器。

您可以将这些对象与 Firewall Threat Defense 设备一起使用。

过程

步骤 1 选择**对象** > **SLA 监控器**。

步骤 2 点击**添加 SLA 监控器 (Add SLA Monitor)**。

步骤 3 在**名称 (Name)** 字段中输入对象的名称。

步骤 4 （可选）在**说明**字段中输入对象的说明。

步骤 5 在**频率 (Frequency)** 字段中输入 ICMP 回应请求传输的频率（以秒为单位）。有效值范围为 1 到 604800 秒（7 天）。默认值为 60 秒。

注释
频率不能小于超时值；您必须将频率转换为毫秒才可比较两个值。

步骤 6 在 **SLA 监控器 ID** 字段中输入 SLA 操作的 ID 编号。值范围为 1 到 2147483647。在一个设备上最多可以创建 2000 个 SLA 操作。每个 ID 编号在策略和设备配置中必须是唯一的。

步骤 7 在**阈值**字段中，输入在 ICMP 回应请求之后且在宣告上升阀值之前必须经过的时间（以毫秒为单位）。值的范围为 0 到 2147483647 毫秒。默认值为 5000 毫秒。阈值仅用于指示超过定义值的事件。可以使用这些事件来评估适合的超时值。它不是受监控地址可达性的直接指标。

注释
阈值不应超过超时值。

步骤 8 在**超时 (Timeout)** 字段中，输入 SLA 操作等待 ICMP 回应请求响应的时间量（以毫秒为单位）。值范围为 0 到 604800000 毫秒（7 天）。默认值为 5000 毫秒。如果在此字段中定义的时间内未从受监控地址收到响应，则从路由表中删除静态路由并用备份路由来替换。

注释
超时值不能超过频率值（将频率值转换为毫秒以比较两个数字）。

步骤 9 在**数据大小 (Data Size)** 字段中输入 ICMP 请求数据包负载的大小（以字节为单位）。值范围为 0 到 16384 字节。默认值为 28 字节，它会创建一个总计 64 字节的 ICMP 数据包。请勿将此值设置为高于协议或路径最大传输单位 (PMTU) 允许的最大值。为了实现可达性，可能需要增大默认数据大小，以检测源和目标之间的 PMTU 更改。低 PMTU 会影响会话性能，如果检测到此情况，则可能表示应使用辅助路径。

步骤 10 在 **ToS** 字段中输入在 ICMP 请求数据包的 IP 报头中定义的服务类型 (ToS) 的值。值范围为 0 到 255。默认值为 0。此字段包含延迟、优先级、可靠性等信息。可供网络上其他设备用于策略路由和承诺接入速率等功能。

步骤 11 在**数据包数量 (Number of Packets)** 字段中输入发送的数据包数量。值范围为 1 到 100。默认为 1 个数据包。

注释
如果担心丢包可能会错误地导致 Cisco Secure Firewall Threat Defense设备认为受监控的地址无法访问，则请增加默认数据包数量。

步骤 12 在**受监控的地址 (Monitored Address)** 字段中，输入由 SLA 操作监控其可用性的 IP 地址。

步骤 13 **可用区域**列表同时显示区域和接口组。在**区域/接口**列表中，添加包含设备可通过其与管理站通信的接口的区域或接口组。要指定单个接口，则需要为该接口创建区域或接口组；请参阅创建安全区域和接口组对象，第 715 页。仅在设备包含所选接口或区域时，系统才会在设备上配置主机。

步骤 14 点击**保存**。

时间范围

使用时间范围对象定义用于确定规则应用时间的时间段。

注释 从 防火墙管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

创建时间范围对象

如果希望策略仅在指定的时间范围内应用，请创建一个时间范围对象，然后在策略中指定该对象。请注意，此对象仅适用于 Firewall Threat Defense 设备。

只能在本主题底部列出的策略类型中指定时间范围对象。

注释 时区表示设备的本地时间，仅用于在支持时间范围的策略中应用时间范围。时区不会更改设备的配置时间。要验证配置，请在 Firewall Threat Defense CLI 中，使用 **show time-range timezone** 和 **show time** 命令（请参阅 *Cisco Secure Firewall Threat Defense 命令参考* 指南）。此外，机箱的时区会覆盖管理中心时区。

开始之前

根据与处理流量的设备关联的时区应用时间范围。默认情况下为 UTC。要更改与设备关联的时区，请转至 设备 > 平台设置。**设备** > **平台设置**

过程

步骤 1 从对象类型列表中选择 URL。**对象** > **时间范围**

步骤 2 点击**添加时间范围 (Add Time Range)**。

步骤 3 输入值。

请遵守以下准则：

- 如果您在输入的对象名称周围看到一个红色的错误框，则将光标移到**名称**字段上可查看命名限制。
- 所有时间均为 UTC，除非您在 **设备** > **平台设置**中为设备指定时区。
- 使用 24 小时制时钟输入时间。例如，输入 1:30 表示 13:30。
- 要指定一个连续的范围，例如典型的周末时间（星期五下午 5 点到星期一上午 8 点，包括晚上和夜晚），请选择“范围类型”**范围**。

- 要指定多天的一部分，例如星期一到星期五的上午 8 点到下午 5 点（不包括每日的晚上、夜晚和凌晨），请选择“范围类型”**每日间隔**。
- 您可以在单个对象中最多指定 28 个时间段。
- 要为一天或不同天的不同时间制定多个不连续时间，请创建多个重复间隔。例如，要在标准工作时间以外的所有时间应用策略，请创建一个具有以下两个重复间隔的单个时间范围对象：
  - 星期一到星期五的下午 5 点到上午 8 点的每日间隔，以及
  - 星期五下午 5 点到星期一上午 8 点的范围重复间隔。

步骤 4 点击**保存**。

下一步做什么

配置以下任意时间范围：

- 访问控制规则
- 预过滤器规则
- 隧道规则
- VPN 组策略

在 VPN 组策略对象中，使用 **访问时间** 字段指定时间范围对象。有关详细信息，请参阅配置组策略对象，第 2724 页和组策略高级选项，第 2730 页。

时区

要为托管设备指定本地时区，请创建时区对象，并在分配给设备的设备平台设置策略中指定该对象。

该设备本地时间仅用于在支持时间范围的策略（例如访问控制、预过滤器和VPN组策略）中应用规则中的时间范围。如果不为设备分配时区，在这些策略中应用时间范围时，将默认使用 UTC。系统中的任何其他功能都不会使用时区对象中指定的时区。

只有 Firewall Threat Defense 设备支持时区对象。

注释 从 防火墙管理中心 7.0 开始，Snort 3 也支持基于时间的 ACL。

隧道区域

隧道区域代表您为进行特殊分析而明确标记的特定类型的明文、传递隧道。虽然您可以将隧道区域用作某些配置中的接口限制，但它不是接口对象。

有关详细信息，请参阅使用隧道区域在隧道级别应用访问控制，第 2238 页。

URL

重要事项 有关在安全智能配置中使用此选项和类似选项的最佳实践，以及访问控制 和 QoS 策略中的 URL 规则，请参阅手动 URL 过滤选项，第 1800 页。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。您可在系统 Web 界面中的不同位置使用 URL 对象和对象组，包括访问控制策略和事件搜索。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项：
  - 字符串位于 URL 的开头。
  - 字符串后面有一个点。
  - 字符串开头包含一个点。
  - 字符串后面跟有 :// 字符。

  例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。

注释 我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。

- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

- 将 URL 对象用作远程访问 VPN 策略中的 URL 别名时，请确保 URL 不超过 128 个字符。

创建 URL 对象

过程

步骤 1 从对象类型列表中选择 **对象** > **URL**。

步骤 2 从**添加 URL (Add URL)** 下拉列表中选择**添加对象 (Add Object)**。

步骤 3 输入 **Name**。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 输入 **URL** 或 IP 地址。

步骤 6 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

变量集

变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止、自适应配置文件 和动态规则状态中的 IP 地址。

提示 无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。

可以使用变量集对变量进行管理、自定义和分组。可以使用系统提供的默认变量集，也可以创建您自己的自定义变量集。可以在任何变量集中修改预定义默认变量，以及添加和修改用户定义的变量。

系统提供的大多数共享对象规则和标准文本规则均使用预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。

当变量更准确地反映网络环境时，规则更加有效。至少应修改默认变量集中的的默认变量。通过确保变量（例如 `$HOME_NET`）正确地定义网络且 `$HTTP_SERVERS` 包括网络上的所有网络服务器，从而优化处理和监控所有相关系统的可疑活动。

要使用变量，请将变量集链接到与访问控制规则相关的入侵策略或访问控制策略的默认操作。默认情况下，默认设置集链接到访问控制策略使用的所有入侵策略。

将一个变量添加到任意变量集会将其添加到所有变量集；也就是说，每个变量集都是系统中当前配置的所有变量的集合。在任何变量集中，都可以添加用户定义的变量以及自定义任何变量的值。

最初，系统提供由预定义默认值组成的单个默认变量集。默认变量集中的每个变量最初设置为其默认值，对于预定义变量，该默认值是由Talos 智能小组 设置并在规则更新中提供的值。

虽然可以将预定义默认变量保留为所配置的默认值，但思科建议您修改预定义变量的子集。

可以仅使用默认变量集中的变量，但在许多情况下，执行以下操作可得到最大益处：添加一个或多个自定义变量集；在不同变量集中配置不同的变量值；甚至添加新变量。

使用多个变量集时务必谨记，默认变量集中任何变量的当前值决定所有其他变量集中该变量的默认值。

如果选择“对象管理器”(Object Management) 页面上的**变量集 (Variable Sets)**，则对象管理器会列出默认变量集以及您创建的任何自定义变量集。

在全新安装的系统上，默认变量集仅由思科预定义的默认变量组成。

每个变量集都包括系统提供的默认变量以及从任何变量集添加的所有自定义变量。请注意，可以编辑默认变量集，但不能重命名或删除默认变量集。

⚠

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

相关主题

管理变量，第 2717 页
管理变量集，第 2716 页

入侵策略中的变量集

默认情况下，Firepower 系统会将默认变量集链接到访问控制策略中使用的所有入侵策略。部署使用入侵策略的访问控制策略时，入侵策略中已启用的入侵规则将使用已链接变量集中的变量值。

修改访问控制策略中的入侵策略所使用的自定义变量集时，系统会反映该策略的状态，在 Access Control 页面上将其状态显示为过时。必须重新部署该访问控制策略，才能使变量集的更改生效。修改默认变量集时，系统会将使用入侵策略的所有访问控制策略的状态显示为过时，因此，必须重新部署所有访问控制策略才能使更改生效。

变量

变量属于以下类别之一：

默认变量

Firepower 系统提供的变量。不能重命名或删除默认变量，也不能更改其默认值。但是，可以创建默认变量的自定义版本。

自定义变量

您创建的变量。这些变量可包括：

- 自定义的默认变量

  编辑默认变量的值时，系统会将该变量从“默认变量”(Default Variables) 区域转移到“自定义变量”(Customized Variables) 区域。由于默认变量集中的变量值决定自定义变量集中变量的默认值，因此，自定义默认变量集中的默认变量会修改所有其他变量集中该变量的默认值。

- 用户定义的变量

  您可以添加和删除自己的变量，在不同变量集中自定义这些变量的值，以及将自定义变量重置为默认值。重置用户定义的变量时，该变量保留在“自定义变量”(Customized Variables) 区域。

  用户定义的变量可以是以下类型之一：

  - 网络变量指定网络流量中的主机的 IP 地址。
  - 端口变量指定网络流量中的 TCP 或 UDP 端口，包括这两种端口类型的值 `any`。

例如，如果您创建自定义标准文本规则，您可能还希望添加自己的用户定义的变量，以便更准确地反映流量或作为快捷方式简化规则创建过程。或者，如果创建只检查“隔离区”(DMZ) 中流量的规则，可以创建名为 `$DMZ` 的变量，其值列出已暴露的服务器 IP 地址。这样，在所有为该区域编写的所有规则中都可以使用 `$DMZ` 变量。

高级变量

Firepower 系统在特定情况下提供的变量。这些变量的部署非常有限。

预定义默认变量

默认情况下，Firepower 系统提供一个由预定义默认变量组成的默认变量集。Talos 智能小组 使用规则更新来提供新的和已更新的入侵规则及其他入侵策略元素，包括默认变量。

由于系统提供的许多入侵规则使用预定义默认变量，因此应为这些变量设置适当的值。可以在任何或所有变量集中修改这些默认变量的值，具体取决于如何使用变量集识别网络流量。

注意 导入访问控制策略或入侵策略会以导入的默认变量覆盖默认变量集中的现有默认变量。如果现有默认变量集包含不属于导入默认变量集的自定义变量，则会保留该唯一的变量。

下表介绍系统提供的变量并指示通常会修改哪些变量。要获得为网络定制自定义变量方面的帮助，请联系专业服务或支持部门。

表 *161:* 系统提供的变量

变量名称	说明	是否修改？
`$AIM_SERVERS`	定义已知的 AOL Instant Messenger (AIM) 服务器，并用于基于聊天的规则和查找 AIM 漏洞攻击的规则。	不需要。
`$DNS_SERVERS`	定义域名服务 (DNS) 服务器。如果创建专门影响 DNS 服务器的规则，可以使用 `$DNS_SERVERS` 变量作为目标或源 IP 地址。	在当前规则集中不需要。
`$EXTERNAL_NET`	定义 Firepower 系统视为未受保护的网络，并在许多规则中用于定义外部网络。	需要；应该充分定义 `$HOME_NET`，然后避免将 `$HOME_NET` 作为 `$EXTERNAL_NET` 的值。
`$FILE_DATA_PORTS`	定义非加密端口，用于检测网络数据流中的文件的入侵规则。	不需要。
`$FTP_PORTS`	定义网络上 FTP 服务器的端口，用于 FTP 服务器漏洞攻击规则。	如果 FTP 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
`$GTP_PORTS`	定义数据包解码器用于提取 GTP（通用分组无线业务 [GPRS] 隧道协议）PDU 中的负载的数据信道端口。	不需要。
`$HOME_NET`	定义相关入侵策略监控的网络，用于许多定义内部网络的规则。	需要，以便包括内部网络的 IP 地址。
`$HTTP_PORTS`	定义网络上 Web 服务器的端口，用于 Web 服务器漏洞攻击规则。	如果网络服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
`$HTTP_SERVERS`	定义网络上的 Web 服务器。用于 Web 服务器漏洞攻击规则。	如果运行 HTTP 服务器，需要修改。
`$ORACLE_PORTS`	定义网络上的 Oracle 数据库服务器端口，用于扫描针对 Oracle 数据库的攻击的规则。	如果运行 Oracle 服务器，需要修改。

变量名称	说明	是否修改？
$SHELLCODE_PORTS	定义希望系统对其扫描外壳代码漏洞的端口，用于检测使用外壳代码的漏洞的规则。	不需要。
$SIP_PORTS	定义网络上 SIP 服务器的端口，用于 SIP 服务器漏洞攻击规则。	不需要。
$SIP_SERVERS	定义网络上的 SIP 服务器，用于针对 SIP 的漏洞攻击的规则。	需要；如果运行 SIP 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SIP_SERVERS 的值。
$SMTP_SERVERS	定义网络上的 SMTP 服务器，用于解决针对邮件服务器的漏洞的规则。	如果运行 SMTP 服务器，需要修改。
$SNMP_SERVERS	定义网络上的 SNMP 服务器，用于扫描针对 SNMP 服务器的攻击的规则。	如果运行 SNMP 服务器，需要修改。
$SNORT_BPF	识别旧版高级变量，仅在 V5.3.0 之前的 Firepower 系统软件版本（后来升级到 V5.3.0 或更高版本）中的系统上存在该变量时，才会显示该变量。	不需要，只能查看或删除此变量。不能对其进行编辑，删除后也不能再恢复。
$SQL_SERVERS	定义网络上的数据库服务器，用于解决针对数据库的漏洞的规则。	如果运行 SQL 服务器，需要修改。
$SSH_PORTS	定义网络上 SSH 服务器的端口，用于 SSH 服务器漏洞攻击规则。	如果 SSH 服务器使用除默认端口以外的端口，需要修改（可以在 Web 界面中查看默认端口）。
$SSH_SERVERS	定义网络上的 SSH 服务器，用于解决针对 SSH 的漏洞的规则。	需要修改；如果运行 SSH 服务器，应该充分定义 $HOME_NET，然后包括 $HOME_NET 作为 $SSH_SERVERS 的值。
$TELNET_SERVERS	定义网络上的已知 Telnet 服务器，用于解决针对 Telnet 的漏洞的规则。	如果运行 Telnet 服务器，需要修改。
$USER_CONF	提供一个通用工具，让您能够配置无法通过网络界面使用的一个或多个功能。 存在冲突或重复的 $USER_CONF 配置会导致系统停止。	不需要，除非功能描述中有指示或在支持人员的指导下进行。

网络变量

网络变量代表可在已在入侵策略、入侵策略规则抑制、动态规则状态和自适应配置文件中启用的入侵规则中使用的 IP 地址。网络变量与网络对象和网络对象组的不同之处在于，网络变量特定于入侵策略和入侵规则，但可以使用网络对象和网络对象组在系统网络界面中的不同位置（包括访问控制策略、网络变量、入侵规则、网络发现规则、事件搜索和报告等）来代表 IP 地址。

可在以下配置中使用网络变量来指定网络上主机的 IP 地址：

- 入侵规则 - 通过入侵规则**源 IP (Source IPs)** 和**目标 IP (Destination IPs)** 报头字段，您可以将数据包检测限于源自或发往特定 IP 地址的数据包。
- 抑制 - 在特定 IP 地址或某个范围的 IP 地址触发入侵规则或预处理器时，通过源或目标入侵规则抑制中的**网络 (Network)** 字段，您可以抑制入侵事件通知。
- 动态规则状态 - 通过源或目标动态规则状态中的**网络 (Network)** 字段，您可以检测在给定时间段内出现入侵规则或预处理器规则的过多匹配项的情况。
- 自适应配置文件 - 启用自适应配置文件更新时，自适应配置文件**网络**字段识别您希望在其中改进被动部署中的数据包分段和 TCP 流的重组的主机。

在本节所述字段中使用变量时，链接至入侵策略的变量集决定使用该入侵策略的访问控制策略处理的网络流量中的变量值。

可以将以下网络配置的任意组合添加到变量：

- 从可用网络列表中选择的网络变量、网络对象和网络对象组的任意组合
- 从“新建变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个网络对象（这些对象随后可添加到变量以及其他现有和将来的变量）
- 单个文字 IP 地址或地址块

  可以通过逐个添加来列出多个文字 IP 地址和地址块。可以单独列出 IPv4 和 IPv6 地址以及地址块，或者列出它们的任意组合。指定 IPv6 地址时，可使用 RFC 4291 中定义的任意寻址约定。

在任何变量中添加的包含网络的默认值是单词 `any`，它表示任意 IPv4 或 IPv6 地址。已排除网络的默认值为 `none`，它表示无网络。还可以使用文字值指定地址 `::`，以指示包含网络列表中的任何 IPv6 地址，或排除列表中没有 IPv6 地址。

将网络添加到排除列表会使指定的地址和地址块无效。也就是说，可以匹配除了被排除的 IP 地址或地址块以外的所有 IP 地址。

例如，排除文字地址 `192.168.1.1` 会指定除 192.168.1.1 以外的所有 IP 地址，排除 `2001:db8:ca2e::fa4c` 会指定除 2001:db8:ca2e::fa4c 以外的所有 IP 地址。

使用文字网络或可用网络可以排除任意的网络组合。例如，排除文字值 `192.168.1.1` 和 `192.168.1.5` 会包含除 192.168.1.1 或 192.168.1.5 以外的任何 IP 地址。也就是说，系统将此解释为“**既不是** 192.168.1.1 **也不是** 192.168.1.5”，这就会匹配除括号中列出的 IP 地址以外的所有 IP 地址。

添加或编辑网络变量时，请注意以下几点：

- 在逻辑上，不能排除值 `any`，如果排除该值，将表示无地址。例如，不能将具有值 `any` 的变量添加到排除网络列表。
- 网络变量为指定的入侵规则和入侵策略功能识别流量。请注意，无论入侵规则中使用的网络变量定义的主机如何，预处理器规则都可以触发事件。
- 已排除的值必须解析到已包括的值的子集。例如，不能包含地址块 192.168.5.0/24 并排除 192.168.6.0/24。

端口变量

端口变量代表可在入侵策略中启用的入侵规则的**源端口 (Source Port)** 和**目标端口 (Destination Port)** 报头字段中使用的 TCP 和 UDP 端口。端口变量与端口对象和端口变量特定于入侵规则的端口对象组不同。可以为除 TCP 和 UDP 以外的其他协议创建端口对象，还可以在系统 Web 界面中的不同位置使用端口对象，包括端口变量、访问控制策略、网络发现规则和事件搜索。

可以在入侵规则 **Source Port** 和 **Destination Port** 报头字段中使用端口变量来限制仅检查来自或发往特定 TCP 或 UDP 端口的数据包。

在这些字段中使用变量时，链接到与访问控制规则或策略相关的入侵策略的变量集决定部署访问控制策略的网络流量中这些变量的值。

可以将以下端口配置的任意组合添加到变量：

- 端口变量与您从可用端口列表中选择的端口对象的任何组合

  请注意，可用端口的列表不会显示端口对象组，因此您不能将这些端口对象组添加到变量。

- 从“新变量”(New Variable) 或“编辑变量”(Edit Variable) 页面添加的单个端口对象（这些对象随后可添加到变量以及其他现有和将来的变量）

  只有 TCP 和 UDP 端口（包括任一类型的值 `any`）是有效的变量值。如果您使用新的或编辑变量页面以添加不是有效变量值的有效端口对象，则该对象将被添加到系统，但不会显示在可用对象列表中。当您使用对象管理器来编辑变量中使用的端口对象时，只能将其值更改为有效的变量值。

- 单个文字端口值和端口范围

  您必须使用破折号 (-) 分隔端口范围。使用冒号 (:) 指示的端口范围支持向后兼容性，但您不能在您创建的端口变量中使用冒号。

  您可以通过在任何组合中单独添加每个文字端口值和范围，来列出多个文字端口值和范围。

在添加或编辑端口变量时，请注意以下要点：

- 在您添加的任何变量中，包括的端口的默认值为文字 `any`，它表示任何端口或端口范围。排除端口的默认值为 `none`，它表示无端口。

提示 要创建值为 `any` 的变量，请命名并保存该变量，而不要添加具体的值。

- 您不能在逻辑上排除值 `any`，如果排除，这将表示无端口。例如，您不能在将值为 `any` 的变量添加到已排除端口的列表时保存变量集。
- 将端口添加到已排除列表将使指定端口和端口范围无效。即您可以将任何端口与已排除的端口或端口范围进行匹配。
- 已排除的值必须解析到已包括的值的子集。例如，您不能包括端口范围 10-50 并排除端口 60。

高级变量

高级变量让您能够配置通常无法通过网络界面配置的功能。系统当前只提供一个高级变量，即 USER_CONF 变量。

USER_CONF

USER_CONF 提供一个通用工具，让您能够配置无法以其他方式通过 Web 界面获得的一个或多个功能。

注意 请**勿**使用高级变量 USER_CONF 来配置入侵策略功能，除非功能描述或支持人员指示您这样做。存在冲突或重复的配置会导致系统停止。

编辑 USER_CONF 时，单行最多总共可输入 4096 个字符；达到该限制后，行会自动换行。可以包含任意数量的有效说明或行，直至达到变量的最大字符长度限制（8192 个字符）或物理限制（例如磁盘空间）。在命令指令中，可以在任何完整参数之后使用反斜线 (\) 续行符。

重置 USER_CONF 会将其清空。

变量重置

在变量集新建或编辑变量页面上，可以将变量重置为默认值。下表总结了重置变量的基本原则。

表 *162:* 变量重置值

要重置的变量类型	所属变量集类型	重置后的值
default	默认值	规则更新值
用户定义	默认值	any
默认变量或用户定义的变量	自定义	当前默认变量集值（已修改或未修改）

重置自定义变量集中的变量会将其重置为该变量在默认变量集中的当前值。

相反，重置或修改默认变量集中某个变量的值总是会更新所有自定义变量集中该变量的默认值。如果重置图标呈灰色显示，表示不能重置变量，这意味着该变量在该变量集中没有自定义值。除非自定义了自定义变量集中某个变量的值，否则对默认变量集中该变量的更改会更新与该变量集链接的任何入侵策略中使用的值。

注释 理想做法是修改默认变量集中的某个变量，以评估这些更改如何影响使用链接自定义变量集中的该变量的任何入侵策略，尤其是在尚未定制自定义变量集中的变量值时。

将指针悬停在变量集中的**重置图标** 上可查看重置值。当自定义值和重置值相同时，这表示以下其中一种情况属实：

- 您在自定义或默认变量集中，而且在其中添加了值为 any 的变量
- 您在自定义变量集中，在其中添加了具有显式值的变量，并且选择了使用配置值作为默认值

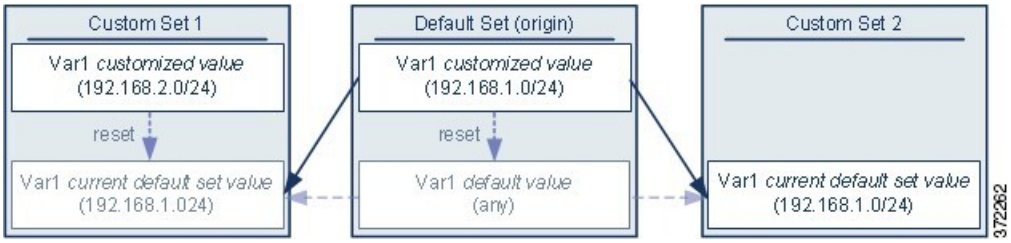
将变量添加到变量集

将变量添加到变量集会将其添加到所有其他变量集。添加自定义变量集中的变量时，必须选择是否使用配置值作为默认变量集中的定制值：

- **如果使用配置值**（例如 192.168.0.0/16），则该变量会被添加到使用配置值作为定制值、默认值为 any 的默认变量集中。由于默认变量集的当前值决定其他变量集的默认值，所以其他自定义变量集的初始默认值为配置值（在本例中为 192.168.0.0/16）。
- **如果不使用配置值**，则该变量将被添加到仅使用默认值 any 的默认变量集中，因此其他自定义变量集的初始默认值将为 any。

示例：将用户定义变量添加到默认变量集

下图说明了将用户定义的变量 Var1（其值为 192.168.1.0/24）添加到默认变量集时发生的变量集交互。



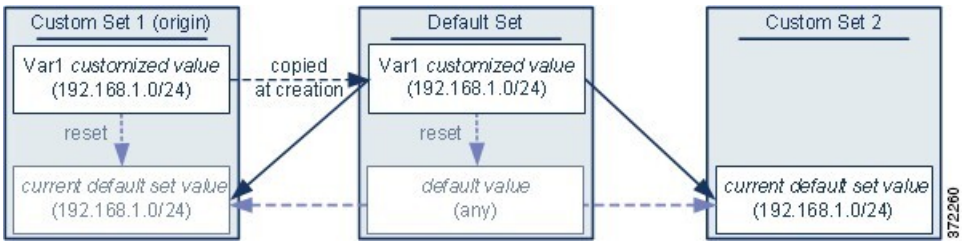
您可以在任何变量集中自定义 Var1 的值。在未自定义 Var1 的自定义变量集 2 中，此变量的值是 192.168.1.0/24。在自定义变量集 1 中，Var1 的自定义值 192.168.2.0/24 覆盖了默认值。重置默认变量集中某个用户定义的变量会将所有变量集中该变量的默认值重置为 any。

须注意的一点是，在本示例中，如果不更新自定义变量集 2 中的 Var1，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

请注意，虽然在本示例中未显示，但用户定义的变量和默认变量的变量集交互是相同的，唯一不同的是重置默认变量集中的默认变量会在当前规则更新中将其值重置为由思科配置的值。

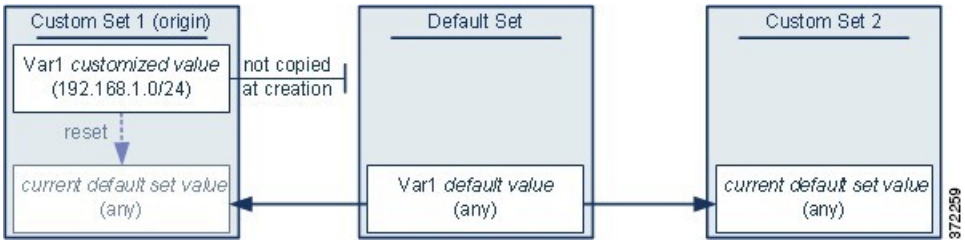
示例：将用户定义变量添加到自定义变量集

以下两个示例说明了将用户定义的变量添加到自定义变量集时变量集之间的交互。保存新变量时，系统会提示您选择是否将配置值用作其他变量集的默认值。在以下示例中，您选择**使用**配置值。



请注意，除了 Var1 来自自定义变量集 1 以外，本示例与以上将 Var1 添加到默认变量集的示例完全相同。将 Var1 的自定义值 192.168.1.0/24 添加到自定义变量集 1 会将该值复制到默认变量集，以作为默认值为 any 的自定义值。之后，Var1 值和交互就像之前将 Var1 添加到默认变量集一样。请记住，与前一个示例一样，进一步自定义或重置默认变量集中的 Var1 会导致更新自定义变量集 2 中 Var1 的默认值，从而影响与变量集相关联的所有入侵策略。

在下一个示例中，像前一个示例一样，将 Var1（其值为 192.168.1.0/24）添加到自定义变量集 1，但选择**不使用** Var1 的配置值作为其他变量集中的默认值。



此方法会将 Var1（其默认值为 any）添加到所有变量集。添加 Var1 后，可以在任何变量集中自定义它的值。此方法的优点是，通过最初不在默认变量集中自定义 Var1，可以降低这样的风险：在默认变量集中自定义此变量的值时，无意中更改了尚未自定义 Var1 的变量集（例如，自定义变量集 2）中的当前值。

嵌套变量

只要嵌套不是循环的，就可以嵌套变量。不支持嵌套的、否定的变量。

有效的嵌套变量

在此示例中，SMTP_SERVERS、HTTP_SERVERS 和 OTHER_SERVERS 是有效的嵌套变量。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	—
HTTP_SERVERS	自定义默认值	10.1.1.2	—
OTHER_SERVERS	用户定义的变量	10.2.2.0/24	—
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

无效的嵌套变量

在本例中，HOME_NET 是一个无效的嵌套变量，因为 HOME_NET 的嵌套是循环的；即，OTHER_SERVERS 的定义包括 HOME_NET，因此您将在其自身中嵌套 HOME_NET。

变量	类型	包含的网络	排除的网络
SMTP_SERVERS	自定义默认值	10.1.1.1	—
HTTP_SERVERS	自定义默认值	10.1.1.2	—
OTHER_SERVERS	用户定义的变量	10.2.2.0/24 HOME_NET	—
HOME_NET	自定义默认值	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

不受支持的嵌套的、否定的变量

由于嵌套的、否定的变量不受支持，因此不能使用本例所示的变量 NONCORE_NET 来表示受保护网络之外的 IP 地址。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	自定义默认值	—	HOME_NET
DMZ_NET	用户定义的变量	10.4.0.0/16	—
NOT_DMZ_NET	用户定义的变量	—	DMZ_NET
NONCORE_NET	用户定义的变量	EXTERNAL_NET NOT_DMZ_NET	—

不受支持的嵌套的、否定的变量的替代方法

作为上述示例的替代方法，您可以通过创建变量 NONCORE_NET 来表示受保护网络之外的 IP 地址，如本例所示。

变量	类型	包含的网络	排除的网络
HOME_NET	自定义默认值	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	用户定义的变量	10.4.0.0/16	—
NONCORE_NET	用户定义的变量	—	HOME_NET DMZ_NET

管理变量集

要使用变量集，您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **变量集**。

步骤 2 管理变量集：

- 添加 - 如果要添加自定义变量集，请点击**添加变量集 (Add Variable Set)**；请参阅创建变量集，第 2716 页。
- 删除 - 如果要删除自定义变量集，请点击变量集旁边的 **删除** ()，然后点击**是**。不能删除默认变量集或属于祖先域的变量集。

  注释
  在删除的变量集中创建的变量不会被删除或以其他方式在其他集合中受影响。

- 编辑 - 如果要编辑变量集，请点击要修改的变量集旁边的 **编辑** ()；请参阅编辑对象，第 2613 页。
- 过滤 - 如果要按名称过滤变量集，请开始输入名称；当您键入时，页面会刷新以显示匹配的名称。如果要清除名称过滤，请点击过滤器字段中的 **清除** ()。
- 管理变量 - 要管理变量集中包含的变量，请参阅管理变量，第 2717 页。

创建变量集

过程

步骤 1 选择**对象** > **变量集**。

步骤 2 点击**添加变量集 (Add Variable Set)**。

步骤 3 输入 **Name**。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 管理变量集中的变量；请参阅管理变量，第 2717 页。

步骤 6 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

管理变量

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 选择**对象** > **变量集**。

步骤 2 点击要编辑的变量集旁边的 **编辑** ()。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 管理变量：

- 显示 - 如果要显示变量的完整值，请将指针悬停在变量旁边的**值 (Value)** 列中的值上方。
- 添加 - 如果要添加变量，请点击**添加 (Add)**；请参阅添加变量，第 2718 页。
- 删除 - 点击变量旁边的 **删除** ()。如果自添加变量后已保存变量集，请点击**是 (Yes)** 以确认是否要删除变量。

  不能删除以下变量：

  - 默认变量
  - 入侵规则或其他变量所使用的用户定义的变量
  - 属于祖先域的变量

- 编辑 - 点击要编辑的变量旁边的 **编辑** ()；请参阅编辑变量，第 2719 页。
- 重置 - 如果要将已修改变量重置为其默认值，请点击已修改变量旁边的 **重置** 。如果重置呈灰色显示，则表明以下情况之一成立：

  - 当前值已是默认值。
  - 配置属于祖先域。

  提示

将指针悬停在活动的重置图标上可显示默认值。

步骤 4 点击**保存**以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)**以确认要保存更改。

由于默认变量集中的当前值决定所有其他变量集中的默认值，因此，修改或重置默认变量集中的变量会更改未对该变量默认值进行自定义的那些变量集中的该变量当前值。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅部署配置更改，第 180 页。

添加变量

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

过程

步骤 1 在变量集编辑器中，点击**添加 (Add)**。

步骤 2 在 **Name** 字段中为变量输入一个唯一名称。

步骤 3 从**类型 (Type)** 下拉列表中，选择**网络 (Network)** 或**端口 (Port)**。

步骤 4 为变量指定值：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示
  如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符(-)隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除** (🗑) 。

注释
要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 5 点击 **Save** 保存变量。如果是添加自定义变量集中的新变量，可以选择以下选项：

- 点击**是 (Yes)** 添加使用配置值作为默认变量集中的自定义值（进而也是其他自定义变量集中的默认值）的变量。

- 点击**否 (No)** 将变量添加为默认变量集中的默认值 `any`（进而在其他自定义变量集中也使用此默认值）。

步骤 6 点击**保存** 以保存变量集。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

编辑变量

您必须拥有 IPS 许可证（适用于 Firewall Threat Defense 设备）或保护许可证（所有其他设备类型）。

可以同时编辑自定义变量和默认变量。

无法更改现有变量中的**名称 (Name)** 或**类型 (Type)** 值。

过程

步骤 1 在变量集编辑器中，点击要修改的变量旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明对象属于祖先域，或者您没有修改对象的权限。

步骤 2 修改变量：

- 如果要将项目从可用网络或端口列表移动到包含或排除项目列表，可以选择一个或多个项目，然后进行拖放，或者点击**包含 (Include)** 或**排除 (Exclude)**。

  提示
  如果网络或端口变量的包含变量列表和排除变量列表中的地址或端口重叠，排除的地址或端口优先。

- 输入一个文字值，然后点击**添加 (Add)**。对于网络变量，可以输入单个 IP 地址或地址块。对于端口变量，可以添加单个端口或端口范围，用连字符 (-) 隔开上限和下限值。如有需要，可重复此步骤输入多个文字值。
- 如果要从包含或排除列表中删除项目，请点击该项目旁边的 **删除** (🗑) 。

注释
要包含或排除的项目列表可以包括原义字符串和现有变量、对象及网络对象组（对于网络变量）的任意组合。

步骤 3 点击 **Save** 保存变量。

步骤 4 点击**保存** 以保存变量集。如果变量集正在供访问控制策略使用，请点击**是 (Yes)** 以确认要保存更改。更改保存成功，与该变量集链接的所有访问控制策略均显示为过期状态。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

VLAN 标记

配置的每个 VLAN 标记对象代表一个 VLAN 标记或标记范围。

可以将VLAN标记对象进行分组。组表示多个对象；就此意思而言，在单个对象中使用一系列VLAN标记不被视为组。

可以在系统 Web 界面中的各种位置使用 VLAN 标记对象和组，包括规则和事件搜索。例如，可以编写仅适用于特定 VLAN 的访问控制规则。

创建 VLAN 标记对象

过程

步骤 1 选择**对象** > **VLAN 标记**。

步骤 2 从**添加 VLAN 标记 (Add VLAN Tag)** 下拉列表中，选择**添加对象 (Add Object)**。

步骤 3 输入 **Name**。

步骤 4 输入**说明**。

步骤 5 在 **VLAN 标记 (VLAN Tag)** 字段中输入值。使用连字符可指定 VLAN 标记范围。

步骤 6 管理对象的覆盖：

- 如果要允许对此对象进行覆盖，请选中**允许覆盖**复选框；请参阅允许对象覆盖，第 2618 页。
- 如果要将覆盖值添加到此对象，请展开“覆盖”(Override) 部分并点击**添加 (Add)**；请参阅添加对象覆盖，第 2619 页。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改，第 180 页。

VPN

您可以在 Firewall Threat Defense 设备上使用以下 VPN 对象。要使用这些对象，您必须具有管理员权限，并且您的智能许可证帐户必须满足导出控制要求。您只能在分叶域中配置这些对象。

证书映射对象

证书映射对象是一组命名的证书匹配规则。这些对象用于在接收的证书和远程接入VPN连接配置文件之间提供关联。连接配置文件和证书映射对象都是远程接入VPN策略的一部分。如果接收的证书与证书映射中包含的规则相匹配，则连接将被“映射”，或者与指定的连接配置文件相关联。规则按优先级顺序排列，并且按照它们在UI中的显示顺序进行匹配。当证书映射对象中的第一个规则产生一个匹配时，匹配结束。

导航

对象 > **VPN** > **证书映射**

字段

- **名称** - 标识此对象，以便可以从其他配置（如远程接入 VPN）引用该对象。
- **映射条件** - 指定要评估的证书的内容。如果证书认为这些规则满足要求，则用户将被映射到包含此对象的连接配置文件。
  - **字段** - 根据客户端证书的使用者或颁发者选择匹配规则的字段。

    如果**字段**设置为替代使用者或扩展密钥用法，则该组件将被冻结为整个字段
  - **组件** - 选择要用于匹配规则的客户端证书的组件。



注释 **SER（序列号）组件** - 确保为“主题”字段指定序列号。证书映射仅与使用者名称中的序列号属性匹配。

  - **运算符** - 为匹配规则选择运算符，如下所示：
    - 等于 - 证书组件必须与输入的值匹配。如果它们不完全匹配，则连接将被拒绝。
    - 包含 - 证书组件必须包含输入的值。如果组件不包含该值，则连接将被拒绝。
    - 不等于 - 证书组件不能等于输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值等于“美国”，则连接将被拒绝。
    - 不包含 - 证书组件不能包含输入的值。例如，对于一个选定的“国家/地区”证书组件，以及输入的“美国”值，如果客户的“国家/地区”值包含“美国”，则连接将被拒绝。
  - **值** - 匹配规则的值。输入的值域所选的组件和运算符关联。

相关主题

配置证书映射，第 1576 页

Secure Client 自定义属性对象

自定义属性由 Secure Client 用于配置 Per App VPN、允许或延迟升级和动态拆分隧道等功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。您可以使用 防火墙管理中心 来创建 安全客户端 (Secure Client) 自定义属性对象，将对象添加到组策略，并将组策略与远程接入 VPN 关联，以启用 VPN 客户端的功能。

Firewall Threat Defense 使用自定义属性对象支持以下功能：

- **Per App VPN**- Per App VPN 功能可帮助识别 Firewall Threat Defense 管理员通过 VPN 允许的应用和仅隧道应用。
- **允许或延迟升级**- 延迟升级允许 Secure Client 用户延迟 Secure Client 升级的下载。如果有客户端更新，您可以配置 Secure Client 的属性，以便打开一个询问用户是想要进行更新还是想要延迟升级的对话框。
- **动态拆分隧道 (Dynamic Split Tunneling)** - 通过动态拆分隧道，您可以调配在 VPN 隧道中包含或排除 IP 地址或网络的策略。通过创建自定义属性并将其添加到组策略，可配置动态分割隧道。

有关配置 Secure Client 自定义属性的分步说明，请参阅 添加 Secure Client 自定义属性对象，第 2722 页 和

有关为某个功能配置特定自定义属性的详细信息，请参阅所用 Secure Client 版本的《*Cisco Secure Client*（包括 *AnyConnect*）管理员指南》。

相关主题

组策略 Secure Client 选项，第 2727 页

添加 Secure Client 自定义属性对象

开始之前

在为Per App VPN添加自定义属性对象之前，请确保已完成以下操作：

- Per App VPN 必须通过 MDM 正确配置，并且每个设备都必须注册到 MDM 服务器
- 使用 Cisco Secure Client 企业应用选择器工具为每个应用创建 base64 编码字符串。
  1. 从这里下载 Cisco Secure Client 企业应用选择器工具。
  2. 打开应用选择工具，然后从左上角的下拉菜单中选择移动平台。
  3. 通过输入友好名称和应用 ID 添加规则；其余字段为可选字段。
  4. 在菜单栏上，点击 **策略 (Policy)**。编码的 base65 规则以其编码格式显示。
  5. 选择并复制策略字符串，并将其保存以供稍后在创建 Secure Client 自定义属性对象时使用。

过程

步骤 1 选择对象 > **VPN** > 自定义属性。

步骤 2 点击安全客户端自定义属性 **(Secure Client Custom Attribute)**。

步骤 3 输入 名称 和可选属性的 说明 。

步骤 4 从 安全客户端属性 **(Secure Client Attribute)** 下拉列表中选择一个属性：

- **Per App VPN**-选择此选项并在 属性值 框中指定 base64 编码的字符串。
- 允许延迟更新-选择以下选项之一并指定所需的信息以允许或延迟 Secure Client 客户端更新：
  - 显示提示直到用户执行操作-显示提示给 VPN 用户，直到用户选择允许或推迟 VPN 客户端更新。
  - 显示提示直到超时-选择此选项可显示指定持续时间的提示，并在 超时 框中指定持续时间。
  - 不显示提示并采取自动操作-选择此选项以自动允许或推迟 VPN 更新。
  - 默认操作-选择在用户不响应时或在您希望配置自动操作而无需用户干预时要采取的默认操作。您可以选择更新 Secure Client 客户端或推迟更新。
  - 最低版本-指定客户端系统上允许或推迟更新的最低 安全客户端 版本。
- 动态拆分隧道-选择此选项可在 VPN 隧道中包含或排除 IP 地址或网络。
  - 包含域-指定将包含在远程访问 VPN 隧道中的域名。
  - 排除域-指定将从远程访问 VPN 隧道中排除的域名。

步骤 5 选中 允许覆盖 复选框，允许对此对象组进行覆盖。

步骤 6 点击保存。
自定义属性对象添加到列表中。

下一步做什么

将自定义属性与组策略相关联。请参阅向组策略中添加自定义属性，第 2723 页。

向组策略中添加自定义属性

您必须将 安全客户端 自定义属性与组策略相关联，才能将其用于远程访问 VPN 连接。您

过程

步骤 1 选择对象 > **VPN** > 组策略。

步骤 2 添加新的组策略或编辑现有组策略。

步骤 3 点击 **安全客户端 (Secure Client)** > **自定义属性 (Custom Attributes)**。

步骤 4 点击**添加 (Add)**。

步骤 5 选择 **安全客户端属性 (Secure Client Attribute)**：Per App VPN、允许延迟更新或动态拆分隧道。

步骤 6 从列表中选择 **自定义属性对象** 。

注释
点击添加（+）以为所选 安全客户端 属性创建新的自定义属性对象。您还可以在 **对象** > **VPN** > **自定义属性**创建自定义属性对象。请参阅添加 Secure Client 自定义属性对象 ， 第 2722 页。

步骤 7 点击 **添加 (Add)** 将属性保存到组策略，然后点击**保存** 将更改保存到组策略。

相关主题

组策略 Secure Client 选项 ， 第 2727 页

Firewall Threat Defense组策略对象

组策略是存储在组策略对象中的一组属性和值对，用于定义远程访问VPN体验。例如，在组策略对象中，可以配置地址、协议和连接设置等常规属性。

在建立VPN隧道时，将确定应用于用户的组策略。RADIUS授权服务器将会分配组策略，或从当前连接配置文件中获取。

注释 Firewall Threat Defense 上没有任何组策略继承属性。对于用户使用完整的组策略对象。使用登录时 AAA 服务器识别的组策略对象；如果未指定组策略对象，则使用为 VPN 连接配置的默认组策略。提供的默认组策略可以设置为默认值，但仅在将该策略分配给连接配置文件且用户未识别其他组策略时使用该策略。

要使用组对象，您必须有与您的智能许可证帐户关联的这些 Secure Client 许可证之一，并启用了导出控制功能：

- 仅限 Secure Client VPN
- Secure Client Advantage
- Secure Client Premier

相关主题

配置组策略对象 ， 第 2724 页

配置组策略对象

请参阅Firewall Threat Defense组策略对象 ， 第 2724 页。

过程

步骤 1 选择**对象** > **VPN** > **组策略**。

系统将列出之前配置的策略，包括系统默认值。根据您的访问级别，可以编辑、查看或删除组策略。

步骤 2 点击**添加组策略**或选择要编辑的当前策略。

步骤 3 输入该策略的**名称**，还可以选择输入**说明**。

此名称最多可包含 64 个字符，允许使用空格。说明最多可以有 1,024 个字符。

步骤 4 如组策略常规选项，第 2725 页中所述，为此组策略指定**常规**参数。

步骤 5 如组策略 Secure Client 选项，第 2727 页中所述，为此组策略指定 **安全客户端**参数。

步骤 6 如组策略高级选项，第 2730 页中所述，为此组策略指定**高级**参数。

步骤 7 点击**保存**。

新的策略组将添加到列表中。

下一步做什么

将组策略对象添加到远程访问 VPN 连接配置文件。

组策略常规选项

导航路径

对象 > **VPN** > **组策略**，点击**添加组策略**或选择要编辑的当前策略，然后选择**常规**选项卡。

VPN 协议字段

指定应用此组策略时可使用的远程访问 VPN 隧道的类型。**SSL** 或 **IPsec IKEv2**。

IP 地址池

指定根据特定于远程访问 VPN 中用户组的地址池应用的 IPv4 地址分配。对于远程访问 VPN，可以为识别的使用 RADIUS/ISE 进行授权的用户组分配特定地址池中的 IP 地址。通过为特定用户组配置特定的组策略作为“RADIUS 授权”属性 (GroupPolicy/Class)，可以为系统中不知道身份的用户或用户组无缝执行策略实施。例如，您必须为使用这些地址的承包商和策略实施选择一个特定的地址池，以允许他们限制性地访问内部网络。

Firewall Threat Defense 设备向客户端分配 IPv4 地址池的优先顺序：

1. IPv4 地址池的 RADIUS 属性
2. 组策略的 RADIUS 属性
3. 映射到连接配置文件的组策略中的地址池

4. 连接配置文件中的 IPv4 地址池

关于组策略中使用 IP 地址池的一些限制：

- 不支持 IPv6 地址池。
- 一个组策略中最多可配置六个 IPv4 地址池。
- 修改使用中的地址池时会出现部署失败。在对地址池进行任何更改前，必须注销所有用户。
- 重命名地址池或配置的地址池重叠时，部署可能会失败。您必须删除旧地址池，稍后再部署更改的地址池，以此来部署更改。

  部分故障排除命令：

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

横幅字段

指定登录时要向用户显示的横幅文本。长度最多可以为 491 个字符。没有默认值。IPsec VPN 客户端对于条幅支持完全 HTML，但 Secure Client 仅支持部分 HTML。要确保向远程用户正确显示横幅，请对 IPsec 客户端使用 /n 标记，对 SSL 客户端使用
 标记。

DNS/WINS 字段

域命名系统 (DNS) 和 Windows Internet 命名系统 (WINS) 服务器。用于 Secure Client 名称解析。

- **主 DNS 服务器**和**辅助 DNS 服务器** - 选择或创建一个网络对象，定义希望此组使用的 DNS 服务器的 IPv4 或 IPv6 地址。
- **主 WINS 服务器**和**辅助 WINS 服务器** - 选择或创建一个网络对象，其中包含希望此组使用的 WINS 服务器的 IP 地址。
- **DHCP 网络范围 (DHCP Network Scope)** - 选择或创建一个网络对象，其中包含一个可路由的 IPv4 地址，与所需池子在同一子网，但不在池子内。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。如果未正确设置，VPN 策略部署将失败。

  如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

  如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

  建议尽可能将接口的 IP 地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

  目前不支持 LINK-SELECTION（RFC 3527）和 SUBNET-SELECTION（RFC 3011）。

- **默认域** - 默认域的名称。指定顶级域，例如 example.com。

拆分隧道字段

拆分隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或“以明文形式”）。

- **IPv4 拆分隧道/IPv6 拆分隧道** - 默认情况下，不启用拆分隧道。对于 IPv4 和 IPv6，此字段均设置为**允许所有流量通过隧道**。如果保留此设置，来自终端的所有流量都将通过 VPN 连接。

  要配置拆分隧道，请选择**下面指定的隧道网络**或**排除下面指定的网络**策略。然后为该策略配置访问控制列表。

- **拆分隧道网络列表类型** - 选择所使用的访问列表类型。然后选择或创建**标准访问列表**或**扩展访问列表**。有关详细信息，请参阅访问列表，第 2625 页。



注释 从版本 7.4 开始，默认情况下会禁用 **标准访问列表** 选项。使用 **“扩展访问列表”(Extended Access List)** 选项添加访问列表。

- **DNS 请求拆分隧道** - 也称为拆分 DNS。配置环境中预期的 DNS 行为。

  默认情况下，不启用拆分 DNS，并将其设置为**按拆分隧道策略发送 DNS 请求**。选择**始终通过隧道发送 DNS 请求**强制将所有 DNS 请求通过隧道发送到专用网络。

  要配置拆分 DNS，请选择**仅通过隧道发送指定的域**，然后在**域列表**字段中输入域名列表。这些请求通过拆分隧道解析到专用网络。所有其他名称使用公用 DNS 服务器进行解析。在域列表中最多输入十个条目，条目之间用逗号分隔。整个字符串的长度不能超过 491 个字符。

相关主题

配置组策略对象，第 2724 页

组策略 Secure Client 选项

这些规范适用于 Secure Client VPN 客户端的操作。

导航

对象 > **VPN** > **组策略**。点击**添加组策略**或选择要编辑的当前策略。然后选择 **安全客户端 (Secure Client)** 选项卡。

配置文件字段

配置文件 - 选择或创建包含 安全客户端配置文件 的文件对象。有关对象创建详细信息，请参见文件对象，第 2737 页。

安全客户端配置文件 是存储在 XML 文件中的一组配置参数。Secure Client 软件使用它来配置出现在客户端用户界面中的连接条目。这些参数（XML 标记）还配置相应设置以启用更多 Secure Client 功能。

使用基于GUI的安全客户端配置文件编辑器（一个独立的配置工具）来创建安全客户端配置文件。有关详细信息，请参阅相应版本的 《Cisco Secure Client（包括 AnyConnect）管理员指南》的 安全客户端配置文件编辑器 一章。

管理配置文件字段

管理 VPN 隧道可提供在终端开启时连接到企业网络，即使最终用户未通过 VPN 连接也是如此。

管理 VPN 配置文件-管理配置文件包含用于在终端上启用和建立管理 VPN 隧道的设置。

独立管理VPN隧道配置文件编辑器可用于创建新的配置文件或修改现有的配置文件。您可以从思科软件下载中心下载配置文件编辑器。

有关添加配置文件的详细信息，请参阅 文件对象，第 2737 页。

客户端模块字段

Cisco 仅限 Secure Client VPN 通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

以下 Secure Client 模块是可选的，您可以将这些模块配置为在 VPN 用户下载 AnyConnect 时下载 Secure Client：

- **AMP 启用程序 (AMP Enabler)** - 为终端部署高级恶意软件防护 (AMP) 。
- **DART**-捕获系统日志和其他诊断信息的快照，可将其发送到 Cisco TAC 进行故障排除。
- **ISE 终端安全评估 (ISE Posture)** - 使用 OPSWAT 库执行终端安全评估检查，评估终端的合规性。
- **网络访问管理器 (Network Access Manager)** - 为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
- **网络可视性 (Network Visibility)** - 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 Secure Client，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全 (Umbrella Roaming Security)** - 在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **Web 安全 (Web Security)** - 根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

点击**添加 (Add)** 并为每个客户端模块选择以下选项：

- **客户端模块 (Client Module)** - 从列表中选择 Secure Client 模块。
- **要下载的配置文件 (Profile to download)** - 选择或创建包含 安全客户端配置文件 的文件对象。有关对象创建详细信息，请参见 文件对象，第 2737 页。

- **启用模块下载**-选择启用终端以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

使用基于GUI的安全客户端配置文件编辑器（一个独立的配置工具）来创建每个模块的客户端分析文件。您可以从Cisco 软件下载中心下载 安全客户端配置文件编辑器。有关详细信息，请参见相应版本的 《Cisco Secure Client（包括 AnyConnect）》中的 安全客户端配置文件编辑器 一章。

SSL 设置字段

- **SSL 压缩** - 是否启用数据压缩，如果是，则设置要使用的数据压缩方法：Deflate 或 LZS。默认情况下会禁用 SSL 压缩。

  数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和CPU使用率。因此，降低了安全设备的总体吞吐量。

- **DTLS压缩** - 是否使用LZS为此组压缩数据报传输层安全(DTLS)连接。默认情况下会禁用DTLS压缩。

- **MTU 大小 (MTU Size)** - 思科 仅限 Secure Client VPN 为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节，有效范围为 576 到 1462 字节。

  - **忽略 DF 位** - 是否忽略需要分片的数据包中的“不分片 (df)”位。允许强制将已设置 DF 位的数据包分片，从而使其能够通过隧道传递。

连接设置字段

- **在安全客户端和 VPN 网关之间启用保持连接消息**。及其**间隔**设置 - 是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。默认设置为启用。保持连接消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 IKE 保持连接数据包之间等待的时间间隔（以秒为单位）。默认间隔为 20 秒，有效范围为 15 到 600 秒。

- **启用失效对等体检测...** 。及其**间隔**设置 - 死对等检测 (DPD) 可确保 VPN 安全网关或 VPN 客户端快速检测到对等体不再响应以及连接失败的情况。默认情况下，会为网关和客户端启用该设置。DPD 消息以设置的时间间隔传输。如果启用，请输入远程客户端在发送 DPD 消息之间等待的时间间隔（以秒为单位）。默认间隔为 30 秒，有效范围为 5 到 3600 秒。

- **启用客户端绕行协议** - 使您可以配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv4 流量（安全网关仅允许 IPv4 流量时）的方式。

  当 Secure Client 建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 Secure Client 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

  例如，假设安全网关只将一个 IPv4 地址分配给 Secure Client 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。

- **SSL 重新生成密钥** - 使客户端能够为连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。默认情况下将禁用此复选框。启用后，可以在指定的时间间隔进行重新协商，对现有隧道重新生成密钥，或通过设置以下字段来创建新隧道：
  - **方法** - 启用 SSL 重新生成密钥时可用。创建**新隧道**（默认）或重新协商**现有隧道**的规范。
  - **间隔** - 启用 SSL 重新生成密钥时可用。设置为 4 分钟的默认值，其范围为 4-10080 分钟（1 周）。
- **客户端防火墙规则** - 使用客户端防火墙规则为 VPN 客户端的平台配置防火墙设置。规则基于诸如源地址、目标地址和协议等条件。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的扩展 ACL。定义**专用网络规则**以控制流向专用网络的数据，且/或定义**公用网络规则**以控制在已建立的 VPN 隧道之外以“明文”形式传输的数据。

注释 确保 ACL 仅包含 TCP/UDP/ICMP/IP 端口以及“任意”、“任意 IPv4”或“任意 IPv6”类型的源网络。

只有运行 Microsoft Windows 的 VPN 客户端才能使用这些防火墙设置。

自定义属性字段

本部分列出 Secure Client 用于配置 Per App VPN，允许或延迟升级和动态拆分隧道等功能的 安全客户端 自定义属性。点击**添加 (Add)** 以向组策略添加自定义属性。

1. 选择 **安全客户端属性 (Secure Client Attribute)**：Per App VPN、允许延迟更新或动态拆分隧道。
2. 从列表中选择 **自定义属性对象** 。

注释 点击添加（+）以为所选 安全客户端 属性创建新的自定义属性对象。您还可以在 **对象** > **VPN** > **自定义属性**创建自定义属性对象。请参阅添加 Secure Client 自定义属性对象 ， 第 2722 页。

3. 点击 **添加 (Add)** 将属性保存到组策略，然后点击**保存** 将更改保存到组策略。

相关主题

配置组策略对象 ， 第 2724 页

组策略高级选项

导航路径

对象 > **VPN** > **组策略**。点击**添加组策略**或选择要编辑的当前策略。，，然后选择**高级 (Advanced)** 选项卡。

流量过滤器字段

- **访问列表过滤器** - 这些过滤器包含相应规则来确定是允许还是阻止通过 VPN 连接隧道传输的数据包。规则基于诸如源地址、目标地址和协议等条件。请注意，VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。扩展访问控制列表构建块对象用于定义流量过滤条件。选择或创建此组策略的新扩展 ACL。
- **限制 VPN 到 VLAN** - 也称为“VLAN 映射”，此参数指定该组策略应用到的会话的出口 VLAN 接口。ASA 将所有流量从该组转发到所选 VLAN。

  使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。除默认值（未限制）外，该下拉列表仅显示此 ASA 中配置的 VLAN。允许的值范围为 1 到 4094。

会话设置字段

- **访问时间** - 选择或创建时间范围对象。此对象指定该组策略可用于远程访问用户的时间范围。有关详细信息，请参阅时间范围，第 2702 页。
- **每个用户的同时登录数** - 指定允许某个用户执行的最多同时登录数。默认值为 3。最小值为 0，表示禁止登录并阻止用户访问。允许多个同时连接可能会危害安全性并影响性能。
- **最大连接时间/警报间隔** - 指定最大用户连接时间，以分钟为单位。此时间结束时，系统会终止连接。最小值为 1 分钟)。警报间隔指定在到达最大连接时间以向用户显示消息之前的时间间隔。
- **空闲超时/警报间隔** - 指定此用户的空闲超时时间，以分钟为单位。如果在此时间段内用户连接上没有通信活动，则系统会终止连接。最短时间为 1 分钟。默认值为 30 分钟。警报间隔指定在到达空闲时间以向用户显示消息之前的时间间隔。

相关主题

配置组策略对象，第 2724 页

Firewall Threat Defense IPSec 提议

在配置 VPN 拓扑时，使用 IPsec 方案（或转换集）。在与 ISAKMP 进行 IPsec 安全关联协商期间，对等体同意使用特定方案来保护特定数据流。两个对等体的方案必须相同。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 方案对象：

- 当创建 IKEv1 IPsec 方案（转换集）对象时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在VPN中支持多个组合，请创建多个IKEv1 IPsec 方案对象。
- 当创建 IKEv2 IPsec 方案对象时，可以选择 VPN 中允许的所有加密和散列算法。在 IKEv2 协商期间，对等体选择其分别支持的最合适选项。

IKEv1 和 IKEv2 IPsec 方案都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

注释 我们建议对 IPsec 隧道使用加密和身份验证。

配置 IKEv1 IPsec 方案对象

过程

步骤 1 选择 对象 > VPN > IKEv1 IPsec 提议，然后从目录中选择 VPN > IPsec IKev1 方案。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，您可以 编辑 (✎)、视图 (👁) 或 删除 (🗑) 方案。

步骤 2 选择添加 IPsec IKEv1 方案 (Add IPsec IKEv1 Proposals) 以创建新的方案。

步骤 3 为此方案输入名称 (Name)

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入说明 (Description)。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择 ESP 加密方法。此方案的封装安全协议 (ESP) 加密算法。

对于IKEv1，选择相关选项之一。在决定用于IPsec方案的加密和散列算法时，您的选择仅限于VPN中的设备所支持的算法。 有关选项的完整说明，请参阅为 VPN 策略决定加密算法，第 1432 页。

步骤 6 为 ESP 散列 (ESP Hash) 选择一个选项。

有关选项的完整说明，请参阅决定使用哪些散列算法，第 1433 页。

步骤 7 点击保存
将新方案添加到列表中。

配置 IKEv2 IPsec 方案对象

过程

步骤 1 从目录中选择 对象 > VPN > IKEv2 IPsec 提议。

系统将列出以前配置的方案，包括系统定义的默认值。根据您的访问级别，您可以 编辑 (✎)、视图 (👁) 或 删除 (🗑) 方案。

步骤 2 选择添加 IKEv2 IPsec 方案 (Add IKEv2 IPsec Proposal) 以创建新的方案。

步骤 3 为此方案输入**名称 (Name)**

策略对象的名称。最多允许 128 个字符。

步骤 4 为此方案输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 选择要在方案中用于身份验证的 **ESP 散列 (ESP Hash)** 方法、散列或完整性算法。

注释
Firewall Threat Defense 不支持使用 NULL 加密的 IPSec 隧道。确保不为 IPSec IKEv2 提议选择 NULL 加密。

对于 IKEv2，选择要用于支持 **ESP 散列 (ESP Hash)** 的所有选项。 有关选项的完整说明，请参阅决定使用哪些散列算法，第 1433 页。

步骤 6 选择 **ESP 加密**方法。此方案的封装安全协议 (ESP) 加密算法。

对于 IKEv2，点击“选择”(Select) 以打开一个对话框，在对话框中可以选择要支持的所有选项。在决定用于 IPsec 方案的加密和散列算法时，您的选择仅限于 VPN 中的设备所支持的算法。 有关选项的完整说明，请参阅为 VPN 策略决定加密算法，第 1432 页。

步骤 7 点击**保存**
将新方案添加到列表中。

IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

对于 IKEv1，IKE 方案包含单个算法集和模数组。您可以创建确保多个优先化的策略来确保至少一个策略与远程对等体的策略匹配。与 IKEv1 不同，在 IKEv2 方案中，您可以在一个策略中选择多个算法和模数组。由于对等体在第 1 阶段协商期间进行选择，因此可创建单个 IKE 方案，但是考虑多个不同的方案，以向最需要的方案提供更高的优先级。对于 IKEv2，策略对象不指定身份验证，其他策略必须定义身份验证要求。

当配置站点间 IPsec VPN 时，需要 IKE 策略。。

配置 IKEv1 策略对象

使用“IKEv1 策略”(IKEv1 Policy) 页面创建、编辑或删除 IKEv1 策略对象。这些策略对象包含 IKEv1 策略所需的参数。

过程

步骤 1 从目录中选择**对象** > **VPN** > **IKEv1 策略** 。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以 **编辑** ()、**视图** () 或 **删除** () 方案。

步骤 2 （可选） 选择**添加 IKEv1 策略 (Add IKEv1 Policy)** 以创建新策略对象。

步骤 3 为此策略输入**名称 (Name)**。最多允许 128 个字符。

步骤 4 （可选） 为此方案输入**说明 (Description)**。最多允许 1,024 个字符。

步骤 5 在**优先级 (Priority)** 中输入 IKE 策略的优先级值。

当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个优先级中定义的参数。有效值范围为 1 到 65,535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

步骤 6 在**加密**中选择加密方法。

在决定为 IKEv1 策略使用哪种加密和散列算法时，您的选择限于对等设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。对于 IKEv1，选择相关选项之一。 有关选项的完整说明，请参阅为 VPN 策略决定加密算法 ， 第 1432 页。

步骤 7 选择创建消息摘要的**散列 (Hash)** 算法，用于确保消息的完整性。

在决定为 IKEv1 方案使用哪种加密和散列算法时，您的选择限于托管设备支持的算法。对于 VPN 拓扑中的外部设备，必须选择与两个对等体匹配的算法。 有关选项的完整说明，请参阅决定使用哪些散列算法 ， 第 1433 页。

步骤 8 设置 **Diffie-Hellman 组**。

用于加密的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。选择要在 VPN 中允许的组。 有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组 ， 第 1434 页。

步骤 9 设置安全关联 (SA) 的 **持续期限**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商越安全。但是，持续期限越长，将来设置 IPsec 安全关联的速度相比较短持续期限的更快。

步骤 10 设置在两个对等体之间使用的**身份验证方法 (Authentication Method)**。

- **预共享密钥 (Preshared Key)** - 在身份验证阶段，预共享密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置其中一个参与的对等体，则无法建立 IKE SA。
- **证书 (Certificate)** - 当您将“证书”(Certificate) 用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

注释
在支持 IKEv1 的 VPN 拓扑中，所选 IKEv1 策略对象中指定的**身份验证方法**会成为 IKEv1 **身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

步骤 11 点击**保存**
IKEv1 策略添加到列表中。

配置 IKEv2 策略对象

使用“IKEv2 策略”(IKEv2 Policy) 对话框来创建、删除和编辑 IKEv2 策略对象。这些策略对象包含 IKEv2 策略所需的参数。

过程

步骤 1 从目录中选择**对象** > **VPN** > **IKEv2 策略** 。

系统将列出之前配置的策略，包括系统定义的默认值。根据您的访问级别，您可以**编辑** ()、**视图** ()或**删除** ()策略。

步骤 2 选择**添加 IKEv2 策略 (Add IKEv2 Policy)** 以创建新策略。

步骤 3 为此策略输入**名称 (Name)**。

策略对象的名称。最多允许 128 个字符。

步骤 4 为此策略输入**说明 (Description)**。

策略对象的说明。最多允许 1024 个字符。

步骤 5 输入**优先级 (Priority)**。

IKE 方案的优先级值。当尝试查找常见安全关联 (SA) 时，优先级值可确定两个协商对等体比较的 IKE 方案顺序。如果远程 IPsec 对等体不支持在您的第一个策略中选定的参数，它会尝试使用下一个最低优先级策略中定义的参数。有效值范围为 1 到 65535。数值越低，优先级越高。如果将此字段留空，管理中心将分配最低的未分配值，从 1 开始然后为 5，并以 5 为增量继续。

请注意，如果您在步骤 #unique_1536 unique_1536_Connect_42_pqc中启用其他密钥交换，请确保优先级为高。

步骤 6 设置安全关联 (SA) 的 **持续期限**（以秒为单位）。可指定 120 到 2,147,483,647 秒之间的值。默认值为 86400。

当超过持续期限时，SA 到期且必须在两个对等体之间重新协商。通常，持续期限越短（某种程度上），IKE 协商越安全。但是，持续期限越长，将来设置 IPsec 安全关联的速度相比较短持续期限的更快。

步骤 7 选择 IKE 策略中使用的散列算法的**完整性算法 (Integrity Algorithms)** 部分。散列算法创建消息摘要，它用于确保消息的完整性。

在决定为IKEv2方案使用哪种加密和散列算法时，您的选择限于托管设备支持的算法。对于VPN拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在VPN中允许的所有算法。有关选项的完整说明，请参阅决定使用哪些散列算法，第 1433 页。

步骤 8 选择用于建立第 1 阶段 SA（用于保护第 2 阶段协商）的**加密算法 (Encryption Algorithm)**。

在决定为IKEv2方案使用哪种加密和散列算法时，您的选择限于托管设备支持的算法。对于VPN拓扑中的外部设备，必须选择与两个对等体匹配的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅为 VPN 策略决定加密算法，第 1432 页。

步骤 9 选择**PRF 算法 (PRF Algorithm)**。

IKE 策略中使用的散列算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要在 VPN 中允许的所有算法。 有关选项的完整说明，请参阅决定使用哪些散列算法，第 1433 页。

步骤 10 选择一个**Diffie-Hellman 组**进行加密。

模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。选择您想要在 VPN 中允许的组。 有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 1434 页。

步骤 11 点击**保存**

如果已选择有效的选项组合，则新的IKEv2策略会添加到列表中。如果未选择，在会显示错误消息，且必须相应地做出更改，以便成功保存此策略。

Secure Client 自定义

现在，您可以自定义安全客户端，并将这些自定义部署到VPN头端。当最终用户从安全客户端连接时，威胁防御会将这些自定义分发到终端：

安全客户端自定义对象表示用于自定义安全客户端的文件。以下是支持的安全客户端自定义：

- GUI 文本和消息
- 图标和图像
- 脚本
- 二进制文件
- 自定义安装程序转换
- 本地化安装程序转换

有关配置这些安全客户端自定义的详细信息，请参阅 自定义 Cisco Secure Client，第 1588 页。

文件对象

使用“添加文件对象”和“编辑文件对象”对话框可以创建和编辑文件对象。文件对象表示配置中使用的文件，通常适用于远程访问 VPN 策略。它们可以包含 安全客户端配置文件和 安全客户端映像文件。

还使用独立的配置文件编辑器为每个 AnyConnect 模块和 Secure Client 管理 VPN 创建配置文件，并作为 安全客户端 的一部分部署到管理员定义的终端用户要求和端点上的身份验证策略，他们将预配置的网络配置文件提供给终端用户使用。

在创建文件对象时，防火墙管理中心将在其存储库中创建该文件的副本。在创建数据库的备份时，将备份这些文件；如果恢复该数据库，也将恢复这些文件。在将文件复制到管理中心平台以用于文件对象时，请不要将该文件直接复制到文件存储库。

在部署指定文件对象的配置时，会将相关联的文件下载到相应目录中的设备。

您可以针对每个文件点击以下选项之一：

- **下载 (Download)** - 点击下载 安全客户端文件。
- **编辑** -修改文件对象详细信息。
- **删除 (Delete)** - 删除 Secure Client 文件对象。 在删除文件对象时，不会从文件存储库中删除相关联的文件，而只会删除该对象。

导航路径

。

字段

- **名称**-输入文件的名称以识别文件对象；最多可以添加 128 个字符。
- **文件名称**-点击 **浏览** 以选择文件。选择文件时，系统会添加文件名和完整路径。
- **文件类型**-选择与所选文件对应的文件类型。以下文件类型可用：
  - **安全客户端映像 (Secure Client Image)** - 当您添加从 Cisco 软件下载中心下载的 Secure Client 映像时，请选择此类型。

    您可以将新的或附加的 Secure Client 映像与 VPN 策略相关联。您也可以取消关联不受支持的或生命周期终止的客户端程序包。
  - **安全客户端 VPN 配置文件 (Secure Client VPN Profile)** - 为 安全客户端 VPN 配置文件选择此类型。

    使用基于GUI的 安全客户端配置文件编辑器（独立配置工具）来创建配置文件。有关详细信息，请参见相应版本的 《Cisco Secure Client（包括 AnyConnect）用户指南》中的 安全客户端配置文件编辑器 一章。
  - **安全客户端管理 VPN 配置文件 (Secure Client Management VPN Profile)** - 在为 安全客户端管理 VPN 隧道添加配置文件时选择此类型。

从 Cisco 软件下载中心下载 安全客户端 **VPN 管理隧道独立配置文件编辑器**（如果尚未下载），并使用 安全客户端 管理 VPN 隧道的所需设置创建配置文件。

- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 安全客户端 AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 Firewall Threat Defense 推送到终端。
- **反馈配置文件**-您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 安全客户端 ISE 终端安全评估模块添加配置文件，请选择此选项。
- **NAM 服务配置文件**-使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。
- **网络可视性服务配置文件 (Network Visibility Service Profile)** - 安全客户端 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。
- **Umbrella 漫游安全配置文件**-如果使用使用配置文件编辑器创建的 .json 文件部署 Umbrella 漫游安全模块，则必须选择此文件类型。
- **网络安全服务配置文件**-在为网络安全模块添加配置文件时选择此文件类型。
- **Cisco Secure Firewall 终端安全评估 软件包** — 添加 Cisco Secure Firewall 终端安全评估 软件包文件时选择此文件类型。此文件在配置动态访问策略（DAP）时用于收集有关终端上安装的操作系统，防病毒，反间谍软件和防火墙软件的信息。
- **安全客户端外部浏览器软包 (Secure Client External Browser Package)** - 此文件类型用于为 SAML 单点登录网络身份验证选择外部浏览器软件包文件。

  您可以在新版本的外部软件包文件可用时添加软件包文件。

  有关详细信息，请参阅配置远程访问 VPN 的 AAA 设置，第 1555 页。

- **说明**-添加可选说明。

相关主题

思科 安全客户端 映像，第 1573 页
组策略 Secure Client 选项，第 2727 页

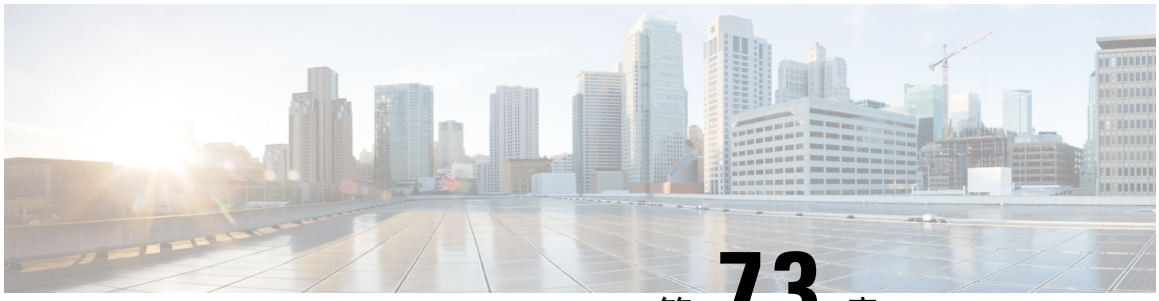
对象管理的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
合并的 ACL 和 AV ACL	7.4.1	任意	新增/修改的屏幕：**对象 (Objects)** > > **对象管理 (Object Management)** > **RADIUS 服务器组 (RADIUS Server Group)** > 添加 **RADIUS 组 (Add RADIUS Server Group)** > 将可下载 **ACL 与思科 AV 对 ACL 合并 (Merge Downloadable ACL with Cisco AV Pair ACL)** 新的 CLI 命令： • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair**
Secure Client 自定义	任意	7.4	现在，您可以自定义安全客户端，并将这些自定义部署到 VPN 头端。当最终用户从安全客户端连接时，威胁防御会将这些自定义分发到终端：
对 CRL 和 OCSP URL 的 IPv6 支持	任意	7.4	您现在可以配置 IPv6 OCSP 和 CRL URL。
环回和管理类型接口组对象	任意	7.4	现在，您可以创建仅包含管理专用接口或仅包含环回接口的接口组对象。然后，您可以将这些组用于管理功能，例如DNS服务器、HTTP访问或SSH。支持环回接口的任何功能都支持环回组。请注意，DNS不支持管理接口。 新增/修改的屏幕： **对象** > **对象管理** > **接口** > **添加** > **接口组**
环回接口支持 AAA	任意	7.4	可以使用环回接口组配置 RADIUS 服务器。 新增/修改的屏幕： **对象** > **对象管理** > **AAA 服务器** > **Radius 服务器组**
克隆网络和端口对象	任意	7.4	您现在可以克隆网络和端口对象。在对象管理器（**对象** > **对象管理**）中，点击端口或网络对象旁边的新 **克隆** 图标。然后，您可以更改新对象的属性并使用新名称保存它。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
DHCP IPv6 池	任意	7.3	使用 DHCPv6 前缀委派客户端时，Firewall Threat Defense 现在支持轻型 DHCPv6 无状态服务器。当 SLAAC 客户端向 Firewall Threat Defense 发送信息请求 (IR) 数据包时，Firewall Threat Defense 会向它们提供域名等其他信息。Firewall Threat Defense 仅接受 IR 数据包，不向客户端分配地址。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **添加/编辑接口 (Add/Edit Interfaces)** > **IPv6** > **DHCP** • **对象 (Objects)** > **对象管理 (Object Management)** > **DHCP IPv6 池 (DHCP IPv6 Pool)** 新增/修改的命令：**show ipv6 dhcp**
BFD 模板	任意	7.3	在之前的版本中，BFD 只能通过 FlexConfig 在威胁防御上进行配置。FlexConfig 不再支持 BFD 配置。现在，您可以在管理中心 UI 中为威胁防御配置 BFD 策略。因此，引入了 BFD 模板对象。 新增/修改的菜单项： • **设备** > **设备管理** > **路由** > **BFD**。 • **对象 (Objects)** > **对象管理 (Object Management)** > **BFD 模板 (BFD Template)**
用于策略型路由的“新应用”(New Applications) 选项卡	任意	7.1	扩展访问列表对象中引入了一个新选项卡，用于选择用于配置直接互联网访问策略（策略型路由）的应用。 新增/修改的屏幕：用于在配置**对象** > **对象管理** > **访问列表** > **扩展**页面时选择应用的新选项。 支持的平台： Secure Firewall Management Center
新建扩展社区列表对象和	任意	7.1	引入了扩展社区列表对象，用于策略列表和路由地图对象。扩展社区列表对象仅适用于在虚拟路由器的 BGP 路由支持中导入或导出路由。 新增/修改的屏幕：用于配置策略列表和路由地图的新对象**对象** > **对象管理** > **社区列表** > **扩展社区**页面。 支持的平台： Secure Firewall Management Center

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
对策略列表对象和路由映射对象的增强	任意	7.1	用于在策略列表和路由映射中选择新引入的扩展社区列表对象的选项。 新增/修改的屏幕：用于配置策略列表和路由映射的新选项**对象** > **对象管理** > **策略列表** > **社区规则**选项卡，以及**对象** > **对象管理** > **路由地图** > **BGP** > **社区列表**选项卡。 支持的平台： Secure Firewall Management Center
Snort 3 基于时间的 ACL 支持	任意	7.0	Snort 3 中也支持访问控制和预过滤器策略中基于时间的规则。 支持的平台： Firewall Threat Defense
适用于证书注册的EST	任意	7.0	支持通过安全传输进行证书注册。 新增/修改的屏幕：在配置**对象** > **PKI** > **证书注册** > **CA 信息**选项卡时的新注册选项。 支持的平台： Secure Firewall Management Center
支持 EdDSA 证书类型	任意	7.0	添加了新的证书密钥类型 - EdDSA，密钥大小为 256。 新增/修改的屏幕：在配置**对象** > **PKI** > **证书注册** > **密钥**选项卡时的新证书密钥选项。 支持的平台： Secure Firewall Management Center
密码和密钥大小限制	任意	7.0	不支持使用 RSA 加密签名算法的 SHA-1 证书以及小于 2048 位的 RSA 密钥。要绕过现有证书上的这些限制，您可以在 Firewall Threat Defense 上启用弱加密选项。但是，您不能生成小于 2048 位的 RSA 密钥。 新增/修改的屏幕：在配置**设备** > **证书**时的新切换按钮。 支持的平台： Secure Firewall Management Center
安全智能源选项	任意	6.7	自定义安全智能源的新更新频率选项（5 分钟和 15 分钟）。 小于 30 分钟的更新频率需要 MD5 URL，以防止在未更改源的情况下进行不必要的下载。 新增/修改的屏幕：在配置**安全智能** > **网络列表和源**时的新频率选项。 支持的平台： Secure Firewall Management Center

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
使用逗号分隔值 (csv) 文件批量上传对象	任意	6.7	可以从逗号分隔值文件导入对象。一次最多可以导入 1000 个对象。 新增/修改的屏幕：以下对象类型在**添加 [对象类型] (Add [Object Type])** 下拉列表中具有新的**导入对象 (Import Object)** 选项。 • **可分辨名称 (Distinguished Name)** > **单个对象 (Individual Objects)** • **网络对象** • **端口** • **URL** • **VLAN 标签** 支持的平台： Secure Firewall Management Center
查看使用接口对象的策略	任意	6.6	查看使用接口对象的策略。 新增/修改的屏幕：**对象** > **对象管理**中的**接口**对象页面有一个新的**查找**按钮。 支持的平台： Secure Firewall Management Center
引入了时区对象	任意	6.6	您可以将时区分配给 Firewall Threat Defense 设备，以供在应用基于时间的策略时使用。 新增/修改的屏幕：**对象** > **对象管理**中新的**时区对象**。 支持的平台： Secure Firewall Management Center
现在可在访问控制和预过滤策略中使用基于时间的对象	任意	6.6	将时间范围对象与新的时区对象结合使用，以便在访问控制和预过滤策略中应用基于时间的规则。 可以为要应用的规则指定绝对时间或循环时间或时间范围。规则会根据处理流量的设备的时区来应用。
从预过滤器规则页面查看对象详细信息	任意	6.6	引入的功能：在查看预过滤器规则时，用于查看对象或对象组的详细信息的选项。 新选项：右键点击预过滤器规则列表中任何列中的值，提供用于查看对象详细信息的选项：源网络、目标网络、源端口、目标端口和VLAN标记。 支持的平台： Secure Firewall Management Center



第 73 章

证书

- 证书的要求和前提条件， 第 2743 页
- Cisco Secure Firewall Threat Defense VPN 证书准则和限制， 第 2743 页
- 管理 Firewall Threat Defense 证书， 第 2744 页
- 使用自签注册安装证书 ， 第 2747 页
- 使用 EST 注册安装证书， 第 2748 页
- 使用 SCEP 注册安装证书， 第 2749 页
- 使用手动注册安装证书， 第 2750 页
- 使用 PKCS12 文件安装证书， 第 2751 页
- 使用 ACME 注册安装证书， 第 2751 页
- 排除 Firewall Threat Defense 证书问题， 第 2752 页
- 证书的历史记录， 第 2753 页

证书的要求和前提条件

支持的域

任意

用户角色

管理员

网络管理员

Cisco Secure Firewall Threat Defense VPN 证书准则和限制

- 如果 PKI 注册对象与某个设备关联并要安装在该设备上，证书注册过程将立即开始。对于自签名和 SCEP 注册类型，此过程将自动执行；它不需要任何额外的管理员操作。手动证书注册需要管理员操作。

- 将身份证书导入 Firewall Threat Defense 设备时，证书的到期日期不得超过 2106 年 2 月 6 日。确保设备中使用的所有证书的到期日期都在 2106 年 2 月 6 日之前，以避免证书导入或续订期间出现问题。
- 注册完成后，设备上会出现一个信任点，其名称与 证书注册对象相同。在配置 VPN 身份验证方法时会使用此信任点。
- Firewall Threat Defense设备支持使用 Microsoft 证书颁发机构 (CA) 服务和思科自适应安全设备 (ASA) 和思科 IOS 路由器中提供的 CA 服务的证书注册。
- Firewall Threat Defense 设备无法配置为证书颁发机构 (CA)。

证书和多租户准则

- 证书注册可以在子域或父域中完成。
- 当从父域执行注册时，证书注册对象也需要在同一个域中。如果该设备上的信任点在子域中被覆盖，则将在该设备上部署被覆盖的值。
- 当在分叶域中的设备上执行证书注册时，该注册对父域或其他子域是可见的。此外，还可以添加其他证书。
- 当一个叶域被删除时，将自动删除所包含的设备上的证书注册。
- 设备在一个域中注册了证书后，该设备将允许在其他任何域中进行注册。可以在其他域中添加该证书。
- 当您将一台设备从一个域移动到另一个域时，还会相应移动证书。您将收到一个警报，要求您删除这些设备上的注册。

管理 Firewall Threat Defense 证书

有关数字证书的介绍，请参阅PKI 基础设施与数字证书，第 1435 页。

有关用于在托管设备上注册和获取证书的对象的说明，请参阅证书注册对象，第 2669 页。

过程

步骤 1 选择**设备** > **证书**。

您可以看到此屏幕上列出的每个设备的以下列：

- **名称**-列出已经与信任点关联的设备。展开设备可查看关联的信任点列表。
- **域**-显示特定域中注册的证书。
- **注册类型**-显示此信任点使用的注册类型。
- **状态**-提供 **CA 证书** 和 **身份证书** 的状态。当 可用时，您可以通过点击放大镜来查看证书内容。

查看CA证书信息时，可以查看颁发CA证书的所有证书颁发机构的层次结构。如果注册失败，点击状态可显示故障消息。

- 点击右侧的**启用弱密码**，启用证书中的弱密码使用。当您点击切换按钮时，系统会在启用弱密码之前收到警告确认。点击 **是** 以启用弱密码。

  注释
  当由于弱密码使用导致证书注册失败时，系统会提示您启用弱密码。您可以选择在需要使用弱加密时启用弱密码。

- 附加列列出了用于执行以下任务的图标：
  - **导出证书**-点击以导出并下载证书的副本。您可以选择导出 PKCS12（完整证书链）或 PEM（仅身份证书）格式。

    您必须提供密码才能导出 PKCS12 证书格式，以便稍后导入文件。
  - **重新注册证书**-重新注册现有证书。
  - **刷新证书状态** - 刷新证书会将设备证书状态同步到 防火墙管理中心。
  - **删除证书**-删除信任点的所有关联证书。

步骤 2 选择 **(+) 添加**以关联注册对象，并在设备上安装该注册对象。

在证书注册对象与某个设备关联并安装到该设备后，证书注册过程将立即开始。对于自签名和SCEP注册类型，此过程将自动执行，这意味着不需要任何额外的管理员操作。手动证书注册需要额外的管理员操作。

注释
在设备上注册证书不会阻止用户界面，并且注册过程将在后台执行，从而使用户能够在其他设备上并行执行证书注册。在同一个用户界面可以监控这些并行操作的进度。各自的图标显示各自的证书注册状态。

相关主题

使用自签注册安装证书 ，第 2747 页
使用 SCEP 注册安装证书，第 2749 页
使用手动注册安装证书，第 2750 页
使用 PKCS12 文件安装证书，第 2751 页

自动更新 CA 捆绑包

您可以将管理中心设置为通过 CLI 命令自动更新 CA 证书。默认情况下，当您安装或升级到版本 7.0.5 时，CA 证书会自动更新。

注释 在仅 IPv6 部署中，CA 证书的自动更新可能会失败，因为某些思科服务器不支持 IPv6。在这种情况下，请使用 **configure cert-update run-now force** 命令强制更新 CA 证书。

过程

步骤 1 使用 SSH 登录 FMC CLI，或者打开 VM 控制台（如果是虚拟的）。

步骤 2 您可以验证本地系统中的 CA 证书是否是最新的：

configure cert-update test

此命令将本地系统上的CA 捆绑包与最新的CA 捆绑包（来自思科服务器）进行比较。如果CA 捆绑包是最新的，则不会执行连接检查，并且会显示测试结果，如下所示：

示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

如果 CA 捆绑包已过期，则对下载的 CA 捆绑包执行连接检查，展示结果。

示例：

当连接检查失败时：

```
> configure cert-update test
Test failed, not able to fully connect.
```

示例：

当连接检查成功时，或者 CA 捆绑包已经是最新的：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

步骤 3 （可选）要立即更新 CA 捆绑包，请执行以下操作：

configure cert-update run-now

示例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

执行此命令时，将验证 CA 证书（来自思科服务器）以进行 SSL 连接。如果其中一台思科服务器的 SSL 连接检查失败，该流程也会终止。

示例：

```
> configure cert-update run-now
```

```
Certs failed some connection checks.
```

要在连接失败的情况下继续更新，请使用 **force** 关键字。

示例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

步骤 4 如果您不希望自动更新 CA 捆绑包，请禁用配置：

configure cert-update auto-update disable

示例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

步骤 5 要重新启用 CA 捆绑包的自动更新：

configure cert-update auto-update enable

示例：

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

当您对 CA 证书启用自动更新时，系统将每天在系统定义的时间执行更新流程。

步骤 6 （可选）显示 CA 证书的自动更新状态。

show cert-update

示例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

使用自签注册安装证书

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开添加新证书对话框。**设备 > 证书**

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“自签名”类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象，第 2671 页。

步骤 4 按**添加**开始自动自签名注册过程。

对于自签名注册类型的信任点，**CA 证书** 状态将始终显示，因为托管设备会充当自己的 CA，而不需要 CA 证书来生成自己的身份证书。

身份证书 (Identity Certificate) 状态会在设备创建自己的自签身份证书时由“进行中”(InProgress) 转变为“可用”(Available)。

步骤 5 点击放大镜可查看为此设备创建的自签身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用 EST 注册安装证书

开始之前

注释 使用 EST 注册创建托管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

注释 不支持 EST 在证书过期时自动注册设备的功能。

过程

步骤 1 点击**添加**，打开**添加新证书**对话框。**设备** > **证书**

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从 **认证登记** 下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+)** 添加新证书注册对象，请参阅添加证书注册对象，第 2671 页。

步骤 4 点击 **添加** 以在设备上注册证书。

身份证书 将在设备使用 EST 从指定的 CA 获取其身份证书后从 进行中 转变为 可用 。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

使用 SCEP 注册安装证书

开始之前



注释 使用 SCEP 注册创建托管设备与 CA 服务器之间的直接连接。在开始注册流程之前，请确保您的设备已连接到 CA 服务器。

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开添加新证书对话框。**设备 > 证书**

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 SCEP 类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象 ，第 2671 页。

步骤 4 按**安装**，以开始自动注册过程。

对于 SCEP 注册类型信任点，**CA 证书**状态将在从 CA 服务器获取 CA 证书并安装在设备上后，从“进行中”过渡到“可用”。

身份证书将在设备使用 SCEP 从指定的 CA 获取其身份证书后从进行中转变为可用。有时，可能需要手动刷新才能获取身份证书。

步骤 5 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用手动注册安装证书

过程

步骤 1 在**设备 > 证书**屏幕上，选择**添加**，以打开添加新证书对话框。**设备 > 证书**

步骤 2 从**设备**下拉列表中选择设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择“手动”类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象，第 2671 页。

步骤 4 按**添加**，以开始注册过程。

步骤 5 使用 PKI CA 服务器执行适当的活动，以获取身份证书。

a) 点击 **身份证书** 警告图标以查看和复制 CSR。

b) 使用 PKI CA 服务器执行适当的活动，以使用此 CSR 获取身份证书。

此活动完全独立于 Secure Firewall Management Center或托管设备。完成后，您将获得托管设备的身份证书。您可以将其放置在文件中。

c) 要完成手动过程，请将获得的身份证书安装到托管设备。

返回到 Secure Firewall Management Center对话框，并选择**浏览身份证书**以选择身份证书文件。

注释
确保不要选择二进制证书（PKCS12、DER 等）文件，因为 Firewall Threat Defense 不支持这些文件。

步骤 6 选择**导入 (Import)** 以导入身份证书。

导入完成时，身份证书状态将为 `Available`。

步骤 7 点击放大镜可查看此设备的**身份证书**。

下一步做什么

注册完成后，设备上会出现一个信任点，其名称与证书注册对象相同。请在您的“站点间”和“远程访问 VPN 身份验证方法”的配置中，使用此信任点。

使用 PKCS12 文件安装证书

过程

步骤 1 转至**设备 > 证书**屏幕，然后选择**添加**，以打开添加新证书对话框。**设备 > 证书**

步骤 2 从**设备 (Device)** 下拉列表中选择预先配置的托管设备。

步骤 3 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 PKCS 类型的证书注册对象。
- 点击 **(+)** 添加新证书注册对象，请参阅添加证书注册对象 ， 第 2671 页。

步骤 4 按**添加 (Add)**。

CA 证书和身份证书状态会在其在设备上安装 PKCS12 文件时从 `In Progress` 变为 `Available`。

注释
第一次上传 PKCS12 文件时，该文件作为 CertEnrollment 对象的一部分存储在 防火墙管理中心。对于因密码错误或部署失败导致的任何失败注册，请重试注册 PKCS12 证书，无需再次上传文件。此外，每当您修改证书注册对象以允许覆盖时，都必须更新证书的 **密码** 才能成功注册。PKCS12 文件的大小不应超过 24K。

步骤 5 状态转变为可用 （`Available`）后，请点击放大镜查看此设备的身份证书。

下一步做什么

托管设备上的证书（信任点）的名称与 PKCS#12 文件的名称相同。在 VPN 身份验证配置中使用此证书。

使用 ACME 注册安装证书

过程

步骤 1 选择**设备 > 证书**。

步骤 2 点击**添加**，打开**添加新证书**对话框。

步骤 3 从**设备**下拉列表中选择设备。

步骤 4 按照下列方式之一将证书注册对象与此设备关联：

- 从下拉列表中选择 ACME 类型的证书注册对象。
- 点击 **(+)**，以添加新的证书注册对象，请参阅添加证书注册对象 ， 第 2671 页。

步骤 5 点击**添加**，以开始自动注册过程。

对于 ACME 注册类型的信任点，在注册成功之前，状态将显示为正在进行。CA 不适用于 ACME。

步骤 6 点击放大镜可查看为此设备创建和安装在此设备上的身份证书。

下一步做什么

注册完成后，设备上会配置一个信任点，其名称与证书注册对象相同。在远程访问VPN身份验证配置中使用此信任点。

排除 Firewall Threat Defense 证书问题

请参阅 Cisco Secure Firewall Threat Defense VPN 证书准则和限制，第 2743 页 确定您的证书注册环境中的变体是否可能导致问题。然后，考虑以下事项：

- **症状**：服务身份验证证书过期。

  证书监控健康模块会在 防火墙管理中心 和托管设备上的服务身份验证证书过期前向您发出警报。选择 **故障排除** > **+ 显示更多** > **运行状况** > **策略**，点击**运行状况模块**选项卡，然后导航至**证书监控**磁贴。

注释 导入的证书的到期日期不能晚于 2106 年 2 月 6 日。

- 确保存在从设备到 CA 服务器的路由。

  如果在注册对象中给出了 CA 服务器的主机名，请使用 Flex Config 来配置 DNS 以适当方式到达服务器。或者，使用 CA 服务器的 IP 地址。

- 如果您使用的是 Microsoft 2012 CA 服务器，则托管设备不接受默认的 IPsec 模板，必须更改模板。

  请参阅您使用 MS CA 文档时的以下步骤来配置工作模板。

  1. 复制 IPsec（脱机请求）模板。
  2. 在**扩展 (Extensions) > 应用策略 (Application policies)** 中，请选择 *IP* 安全端系统 *(IP security end system)*，而不是 *IP* 安全 *IKE* 中间系统 *(IP security IKE intermediate)*。
  3. 设置权限和模板名称。
  4. 添加新模板并更改注册表设置以反映新的模板名称。

- 在 防火墙管理中心上，您可能会收到与 Firewall Threat Defense 设备相关的以下运行状况警报：

  `代码 - F0853； Description - default Keyring's certificate is invalid, reason: expired`

  解决方案：在这种情况下，请使用以下命令在 CLISH CLI 中重新生成默身份验证书：

```
> system support regenerate-security-keyring default
```

- CA 证书状态中出现一个红色叉，并伴随出现以下错误：

  未能配置 CA 证书

  解决方案：请参阅对 FMC 上的证书错误进行故障排除。

- 要检查 .pfx 文件中的证书列表，请使用 `certutil` 或 `openssl` 等工具。您可以查看包含 ID 证书、子 CA 证书和 CA 证书（如有）的整个证书链。

  - `certutil -dump cert.pfx`
  - `openssl pkcs12 -info -in cert.pfx`

- 会出现以下错误：

  需要导入身份证书

  解决方案：请参阅对 FMC 上的证书错误“需要导入身份证书”进行故障排除。

证书的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
对 ACME 证书的支持	10.0	10.0	现在，您可以注册 ACME 证书并将其用作身份证书，以对充当 RA VPN 网关的 Firewall Threat Defense 设备或 Zero Trust 应用策略的 SAML 服务提供商 (SP) 进行身份验证。
支持 OCSP 和 CRL IPv6 URL	7.4	任意	您现在可以添加 IPv6 OCSP 和 CRL URL 以进行证书身份验证（吊销检查）。IPv6 地址必须用方括号括起来。
手动注册的增强功能	6.7	任意	您现在无需身份证书即可以仅创建 CA 证书。您也可以在没有 CA 证书的情况下生成 CSR，并从 CA 获得身份证书。
PKCS CA 链	6.7	任意	您可以查看和管理颁发证书的证书颁发机构 (CA) 链。您也可以导出证书的副本。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。